A survey on cybersecurity awareness concerns, practices and conceptual measures

S S Tirumala
Auckland University of Technology,
Auckland, New Zealand

Maheswara Rao Valluri
Fiji National University,
Suva,Fiji

GA Babu
Sri Venkateswara University,
Tirupati, India

Abstract—Cybersecurity, a word that attained considerable attention and is regarded as most widely used term across all the domains that use internet. Recent technological advances have mandated the necessity of exploring various aspects of cybersecurity. Rapid cyberisation with the introduction of smart devices has enforced both government and private organizations to create an awareness on cyber threats and cybersecurity. Developed countries like New Zealand has been a frontrunner in introducing new technology and in some cases has legally mandated to implement cybersecurity procedures in various sectors including educational institutions. Though, the necessity of such implementations are never questioned, however, there has been a continues debate on implementation framework particularly for school, bursary and undergraduate syllabus.

This paper is divided into three parts. Firstly, the importance of cybersecurity awareness is established by presenting various statistics, followed by the current implementations for cybersecurity awareness in terms of courses, seminars etc. The results of a comprehensive survey among various age groups is presented which gives a generic opinion on different implementations. Finally, we propose a framework that leads to the process of implementing cybersecurity awareness.

The survey provides a comprehensive understand of cyber security awareness. This work will contributes on understanding the cyber security awareness state of internet users, what are important aspects and statistics to be collected as well as on the important concepts of internet security that are to be considered while designing a survey. Further, the conclusions obtained from the survey result will guide the new works on cyber security awareness programmes.

Keywords: cybersecurity, cybersecurity awareness, cybersecurity in education, NZ cybersecurity

Internet, a term that needs no introduction has been a key aspect of daily life and its usage has seen a rapid growth of over 900% due to its implementations and usage on various types of devices. Majority of this growth of internet or what we called cyberisation has taken place in last decade due to smart devices like smart-phones, tablet etc. This cyber revolution has created a very high impact on various aspects of society as well individuals through social media, online videos and gaming. The introduction of Bring Your Own Device or simply BYOD in the education sector had highest impact of cyberisation among developed countries like New Zealand [1]. New Zealand is listed among the top countries in terms of internet reach and usage and has been top among Oceania countries [2]. The frequency of internet usage in new zealand is quite intense with over 80% of people using internet more than one time as shown in Fig. 1.

Traditionally, New Zealand has been first to introduce new

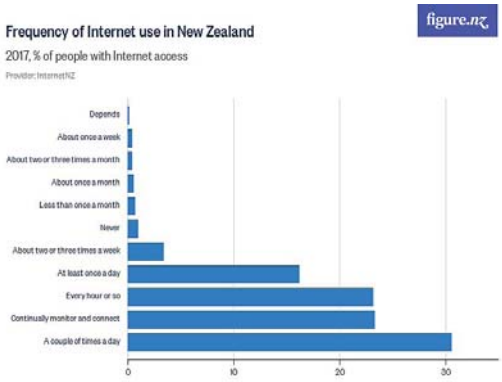


Fig. 1: Frequency of internet usage in New Zealand (source:

internet.nz)

E-learning based pedagogical methods in schools and other educational institutions [3]. This has raised concerns over security and privacy of information as well as exploitation of user information like personal data, financial etc [4] . Further, it is necessary to have an organization or group to look over the security concerns and help the government and private organizations in policy making [5]. InternetNZ is one such organization in new zealand which involves in identifying security challenges and working out the policies and procedures through research, projects, awareness programs and legislation. This research utilized the

978-1-5386-8260-9/19/$31.00 ©2019 IEEE

statistics provided by InternetNZ for preparing survey questions and understanding the responses.

Cybersecurity is a generic term that is attributed to internet security, information security and computer security. However, it is important to understand the scope, application and its proper usage. As misunderstood by many people, cybersecurity is not confined to securing computers on internet [6]. Cybersecurity can be defined as securing hardware, software, data and information that exists in an online system (internet) from any form of breach. Now a days, the scope of the cybersecurity is extended securing electronic devices and equipments (including household) for unauthorized usage, misleading projection and diversions. For implementing cybersecurity, Data protection and information security highest priority for organization whereas privacy and access control for individuals [7] [8]. At present, the capacity of cybersecurity is extended towards protecting individuals from cyber bulling and identifying cyber warfare using advanced machine learning techniques [9] [10].

This paper provides various aspects of cybersecurity concerns concerns existing among various categories of people. This is followed by a comprehensive survey results based on the existing cybersecurity concerns. From the results, it can be concluded that ..... Though the survey results are limited to New Zealand, this paper presents a direction for such implementations in various countries.

This paper is presented as follows. Section I provides a brief introduction and background on internet usage and cybersecurity. Section II presents the statistical data regarding various aspects of cybersecurity that influenced the design of the research. This is followed by the details of research approach and data collection in section III. The results of the survey and a brief discussion is presented as section IV followed by conclusion and future work as section V.

I. CONCERNS ABOUT VARIOUS CYBERSECURITY ASPECTS A. Type of Connectivity

Kiwi are active users of internet and they relies on internet for majority of day to day activities. This is reflected in the Fig. 2 (a) which clearly shows that there are only a handful of people (less than 10% of population) are not internet active. Among the population of internet users, over 80% connects to the internet through home broadband connection (wired wireless) as shown in Fig. 2 (b). This is followed by a considerable amount of 15% using work connections and rest of the minority users connect to the internet through data plans.

However, when the internet usage is presented based on education qualification as shown in Fig. 2 (b), amount of internet usage only at home is higher for school children. Further, students tends to use less home internet as they get qualified at university level. It is to be noted that, users have more privacy and less restrictions at home when compared to school and work environments. So, it is necessary to implement strict cybersecurity policies and access restrictions. Based on this, two questions were designed for the survey as follows:

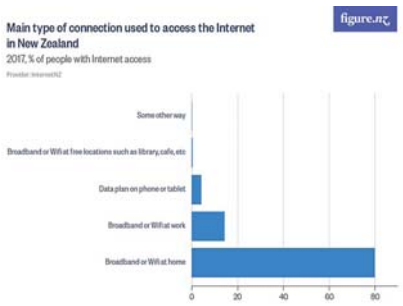
Restriction: Are you implementing any restrictions like content filtering, website blocking etc at home ? if so, is it for everyone or user based ?

Monitoring: Do you have any monitoring software that alert you for illegitimate activities ?

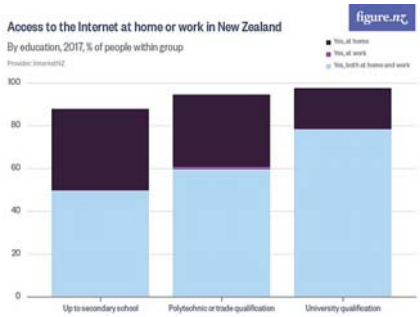
B. Threats and measures

Cyber threats are often associated with big organization and financial institutions which is definitely a misinterpretation of existing environment. Individuals with preliminary hacking skills may not be able to invest time and effort in hacking through secured databases of large organizations. At present, social engineering is one of the widely used approaches for stealing individual information and private data. To investigate further, it is necessary to understand the major concerns of various sections of population so that an appropriate level of association can be created between concerns and awareness framework.

According to the survey conducted on security concerns over cyber threats 93% of population is concerned over the security as shown in Fig. 3 (a). Further, about 34%of people



Location



Based on Education

Fig. 2: Internet usage in New Zealand (source: internet.nz)

are very concerned about security breaches whereas 30% being concerned and 20% being very little concerned. In case of concerns over privacy as shown in Fig. 3 (b), about 40% of people are very concerned about their personal data and privacy whereas 28% and 22% people are concerned or somewhat concerned respectively.

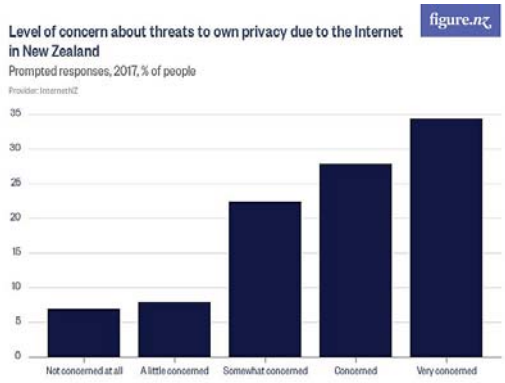
It is worrisome to see that about 10% are little or not at all concerned about security (3 (a)) and whereas this about 13% (3 (b)) for privacy and personal data. Moreover, different types of security measures taken by various individuals as shown in . Fig. (4 (b)) causes a serious concern since individual using powerful authentication methods like two-factor authentication and backup are under 50%. With current level of cyber threats using only a password or pin may invite serious security breaches which must be addressed.

Based on above information, the following questions are framed based :

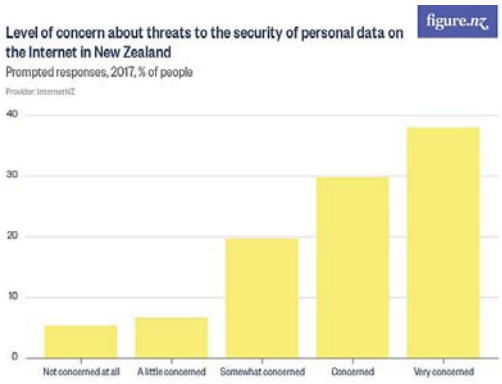
Familiarity: Are you familiar with two-factor authentication ?

Common Password: Do you have a password that you use for more than one device / system ?

Password Strength: Do your password contains number, alphabet in more than once case and a special character ?



Privacy



Personal

Fig. 3: Level of Concern over privacy and personal data in New Zealand (source: internet.nz)

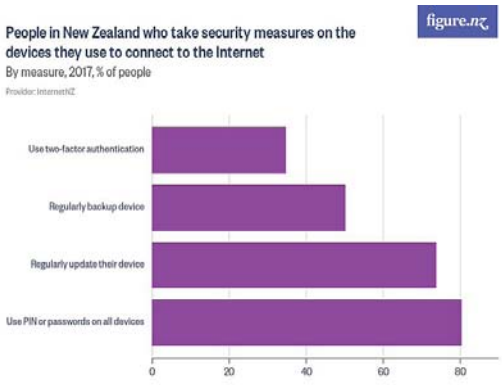


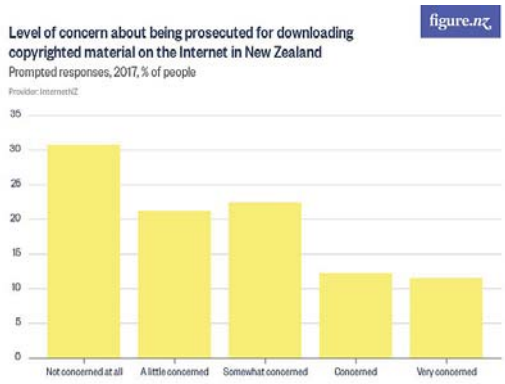
Fig. 4: Security measures on various devices (source: internet.nz)

Change of Password: Do you change your password over a period of time before being alerted ?

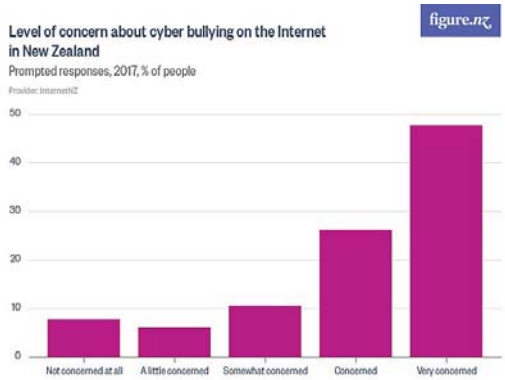
C. Security concerns

It is always important to consider the mood and motive of the people before design a process or procedure for them. This understand of their intentions and personality will help in smooth implementation with least possible resistance. By understanding the instinct, the diplomacy levels required for the implementation of proposed approach can be correctly identified. Majority of the internet users or in fact any users tends to follow the procedures based on requirements. For instance, when someone is asked to create a password, majority of the people tends to follows minimum requirements that are mandated by the software, website or social media platform rather than thinking about how secure their password is [11]. Sometimes the law of the land also governs these principles and procedures which are to be followed. An interesting statistics about copyright infringement is presented in Fig. 5 (a) which shows how users are feeling responsible about a

particular law. When asked about the their opinion on concern of being prosecuted for downloading copyright content which is illegal, highest number of people (about 31%) said they are not at all concerned about these acts. Further, it is interesting to see that only 23% of people are concerned or seriously concerned about downloading illegitimately. This possess a question on respecting law of the land or as well as its implementation in the country.



Downloading copyright material



Cyber bullying

Fig. 5: Level of Concern over privacy and personal data in New Zealand (source: internet.nz)

Contrastingly, Fig. 5 (b) shows that about 48% of internet users are very concerned about cyber bulling which can be addressed only by law. Moreover, percentage of users who are concerned and very concerned when put together reaches over 75% whereas 8% of people are not at all concerned about cyber bullying.

The following questions are framed based :

Awareness: Are you aware that some of your data will be collected by websites and apps irrespective of your consent ?

Protection: Are you aware of security features in browsers ?

Parental lock Do you use parental lock on your devices?

Safe Search: Do you use any software for blocking illegitimate sites ?

II. SURVEY RESULTS AND DISCUSSION

A. Data Collection

The survey was conducted without any targeted number which ended up with 4795 valid participants after filtering invalid and incomplete responses. The participants were divided in four categories based on their age. The framing of the question is changed by adding some description and explanation for participants of some categories to make them understand easily.

Category I: 13-21 years

Category II: 22-35 years

Category III: 36-51 years

Category IV: 52-above years

The survey is conducted without storing any personal information maintaining complete anonymity. The survey is conducted through online and offline sources through personal invitation with complete user consent. No personal details were asked in any format other than asking to identify the age group and gender. The validity of the responses were calculated and the results were cumulatively added without storing any individual records. Gender and age wise statistics of the participants is presented in table I.

ge	ale	emale	A	otal	atio
	82	4	3	89	.03
I	25	66	3	284	6.78
II	64	15	56	835	8.27
V	44	21	22	387	8.93

TABLE I: Statistics of age and gender-wise participation

B. Results and Discussion

There were two questions on connectivity constraints which covers restrictions and monitoring and the results are

presented in Fig. 6. The results reflect the feeling about regulations that are implemented. Only 38% of total participants are implementing at least one type of restriction with majority being through automatic software like firewalls or through browser default setting. Further the use of monitoring software or tools is diminishing at its low with only 15% of total participants implementing the same. The mind set of majority

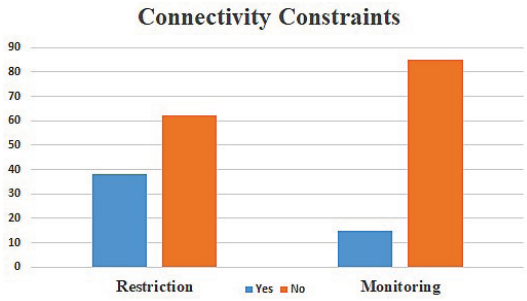


Fig. 6: Responces on Connectivity

of the users tends to underestimate the importance of preventing unauthorized usage. Moreover, implementing restriction and monitoring practices are considered as highly technical jobs according comments provided by the participants. So, it is necessary to provide sufficient technical tutorials towards implantation of monitoring software as part of awareness framework.

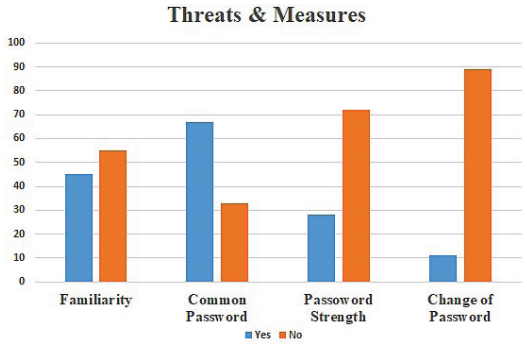


Fig. 7: Security measures on various devices

For the second category of questions based on password management and familiarity, the survey results reasserts the need of profound and stringent password enforcement as shown in Fig. 8. Firstly, it is surprising to see that about 45% of participants are familiar with two-factor authentication. However considering the statistics about people using twofactor authentications (Section II), it is noteworthy to observe that major portion of new zealand internet users are not using two-way authentication. Coming to the second part of password management, it is definitely alarming to see that 68% are using common passwords across various authorizations and only about 30% of users are having strong passwords with at least a number, an alphabet and a special character. Further, it is startle to observe that about 90% of users are not changing their password unless they are asked to do so.

The third and most crucial part of the survey is assessing the awareness on security concerns and user responsibilities. From the results shown in Fig. 8 , it is evident that more awareness needs to be created for better understanding of various security aspects and their implementation. Majority of the internet users are familiar with parental locking due to the restriction enforced on the devices used by school children. The awareness about data collection and inbuilt security features is very low probably due to difficulty in

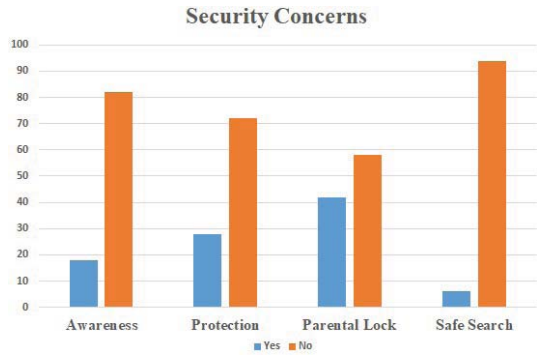


Fig. 8: Security Concerns

use or less advertisements. According to the comments of the majority of participants, anti-virus with firewall is the only requirement for protecting data, privacy and security. Further, cookies and macros are considered as least affecting whereas in reality they were most affected and cause of high concern for data theft and privacy breaches. Safe Search is the one of most powerful and important feature of widely used Google search engine. However, only less than 9% of internet users are familiar and using it when and where required. These results on the security concerns raises a strong early warning on how internet users are been kept in dark wilfully or unknowingly which is immediate point of concern.

III. CONCLUSION AND FUTURE WORK

This papers presents various statistics to assess the mindset of internet users for preparing a cyber security awareness framework. A survey questionnaire was prepared based on various statistics obtained from internet users through reputed organization called InternetNZ. A survey was conducted with about 4800 participants and the following conclusions were made based on the survey results.

It is necessary to provide practical sessions on various cyber restriction and monitoring tools.

A guide on how to install cyber restriction monitoring tools particularly about parental locking, website blocking etc. must be provided.

Two-factor authentication must be made mandatory

A clear guidelines on password management has to be provided to internet users as a part of training procedures

Internet users must be provided with clear guidelines on creating strong password as well as enforcing

stringent rules

Instruction and practical awareness must be provided

on various browser based security and built-in protection option

Awareness must be provided on internet cookies, temporary data, private mode and other security aspects of browser

Practices are on different search engine restriction and enforcements must be explained in detail.

The survey provided a comprehensive understand of status of internet users which could not be completely furnished in this paper due to size and scope limitations. However, this work will contribute on how to understand the cyber security state of internet users, what are important aspects and statistics to be collected as well as on the important concepts of internet security that are to be considered while designing a survey. Further, the conclusions obtained from the survey result will guide the new works on cyber security awareness programmes.

REFERENCES

[1] I. Pogarcic, M. Gligora Markovic, and V. Davidovic, "Byod: a challenge for the future digital generation," in Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on, pp. 748–752, IEEE, 2013.

[2] W. Internet, "World internet users and 2016 population stats," 1999.

[3] D. Nandigam, S. S. Tirumala, and N. Baghaei, "Personalized learning: Current status and potential," in e-Learning, e-Management and eServices (IC3e), 2014 IEEE Conference on, pp. 111–116, IEEE, 2014.

[4] I. Arpaci, "A theoretical framework for it consumerization: Factors influencing the adoption of byod," in Handbook of Research on Technology Integration in the Global World, pp. 114–129, IGI Global, 2019.

[5] J. N. Pelton and I. B. Singh, "Challenges and opportunities in the evolution of the internet of everything," in Smart Cities of Today and Tomorrow, pp. 159–169, Springer, 2019.

[6] P. W. Singer and A. Friedman, Cybersecurity: What everyone needs to know. Oxford University Press, 2014.

[7] S. S. Tirumala, H. Sathu, and V. Naidu, "Analysis and prevention of account hijacking based incidents in cloud environment," in Information Technology (ICIT), 2015 International Conference on, pp. 124–129, IEEE, 2015.

[8] E. Toch, C. Bettini, E. Shmueli, L. Radaelli, A. Lanzi, D. Riboni, and B. Lepri, "The privacy implications of cyber security systems: A technological survey," ACM Computing Surveys (CSUR), vol. 51, no. 2, p. 36, 2018.

[9] S. S. Tirumala and A. Narayanan, "Transpositional neurocryptography using deep learning," in Proceedings of the 2017 International Conference on Information Technology, pp. 330–334, ACM, 2017.

[10] S. Blanke, P. C. Nielsen, and B. Wrozek, "How can a cybersecurity student become a cybersecurity professional and succeed in a cybersecurity career?," in Global Cyber Security Labor Shortage and International Business Risk, pp. 111–128, IGI Global, 2019.

[11] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, "A survey on internet usage and cybersecurity awareness in students," in Privacy, Security and Trust (PST), 2016 14th Annual Conference on, pp. 223–228, IEEE, 2016.