PalArch's Journal of Archaeology of Egypt / Egyptology

PRELIMINARY STUDY ON IT SECURITY MAINTENANCE MANAGEMENT IN MALAYSIA ORGANIZATIONS

Firkhan Ali Bin Hamid Ali[1]Mohd Zalisham Jali[2], Mohd Norazmi bin Nordin
[1]FSKTM, UniversitiTun Hussein Onn Malaysia, Malaysia, firkhan77@yahoo.com
[2]FST, UniversitiSains Islam Malaysia, Malaysia
Open University Malaysia, Malaysia

Firkhan Ali Bin Hamid Ali, Mohd Zalisham Jali, Mohd Norazmi bin Nordin, Preliminary Study on IT Security Maintenance Management in Malaysia Organizations-Palarch's Journal Of Archaeology Of Egypt/Egyptology 18(1), ISSN 1567-214x

ABSTRACT

The development of the Information Technology (IT) in the organizations at Malaysia has become more expanding in these present and future years. This is because of the active participating by Malaysian government to promote the IT usage among all the organizations in Malaysia whether in the government agencies or private sectors. The usage of the IT will make an organization have the best productivity and quality. So, their needs a well plan to implement the IT infrastructures and equipment. IT will make sure its run in successfully to support the strategic business plans. This IT needs form part of the demand pressures upon is and focusing on IT activities in their budgets and future planning. Besides that, the IT security maintenance play important role to ensure that the IT components or infrastructures execute well along the organization's business successful. Most of the Malaysian organizations had taken for granted on this part very well. May be these parts is not a Malaysian's culture in IT world. Then, they didn't have enough and tough knowledge on the IT security. Other reasons are it needs very expensive budgets and it can't show the revenues quickly. So, is these IT environments in the organizations are safe? However, how to promote the IT security to the Malaysian organizations? So, promotion can be done by using the IT services itself by putting more knowledge on the secure usage of IT facilities in the organizations.

Keywords: IT security, security maintenance, IT, Malaysian

1. INTRODUCTION

In Malaysia, IT facilities had been use in many organizations for doing their activities in efficiently and effective to support a quality production. The study will discuss about the issues of digital security in IT usage. Security issues in the digital environment are not too important things in many organizations in the Malaysia. This subject is happen in the digital environment because it has a lot of IT facilities. IT knowledge had become familiar with the Malaysian peoples.

The governments and the private sectors had promoted the IT technology very hardly whether in the advertisement, party, contest or others incentive. Inside the IT technology, they had promoted multimedia technology, web applications, networking technology, programming and the others that related but they leave or had taken a little bit in the digital security aspects.

IT is a short form of the Information and Communication Technology, which are about all the devices and components in the digital environment and communication such as software, hardware, system, database, and network, Internet and others related.

Digital Security is the method that we use to prevent and protect our digital environment by using IT facilities and communications from the threats like disasters, systems failure or unauthorized access that can result in damage or loss [1].

2. THREATS TO THE IT COMPONENTS

The usage of IT services can be disabled or become poorly its processes by many factors. It will be down the productivity of the organizations [2]. All this factors may be become from one of these agents which it is the components of the IT itself whether it is in indirectly or not indirectly like peoples, procedural, software errors, applications, electromechanical problems, dirty data, and hardware and communication parts.
It also can be threatened by natural hazards and by civil strife and terrorism. It also can be happen in indirectly or not indirectly situations. So, we must know all this threats first for easy to us to make sure that the digital security in the Malaysian organizations are in safely [3].

Threats in IT can be happen in several ways like below: -

1. Errors and accident.
These threats are happen from many agents like people errors, procedural errors, software errors, electromechanical problems and dirty data problems.

In the aspect of people errors, it is more happen in the end users whose are key in the data or make changing the data or run the processes. Example, they key in the wrong data and forgot to correct it back.

In the procedural errors, the user didn’t follow the procedures or use it in carelessly. Example, they didn’t use the rule to use the devices properly such as using of printers [4].

In the software errors, it is come from the system or applications that had been used or software bug. Those errors can causes the applications cannot work properly or dead. Example, Y2K bugs in many systems or application which is because the system or application lost its control cause of cannot determine the date properly.

In the electromechanical problems, it’s happening in the hardware site itself like electrical system or mechanical system down, power failure and others. All these things may be faulty constructed and get dirty or over heat, wear out or become damaged in some other ways.

In the dirty data problems are the problem with the data in records or systems are incomplete, outdated or otherwise in accurate.

2. Natural and other hazards.
Some of these threats can causes all the systems or applications will be down overall and permanently.

In natural hazards, it happens in situation such as fire, flood, earthquake, tornadoes and others related. All the systems will be down or damage in badly.

In other hazards, it happen in certain situation such as civil strife or terrorism. War and insurrections can take the place in others parts of the world. IT’s cannot immune to this civil strife or terrorism such as tragedy of the 11 September 2002 which happen in the New York City, USA.

3. Crimes against the IT.
This kind of the threat is about illegal act perpetrated against the IT. There is having several way that how this threat happen against the IT such as theft of the hardware, software, computer time, cables, telephone services or got the information illegally. Others are crimes of malice and destructions like abuse or vandalize computers, computers networks and the telecommunications system.

4. Crimes using the IT.
Before that, it had discussed about how the crimes act to the IT facilities but now how the crimes happen by using IT facilities. Such as, in Malaysia one of the clerk in one of the finance institution had claim a several cents from all the customer’s account into its account by using the system itself or student in the one of the University at Malaysia had using the university’s system in illegally to changed their academic status and others.

5. Viruses.
This is a form of high tech wick nesses. It is computer programs or software that can causes destruction or slowly the operations of the computers, systems or other IT facilities and it will infected to the other IT facilities which had interact with it.

It can come in several ways like by floppy, email, USB drive and downloaded file via network or Internet. Usually it will attach itself to the hard disks.

Viruses exist in many kinds of form such as Boot-sector virus, File virus, worm, logic bomb, Trojan horse, polymorph virus and virus mutation engines.

6. Computer criminals.
This is discussing about types of the people who’s involved in this IT threats. People in the organization such as the employees and the people outside the organizations such as

suppliers, customers, hackers, crackers and professional criminals can be categorizing as that types [5].

In the many cases of the computer criminals, the organizational employees do it itself. This is happen because they can access the IT infrastructure own by the organizational from the inside of the organizational. They may be use the IT facilities in the organization in the dishonesty purpose for his personal profit, sell the information or steal the hardware [6].

Outside users such as suppliers and customers may be having a link or certain access to the IT infrastructure of that organizational. So, they can use this ability to make a threat to the IT facilities of that company.

But in the cases of the hackers and crackers, which are usually categorized as the outside people, are the peoples that are can get the unauthorized access to the IT infrastructure of the company [7]. The different between these two kinds of users are the hacker does it for challenging but the cracker does it for malicious purpose.

Professional criminals are members of the crime are organizational. They didn’t only using IT but also does the illegally business or process like selling the drugs or gambling.

All this threat to the IT had become more seriously to the any organizations because of the increments of the more sophisticated user which is using its ability to make an unauthorized access and make several software that can break the any organization’s digital security. By this problem any organization must have its control and safeguarding on their IT infrastructures that will be in details on the next part.

3. CYBER SECURITY MALAYSIA

In Malaysia, we have a government agency, Cyber Security Malaysia or formerly known as Malaysia Computer Emergency Response Team (MyCERT) that have responsibility to perform any issues and problem solving in digital security [8]. It was formed on 13 January 1997 and had done fully operated on 1 March 1997.

Cyber Security Malaysia have provided a point of the reference for the Internet and computer community in Malaysia, which had deal with the computer security incidents and also provide the methods of the prevention. They are also works closely together with the others country CERT Coordinating Center like AUSCERT and the Malaysian Police, in dealing with the digital security incident, which had reports to it.

In Figure 1, Figure 2 and Figure 3 is the examples of incident statistic had provided by Cyber Security Malaysia from 2017 to 20019. Types of the incident that had used by Cyber Security Malaysia had categorized to intrusion, destruction, denial of services, virus, and hack threat, forgery, and harassment, Spam and mail bomb. This statistic had provided according to the reports that they had received from the all-Malaysian organizations [9].

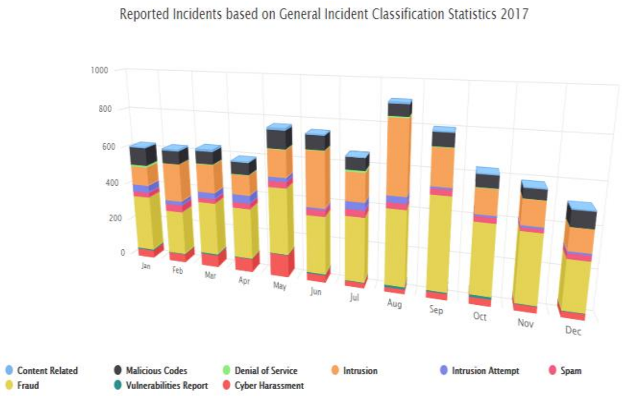

Figure 1: Incidents Statistics 2017

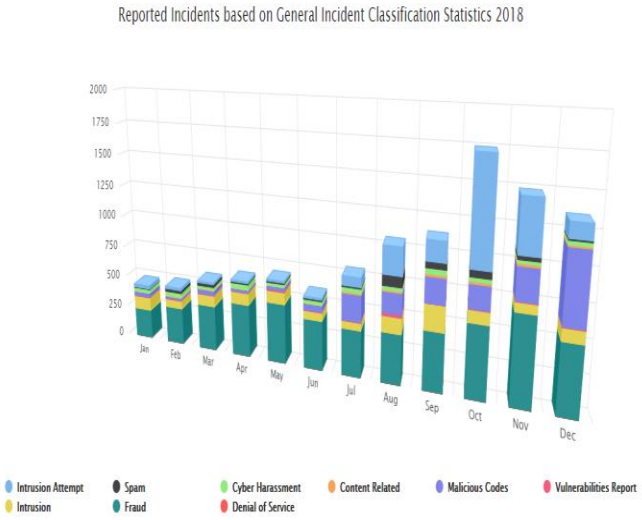

Figure 2: Incidents Statistics 2018

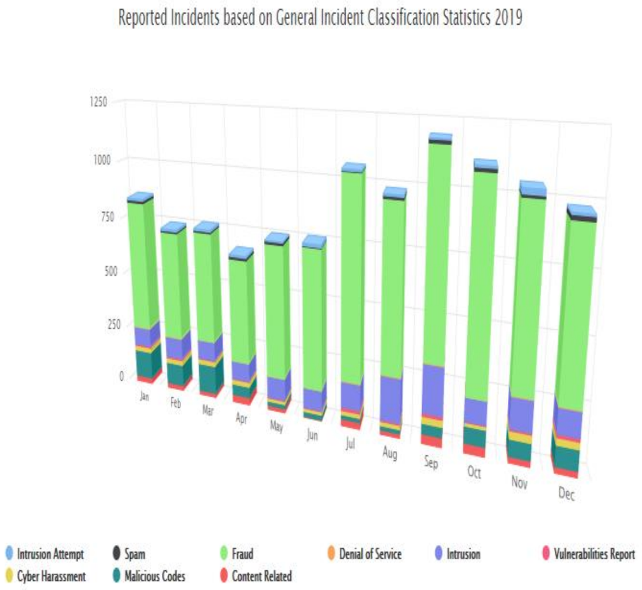

Figure 3: Incidents Statistics 2019

4. CONTROL

All organization needs the controls in their organization to ensure the quality and security of the all resources in the IT including information systems, hardware, software, networks and data. Controls are needed to prevent error occur in the computer based system, using IT for fraudulent purposes and prevent data and software from accidentally or maliciously destroyed.

If the control had been provided by organization to their IT components are successfully, it will be increase accuracy, integrity and safety of IT activities and resources because of their ability to minimize errors, fraud and destruction in the networking environment in that Malaysia's organization. It will also provide a quality assurance for IT facilities and reduce potential negative impact to the business strategy of the organizations in Malaysia.

Three major types of controls must be developed in any organization in Malaysia to achieve the successfully of using IT which are IT, procedural and facility control.

IT controls are methods and devices that attempt to ensure the accuracy, validity and propriety of all IT activities. This control must be developed to make sure proper data entry, processing techniques, storage methods and information output.

Facility controls are ways to protect an organization's IT facilities and their contents from loss or destruction. Computer centers and networks are subject to such hazard as accidents, natural disasters, sabotage, vandalism, unauthorized use, industrial espionage and destruction or theft of resources.

Usually the IT department of the organization has steps to prevent IT equipment from failure and minimize its detrimental effects.

These steps can be program of preventative maintenance of hardware and management of software updates are commonplace, using computers equipped with automatic and remote maintenance capabilities, establishing standards for electrical supply, air conditioning, humidity control and fire prevention standards, arrange for a backup computer system capability with disaster recovery of the organization, scheduling and implementing major hardware or software changes to avoid problems, training and supervision of computers operators, and using fault tolerant computers systems. (Fail-safe and fail-soft capabilities)

Fault tolerant mean that, these computer systems ensure against computer failure by using multiple CPU's, peripherals, IT facilities and system software. Fail-safe refers to computer systems that are continue to operate at the same level of performance after a major failure. Fail-soft refers to computer systems that are continuing to operate at reduced but acceptable level after a system failure.

Procedural controls are ways to determine how an organization's computer and network resources should be operated for maximum security. It's facilitating the accuracy and integrity of computer operations and system development activities. All these can be categorized by standard procedures and documentation, authorization requirements disaster recovery and controls for end user of the IT

5. AUDITING THE IT FACILITIES

The IT department of the organizations in Malaysia must be periodically examined or audited by internal auditing staff from the business division. For an extra auditing, it can be periodic audits by outside auditors from professional company in accounting side. That is a good practice for the organizations. In auditing, it should review and evaluate whether proper and adequate in IT controls, procedural controls, facility controls and other parts in managerial control, which had involved in development and implemented.

There are two ways that an organization can make an auditing in IT. There are can know as auditing around the computer and auditing through the computer. It is using computer as a subject for auditing because all IT facilities are depends on the computers whether depend it indirectly or none indirectly.

This auditing around the computer will involve in determine the accuracy and propriety of the IT input and output produced without evaluating the software that processed the data. There is more on hardware or IT devices sites that are related with the computers.

This auditing is simple and easy because it is involve only with the material or devices that you can see and hold. This auditing doesn’t involve in tracing the transaction of the input output processes and testing the accuracy and the integrity of the software that had being used.

This auditing through the computer will involve determine the accuracy and the integrity of the software or system that processes the data as well as the input of the data and the output produced by the computer systems and networks.

It will test the accuracy and the integrity of computer systems or programs. It also will test the input and output of the computer systems. It requires knowledge of the process or data flows in the computer systems, network operations and software development. This auditing sometimes is costly for certain computer systems or applications.

The truly important in this auditing procedure is to test the integrity of an application audit trail. Audit trail is the way to presence of documentation that allows a transaction to be traced through all stages of its information processing.

6. SAFEGUARDING IT FACILITIES

IT requires vigilance in security. It can look in four parts of concern that it is identification and access, encryption, protection of software and data and disaster recovery planning.

Today, anyone can connected to the Internet at everywhere. It can easily find any people’s name and email address. Then, it can trace whether that peoples are working online at the office and the true place about log in to the computer. Security is a system of safeguards for protecting IT against disasters, systems failure or unauthorized access that can result in damage or loss.

In digital security, it has several components in security safeguard. It’s including identification and access, encryption, protection of software, firewall, network security and data and disaster recovery plan.

6.2 Identification and Access

In identification and access, the computer wants to know whose the access person is. Computer system can determine the legitimate right of access by these three ways or mix among of these three ways. The computer system will be tried to identify any person by knowing what you are, what you know or who you are.

By what you have, the computer system will determine your identity by any cards, keys, signature or badges that you have it. Examples are credit card, debit card, identity card and cash machine cards, which all these have, magnetic strips or built-in computer chips that identify you to the machine. Many require your signature to compare it with the original one.

Computer rooms or large/high technologies server always kept locked, required key. This weaknesses of this material is its can be easily to be stolen or lost. Signature can be forged. Badges can be counterfeited.

By what you know, the computer system will determine your identity by PINs, passwords and digital signatures that you keep it in your mind. So, for someone to gain access to the bank account through an automated teller machine (ATM), PIN number will be key in. PIN or personal Identification Number is the security number known only to you that is required to access the system.

A password is a special word, code or symbol that is required to access the computer system. Password can be stolen, guessed or forgotten.

A digital signature is the new technology that developed to an electronic world in any fields. A digital signature is a string of characters and numbers that a user signs to an electronic document being sent by his or her computer system. The receiving computer system performs mathematical operations on the alphanumeric string to verify its validity. They are works with the system that we called it, public-private key system. This process in effect notarizes the document and ensures its integrity.

In by who you are, we can use this item for our security because of usually only we are known well about our self [10]. This form of identification cannot be easily to fake as like your physical character. Biometrics is the knowledge in science to measure individual’s body characteristics. So, this knowledge is being use in security devices following its features.

By example we can see at University of Georgia which the students whose want to use the all-you-can-eat plan at campus cafeteria, they must have their own hand first. A camera automatically compares the shape of a student’s hand with an image of the same hand pulled from the magnetic strip of an ID card. If the pattern matches, the cafeteria turnstile automatically clicks open. If not, they would be moocher eats elsewhere [11].

In Malaysia, this technology had been used at Putrajaya for attendances using fingerprints. Other biological criteria that can read by biometric devices are voices, the lips and the blood vessels in the back of the eyeball.

Beside these three types that had used for identification and access for security purpose, the call back system has use too for identification and access. The call back system is work by user calls the computer system, key in the passwords and hangs up. Then, the computers will call back the user and request a certain preauthorized number. System will block the wrong user.

6.3 Encryption

Encryption is the getting the data and changes it into unusable form within a secret code and changes the data in this unusable form into the usable form within the secret code or can read the data. It has program or software to do the encryption. The very famous and stable program for encryption is Pretty Good Privacy or PGP. It's very important to protect data or resources in the network environment especially on the Internet, Intranet and Extranets.

This encryption had a several criteria that make it good as security devices.

Firstly, passwords, messages, files and other data can be transmitted in scrambled form and unscrambled by computer systems for authorized users only.

Secondly, encryption involves using special mathematical algorithms or keys to transform digital data into a scrambled code before they are transmitted and to decode the data when they are received.

Thirdly, the most widely used encryption method uses a pair of public and private key unique to each individual like in PGP [12]. Example, e-mail could be scrambled and encoded using a unique public key for the recipient that is known to the sender. After the email is transmitted, only the recipient‘s secret private key could unscramble the message.

Lastly, encryption programs are sold as separate products or built into other software used for the encryption process.

6.4 Network security

This network security usually is provided by specialized applications or systems which known as Network Security Monitoring System. These programs are used to monitor the use of the computer systems, network or IT facilities and then protect them from unauthorized use, fraud and destruction [13].

This program will include many functions such as needed of the security measure to ensure that only authorized users will access the networks. Security monitors will also doing control of the use of the IT facilities such as data resources, software, hardware, computer systems and others.

This program will monitor the use of the IT facilities in the networks and make it in statistic form to attempt the improper use.

6.5 Protection of software and data

Today, organization in Malaysia goes to tremendous lengths to protect the data and programs that it is belong to them. This are include the training to the It's staff such as making back up data on the disks, protecting against virusand others.

Security procedure in protection of data and software is about the control of access, audit control and people control [14]. Some of this had discussed before and will discuss later. In control access, all organizations must have procedure on the right person and the right things on that system they must access according to his job. In audit control, have a system to check and track the use of IT infrastructure and overall the system.

In people control, all organization must keep track the peoples whose are internal to the organization or external to the organization.

6.6 Firewall

These security tools are including software or hardware but the most important thing is the method usage for control and security on the Internet and networks. Whether this firewall is in the software form or hardware form, it must have these several characteristics.

A network firewall is work as a gatekeeper for the computer system to protect it organization's IT facilities on the network from intrusion by serving as a filter and safe transfer point for access to and from the Internet and networks [15].

It will screen all the network traffic for the proper use of the passwords and other security codes. It only allows the authorize transmission in and out from the network.

It had become essential things to the organization that has connecting to the Internet because of its vulnerability and lack of the security.

It can fully deter but not completely prevent the unauthorized access into the computer networks. So, sometime it may allow access only from trusted locations on the Internet to the computers inside it and may allow only safe information to pass [16].

All the request must be block first because it very hard to distinguish the safe use and the unsafe use. It may then provide substitutes for some network services that perform most of the same functions but are not as vulnerable to penetration.

6.7 Disaster recovery plans

Disaster recovery plan is one process or system to restore information about operation's process from destruction or accident. Its plan is going more into a big fire drill. It’s includes a list of hardware, software, data, business functions, the peoples whose support that functions and alternate of the locations [17].

This location can be a hot sites or cold sites. A hot side is one location, which had all IT equipment and all this are needed to resume the functions. A cold site is one location, which are suitable place to install the computer system. This method is also including the method to back up and storing the data and programs in another place, method to alert the certain staffs and training for that staffs.

6. DISCUSSION

In this very though time for Malaysian organizations to face many issues in the digital security according to the statistic that had provide by Cyber Security Malaysia. It will cause the IT facility usage in damage; slow the process or non-usable use. This will be effect the quality and quantity of the productions for the organization and make business strategy fail.

The most important things are all the Malaysian organization must be realize, participate and given full support to implement the digital security aspect or issues especially for the high level management. Firstly, the organization must know all the types of threats that will overcome to the organization and make the IT facilities become lost, slow and damage.

Known that threats from their behavior by theory and technically. After that, the organization can make well plan for implementation of digital security. The purpose is for controlling all the IT facilities from the threats by using certain devices, system, software, IT facilities, policies or others related for controlling [18].

Malaysian organization can get any help or advice services from the other organization like Cyber Security Malaysia or IMPACT. With their expertise and experiences, it will help organization to make an improvement in the digital security aspect by using the IT facilities and the plans. This organization will help Malaysian organization to face any threats in the digital security whether it had happen or not happen like provide cure for any damage systems by virus, protection from any hackers and others related.

Today too many IT facilities and technologies had produced to help the organization in the digital security [19]. These IT facilities and technologies had always update and changes and grown well like the threats too. So, Malaysian organization must be always realized and take an action to the any updated of the IT facilities and technologies according to the digital security.

The organization must practice the same too to the updated of the any threats. That is why in the digital security, it’s needed more budget and full commitment from the high level management. It cannot see the income or revenue in the next hour or days or months like transaction program or others related to the production but maybe it become in 2 to 5 years or more.

Otherwise, the last thing that is very important after the organization had provided the IT facilities and technologies are to overcome the threats against the organization is auditing the IT facilities. It is important because to ensure the IT facilities usage in the organization especially in digital security aspects are working well, functional and ready to use it [20].

Is the Malaysian organizations are safely in the global digital environment? Only that organization will answer that question. The most important things are participating from the top management and the organization had ready to face or fight the threats with the updated and relevant IT facilities, technology and policies. Others are smart sharing about the issues according to the digital security among all the Malaysian organizations through Cyber Security Malaysia [21].

7. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

The study had discussed about the types of the threat in the organization regarding to the digital security and how it used IT facilities to make the threats. This problem had cover up by one government agency in Malaysia, Cyber Security Malaysia.

Cyber Security Malaysia had a function regarding to the digital security in Malaysia.It will receive any report on the digital security issues and try to solve the problems.
How about the organization in Malaysia can prevent on these threats in the digital environment using IT facilities and technologies had been discussed too.
The most important things are the organizations have a system to control and audit IT facilities. It will support to prevent Malaysian organization from any threats.

Finally, the use of IT facilities in Malaysia has a good support and budget from the high level of management in organizations. So, it could be done to the implementation of digital security in organization to make the usage of IT facilities secure, available and efficient.

ACKNOWLEDGEMENT

Thanks to UniversitiTun Hussein Onn Malaysia for sponsoring and support this article.

REFERENCES

1. Definition for Common Security Terms, http://www.mycert.org.my/html [1 MARCH 2020]
2. Davis, G.B. and Olson, M.H. (1985) Management Information System: Conceptual Foundations, Structure and Development (2ndedn), McGraw-Hill.
3. Firkhan Ali, H. A., MaziahNa'aman, "Vulnerability Assessment on the Network Security" in NCSTIE 2006: *Proceedings of the International Conference on Science and Technology 2006*. PWTC, UiTMPulau Pinang.
4. Galliers, R. and Sutherland (1991) Information System Management and Strategy Formulation: The 'Stages of Growth' Model Revisited, *Journal of Information Systems*, Vol 1 No 2 pp. 89-114.

5. Firkhan Ali, H. Aetl. , "Development Of Dual-Factor Authentication For Web Based Application Using SMS", *Proceedings of the ICITS 2008*, Kusadasi, Turkey, 2008.
6. Firkhan Ali, H. A etl., "Development of Vulnerability and Security Reporting System for Computer System and Networking" in SITIA 2008*: Proceedings of the Seminar In The Intelligent Applications 2008*, Surabaya, Indonesia, 2008.
7. Guomin Yang, Duncan S. Wong, Huaxiong Wang danXiaotie Deng (2006). "*Formal Analysis and Systematic Construction of Two-factor Authentication Scheme*." City University of Hong Kong, China.
8. MyCERT About Us', http://www.mycert.org.my/html [1 MARCH 2020]
9. Incident Statistic (2017-2019), http://www.mycert.org.my/html [1 MARCH 2020]
10. Wendy, R. (1997) *Strategic Management and Information Systems* (2ndedn), Prentice Hall.
11. Lederer, A.L and Gardiner, V. (1992) The Process of Strategic Information System Planning, *Journal of Strategic Information System Planning*, Vol 1No 2 Mar pp. 76-83
12. Hatch, B., Lee, J. and Kurtz G. (2001) *Hacking Linux Exposed: Linux Security and Solutions,* Osborne/McGraw-Hill.
13. Hole, Y., &Snehal, P. &Bhaskar, M. (2018). Service marketing and quality strategies. Periodicals of engineering and natural sciences,6 (1), 182-196.
14. Hole, Y., &Snehal, P. &Bhaskar, M. (2019). Porter's five forces model: gives you a competitive advantage. Journal of Advanced Research in Dynamical and Control System, 11 (4), 1436-1448.
15. Yogesh Hole et al 2019 J. Phys.: Conf. Ser. 1362 012121
16. Scambray, J., Mcclure, S. and Kurtz G. (2001) *Hacking Exposed: Network Security and Solutions,* Osborne/McGraw-Hill.
17. Richard A. Kemmerer et al., (2002), *Intrusion Detection: A Brief History and Overview, SECURITY & PRIVACY–2002,* Reliable Software Group, Computer Science Department, University of California Santa Barbara.
18. Norton, P and Stockman, M. (1999) *Peter Norton's Network Security Fundamentals*, SAMS Publishing.
19. Wenke Lee et al., (2000), A Framework for Constructing Features and Models for Intrusion Detection Systems, *ACM Transactions on Information and System Security* (TISSEC), Volume 3 Issue 4, ACM Press.
20. Williams, B.K., Sawyer, S.C. and Hutchinson, S.E. (1995) *Using Information technology*, Richard D. Irwin, Inc.
21. Ward, J. and Griffiths, P. (1996) *Strategic Planning for Information Systems* (2ndedn), Wiley.
22. Zacker, C. (2001) *Networking: The Complete Reference*, Osborne/McGraw-Hill.
23. Tipton, H.F. and Krause, M. (2000) *Information Security Management Handbook (4th Edition*), Auerbach Publications.
24. Security FAQs', http://www.mycert.org.my/html [1 MARCH 2020]