DESIDOC Bulletin of Information Technology, Vol. 27, No. 6, November 2007, pp. 41-53

Awareness of Cyber Laws in Young Singaporeans

Tan Kar Peng and Chennupati K. Ramaiah*

American Casualty Express Insurande Asia Pacific, Singapore
E-mail: kar_peng_tan@yahoo.com.sg

**Muffakham Jah College of Engineering & Technology*
Road No. 3, Banjara Hills, Hyderabad-500 034
E-mail: chennupati_kramaiah@yahoo.com

ABSTRACT

Security threats over Internet have necessitated information security awareness among the users. Concern about information security is also on because of financial risks associated with it. Importance of safe computing practices being advocated by several governments, professional organisations, and individuals has impelled the need for secured commercial computer and application systems. Many countries have formulated cyber laws to protect their business, security, and user's rights and privacy and for educating people about their own and other countries cyber laws so that they do not have any problems relating to information security over Internet. The paper presents the result of a survey conducted to find out the general awareness of cyber laws and computer security among Singaporeans, covering a cross section of the computer users in the country. The paper shows that most of the participants of the survey were not able to actively keep themselves updated with the latest information related to computer security and this fact seems consistent across the different professions. Also, all the participants of the survey agreed on the need for ethics in the pervasive use of the Internet where problems in security, privacy enforcement and threats of viruses are obvious and cannot be avoided.

Keywords: Information security, Singapore cyber laws, users awareness studies, Internet security

1. INTRODUCTION

Internet was developed to provide a network to share, exchange and communicate information among researchers. Later, it evolved as a medium to publish and deliver information for all types of users including the government and academicians. Today Internet has become essential platform for all kinds of transactions such as information publishing, delivering and searches, e-commerce, education, research, etc. But evolution of information technology has also created problems and risks to computers in context of security of information available on the Internet and computer networks. Computers, networks and software are now potentially more vulnerable because of improper protection measures, viruses, hackers, and several other loopholes present in the computer communication and network technologies.

Intentional attacks or accidental mistakes can easily destroy or compromise a computer's ability to perform its original intended functions. Therefore, security is the basic necessity for all types of computer-related systems especially where leakage of information could affect the business or work. The security industry is enabling people to communicate, do online purchases and commerce, using technology products and services that provide the necessary protections[1]. One common misconception among the users is that technology provides 100 per cent protection in all types of activities/tasks. This is a fact that a combination of products or factors works hand-in-hand in constant harmony to ensure absolute security on the Internet, and this is also the guiding principle of Microsoft's new slogan "Secure by design, secure by default, secure in deployment".

Securing computers, information systems and cyberspace requires continuous efforts ranging from the individuals, corporations and governments. In other words, the whole society in general plays equally an important role in protecting the security of information and information systems. Users today are increasingly interconnected and these connections typically cut across boundaries of towns, cities, states, and countries. Critical infrastructure like transportation, energy and finances of developed countries are now being managed on the Internet, which shows its growing importance. This is coupled with the increasing number of wireless devices and private networks, which in turn have increased the volume of protected information being exchanged between people. With the advancement of technology, the need for users' privacy has also increased significantly; because of the ease at which personal information of a user can be collected, stored and disseminated. Authentication, integrity, non-repudiation, confidentiality and availability are the other components of online/computer security.

The information, media and telecommunication industry in Singapore have evolved rapidly over the past 10 years, and the Information Development Authority (IDA) of Singapore, a statutory board of the government under Ministry of Information, Communications and Arts is responsible for the promotion of cyber laws in the country.

This study mainly explores the current awareness of knowledge about cyber laws in Singapore. Majority of the people surveyed were Internet user for various purposes such as e-commerce, money transactions, communication, education, governance, etc. in their day-to-day life. At the same time, the study also identified the difficulties encountered by the individuals; and the preferred mode of communication between the state and individuals. The objectives of the study were: (i) to investigate Singapore's initiatives and progress in cyber laws; (ii) to highlight the barriers to comprehending cyber laws in Singapore; (iii) to identify the level of awareness of cyber laws among Singaporeans; (iv) to find out the impact of cyber laws in Singapore; and (v) to identify the user's preferred mode of communication and information delivery.

2. BACKGROUND

The elements of any security infrastructure include information technology (IT), procedures, practices, laws and regulations, and people and organisations[2]. Management support and the organisation are the keys to the success of any security infrastructure[3]. Some of the challenges faced while enforcing cyber laws in the international front include: harmonisation of country's criminal laws, locating and identifying perpetrators across borders, and securing electronic evidence of their crimes[4] so that they may be brought to the notice of the court of law. The existing major cyber laws in the world include the Computer and Fraud Act of the United States and the Computer Misuse Act of the United Kingdom and some other Acts across Asia. According to Ang[5], key policies and legal issues related to cyber laws can be grouped into six categories: (i) intellectual property rights, (ii) issues related to e-commerce, (iii) security, (iv) privacy, (v) content regulation, and (vi) access and service provision.

3. RELATED RESEARCH

Information security has become an important part of every business's integrated strategy in risk management. Electronic data and its transmission are vulnerable because of unauthorised interference from criminals and persons having vested interests. Ensuring security of data through legal and technical means has become a matter of concern. Personal information privacy is arguably the most important issue facing the growth and prosperity of the Internet, especially e-commerce. A recent survey result shows that security on Internet is growing and this feeling is lingering with majority of the people of the online community (www.harrisinteractive.com, www.nfoi.com).

Cyber laws encompass the legal, statutory and constitutional provisions that affect computers and computers' networks to individuals, corporate bodies and institutions which (a) mainly work in cyber space, (b) provide access to cyber space, (c) produce hardware and software that enable users to access cyber space, and computer users who work in cyber space. Laws, norms, market, and the code are the four moral values that regulate our behaviour[6]. Governments around the world has a responsibility to pass legislation and educate the general public to combat with high-tech crimes and high-tech criminals[7]. In this regard US has taken an initiative and established a 'Awareness Outreach Task Force' to coordinate and promote awareness about cyber laws. This task force has formulated US National Cyber Security in collaboration with TechNet, US Chamber of Commerce, Business Software Alliance, and other professional bodies. Similarly, Organisation for Economic Cooperation and Development (OECD) has prepared Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security for the sake of cyber laws awareness among public. Following these lines, Singapore also made an effort to raise the awareness of security issues including cyber laws by conducting a 10 days course on 'Internet Security and Cyber Laws in Singapore' for local professionals in September 2004. Business Software Alliance (BSA) conducted a survey to know about cyber laws awareness and found that awareness of information security has increased significantly among the users[8]. The study found that private sector leaders believe that government should take leading role in cyber security by enforcing strict laws particular for cyber security, pass a federal data breech notification bill, and take other necessary steps to safe guard from the cyber threats.

4. METHODOLOGY

The survey used the questionnaire tool to know the awareness of cyber laws among the Singaporeans. The method was cost-effective and helped in collecting different types of information related to the users' attitudes from a cross-section of occupations in a limited time frame. The questionnaire contained 34 questions, both open and closed-ended, organised in six sections: personal profile, computer/web usage, awareness about cyber laws, overall satisfaction/rating, user's preferences/requirements, and barriers/problems faced. Before deploying the actual survey, the questionnaire was piloted with five people. Based on their feedback, the contents and the structure of the questionnaire were improved for the final survey. The questionnaire was sent to 150 professionals (i.e. students, engineers, lecturers, finance-related professionals, etc.). Of the 150 professionals, 72 (48 per cent) responded, but only 66 questionnaires were taken as valid. The remaining were rejected because of illegible writing and incompleteness of answers. All these valid questionnaires were subsequently analysed.

5. RESULTS

5.1 Users' Profile

The respondent's personal details were tabulated (Table 1) according to the gender, age group, basic qualification, profession, ownership of computer, Internet usage, and purpose of Internet use. Of the total, the percentage of males (56 per cent) was slightly more than females (44 per cent). The majority of the respondents (82.9 per cent) belonged to the age group of 21-40 years and almost

Table 1. Demographic profile of respondents

Particulars	Categories	Number	Percentage
Gender	Male	37	56.0
	Female	29	44.0
Age groups (years)	Less than 20	2	3.0
	21 to 30	32	46.5
	31 to 40	24	36.4
	More than 40	8	12.1
Qualification	‘O’ Levels	3	4.5
	‘A’ Levels	1	1.5
	ITE	0	0.0
	Diploma	6	9.1
	Degree & above	54	81.8
	Others	2	3.0
Profession	IT related	16	24.2
	Engineering related	10	15.2
	Finance related	14	21.2
	Academic/Teaching	7	10.6
	Students	10	15.2
	Others	9	13.6
Ownership of computers	PC	61	92.4
	Macintosh	1	1.5
	Notebook	18	27.3
	PDA	10	15.2
Internet usage per week	Less than 10 hr	29	44.0
	10-30 hr	25	37.9
	31-50 hr	8	12.1
	51-70 hr	4	6.0
	More than 70 hr	0	0.0
Purpose of Internet use	Information gathering	54	81.8
	E-mail	31	47.0
	Gaming	2	3.0
	E-commerce	12	18.2
	Work	19	28.8
	Chatting	6	9.1
	Forums	3	4.5

the same percentage (81.8 per cent) had minimum an undergraduate degree or above as basic qualification(s). The sample covered all professions including IT related (24.2 per cent), engineering related (15.2 per cent), finance related (21.2 per cent), academicians and teachers (10.6 per cent), and students (15.2 per cent). Remaining belonged to other professions. Ninety-two per cent of them owned a PC and more than a quarter (27.3 per cent) were also having a notebook computer. A person also had a personal digital assistant (PDA). Macintosh computer was found the least popular among Singaporeans as only

1.5 per cent of the respondents owned the Macnitosh.

The majority of these respondents (81.9 per cent) were using Internet for 30 hr or less per week and the remaining for 31-70 hr per week. Information gathering (81.8 per cent) was the most popular task. Less than half of them (47 per cent) were using Internet for e-mails, and more than a quarter (28.8 per cent) were using Internet for their day-to-day office work. A small percentage (18.2 per cent) of them were also using it for e-commerce. A few were using it for games, chatting, and participating in forums. Overall, the participants of the survey sample were highly IT literates, therefore computer ownership and using Internet either at home or office was also high.

5.2 Awareness of Cyber Laws in Singapore

5.2.1 Keeping up-to-date with Computer Security News

Figure 1 shows that more than three-quarters (76 per cent) of the respondents do not keep in touch with the latest computer-security related news. A small percentage (3 per cent) felt that they considered themselves as "fully aware" and another 14 per cent "somewhat aware" about cyber laws in Singapore. The percentage of persons who are aware about cyber laws in Singapore is almost similar when it was compared to another national survey conducted across the UK where 57 per cent indicated that they had inadequate awareness about computer security laws[9]. For those who kept themselves updated with computer security related news, the print media such as magazines, journals and newspapers were the most popular sources of information. Similar results were also found in another similar study in which printed materials were the most preferred form of information source to the majority of the students[10]. In that study, a quarter (24 per cent) of the respondents felt that keeping up-to-date on the computer-security news is mandatory to IT and related professions without which they cannot progress in their work or career.

5.2.2 Virus attacks and Software Vulnerabilities

The majority of the respondents were aware about the repercussions of various virus attacks (Table 2). This could be the result of a computer-literate society as well as the fact that the majority of the participants of the survey hold at least a degree as their basic qualification. Almost half of them agreed that viruses will certainly affect PCs or Notebooks that are being used at their homes (66.7 per cent) and offices (60.6 per cent). However, software vulnerability and disclosure may not be encouraged at least from the management's point of view[11].

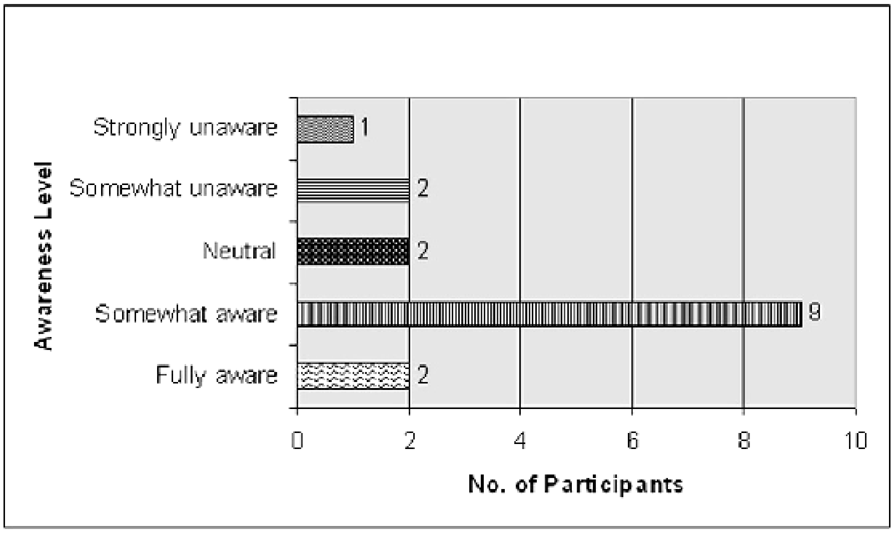

Figure 1. Level of awareness.

5.2.3 Computer Misuse Act

The majority (64 per cent) of the respondents were aware of the Computer Misuse Act of Singapore, but 91 per cent were not aware or keeping up-to-date about the recent amendments to the same Act. However, most of them (90 per cent) agreed that ethics are needed for the Internet users. This was expected because of high literacy level of the respondents willing to assume more responsibility at an individual level.

Similarly, another survey conducted with the US-based small medium enterprises (SME), found that even though IT has become an integral part of the US SMEs, there was lack of awareness on basic ethical issues[12]. Similarly, another study found that anonymity, common among Internet users is due to the lack of cyber ethics[13].

5.2.4 Copyright Law

Eighty-six per cent of the participants surveyed were aware of the Copyright Laws and about 82 per cent also understood its application in the Internet environment. This matched with the 81 per cent of the respondents who had degree and above basic education qualifications indicating that the people having tertiary education are keeping up-to-date with the local cyber laws.

5.2.5 Importance of the Privacy

All respondents felt that privacy is an important, if not very important, issue in the online environment. Of the total, slightly less than three-fourth (71 per cent) respondents mentioned that it was very important in their day-to-day life and more than half (56; 85 per cent) felt that the law should protect every one's privacy. This shows that all these respondents prefer their privacy and regard as an important issue for their work/transactions, perhaps due to Westerners influence on Singaporeans. This finding is similar with another study of consumers in the Federal Republic of Germany where consumers have very strong views about protecting their privacy[14].

5.2.6 Level of understanding of Cyber Laws in Singapore

Sixty-nine and 89.4 per cent of respondents were aware about both the Computer Misuse Act and the Copyright Act of Singapore, respectively. The majority (71 per cent) of the respondents felt that they have "somewhat understood" the above mentioned Acts. This is not surprising because most of the participants in this survey were using Internet frequently, but not keeping up-to-date with relevant laws.

Table 3 gives a snapshot of the level of awareness among the respondents about the available cyber laws in the world. It is surprising that respondents were not familiar with the cyber laws in neighbouring countries (Malaysia, Philippines, etc.). However, almost a fifth of them are familiar with the cyber laws of the USA and the UK. This could be because these people may be working in multinationals companies. Overall, the majority of the respondents were familiar with the Singapore cyber laws, but the same were not that much familiar with the Broadcasting Act (36.4 per cent) and the Electronic Transactions Act (28.8 per cent) though they are regular users of e-commerce applications in their day-to-day life.

Table 2. Effects of viruses

Worms/Viruses/Trojans	No. of respondents	% of respondents
It will affect the PCs or notebook I used at home	44	66.7
It will affect the PCs or notebook used in the office	40	60.6
Heard of it, but I believe I am well protected	17	25.8
Not at all a problem	1	1.5
Never heard/Don't know	0	0

Table 3. Comparison of level of awareness of cyber laws

Various Cyber Laws	No. of respondents	% of respondents
Computer Misuse Act (Singapore)	46	69.7
The Copyright Act (Singapore)	59	89.4
Singapore Broadcasting Act (Singapore)	24	36.4
Electronic Transactions Act (Singapore)	19	28.8
Patriot Act (USA)	3	4.5
Computer Fraud and Abuse Act 1986 (USA)	12	18.2
Computer Abuse Amendments Act 1994 (USA)	12	18.2
Electronic Communications Protection Act (USA)	4	6.1
Health Insurance Portability and Accountability Act (HIPAA, USA)	2	3.0
Computer Misuse Act 1990 (United Kingdom)	15	22.7
Data Protection Act 1998 (United Kingdom)	9	13.6
Computer Crime Act 1997 (Malaysia)	0	0
Electronic Commerce Act 2000 (Philippines)	0	0

5.3 Overall Satisfaction Rating of Existing Cyber Laws

5.3.1 Security Updates/Patches/Advisories

More than half (54 per cent) of respondents were fully aware that the virus scanner updates automatically through downloading at regular intervals (Table 4) whereas about a third (34.8 per cent) of them were ‘not sure’ about how software security updates taking place on their system. One possible explanation for this could be that the software updates may not be done that frequently, hence the respondents were not fully aware about this aspect. It is interesting to note that majority of them were cautious about updating antivirus software (57.6 per cent) by setting in an auto updating mode but in reality only about half (27.3 per cent) of these were doing software security updates.

The percentage of people downloading these patches/updates was double (24.2 per cent) then people downloading software security virus scanners (12.1 per cent). To avoid unforeseen problems due to virus and other security threats, all the end-users got to need basic education or training so that they scan their systems on their own at regular intervals.

5.3.2 Satisfaction of Commercial Computer and Application Software

Close to half (48 per cent) of the respondents expressed their 'mediocre' happiness with the current security provisions with the existing commercial computer system/software. More than half (68 per cent) of the people were 'somewhat happy' or `happy' and less than a third (32 per cent) were not happy with the existing practices. However, it would always be better if the software vendors provide

Table 4. Virus scanner and software security updates

	Virus scanner updates		Software security updates	
	No. of respondents	% of respondents	No. of respondents	% of respondents
Download automatically	38	57.6	18	27.3
Tested before implementation	5	7.6	8	12.1
Downloaded in reaction to an event	8	12.1	16	24.2
Not sure	19	28.8	23	34.8
No formal plan	0	0	5	7.6

enough training/information to the users and make them understand the importance of their system's security.

5.3.3 Cyber Safety Levels in Singapore

Half of the respondents were somewhat comfortable about the existing computer-related laws in Singapore. So, there is a good bit of room for improvement with regard to the cyber laws in Singapore. Although, Singapore has fairly established computer-related laws, about half (49 per cent) of the respondents thought that Singapore still might not be a safer place for computer-related activities showing the concerns of the participants about the high level of uncertainty among those who use Internet extensively for their day-to-day activities. In this context, both the Singapore government and computer industry should come together and work towards the removal of the fear from the minds of the people so that Internet usage improve further in the country.

5.4. User's Preferences/Requirements about the Cyber Laws

5.4.1 Security Responsibility on the Internet

Almost every respondent felt that every individual should take the responsibility for the safety on the Internet, which is similar to a study conducted for the implementation of the OECD guidelines for the security of Information Systems and Networks[15]. For this reason only, Microsoft, the number one IT Company in the world is sending monthly updates as patches for protection from all kinds of vulnerabilities. But government and IT companies should also gain the trust of the people to use their products[16]. According to respondents, different types of agencies such as government, private corporations, MNCs, individuals, etc. should also participate and take responsibility of the security on the Internet (Fig. 2).

5.4.2 User's Privacy

Privacy was considered as an important factor, if not very important by all the respondents. More than a third felt that privacy (35 per cent) and security (33 per cent) were the major concerns while surfing the Internet. The other factors including authentication and integrity may be a bit difficult to comprehend hence less than a third (31 per cent) of them only indicated.

5.4.3 Who should Understand Cyber Laws in Singapore?

Almost 98.5 per cent of the respondents agreed that 'every individual' should understand cyber laws in Singapore. Over half of them (56 per cent) also thought that the government should take lead role in propagating them. Similarly, 25.8 per cent of them thought that this responsibility should be given to the non-governmental organisations (NGOs) and over a third (37.9 per cent) also felt that professional societies/corporate offices should be given the responsibility to educate local people about cyber laws. At the same time, the majority of them felt that all the organisations

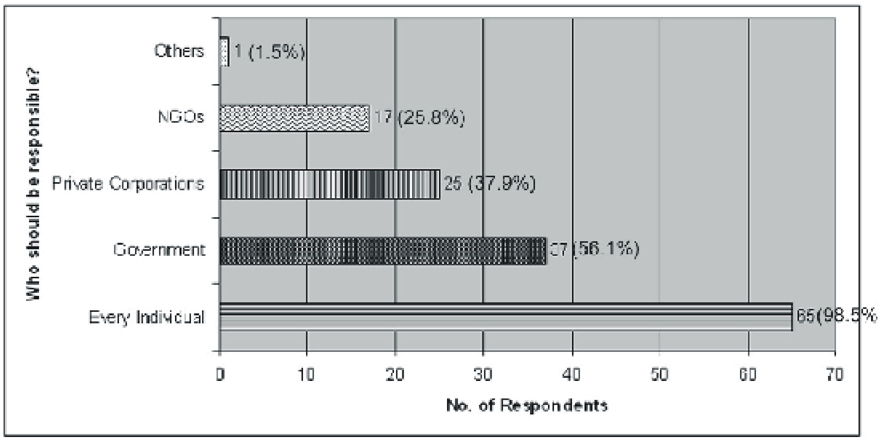

Figure 2. Agency responsible for cyber laws.

including government, NGOs, individuals should take equal responsibility in understanding and implementing the cyber laws in Singapore.

5.4.4 Medium of Communication

Overwhelmingly respondents preferred newspapers and magazines (90.9 per cent), followed by TV and Radio (60.6 per cent) as the best medium for providing cyber laws-related information to public (Fig. 3). Though Internet usage rate is very high in Singapore, authorities still preferred print media to publish the required news on cyber laws. In a study it was found that undergraduate students of computer engineering faculty at NTU still prefer traditional print media for information dissemination. Slightly over a quarter (27.2 per cent) preferred internal broadcasts at their workplace through their Intranet or portal and another (27.3 per cent) also felt that providing information through their local websites may be more appropriate. In general, the rate of reading newspapers and magazines is very high in Singapore.

5.5 Barriers and Problems Faced by the Users

5.5.1 Problems while Using the Internet

Given the recent avalanche of news on new permutation strains of viruses, security breaches with banks and the advent of spyware, it was inevitable that security breaches, lack of privacy from spying, etc. and threats of viruses were the top three problems envisaged by the respondents in the promotion of usage of the Internet.

Similarly in a recent global survey, it was found that viruses threat is considered important in the problems rank list of the Internet users. Table 5 lists the problems faced by the Singaporeans while using Internet. Nowadays spam and pornography mails are flooding everywhere and causing a lot of problems to users while using mailing system and Internet.

5.5.2 Safer Computers!

Besides better more robust software, mindset, ethics and user education were some of the reasons mentioned by the respondents to make computers safer from external threats. Apart form having good hardware and software, human participation is also important if not a critical component in overall security landscape.

These results (Table 6) are quite contrast to what Warren found in his survey of Australian companies that do not take enough security and users awareness training seriously.

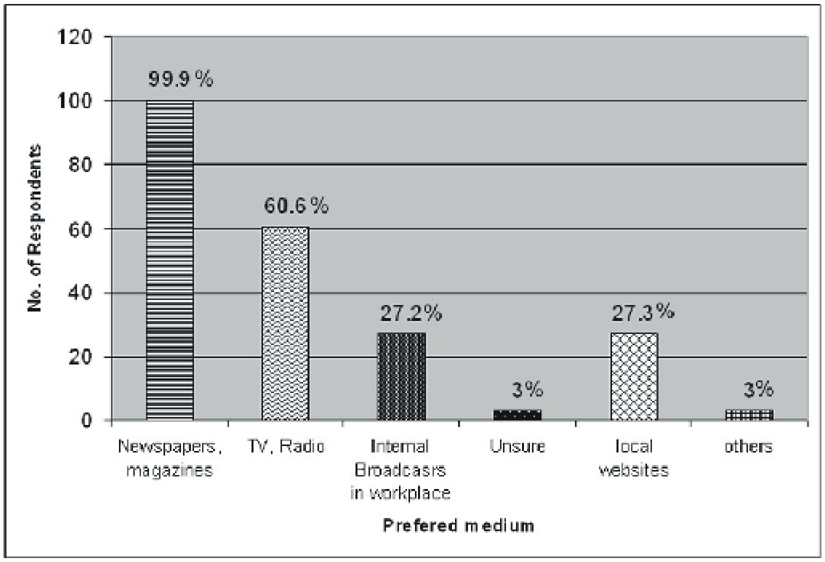

Figure 3. Preferred medium for gaining awareness about cyber laws.

Table 5. Problems encountered by Internet users of Singapore

Problems encountered	No. of respondents	% of respondents
Security breaches	29	43.9
Privacy, include spying	27	40.9
Virus threats	25	37.9
Information overload/quality	14	21.2
Access speed	13	19.7
Cyber fraud	13	19.7
Spam	11	16.7
Pornography	7	10.6
Piracy	6	9.1
Unbalanced view/Internet abuse	3	4.5
Price of Internet surfing	2	3.0
Coverage/accessibility	2	3.0
Less human interaction	2	3.0
Over commercialisation in the net	1	1.5
Inadequate policies/laws	1	1.5

5.5.3 Remedies/Suggestions

Based on the results of the study, the following general guidelines have been prepared to implement an effective security awareness framework:

(i) **Media of communication**: It includes the preferred mode by which the users are more interested to be informed about security news or developments. This is important for the success of any communication strategy introduced for advocating the importance of the security awareness campaign.

(ii) **Target group**: It is easier to convince the educated users having basic qualification(s) such as degree and above. This group can be first targeted with an objective and purpose that they can continue to share their experiences and knowledge along with their peers at the workplace.

(iii) **Laws**: Laws should be clearly communicated and explained through various avenues at the workplace, through print and electronic media or public events, road shows, etc.

(iv) **Psychological comfort**: All the individuals should be addressed so as to ensure a complete understanding, compliance, and cooperation which may be able to share and work towards achieving a common objective.

(v) **Ethics**: Should be adhered by the individuals and organisations on the Internet.

(vi) **Privacy**: Privacy issues are of interest to Singaporean and may be openly

Table 6. Users response to make safer computers

How to make safer computers?	No. of respondents	% of respondents
Better and robust software	19	28.8
User education including mindset and ethics	18	27.3
Better virus protection e.g. auto updates	12	18.2
Enforcement of existing cyber laws	9	13.6
Firewalls	7	10.6
User authentication	3	4.5
Better security policies from ISP	2	3.0
More responsibility from software vendors	1	1.5
Better cooperation/responsibility from all users	1	1.5
More open source programs	1	1.5
Anti hacking tools	1	1.5

discussed about how policies should, in the light of overall security consideration, be practiced.

(vii) **Problems**: Including privacy, security and viruses that are related to software should be taken care by the companies that are producing and due action should be taken or communicated to the users.

(viii) **Best practices**: Software or security updates should be sent regularly and their information may be communicated through the preferred medium like newspapers, workplaces and other avenues available including the government websites on the Internet.

6. CONCLUSION

Today general security is already an international problem that all countries are trying their level best to address at international level. The increasing popularity of the Internet as a medium and its borderless, interconnected nature seeks to exacerbate the security situation which cannot be assumed and taken for granted because many countries had very bad experiences related to critical security problems and some had really painful memories. Cyber laws that seek to protect the sovereignty and property are being constantly monitored, revised and updated to keep up with the changes. It is clear that the awareness of cyber laws and any of their revisions should be further explained and communicated regularly to every individual so that all of them take responsibility to maintain security of individual(s) on Internet.

All the participants in the survey are highly computer literates, owned a computer, and Internet connection either at home or office. Information gathering, communication and collaborative purposes in forum discussion are the common tasks for which computers being used by the participants. Keeping up with computer security-related news was not a common habit among the majority of the participants (56 per cent) and print media such as newspapers, journals and magazines are the most popular form of communication channels opted to publish about cyber laws and other related news by these participants. Since the level of awareness on the possible effects of computer worms, viruses and Trojan horses was comparatively high (66 per cent), hence, it is proposed that software producers should produce reliable software and timely communicate about remedial products available with them. The Computer Misuse Act and the Copyright Laws of Singapore were the most commonly heard of among the list of cyber laws provided to them. However, most of them were not aware of the recent revision to the Computer Misuse Act indicating either a possible disinterest or a case of inadequate and insufficient coverage in the media.

Ethics were considered as most necessary by the Singaporeans in the cyber or Internet because the participants were highly literate and aware of their rights and hence concerned about their privacy and suggested to protect cyber security by providing adequate cyber laws. All the people are fully aware about virus scanner updates in schools or companies environment where the automatic download function was available to protect from unexpected attacks.

The general comfort level of the existing computer related laws is satisfactory (50 per cent only) in Singapore so government need to educate the public about existing cyber laws and also introduce new laws from time to time to protect from the cyber threats. There is a general consensus that everyone has a role to play in the usage of the Internet with a view that the privacy and security factors are important. The lack of security, privacy and the ongoing threats of virus to computer systems were the three pressing problems while using the Internet. Better and more robust software, more user education and better virus protection were deemed as important in an effort to make computers safer to use.

The results of this study provided some useful insights about the cyber laws awareness among Singaporeans which will be useful to the government to take necessary corrective steps that ultimately will remove the fear/ phobia among Singaporeans about information security over Internet.

REFERENCES

1. Kearns, Laura. Inside the minds: Security matters. (Electronic version). Aspatore Books, Boston, MA, 2004.

2. Denning, Dorothy. Bombs and bandwidth: The emerging relationship between IT and security, edited by Robert Latham. The New Press, New York, 2003, pp. 25-48.

3. Andress, Amanda. Surviving Security: How to integrate people, process, and technology. CRC Press, Boca Raton, Florida, 2004.

4. Marcella, J. Albert & Greenfield, S Robert. Cyber Forensics: A field manual for collecting, examining, and preserving evidence of computer crimes. Auerbach Publications, New York, 2002.

5. Ang, Peng Hwa.Information highways-policy and regulation: The Singapore experience. Information Highways: Policy and Regulation in the Construction of Global Infrastructure in ASEAN, edited by Anura Goonesekera and Ang Peng Hwa. Asian Media Information and Communication Centre, Singapore, 1999, pp. 317-29.

6. Spinello, A. Richard. Cyber ethics: Morality and law in cyberspace (2nd Ed). Jones and Bartlett Publishers. Sudbury, MA, 2003.

7. Hinde, Stephen. The law, cyber crime, risk assessment and cyber protection. *Computer and Security*, 2003, **22**(2), 90-95.

8. Forrester consulting survey for the Business Software Alliance on information security in companies (Available at bsa.org/usa/policy/upload/2006-Security-Survey.pdf)

9. Warren, M.J. Security practice: Survey evidence from three countries. *Logistics Information Management*, 2002, **15**(5), 347-51.

10. Majid, Shaheen & Tan, A.T. Usage of information resources by computer engineering students: A case study of Nanyang technological university, Singapore. *Online Information Review*, 2002, **26**(5), 318-25.

11. Rescorla, Eric. Vulnerabilities: Is disclosure the best policy? *Network magazine*, 2004, **19**(5), 98.

12. Phukan, S. & Dhillion, G. Ethics and information technology use: A survey of US based SMEs. *Information Management & Computer Security*, 2000, **8**(5), 239-43.

13. Fiallo, E.H. The lack of ethics in cyber space: A case for cyber ethics. *In* 11th International Conference on Computer Communications and Networks, 14-16 October 2002. Miami, FL, USA.

14. Singh, Tanuja & Hill, M.E. Consumer privacy and the Internet in Europe: A view from Germany. *Journal of Consumer Marketing*, 2003, **20**(7), 634-51.

15. Carblanc, Anne. OECD guidelines for the security of information systems and networks: Towards a culture of society (Available at http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase).

16. Richardson, Robert. The future of Microsoft security. *Computer Security Journal*, 2002, **18**(3-4), 53-60.

Contributors

Mr Kar Peng is currently the Data Security Officer in ACE Insurance for Asia Pacific. He started his IT career as an Oracle analyst programmer and subsequently spent six years as Microsoft Certified Partner. He is cross-trained in the various areas of IT which include professional certifications from Microsoft, Cisco, Disaster Recovery Institute International, Project Management Leadership Group, Institute of Systems Science, Office of the Government Commerce, International Information Systems Security Certification Consortium and finally from the Information Systems Audit and Control Association and Foundation. His formal education includes Master of Science in Information Studies from the Nanyang Technological University and Bachelor of Science from National University of Singapore. Kar Peng can be reached at kar_peng_tan@yahoo.com.sg.

Dr Chennupati K. Ramaiah is working as Professor and Head at Central Library, Muffakham Jah College of Engineering & Technology (MJCET), Hyderabad. Before joining MJCET, Dr Ramaiah worked as Assistant Professor at Nanyang Technological University, Singapore for six years. He had also been Deputy Director at Defence Scientific Information & Documentation Centre (DESIDOC). He was a Commonwealth Scholar for PhD in Information Science in 1989. His formal education includes Master's degrees in Chemistry and in Library and Information Science, and PhD in Information Science from the UK. He is member of many international professional bodies/societies such as the Institute of Information Scientists, LA, ASIST, and ACM. His research interests include multimedia and hypertext technologies, human-computer interaction, user interfaces, e-books and E-publishing, archival informatics, and bibliometrics.