



IBIMA
Publishing

mobile

***Journal of Information Assurance
& Cybersecurity***

*Vol. 2010 (2010), Article ID 305412,
264 mini pages.*

DOI:10.5171/2010.305412

www.ibimapublishing.com

Copyright © 2010. Zuraini Ismail, Maslin Masrom, Zailani Mohamad Sidek, Dayang Suhana Hamzah. This is an open access article distributed under the Creative Commons Attribution License unported 3.0, which permits unrestricted use, distribution, and reproduction in any medium, provided that original work is properly cited

Title

**Framework to Manage
Information Security for
Malaysian Academic
Environment**

Authors

**Zuraini Ismail, Maslin Masrom,
Zailani Mohamad Sidek,
And Dayang Suhana Hamzah**

University Technology Malaysia,
Malaysia

Abstract

Among the ICT challenges of most organizations including those from the academic sector is securing their

information. Apart from technological aspect, Higher Education Institutions (HEIs) also must implement and enforce proper policies, procedures, and standards in

compliance with laws and regulations to safeguard and secure its assets. In this study, four renowned Malaysian HEIs were the chosen in answering the research

questions. Two modes of data collection were adopted in this study; interview and survey. Five major constructs of information security framework (ISF) unique to

HEIs were identified during preliminary investigation. The result provides valuable information on ISF practices in establishing the components of the ISF. A

proposed ISF specific for HEIs was designed. Then a survey was conducted to investigate IT personnel perceptions on the existing information security policy practices at the

various HEIs. The result of the study contributes to the understanding of the status and HEIs practices of information security in Malaysian academic setting.

Keywords: Information Security, Information Security Framework, Standards and Policy, Higher Education Institutions.

Introduction

The demography within Malaysian Higher Education Institutions (HEIs) took an evolutionary change since the

introduction of Information Technology (IT) in the education environment. The significant achievement of IT in Malaysia can be traced from the early nineties after

various adjustments of regulatory and commercial policies, both macroeconomic and within IT's converging sectors (Hancock, 2000). In pace with such adaptation,

Malaysia's HEIs are increasingly utilizing IT in all aspects of its organizational functions.

Apart from obtaining benefits from the use of IT, HEIs are also faced with various emerging network security threat that is the result of increasingly sophisticated

methods of attack and the blending of once distinct types of attack into more complex and damaging forms (Garuba, et al., 2008). As concluded by McKissack et al. (2010) a gap

was noted in terms of the insufficiency of current “best practices where assurance provides confidence on security threats. The survey on the attacks and security

incidents reported by
MyCERT, CyberSecurity
Malaysia for the first quarter
(Q1) 2008 revealed that a
total of 10,354 security
incidents inclusive of spam

incidents were reported (MyCERT, 2008). This represented an increase of 5.59% incidents rate compared to fourth quarter (Q4) in 2007 with total of

9,486 incidents. The categories of incidents identified are intrusion, hack threat, malicious code, denial of service and spam. Thus, HEI IT departments in particular

must balance between
enabling a highly
collaborative, non-restrictive
environment without
discounting confidentiality,
integrity, and availability of

data and computing
resources.

To the best of the researchers'
knowledge, empirical
research on the enforcement

in the context of information security continues to remain an under-investigated research area especially in Malaysian HEIs environment. Hence, this research seeks to

answer two research questions, namely

- What are the main components that are considered in the

proposed ISF for higher education institutions?

- What are the IT personnel perceptions on

the existing Information
Security policy practices?

This paper is organized into
six sections. This section
introduces the study

concerned and provides the research questions. Section two portrays the literature review of existing security frameworks. The research methodology is then

discussed in section three. Section four narrates the results. The next section explains the survey results. Finally the paper ends with discussion and conclusion.

Literature Review

This section, firstly defines information security. Secondly, the various information security

frameworks are examined and then discuss the four standard framework information security commonly used.

Information Security

Information security (InfoSec) is the safeguarding of information, which has a recognized value to any organization including HEIs. It includes both business and

technology related aspects.
The purpose of information security is to preserve the three elements:
confidentiality, integrity and availability (Kasmiran, 2008),

in addition, authenticity,
accountability, non-
repudiation and reliability.

As the business dependence
on information technology has

evolved so too has the imperative and scope of information security. This emergence has been characterized by Von Solms (2006) in term of four waves:

technical, management,
institutional and governance.
The development of security
standards and frameworks
coincide with these four
waves.

AS/NZ ISO/IEC 27002:2006
lists the following success
factors as critical to
information security:

- The creation of a security framework that is consistent with the organizational culture.

- Visible management commitment to security.
- Provision of security awareness, training and education is not only

limited to stakeholders but
also to all employees and
where relevant to
contractors and third party
with relevant to their job
functions.

- Implementation of a measurement system to evaluate the effectiveness of the security program and provide feedback for

improvement of security
framework.

*Information Security Policy
Framework*

Framework is define as an the outline action of the more thorough blueprint, which sets out the model to be followed in the creation of the design, selection and initial

and ongoing implementation of all subsequent security control. It is also includes information security policies and procedures, security education training programs,

and technological controls
(Whitman and Mattord,
2007).

From the Information Security
(InfoSec) policy perspective, a

framework offers a possible starting point for understanding a security policy's impact to an organization, and is intended to guide organizations in

developing, implementing,
and maintaining security
policy (Kasmiran, 2008).
Policy should address both
logical and physical security.
In addition, privacy and

confidentiality, integrity and availability, and legal compliance requirements (Computer Associates International Inc, 2005) also should be included.

A primary objective of InfoSec Policy is to define the user's rights and responsibilities in an organization and the effective InfoSec Policy will helps the users understand

what acceptable and responsible behavior is in regards to information resources to ensure the safe environment (Hone and Eloff, 2002).

InfoSec Policy has attained an international awareness and several international standards have been built (Hong et al., 2006). The following section will explain

the commonly used standards
of Information Security Policy.

Existing Information Security Standards Framework

In this section, we discuss the existing standard information security frameworks such as

MyMIS, ISO/IEC 27001, COBIT
and COSO. Due to the lack of
information security
framework specifically
addressing higher education
institutions, the four

established framework
(MyMIS, ISO/IEC 27001,
COBIT and COSO) provided
some guideline in developing
the proposed information
security framework.

MyMIS

Malaysian Administrative
Modernization and
Management Planning Unit or
MAMPU has introduced a

handbook called MyMIS. MyMIS basically provides a standard guideline especially for government sector. It comprises of management safeguards, basic operation,

technical operation and legal matters (MAMPU, 2002).

ISO/IEC 27001

ISO/IEC 27001 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical

Commission (IEC) as ISO/IEC 17799:2005. It was subsequently renumbered ISO/IEC 27001 and entitled as *Information Technology – Security Techniques – Codes of*

Practice for Information Security Management. It is stated that the objective is to serve as a single reference point for identifying the range of controls needed for most

situations where information systems are used (IEC 27001, 2005).

Various countries like
Australia and New Zealand

follows the standard as the basis of regional information security-related standards. ISO/IEC 27001 and its variants provide point description of what should be

included as a minimum requirement in information security policy. ISO/IEC 27001 also includes a section exclusively on the review and

evaluation of an information security policy.

Among the component outlined by ISO/IEC 27001 are security policy,

organization of information security, asset management, human resources, physical and environmental security, communication and operation management, access control,

information system
acquisition, development and
maintenance, information
security incident
management, business

continuity management and
compliance.

COBIT

The Information Systems
Audit and Control Association
& Foundation (ISACAF)
developed Control Objectives
for Information and related
Technology (COBIT) to

provide management and business process owners with an IT governance model to help understand and manage the risks associated with IT.

COBIT describes the processes and controls needed for implementing an information security policy, rather than focusing on the document itself. It contains a

brief section on the Security and Internal Control Framework Policy, which gives various pointers on writing and maintaining such a document. COBIT consists of

four main components
namely, plan and organize,
acquire and implement,
deliver and support, and
finally monitor and evaluate.

COSO

Committee of Sponsoring
Organizations of the
Treadway Commission
(COSO) concepts involves

organizational internal controls, and is not specific to information security management. However, some aspects of the COSO framework could be adopted

for managing security in the enterprise. COSO specially is a business-oriented framework for implementing enterprise risk management (Ritchie and Brindley, 2001).

Based on these known information on existing frameworks, their main components were noted. The next section sets the methodology applied in order

to answer the research questions.

Methodology

In addressing the research questions, two phases of data collection were involved, namely, interview and survey. The interview is to determine the main component of ISF for

HEIs. Having completed the interviews, a survey was embarked on in examining the IT personnel perceptions on the existing information

security policy practices at
respective HEIs.

Interview

The interview conducted involved four (4) HEIs selected located in the Klang Valley. HEIs chosen are all renowned public universities located in the most populous

area of Malaysia's economic pulse. For anonymity and confidentiality reasons, the selected universities are referred as Alpha, Beta, Chi, and Delta. Alpha is a

university aspired from a contemporary global Muslim community. Beta University prides to be one of Malaysia's first and oldest universities. Chi University is the only

university that has branch campus in every thirteen states of Malaysia. Delta University is a prestigious HEI set among the top universities in Asia. The university

remains to be the main contributor in churning technical expertise. The interviewees comprises of IT-expert staff and personnel in-charge of developing the

Information Security
framework for each HEI. It
was noted that most of the
respondents are above 40
years of age; while the
number of years in their

respective organization and are in the current position recorded as more than five years. This implies that the interviewees are best candidates to provide

information on an aggregated unit of analysis in relation to views of information security and its implementation and best practices. Each of the interview exercises lasted

from 45 minutes to an hour. It was conducted between the months of May to June of 2009.

The Survey Instrument

The outcome of the interviews contributed towards the design of the survey instrument. The aim of this questionnaire is to investigate IT personnel perceptions on

the practices of existing information security policy at HELs. Prior to the actual survey, a pilot study was conducted in order to check the reliability and validity of

the instrument constructed.
The design of the
questionnaire proved to be
acceptable. No major
alterations were needed.

The questionnaire was divided into six sections. Section one highlights user's profile. Section two captures the risk management in the organization. Section three

describes information security policy status. Section four consists of survey on awareness program and training that has been carried out at the organization.

Section five defines the access control, followed by compliance concerns in section six.

Results

Through the interviews, Table 1 summarizes the main components considered by the four HEIs in this research.

(View Table 1 in full pdf version)

As depicted in Table 1, various components were included by the respective HEIs. Beta

University adopted all eleven domain of ISO 27001. Unlike Alpha considered only five incorporated also those from COBIT. MyMIS is the standard adopted by Chi and Delta while

Chi includes technical operations. Besides this, it is noteworthy to understand the current status of InfoSec policy practices.

(View Table 2 in full pdf version)

From Table 2, it is found that none of the HEI has ISF in placed. However, it is minuted that Alpha and Delta both have

IT policies in place in
comparison to Beta and Chi.
Nevertheless, IT guidelines are
in place for all the chosen public
HEIs.

Hence, this research has summarized the current InfoSec policy practices. With this and the component considered from Table 1, we come up with a proposed

conceptual framework
suitable to the Malaysian HEIs
environment.

Conceptual Framework

The ISF constructs identified for HEIs was adopted from ISO 27001, MyMIS and COBIT. With the established

guidelines, we developed the conceptual information security framework as illustrated in Figure 1.

Based on the four (4) interviews, five main constructs were identified to be considered in the HEI ISF. They are information security policy, risk management,

access control, awareness program and training, and compliance. Figure 1 shows the conceptual components with their constructs

considered for the proposed ISF.

(View Fig. 1 in full pdf version)

Five security elements are used to enforce the ISF. The security constructs are briefly described below:

- **Information Security Policy** – This part explains about security policies. Security policies control address management support,

commitment and
direction in
accomplishing
information security goals
including information

security policy (Carlson, 2001).

- **Risk Management** – Risk management is the identification and analysis

of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed (Radack, 2004)

- **Access Control** – Access control addresses an organization's ability to control access to assets based on business and security requirements

including business
requirement, user
management, user
responsibilities, network
access control, host access
control, application access

control, access
monitoring and mobile
computing (Carlson,
2001).

- **Awareness Program & Training** – Based on the awareness on the security issues, and is the single most effective means of ensuring information

security. The most effective measures depend largely on the behavior of the people affected by those measures. For example,

an access control system based on secret password is effective only if people do not share their password (Elliot et al., 1991).

- **Compliance** - Compliance control addresses an organization ability to remain in compliance with regulatory, statutory and security requirement

including legal, technical
and system requirements
and audits (Carlson,
2001).

Nevertheless, from the four established framework (MyMIS, ISO 27001, COBIT, and COSO) indeed provided beneficial guidelines to the HEIs which in turn form the

basis in developing the proposed information security framework depicted in Figure 1.

Survey Results

The survey was conducted in the month of November and December in 2009. The same four (4) HEIs were involved in

the data collection in order to address our second research question. With the assistance of human resource officer of the respective HEI's IT department, we identify the

possible respondents for this survey. Two hundred (200) were selected and questionnaires were distributed. Seventy-two (72) questionnaires were returned.

This interprets to 36% response rate. All returned questionnaires were found to be usable for further analysis.

Respondents Profile

Table 3 portrays the demographic profile of the respondents by gender, age, position in the institution and their years of experience.

(View Table 3 in full pdf version)

As depicted in Table 3 above, slightly over than half of respondents (54.2%) are male.

Nearly half of them (47.2%) are below 31 years old and hold the position as programmers. It is noted that more than a quarter of them (38.9%) have between 4

to 8 years working experience in their organization.

In addition, it was found that nearly three-quarters (70.8%) of the participants are

involved in the development
of Information Security Policy
in their organization.

Information Security Policy

This section deals with the status of information security policy available at the respondent's organization. It

was found that more than half (56.9%) of respondents are aware of the existence of information security policy. Based on these responses,

further explanations are provided.

In response, it was indicated that the policy is consistent, easy to understand, and

readily available to administrator (27.29%), faculties (24.47%), staff (24.47%) and student (23.77%). A high majority (95.25%) of the respondents

agreed that the policy is reviewed and approved by the top management. In addition, more than three-quarter of the respondents (92.64%) rated 'Strongly Agree' and

'Agree' that the policy was reviewed regularly based on significant changes.

Similarly, most respondents (90.18%) strongly agree that

the policy does effectively address the risks identified within their organizations.

(View Table 4 in full pdf version)

Question 1.0 of Table 4, it denotes that more than three-quarter of the respondents (80.49%) agreed the policy is effective. The study did reveal that their organization's

policy paid attention to
administrative (73.29%),
physical environment
(75.75%), system-based
security policy (85.41%),
network security (92.25%)

and database security
(80.49%) area (question 3.0).

There are five (5) constructs
listed according to agreement
in the information security

framework for HEIs. In reference to question 2.0, the result reported that the respondents totally rated to access control (100%) as one of the security elements

required for the framework. Subsequently, the respondents rated information security policy (97.72%), awareness program and training (87.87%),

compliance (80.49%) and risk management (70.83%) accordingly.

Risk Management

The risk management section seeks to investigate the status of risk management in the organization.

More than half of the respondents (52.8%) are aware of the existence of documented risk management policy in their organization. The survey had showed that

scenario analysis is the most preferred technique used to identify risk bearing the highest choice (33.58%) in comparison to the other three techniques. Brainstorming

and interview resulted in 27.33% and 23.45% respectively. The respondents identified risk management using survey questionnaire is

the least used technique
(15.64%).

More than half of respondents
(66.7%) had agreed that it is
very important to have

effective risk management in achieving organization's objectives. More than quarter (27.8%) indicated that it is somewhat important and a few (5.6%) thought that it is

not important at all. On the other hand, a majority (95.8%) of the respondents had rated 'Strongly Agree' and 'Agree' on the issue that effective risk management can

improve organization's
performance.

(View Table 5 in full pdf
version)

From the Table 5 above, question 1.0 reads slightly more than half (65.3%) of the respondents clearly defined that their organizations is able to allocate appropriate

resource to support current risk. Question 2.0 portrayed that more than half of the respondents agreed that their organization give response to analyze risk including the

evaluation of effectiveness (65.3%), assessment of the cost (80.6%) and prioritizing of risk (79.2%). More than half respondents also stated that their organizations has

the following security measure documents which are Business Continuity Plan (58.3%), Disaster Recovery Plan (88.9%) and Risk Management Plan (72.2%).

The result is shown in
question 3.0.

Awareness Program & Training

In this section, result of status awareness program and training conducted in the

organization will be present. Table 6 shows percentage of security awareness program and training conducted for administrator, faculties, staff and students (question 1.0).

More than half of the respondents stated the training are frequently held for administrator (73.6%) and staff (75.0%). As for the faculties (58.3%) and student

(40.3%) seems to record lower agreement on security awareness training.

In examining the duration of awareness program and

training, nearly a third of respondents (30.6%) stated that it was conducted within six months to one year. About another third (31.9%) reveals that the program duration is

more than one year. It is also reported that slightly over a third of the respondents (37.5%) stated that the training is conducted less than six months. It is noted that

more than half of the respondents (52.8%) stated that their training program was conducted by both internally and other external bodies, with nearly half of

respondents (44.4%) reported that it was conducted internally. The rest indicated that their training was conducted by other companies.

(View Table 6 in full pdf version)

In the case of computer security incident occurrence, most of respondents (84.7%) prefer to

contact the person in-charge to fix the problem. Very few (8.3%) would prefer to self-fix the problem. Very fewer still (6.9%) choose to report the problem to administrator via e-mail.

Access Control

This section will present a result of access control status at the respondents'

organizations. The result is shown in Table 7 below.

(View Table 7 in full pdf version)

Table 7 reveals nearly three-quarter (73.6%) of the respondents are aware of the existence of written policy for the use network service in

their organization (question 1.0).

Most of them are also aware of the existence of access control procedure (79.2%)

and policies (75.0%) as to support the access control policy. This has shown in question 2.0. Based on question 3.0, more than three-quarter of the respondents

(81.9%) stated that their organization have control privilege management. The result reported that their organization has protect secured areas by appropriate

entry control (95.8%)
(question 4.0), do a check on
equipment containing storage
media (80.6%) (question 5.0)
and separate the
development, test and

operational facilities to reduce risk (79.2%) (question 6.0). Based on question 7.0, respondents agree that both network infrastructure (88.9%) and administrative

procedures (75.0%) are maintained and updated.

A high majority of respondents (94.4%) stated that their organization use a

Virtual Private Network (VPN) (question 8.0). More than three-quarter (98.6%) of the respondents reported that all connection with external network is protected by

firewall (question 9.0).

According to question 10.0, more than three-quarter of the respondents (87.5%) reported the firewall configurations regularly

reviewed and updated. It is further noted, more than three-quarter of respondents defined the way they monitor their network traffic by bandwidth statistic (91.7%),

top protocol bandwidth consumer (87.5%) and top IP bandwidth consumer (84.7%) (question 11.0).

Compliance

Compliance section seeks to examine the status of compliance in the

organization. The result is presented in Table 8.

(View Table 8 in full pdf version)

Based on question 1.0 in the table above, more than three-quarter of respondents (86.1%) indicate that there is a person or committee in-

charge in securing their organization's information. In question 3.0, slightly more than three-quarter (77.8%) of the respondents stated that there is also a person in-

charge to liaise with other units to identify any new security requirements to the policy.

Slightly more than three-quarter of respondents (77.8%) agreed that their organizations' information security policy has the authority to ensure

compliance with the policy (question 2.0). Still, a majority (87.5%) of the respondents agreed that the policy is actively engage with other units to enforce compliance

with information security policy and practices (question 4.0).

As to ensure the effectiveness and compliance of

information security program and policies, two-third of the respondents (65.3%) indicated that the information security department reports regularly to the governing

board (question 5.0).
Furthermore, result of
question 6.0 showed that
more than half of the
respondents (62.5%) agreed
that there are specific training

programs to comply the policy
and standards are necessary.

Discussion and Conclusion

This study has successfully answered both the research questions. Firstly, the main constructs of HEIs ISF were

determined through interviews. Secondly, based on the IT personal responses through a survey, it establishes their perceptions

on the existing information security policy practices.

Through the interviews, it revealed that largely all the established government-

supported HEIs have some form of IT policies in place. Various establish information security standards were found to form the basis of their efforts towards the

development of their very own policy.

This research further discovers that information security policy, risk

management, access control, awareness program and training, and compliance are the major components or elements that fix upon the suggested framework for

HEIs. These components are in line with the objective of developing the framework which was to apply and cover all hardware, software, data, information, network,

personal computing devices, support personnel, and users within HEIs from intrusion, interception, interruption and denial of services.

Through the survey, generally, the respondents who largely were involved in the development of their organization's InfoSec policy perceived the importance of

each component of the proposed framework. It was found that using a scenario analysis as a technique to identify risk is found to be more effective

since the technique is designed to allow improved the decision-making. It considers the outcomes and their implications. In order to have a good risk management

policy, organization also must be able to allocate an appropriate resource to support the existing risk management policy. The risk analysis should further

emphasize on the assessment of the cost and benefits of addressing risk, similarly prioritizing of risks and its impact and likelihood besides selecting those that need

active management and evaluation on the effectiveness of existing controls and risk management responses. Furthermore, most of the organizations have

realized that having the disaster recovery plan, risk management plan, and business continuity plan are important in order to protect their organizations data and

IT infrastructure in the event of the disruptive situations. This research also found that having an effective risk management can improve organizations' performance

and simultaneously, it also helps towards achieving the organizations' objectives.

This study does disclose top management concerns on the

importance of adequate information security policy in the organizations. This is indicated by periodically reviewing and updating the policy based on significant

changes due in relation to the risk identified by the organizations. Thus, the policy is consistently and readily made available for compliance by the administrator, faculties,

staff, students and third party. Accordingly, the findings indicated the effectiveness of the policy the organizations have addressed all the five security constructs identified

in the ISF. Access control is found to be the most important security element. Additionally, policy also plays an important role in explaining to staff and

students of their responsibility in the protection of the information resources, while stressing the importance of having secured information.

Awareness and compliance is the success key to the policy as implementation will take place after the policy had been endorsed. It was showed that the awareness training has

been conducted to administrator and staff in the organization more frequent than for faculties and the students. As the students form the majority of the campus

population does it remains imperative to suggest more awareness program towards information security exposure. However, the study showed no bearing on the

duration of the awareness program and training in relationship to awareness acceptance specifically.

This study also indicated that HEIs appoints specific person in-charge or committee set up in addressing ISF and policy concerns. In furtherance of ensuring the compliance

enforcement, information security policy department is actively in cooperation with other units of the organization and regular meetings and

scheduled reporting are practiced.

Hence, this effort would provide some clarification and insights into how ISF is

depicted in the academic setting. Further work is obviously necessary to look into the details of the framework. Amongst others, matters pertaining to third

party, asset management, equipment security, communications, systems acceptance, cryptography and incident management. Thus, this research serves as an

expansion of security and assurance in operational areas
literature in the area of ISF engagements.

Despite the study's limitations, we believe that our work makes significant contributions to practice and research.

1. Managerial perspective

- a) It provides as an indicator to the status of ISF implementation from IT personnel perspective.

- b) It identified the various standard adopted by HEI or the lack of it.

- c) HEIs can enjoy significant benefits from

making right choices in terms of construct that are relevant or set a priority- level to its ICT-related activities.

- d) Serves as preparatory guidelines for future planning and improvements to HEIs ISF.

- e) Better understanding of critical ISF construct to ensure successful enforcement of information security.

2. Theoretical Contribution

- a) Clarification and rearrangement of the available constructs: information security

policy, risk management,
access control,
awareness program and
training, and compliance
are delineated in the
proposed ISF model

- b) Identification of new constructs whereby the involvement of top management plays a significant role in sustaining a robust and

effective. Notably,
adequate
implementation and
improvement of the ISF
hinges on management's
commitment.

In a nutshell, this study forms a basis in understanding the status and its practices of information security in Malaysian academic setting. This will further fulfill the

HEIs information security needs towards a more dynamic yet sustaining a secured academic environment.

Acknowledgement

This research is funded by e-Science grant vote number 79317 awarded by the Ministry of Science and

Technology Innovation
(MOSTI) of Malaysia. Our
sincere thanks go to
Malaysia's Ministry of Higher
Education (MOHE), and the

cooperation of participating
universities.

References

AS/NZ ISO/IEC 27002:2006
(2006), 'Information
Technology – Security
Techniques – Code of Practice
for Information Security

Management,' *AS/NZ ISO/IEC 27002*.

Computer Associates
International, Inc. (2005).
'Best Practices: Security

Management.' *White Paper
published in Partnership Inc.*

Elliot, R., Young, O.M., Collins,
D.V., Frawley, D. and Temares,
L.M. (1991), 'Information

Security In Higher Education,'
Cause, 1-35.

Garuba, M., Liu, C. and
Washington, N. (2008). 'A
Comparative Analysis of Anti-

Malware Software, Patch
Management, and Host- Based
Firewalls in Preventing
Malware Infections on Client
Computers' Proceedings of the
Fifth International Conference

on Information Technology:
New Generations, IEEE
Computer Society,
Washington, 628-632.

Hancock, B. (2000), 'New York Times Fired Employees for Violating Internal E-mail Policies,' *Computer Fraud and Security*, 12, 20.

Hone. K. and Eloff. J.H.P.
(2002), 'What Makes An
Effective Information Security
Policy?' *Network Security*, 6,
14-16.

Hong, K.-S., Chi Y.-P., Chao, R. L., and Tang J. H. (2006), 'An Empirical Study Of Information Security Policy on Information Security Elevation in Taiwan,'

Information Management & Computer Security. 14 (2), 104-115.

Kasmiran, J., (2008), 'The Security Factor In The

Information Technology',
[Online], [Retrieved February
14, 2009],

<http://pkukmweb.ukm.my/pkukm/content/view/84/94/>

MAMPU --- Malaysian
Administrative Modernization
and Management Planning
Unit, (2002), *MyMIS -
Malaysian Public Sector
Management of Information &*

*Communication Technology
Security Handbook*, Putra Jaya.

McKossack, J., Hooper, V. and
Hope, B. (2010), 'An Orgdel
for Information security

Assessment,' Proceedings of
the International Conference
on Information Management
and Evaluation(ICIME 2010),
ISBN: 978-1-906638-56-6, 25-

26 March 2010, Reading,
England, 218-227.

[Online] [Retrieved January
22, 2009]

[http://en.wikipedia.org/wiki/
ISO/IEC_27001](http://en.wikipedia.org/wiki/ISO/IEC_27001)

[Online] [Retrieved February
5, 2009]

<http://www.mycert.org.my/e>

[n/services/advisories/mycert/2008/main/detail/579/index.html](#)

Radack, S. (2004) 'Risk management framework:

Helping organizations
implement effective
information security
program,' *INS Whitepaper*,
Santa Clara, INS.

Ritchie, B. and Brindley, C.
(2001), 'The information-risk
conundrum,' *Marketing
Intelligence and Planning*, 19(
1), 29-37.

Carlson, T. (2001),
“Information Security
Management: Understanding
ISO 17799”, *INS Whitepaper*,
Santa Clara, INS.

Von Solms, B.,(2006),
'Information Security – The
Fourth Wave,' *Computer and
Security*, 25, 165-168.

Whitman, E.M. and Mattord,
J.H. (2007), 'Management of
Information Security,'
Thomson Course Technology,
Boston.