Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 9 (15): 2735-2743, 2009
ISSN 1812-5654

Security Mechanism in Computer Network Environment: A Study of Adoption Status in Malaysian Company

[1]N. Darmawan, [1]A. Yee-Loong Chong, [2]Keng-Boon Ooi and [1]V. A/L Venggadasallam
[1]Faculty of Computing and IT, INTI University College, Malaysia
[2]Faculty of Business and Finance, University Tunku Abdul Rahman, Malaysia

Abstract: The principle objective of this study was to examine the computer network security level of Malaysian companies. Original research using a self-administered questionnaire was distributed to 300 Malaysian companies. Data were analyzed by employing descriptive statistics. In general the adoption level of network security tools in Malaysia is still considered low with an average mean of 3.22. Based on the tools adopted, most of the companies are using common network security tool such as antivirus as their main protection for their computers. Tools that have lower adoption include vulnerability scanner and packet crafting tool. This research enables company to have a better understanding of the network security tools usage in Malaysian companies. This research has addressed previous lack of study in the examination of company's security level among Malaysian companies. Information Technology (IT) security personnel in Malaysia will also be able to use this result as a guide as to what type of network security tools is generally being employed among their peers. 3.22 of average mean considered low for the security adoption level in Malaysia, it is necessary to the companies to put more focus on this security mechanism field.

Key words: Security mechanism, computer network, technology adoption

INTRODUCTION

According to Cohen (1999), although most of the computers nowadays are working on a network environment, computer security concerns with regards to information protection are still not receiving the attention they should by many companies. Security breaches or threats could become extremely grave as a consequence of increasing the information technology dependency on society (Power, 2002). With the development of internet technologies and the increase adoption of wireless technologies by organizations such as Wi-Fi, network security is an issue that cannot be ignored by companies. According to Richardson (2008), companies suffer from network attack at least once a year. Because of those high risks of security breaches in the information technology world; the business sector must also consider the network security mechanism as a commodity input (Steward, 2005). Security is defined as a condition of being free from risks or dangers. A security mechanism is defined by Stallings as a method which is includes detection plan, prevention plan and also recovery plan in order to fight the security threats (Stallings, 2006). Shirey (2000) defined the security mechanism as a process which could be used for a system in implementing security service to that particular system.

As explained earlier, computers nowadays are working under a network computing environment. Forcht and Tsai (1994) defined network computing as a group of organization which could makes the world as a single market, a method to connect each others. Shirey (2000) defined the computer network as a group of computers and network devices so that they could exchange data and information.

There is no system connected to network which is entirely secure and it is also a challenge for many companies to predict where the network threats would come (Down *et al*., 1998). The only secure system is the system which never connects to the network and never installs software. This of course, is impossible in today's computer infrastructures which place an importance on connectivity. According to a recent report by The Star Malaysia (1986), a total of 17, 712 bank fraud cases in Malaysia involving 124.13 million ringgit were reported between 1985 and 1992. The estimated average loss annually in USA was under $300,000 summarized by Richardson (2008). According to Helms *et al*. (2000), information thefts are only caught 2% of the time, compares to bank robbers which are caught 80% of the time, but bank robbers are only get about $85 per holdup compares to information theft which gets average of $800,000 in value.

Corresponding Author: Nathan Darmawan, INTI University College, Persiaran Perdana BBN, Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia Tel: +60173775951

This brings to the question as to why it is necessary for Malaysian companies to use security tool and what are some of the common network security tools used by Malaysian organizations. Although, there are reports in the past such as those from Richardson (2008) which surveyed the type of network security tools used in companies, the survey is conducted in the United States. There has been no research in the past to investigate the types of network security tools which are adopted by Malaysian companies. As Malaysia is a developing country which places significant importance to the IT industry, it is important to investigate what are some of the security tools adopted in Malaysia. The Malaysian IT manager or network administrator who are gathering information before making a decision about what security tools to adopt and how to maximize its function, really need to know what others in the industry are doing. Besides needing to know what are the competitor is doing, it is also important to know what its partners and potential partners are doing, therefore this research attempts to provide the current adoption status of security tool in the Malaysian companies so that the IT managers and network administrator could find the answer of those questions.

The research question of this study is thus to investigate the current status of security mechanism adoption among Malaysian companies. The study will provides information concerning the data used in the study including descriptive information on the sample drawn out of Malaysia companies as population. Finally, the results in terms of the current adoption status of security mechanism are discussed followed by limitations of the study, conclusions and implications and also recommendations for future research.

Network Security is defined as the method to protect the information and other resources in the network from unauthorized user and also provide access to the authorized one to use the information and resources (Helms *et al*., 2000). There are 4 different types of threat attack according to Olayemi (2005). They are physical threats, accidental error, unauthorized access and malicious misuse (Olayemi, 2005).

According to Innella (2000), when implementing a network security, the company especially the network administrator must consider several fundamental factors:

- Integrity
- Availability
- Adequate Protection
- Effectiveness
- Depth Protection
- Due Diligence

According to Laudon and Traver (2002), there are 6 dimensions of e-commerce security:

- Integrity
- No Repudiation
- Authenticity
- Confidentiality
- Privacy
- Availability

Although, Laudon's security dimension is meant for e-commerce environment, but it is still relevant to this study because e-commerce field is also working in the network environment/internet. Table 1 shows the Laudon's security dimensions definition and also tool which related and support with each of the dimensions.

Classifying security tools: According to Caelli (1994), there are 2 main types of network security tools:

- Hardware Based
- Software Based

Hardware based security tools is defined by Caelli (1994) as a tool that comes as hardware, has security software inside and works to prevent the attacks of the threats. Software based security tools is defined by Caelli (1994) as a tool that comes as a software, which the user needs to install it to the hardware (client's PC, or server). Caelli (1994) also mention that it is necessary to integrate

Table 1: Laudon's 6 security dimensions

Security dimensions	Definitions
Integrity	Ensuring that the information or data which displayed, transmitted, received over the network has not been changed by an authorized person Example: firewall, encryption tool, intrusion detection system, rootkit detector, packet sniffer, antivirus, spyware detector tool
Non Repudiation	Ensuring that the person/user deny their transactions. Example: encryption tool, port scanner and application specific scanner
Authenticity	Ensuring that the data or information is genuine and also ensuring the user that involved on those particular transactions are really they are. Example: security-oriented OS
Confidentiality	Ensuring that the data or information is only available to see by the authorized user. Example: firewall, encryption tool, intrusion detection system, spyware detector tool
Privacy	Ensuring that the data or information is used with permission by the one who had that particular information. Example: firewall, spyware detector tool, port scanner, rootkit detector
Availability	Ensuring that the security mechanisms will always functioning all the times. Example: firewall, traffic monitoring tool, security-oriented OS, vulnerability scanner, packet crafting tool

Source: Laudon and Traver (2006)

Table 2: Definitions of security tools

Security tools	Definitions
Firewall	Work to block the unauthorized packet from outside and inside the network (Shirey, 2000). Example: Netfilter, Openbsd PF, IP Filter
Encryption Tools	This kind of tools work to make sure the data inside the message or the packet will not be read by unauthorized person (Shirey, 2000). Example: GnuPG, OpenSSL, Tor, Stunnel, OpenVPN, TrueCrypt
Traffic Monitoring Tools	Working to check and monitor the traffic on the network in order to control and maintain the network speed, security, etc., (Bitpipe.com, 2007). Example: Ntop, Ngrep, EtherApe, SolarWinds, Nagios, Argus
Rootkit Detectors	Rootkit is a kind of security threat which works to replace an important system file on the root and makes unauthorized user to gain access as an administrator access (Eset.com, 2007). Example: Sysinternals, Tripwire, RKHunter, chkrootkit
Application-specific Scanner	A tool which works to scan and detect what application used a specific port. Example: THC Amap, Nbtscan, Ike-scan, SPIKE Proxy
Vulnerability Scanner	This tool work to investigate the system to assess its vulnerability (Furnell *et al*., 2001). Example: Nessus, GFI LANguard, Retina, Core Impact, ISS Internet Scanner
Port Scanner	This tool work to investigate the system to assess its available TCP/UDP ports (Furnell *et al*., 2001). Example: Superscan, Angry IP Scanner, Unicornscan, Scanrand
Intrusion Detection System	This tool work to monitor and analyze the packet in the network in order to prevent the intruder's attack (Shirey, 2000). Example: Snort, OSSEC HIDS, Fragroute, Base, Sguil
Packet Crafting Tools	A tool which work to test firewall, get the entry point, so the administrator could patch it (Parker, 2004). Example: Hping2, Scapy, Nemesis, Yersinia
Antivirus	A tool which work to scan, detect and recover the system from computer virus (Mamaghani, 2002). Example: Norton Antivirus, McAfee Antivirus, ESET Antivirus
Spyware Detector Tools	A tool which work to detect a spyware that can gather and sends information about the users unacknowledged (Sipior, 2008). Example: Windows Defender, Max Secure
Security-oriented OS	An operating system which integrated with a security system. Example: BackTrack, Knoppix, OpenBSD, Helix, Bastille
Packet Sniffers	This tool work to sets the network card into a promiscuous mode, to enables the system capture all kind of network traffic (Furnell *et al*., 2001).. Example: Wireshark, Kismet, Tcpdump, Cain and Abel, Ettercap

the hardware based security tool and also software based security tool in order to meet a better security requirements.

Lyon (2006) discussed about the types of network security tools. The study was conducted using the users of his mailing archives. Lyon (2006) conducted the study though a survey distributed to 3243 people who shared the types of network security tools used by them. Lyon also divided the users into several categories. The tools classified are firewall, encryption tools, traffic monitoring tools, rootkit detectors, application-specific scanner, vulnerability scanner, port scanner, intrusion detection system, packet crafting tools, antivirus, spyware detector tools, security-oriented OS, packet sniffers and anti spyware (Lyon, 2006).

Table 2 shows that the security tools used in this study. Those security tools will be adapted from different sources like Shirey (2000), Bitpipe.com (2007), Eset.com (2007), Furnell *et al*. (2001), Parker (2004), Mamaghani (2002) and Sipior and Wand (2008).

MATERIALS AND METHODS

Background: A survey instrument was developed to collect the data in this study. Descriptive statistics such as means, frequency, standard deviation and percentage were used to investigate the current status of security mechanism adoption level. The populations of this survey were the company that selected from the Multimedia Super Corridor directory and chosen randomly. The project was having one year duration and it was started on 12 January 2008 and ended on 1 December 2008. The project was conducted in Malaysia.

Sampling and data collection: The target populations of this study are Malaysian companies. The populations consists of various sizes and types of companies based on their companies= type (i.e., service, manufacturing, local companies, multinational companies and joint venture companies), organization size (number of employees and annual turnover). The survey was administered to 300 IT managers or network administrators from the Malaysia companies. The survey was the main form of data collection, There were 122 responses received, indicating an estimated response rate of 40.6%. However, only 111 of the questionnaires were usable. Eleven of the surveys were incomplete by the users.

Measurement of adoption level: The adoption level of security tools in the Malaysian companies were based on 5 point Likert Scale. The adoption level here is measured using the items from whether the companies has actually 1: unaware, 2: aware, 3: interest, 4: commitment, 5: deployment of the security tools given. The security adoption level was measured using 5 items are modified from Chong and Ooi (2008).

There are 13 types of security tool that used in this study as the dependent variable. The security tools that used in this study are firewall, encryption tool, traffic

monitoring tool, rootkit detector, application specific scanner, vulnerability scanner, port scanner, intrusion detection system, packet crafting tool, antivirus, spyware detector tool, security-oriented OS and packet sniffer.

Thus, the c-commerce adoption level is a composite score comprised of the degree of adoption of the thirteen security tools that was derived from existing literatures.

Each of the security tools has a score of 1 to 5 where 1 is unaware of security tool described and 5 is the deployment of the security tool. This gave a maximum total score of 63 (High adoption level of security tools) and the lowest score of 10 (Unaware of all security tools described). The measure of security tools adoption level based on the average composite score is similar to the measurement developed by Chong and Ooi (2008) in their study of c-commerce adoption level among the Malaysian electrical and electronic industry. The survey data were analyzed by employing descriptive statistics. The analyzing of the data were followed the studied done by Chong and Ooi (2008).

DATA ANALYSIS

Profile of companies: This research collected responses from 111 general companies in Malaysia. Table 3 shows that 35 of these companies are companies in the service industry, 44 of these companies are in the manufacturing industry and 32 of them are other types of company.

Based on the Table 4, 43 of the respondents belong to a local company, while multinationals and joint ventures organizations have a same number of respondents, which are 34.

Table 5 shows that 53 of the companies that took part on this research have less than RM 10 million turnovers per year, 30 of them have turnovers per year between RM 10 million to RM 25 million and 28 companies have more than RM 25 million turnovers per year. Based on Small and Medium Industries Corporation (SMIDEC) of Malaysia in 2007, small organizations are organization that have turnover per year which is less than RM 10 million or have less than 50 employees; middle size organization are organization that have turnover between RM 10 million to RM 25 million per year or have between 51 to 150 employees and a large organization are organization that have turnovers of more than RM 25 million per year or more than 150 employees.

Current status of security tools adoption: This research aims to find out the current status of security tools adoption in Malaysia. Thus it is necessary to see the adoption level for each of the security tool being used in the Malaysian organizations. Table 6 shows the summary of the security tools adoption of Malaysian companies.

Table 3: Companies' industry type

Company type	Frequency	Percentage
Service	35	31.5
Manufacturing	44	39.6
Other	32	28.8
Total	111	100.0

Table 4: Organizations' ownership

Organization type	Frequency	Percentage
Local	43	38.7
Multinational	34	30.6
Joint venture	34	30.6
Total	111	100.0

Table 5: Annual turnovers of company

Annual turnovers	Frequency	Percentage
<RM 10 Million	53	47.7
RM 10 Million – RM 25 Million	30	27.0
>RM 25 Million	28	25.2
Total	111	100.0

Firewall: As shown in Table 6, firewall is considered as a tools that are aware (n = 30) by many Malaysian organizations. The result also suggest that Malaysian companies have deployed (n = 23) the firewall application. 18 companies stated that they are committed to implement firewall tool in the future. Firewall is the third most deployed security tool behind antivirus and spyware detector tool. The result is interesting as 15 companies claimed that they do are not aware what is a firewall tool. Firewall is one of the most common types of network security tools (Richardson, 2008). Thus the findings which show that firewall is still unaware by some organizations showed that network security awareness remains low in many organizations.

Encryption tools: As shown in Table 6, 41 companies have shown an interest in encryption tool, but the actual deployment of encryption tool remain low (n = 13). Thirty six companies in this survey are committed to deploy encryption. Most of the companies which taking part in this survey is only interested (n = 41) on adoption this tool. However, most of the respondents are familiar with encryption tools with only 7 respondents stating that they are unaware of encryption tools.

Traffic monitoring tools: Based on Table 6, most companies are interested (n = 58) to know more about this tool. However in the terms of actual deployment there are only eight of them. Twenty six of them are committed to deploy the traffic monitoring tool. Traffic monitoring tool have the same number of unawareness with encryption tool (n = 7), which is relatively low.

Rootkit detectors: Similar to traffic monitoring tool, most companies are interested (n = 50) in this tool while 29 of them are committed to deploy the rootkit detector

Table 6: Summary of security tools adoption status

Security tools	Unaware	Aware	Interest	Commitment	Deployment
Firewall	15	30	25	18	23
Encryption tool	7	14	41	36	13
Traffic monitoring tool	7	12	58	26	8
Rootkit detector	10	16	50	29	6
Application-specific scanner	9	21	41	31	9
Vulnerability scanner	14	12	54	28	3
Port scanner	15	18	38	33	7
Intrusion detection system	10	19	35	34	13
Packet crafting tool	20	18	39	29	5
Antivirus	0	5	43	30	33
Spyware detector tool	6	8	37	32	28
Security-oriented OS	3	16	36	38	18
Packet sniffer	7	12	34	48	10

application in the future. Only 6 companies have deployed rootkit detector into their network. Ten companies reported that they are unaware of this tool. One reason why many companies have to actually deploy this tool is the fact that rootkit detector are usually more common for Linux/Unix operating systems. Therefore, those organizations that are unaware of this tool could be using other type of operating system.

Application-specific scanner: Only 9 companies out of 111 which taking part of this survey has deployed the application specific scanner. However, 31 respondents are committed to use this kind of tool. Most of the companies are only interested about this tool (n = 41). There are also relatively high number (n = 21) of companies that aware of this tool when compared to rootkit detector, however the number of the companies which unaware of this tool are quite similar to the previous described tool. Application-specific scanner is focused on more non-repudiation dimension of security as stated as Laudon and Traver *et al*. (2002). The result shows that organizations are not protecting their network in terms of ensuring that the users can deny their transactions.

Vulnerability scanner: The actual deployment of vulnerability scanner tool is quite low as only 3 companies have deployed this tool. There is quite a high number (n = 54) of companies which are interested in the vulnerability scanner but they have not deploy the tool. The unawareness among respondents for this tool is relatively high with 14 of them reported to be unaware of this tool.

Port scanner: Table 6 shows that only 33 companies are committed to deploy the port scanner on their network system, while the companies that have deployed this tool are only seven. 15 respondents claimed that they are unaware of this tool. Most of the companies are interested of this tool (n = 38) and only 18 companies are aware of this tool but do not have an interest to implement port scanner. Port scanner has the second lowest unawareness level when compared to the other security tools in this study. Port scanner is quite similar to application specific server as they are to ensure the non-repudiation of network.

Intrusion detection system: Based on Table 6 there are 10 companies which are not aware of this intrusion detection system, while 19 of them are aware of this tool but has no interest to implement it. In general, the interest level for intrusion detection system is quite high (n = 35). When compared to past studies from Richardson (2008), intrusion detection system is also deployed by many organizations in the United States. Thus the results here showed that intrusion detection system is well received by organizations in developed and developing country. Companies which have committed to deploy the intrusion detection system in the future is quite high (n = 34) but only 13 are already deployed intrusion detection system to their network system.

Packet crafting tools: Based on Table 6, packet crafting tool has the highest number of unawareness among companies taking part in this survey (n = 20) and it also has the second lowest deployment. However, many companies are interested about the tool (n = 39) but have not commit to deploying it in the future. Twenty nine of them are committed to deploy this tool in the future, but only 5 companies have deployed packet crafting tool into their network system.

Antivirus: Antivirus is the tool has is most common among the companies that participated in this survey. Table 6 shows that antivirus have zero unawareness. Antivirus also the highest deployment among the companies with 33 companies having deployed antivirus on their network system. However, this is still a surprising finding since although antivirus is such as common tool, there are still many companies which have not deploy this tool. Most companies in this survey are only interested in

Table 7: Mean of adoption level of each security tools

Security Tools	N	Minimum	Maximum	Mean	SE	SD
Antivirus	111	2	5	3.8198	0.08699	0.91650
Spyware detector tool	111	1	5	3.6126	0.10489	1.10512
Security-oriented OS	111	1	5	3.4685	0.09647	1.01641
Packet sniffer	111	1	5	3.3784	0.09582	1.00954
Encryption tool	111	1	5	3.3063	0.09896	1.04266
Intrusion detection system	111	1	5	3.1892	0.10747	1.13228
Traffic monitoring tool	111	1	5	3.1441	0.08853	0.93271
Application-specific scanner	111	1	5	3.0901	0.10041	1.05787
Rootkit detector	111	1	5	3.0450	0.09439	0.99442
Firewall	111	1	5	3.0360	0.12794	1.34791
Port scanner	111	1	5	2.9910	0.10669	1.12408
Vulnerability scanner	111	1	5	2.9459	0.09391	0.98938
Packet crafting tool	111	1	5	2.8288	0.10850	1.14315
Average mean				3.219669	0.100844	

antivirus (n = 43) while 30 companies are committed to deploy antivirus.

Spyware detector tools: Spyware detector tool has the second highest deployment (n = 28) and there are 32 companies which have committed to themselves to deploy this spyware detector tool in the future. Thirty seven companies are interested on this tool. The unawareness of this tool among companies are relatively low (n = 6) and it shows that companies are very concern about privacy of their network. This shows that one of the threats that are increasingly faced by organizations is spyware attacks. This is especially true when there are many websites that are available nowadays and many have installed spyware so that these sites can customize and personalize the websites to users.

Security-oriented OS: Most companies are committed to deploy security-oriented operating system (n = 38). However, in terms of actual deployment there are only 18 of companies which have implemented this tool. Three companies are unaware of such tool. Thirty six companies are interested on this tool but are unwilling to commit or deploy it.

Packet sniffers: Table 6 shows that packet sniffer has a high number of committed companies which would like to deploy this application but only 10 companies have deployed packet sniffer. Thirty seven of the companies are interested about the packet sniffer. There are 7 companies which are unaware of this tool. Twelve of them are only aware of this tool but are not willing and not interested to deploy the tool.

Overall, based on the Table 6, antivirus has the highest number of deployment among Malaysian company. The tool that most companies are unaware of includes firewall and port scanner. Packet crafting tool has the lowest number of unawareness among Malaysian company. Most organizations are implementing security tools that help protect the integrity of their data. This means the organizations are concern with information exchanged in the network or in the system or being changed by authorized party. Most organizations however, seems to be less concern with network privacy as they have not implemented many tools which help to protect privacy such as port scanner, application specific scanner and rootkit detector. This could be due to the lack of awareness on the importance of protecting the privacy of data which is something that needs to be addressed by organizations.

Table 7 shows the average mean of all current security tool adoption level to be at 3.22. This show that most of the companies are still not adopting the security tool listed, but they are mostly interested (Mean = 3.22) in the tools described. The tool that have the highest adoption mean is antivirus (mean = 3.82), followed by spyware detector tool (mean = 3.61), security-oriented OS (mean = 3.47), packet sniffer (mean = 3.38), encryption tool (mean = 3.31), intrusion detection system (mean = 3.19), traffic monitoring tool (mean = 3.14), application-specific scanner (mean = 3.09), rootkit detector (mean = 3.05) and firewall (mean = 3.04). There are a few tools which have a mean of less than 3 and they are port scanner (mean = 2.99), vulnerability scanner (mean = 2.95) and packet crafting tool (mean = 2.83). The results give organizations an understanding of what types of threats of faced by organizations as well. The findings showed that virus as well as spyware are one of the most common types of threats faced by Malaysian organizations thus the high level of deployment. This is consistent with findings from Richardson (2008) in his study of computer security attacks in the United States.

Based on Table 8, the overall deployment of the security tools among Malaysian companies are relatively low. Many companies are deploying antivirus as their security tool. The security tool with the highest deployment in terms of percentage is 29.7% (antivirus) which is quite low.

Table 8: Percentage of the utilization of security tools among Malaysian company

Security tools	Unaware	Aware	Interest	Commitment	Deployment
	(%)				
Firewall	13.5	27.0	22.5	16.2	20.7
Encryption tool	6.3	12.6	36.9	32.4	11.7
Traffic monitoring tool	6.3	10.8	52.3	23.4	7.2
Rootkit detector	9.0	14.4	45.0	26.1	5.4
Application-specific scanner	8.1	18.9	36.9	27.9	8.1
Vulnerability scanner	12.6	10.8	48.6	25.2	2.7
Port scanner	13.5	16.2	34.2	29.7	6.3
Intrusion detection system	9.0	17.1	31.5	30.6	11.7
Packet crafting tool	18.0	16.2	35.1	26.1	4.5
Antivirus	0.0	4.5	38.7	27.0	29.7
Spyware detector tool	5.4	7.2	33.3	28.8	25.2
Security-oriented OS	2.7	14.4	32.4	34.2	16.2
Packet sniffer	6.3	10.8	30.6	43.2	9.0

Table 9: Percentage of the utilization of security tools among Malaysian company with annual turnover of less than RM 10 million (small-sized company)

Security tools	Unaware	Aware	Interest	Commitment	Deployment
	(%)				
Firewall	22.6	47.2	30.2	0.0	0.0
Encryption tool	13.2	26.4	37.7	17.0	5.7
Traffic monitoring tool	11.3	17.0	60.4	9.4	1.9
Rootkit detector	13.2	26.4	47.2	13.2	0.0
Application-pecific scanner	11.3	26.4	45.3	13.2	3.8
Vulnerability scanner	20.8	20.8	43.4	15.1	0.0
Port scanner	24.5	22.6	35.8	15.1	1.9
Intrusion detection system	17.0	22.6	30.2	20.8	9.4
Packet crafting tool	28.3	17.0	39.6	11.3	3.8
Antivirus	0.0	3.8	52.8	26.4	17.0
Spyware detector tool	11.3	9.4	41.5	28.3	9.4
Security-oriented OS	5.7	26.4	43.4	20.8	3.8
Packet sniffer	11.3	17.0	34.0	34.0	3.8

Table 10: Percentage of the utilization of security tools among Malaysian company with annual turnover of between RM 10 million to RM 25 million (medium-sized company)

Security tools	Unaware	Aware	Interest	Commitment	Deployment
	(%)				
Firewall	10.0	13.3	16.7	30.0	30.0
Encryption tool	0.0	0.0	46.7	43.3	10.0
Traffic monitoring tool	3.3	6.7	46.7	40.0	3.3
Rootkit detector	10.0	6.7	50.0	30.0	3.3
Application-specific scanner	10.0	16.7	33.3	26.7	13.3
Vulnerability scanner	10.0	3.3	46.7	33.3	6.7
Port scanner	6.7	16.7	30.0	40.0	6.7
Intrusion detection system	3.3	20.0	30.0	33.3	13.3
Packet crafting tool	16.7	20.0	30.0	26.7	6.7
Antivirus	0.0	10.0	16.7	23.3	50.0
Spyware detector tool	0.0	6.7	26.7	30.0	36.7
Security-oriented OS	0.0	6.7	40.0	33.3	20.0
Packet sniffer	0.0	6.7	30.0	63.3	0.0

The security tool that have very low adoption include vulnerability scanner (2.7%) and packet crafting tool (4.5%) The results also show that many companies are not aware of the many security tools available in the market. For example, packet crafting tool (18%), firewall (13.5%) and port scanner (13.5 %) are quite common tools but the IT personnel are unaware of these tools. This is surprising as firewall is an important tool when it comes to protecting the computer networks.

Based on Table 9, most small-sized company has low deployment of the security tools. As shown in Table 9, only antivirus (17%), intrusion detection system (9.4%) and spyware detector tool (9.4%) are deployed by small sized company. The rest of the tools have very low deployment percentage and even popular tools such as firewall, rootkit detector and vulnerability scanner have 0% deployment. Small-sized company also has 0% commitment to deploy the firewall in the future. Fortunately all small-sized company is aware antivirus for their security system.

Table 10 shows that the deployment percentage of security tool for medium-sized company is better when compared to small-sized company except for packet sniffer which had 0% deployment by the medium-sized company. Antivirus has the highest deployment percentage by the medium-sized company (50%). Compared to small-sized

Table 11: Percentage of the utilization of security tools among Malaysian company with annual turnover of more than RM 25 million (large-sized company)

Security tools	Unaware	Aware	Interest	Commitment	Deployment
	(%)				
Firewall	0	3.6	14.3	32.1	50.0
Encryption tool	0	0.0	25.0	50.0	25.0
Traffic monitoring tool	0	3.6	42.9	32.1	21.4
Rootkit detector	0	0.0	35.7	46.4	17.9
Application-specific scanner	0	7.1	25.0	57.1	10.7
Vulnerability scanner	0	0.0	60.7	35.7	3.6
Port scanner	0	3.6	35.7	46.4	14.3
Intrusion detection system	0	3.6	35.7	46.4	14.3
Packet crafting tool	0	10.7	32.1	53.6	3.6
Antivirus	0	0.0	35.7	32.1	32.1
Spyware detector tool	0	3.6	25.0	28.6	42.9
Security-oriented OS	0	0.0	3.6	60.7	35.7
Packet sniffer	3.6	3.6	25.0	39.3	28.6

company, the overall deployed tools are much higher in medium-sized company. Traffic monitoring tool, rootkitdetector, vulnerability scanner, port scanner and packet crafting tool all have a low deployment percentage.

Based on Table 11, the percentage of the utilization of security tools for companies which has turnover of more than RM 25 million per year has the highest percentage of deployment in the security tools when compared to small-sized and medium-sized company. Only 3.6% of the companies are unaware of the packet sniffer tool. The highest utilized tool in the large-sized company is firewall (50%), followed by spyware detector tool (42.9%) and antivirus (32.1%). As shown from the Table 11, large companies are more aware and are more likely to deploy security tools to protect their computer network when compared to other the SMEs. This could be due to the financial resources they have when compared to the SMEs. However, given the importance of computer securities and the threats on computer networks do not just target the large companies, it is important for SMEs to start thinking about implementing security tools to protect their network.

DISCUSSION

This research aims to investigate the current network security adoption in Malaysia. We will discuss the overall security adoption tools in Malaysia and look at which security dimensions (Laudon and Traver, 2002) are focused by the Malaysian companies. Overall, the adoption level of security mechanism in Malaysian company is still considered low with an average mean of 3.22. Based on the tools adopted, most companies are using antivirus as their main tool to protect their computer network.

The tools that are deployed the most are antivirus, spyware detector tool and firewall. These tools are concern with protecting the integrity of the computer network. As stated in earlier section, data integrity is to ensure that the data in the computer network is not being altered by unauthorized party. Therefore, for many organizations, it is important for them to protect their data. Among the tools with lowest adoption, they are mainly tools which protect the privacy (rootkit detector) and availability (vulnerability tool and packet crafting) of the network. This could mean that most of the Malaysia companies are unaware of the importance of protecting the availability as well as the privacy of their network.

In order to investigate the adoption status among Malaysian companies, we have also compared the adoption in terms of companies size. This will allow us to have a better understanding of security adoptions between SMEs and larger organizations. The results showed that the lowest number of adoption of security tools come from small-sized companies, followed by medium-sized company and the highest is the large-sized companies. Although, this is understandable due to the limited resources in financial and technical resources that smaller companies have when compared to larger companies, it is still vital for these companies to start adopting security tools to prevent their network from threat's attack. This is because the user of the network will automatically choose the more secured companies compared to less secure one. For the larger companies which already applied some security mechanism to their network system, it is advisable to keep updated the security tool with the latest security update, because the world of technology is growing very fast and types of threats on computer networks are growing rapidly as well.

Compared with existing studies on Computer Crime & Security Survey by Richardson (2008), the result of this study is contradicted with Richardson's result. According to Richardson (2008), 94% of the companies are using firewall, 97% of them are using antivirus and such a high number of companies (80%) are using anti spyware. Compared with the condition in Malaysia based on this study, there is low level of security tools adoption. This difference of results in this study when compared to

existing report by Richardson (2008) could be due to the fact that Richardson's study was focused on a developed country B United States, whereas this study is focused on Malaysia, which is a developing country. The results suggest a gap in the adoption of security tools between developed countries and developing country.

CONCLUSION

This research enables companies to have a better understanding of the current status of security tools adoption level. This research has addressed the previous lack of study in the security tool adoption in developing nations such as Malaysia. This research also allows the management and network administrator of the companies to know what is the adoption level of the security tool in Malaysia and allows them to know the tools that they should adopt to protect their computer network.

Limitations and future work: One of the limitations is that this research has been conducted only in Malaysia and whether the results from this research would be consistent with other countries companies would need to be verified through further research. As such, there is a need to compare the adoption level of security tool in Malaysia with other countries to allow us to have a better understanding of overall security tool adoption level in the companies.

REFERENCES

Bitpipe.com, 2007. Network monitoring. http://www.bitpipe.com/tlist/Network-Monitoring.html.

Caelli, W.J., 1994. Security in open and distributed system. Inform. Manage. Comput. Secur., 2: 18-24.

Chong, A.Y.L. and K.B. Ooi, 2008. Collaborative commerce in supply chain management: A study of adoption status in malaysian electrical and electronic industry. J. Applied Sci., 8: 3836-3844.

Cohen, F., 1999. Managing networks security: Simulating network security. Network Secur., 4: 6-13.

Down, P.W. and J.T. McHenry, 1998. Network security: It's time to take it seriously. IEEE Comput. Soc., 31: 24-28.

Eset.com, 2007. Definitions of malware: Rootkit. http://www.eset.com/threat-center/threats/rootkit.php.

Forcht, K.A. and Y.W.A. Tsai, 1994. Security and network management: Changes in the way we work. Inform. Manage. Comput. Secur., 2: 35-41.

Furnell, S.M., P. Chiliarchaki and P.S. Dowland, 2001. Security analysers: Administrator assistants or hacker helpers? Inform. Manage. Comput. Secur., 9: 93-101.

Helms, M.M., L.P. Ettkin and D.J. Morris, 2000. Shielding your company against information compromise. Inform. Manage. Comput. Secur., 8: 117-130.

Innella, P., 2000. Designing Secure Networks Based on the Software Process Model. Tetrad. Digital Integrity LLC., Springer.

Laudon, C.K. and C.G. Traver, 2002. E-commerce: Business, Technology, Society. 1st Edn., Addison Wesley, Boston, pp: 235-236.

Lyon, G., 2006. Top 100 Network security tools. http://sectools.org/.

Mamaghani, F., 2002. Evaluation and selection of an antivirus and content filtering software. Inform. Manage. Comput. Secur., 10: 28-32.

Olayemi, O.A., 2005. University of East London School of Computing and Technology, System Integration, CNM009. http://homepages.uel.ac.uk/u0430614/classification_of_security_threa.htm.

Parker, D., 2004. Packet crafting for firewall and IDS audits (Part 1 of 2). security focus. http://www.securityfocus.com/infocus/1787.

Power, R., 2002. CSI/FBI computer crime and security survey. Comput. Secur. Issues Trends, 8: 1-22.

Richardson, R., 2008. 2008 CSI/FBI computer crime and security survey. Comput. Secur. Issues Trends, 8: 1-30.

Shirey, R., 2000. Internet Security Glossary. IETF., USA., pp: 41-153.

Sipior, J.C. and B.T. Ward, 2008. User perceptions of software with embedded spyware. Inform. Manage. Comput. Secur., 21: 13-23.

Stallings, W., 2006. Cryptography and Network Security: Principles and Practice. 4th Edn., Prentice Hall, Upper Saddle River, New Jersey, ISBN: 0130914290.

Steward, A., 2005. Information security technologies as a commodity input. Inform. Manage. Comput. Secur., 13: 5-15.

The Star Malaysia, 1986. 17, 712 bank fraud cases since 1986. Malaysia, Sept. 8, 1992.