Study of Cyber Security Status in Nepal

Arun Khanal
Graduate
Kathmandu University
Dhulikhel, Nepal
arunkhanalofficial@gmail.com

Subash Shrestha
Graduate
Kathmandu University
Dhulikhel, Nepal
subashshrestha4h4@gmail.com

Rishikesh Bajgain
Graduate
Kathmandu University
Dhulikhel, Nepal
rishikesh07656@gmail.com

Anup Thapa
Assistant Professor
Kathmandu University
Dhulikhel, Nepal
anup.thapa@ku.edu.np

Abstract: Due to the rapid demand for digitalized processes and tasks, to cover basic needs of daily activities like information gaining, transactions, entertainment, etc., the demand for online medium access is increasing at a higher rate. Nevertheless, the primary problem that always associates with any online platform is security. This paper aims to present the study on various online access security aspects considering current scenario of online access security status in Nepal. The study mainly takes into account the security concern associated with security management systems of internet service providers, enterprises and individuals (end users). A survey-based study report is presented to reflect the security awareness among students from different schools, employees from different enterprises like financial institutions, security providers, internet service providers, and web admins. Some of the open issues and their solutions regarding cyber security status in Nepal is also discussed.

Keywords: Cyber Security, Enterprise Security, Cyber Awareness, Cyber Law, Cyber Courses

I. INTRODUCTION

Nepal is heading towards digitization in every possible fields. Nepal's internet penetration rate is 38.4 per cent of the total population at the start of 2022 [1]. NPR 7.13 billion budget was allocated for the Information, Communication and Technology (ICT) sector in the fiscal year 2077/78 with priority to develop ICT sector [2]. However, with digitization, the threat and frequency of cyber-attacks are also increasing. 3,906 cases of cybercrime were registered in the fiscal year 2020/21 according to the Cyber Bureau of Nepal. Reportedly, 2,003 out of them were women. Children under the age of 18 years have also become the victims of cybercrime. According to a preliminary investigation, 3,451 people were found to be involved in cybercrime through social media like Facebook and others in the fiscal year 2020/21 [3]. According to Global Cybersecurity Index (GCI), Nepal ranks at 94th in the GCI. Automatic Teller Machine (ATM) attacks, ransomware, phishing attacks, harassment using social media, privacy leaks, pornography, and broadcasting false information are other major and common cyber-attacks in Nepal. Online swindling, cyberbullying, impersonation or identity theft, data theft, banking frauds, hacking, violence against women and children's, Denial-of-Service (DoS) attack are some of the methods that criminals use to commit cybercrimes.

The available alarming cyber-attacks statists indicate the increasing threat of cybercrime in Nepal. This paper aims to figure out current scenario of cyber security status in Nepal. A survey-based study is developed in this report to reflect the security awareness among students from different schools, employees from different enterprises like financial institutions, security providers, internet service providers, and web admins. Some of the open issues and their solutions regarding cyber security status in Nepal have also been discussed in this paper.

A. Methods and Tools

The project examines the state of cybersecurity in Nepal through a combination of internet research, field visits, interviews with industry professionals, and surveys of university students from both technical and non-technical backgrounds. The research process includes an initial study, data collection through surveys and interviews, data analysis, discussion, drawing conclusion and finally present recommendations. The method is divided basically into a survey of security status of three major representative stakeholders: individuals, enterprises, and ISPs.

II. DATA ANALYSIS AND RESULTS

For the individual-level survey, a quantitative approach is used. With a paper-based questionnaire focused on cybersecurity awareness, various college students are approached. Age groups of around 18 years of age are focused with an assumption that this age group students are one of the most active groups on social sites and are also vulnerable to cyber-attacks. To collect generalized data, we approached students from both ICT and non-ICT backgrounds. We surveyed undergraduate students from Kathmandu University, Bhaktapur Multiple Campus, Reliance College and Sarbamangala Multiple Campus, respectively. 124 samples of data representing different colleges in total are selected for final analysis.

For enterprises, a survey with some cyber security related companies is carried out such as branch manager of agricultural development bank and technical in charge of Kathmandu University's Information System Management System (KU-ISMS). Similarly, technical head of Ultranet Communication Pvt. Ltd. (an ISP representative) and Eminence Ways Pvt. Ltd. (a private company that provides security services) are also approached. In addition, the laws provisioned and implemented on cyber security which are also included on the curriculum have also been analyzed.

A. Findings of Survey on Individual Level

To test and find out the cyber security awareness among college students, as mentioned above, different questions are asked through printed questionnaires. 15 different questions like do you consider yourself knowledgeable about the concept of cybersecurity, do

you know what Two-Factor Authentication (e.g. in mail, Facebook, etc.) is, and do you use it, when you receive a message containing certain link from unfamiliar source, do you open it, do you know the difference between using HTTP and HTTPS, and so on that basically designed to collect the reflection from awareness to technical knowledge were asked. Based on the received answers, responses are categorized into different subheadings that show the cybersecurity awareness level in an individual, especially on the college students.

On a question which was asked as "Do you consider yourself knowledgeable about the concept of cybersecurity?"; out of 124 responses, 50.8% percentage answered "Yes", while 21% answered "no" and the remaining who were not sure answered with "Maybe".

On a cross question on HTTP and Phishing attacks, although 50.8% replied that they knew about related cybersecurity issues, not more than 40% knew about cybersecurity well enough at an individual level.

Similarly, on questions related to good password practice, good number of responses is found with 77.4% using strong passwords and 41.1% using separate passwords for different social media accounts.

On questions related to good security practices such as using 2FA, opening unfamiliar links, HTTPS, and awareness of unsafe public Wi-Fi; 70% of respondents were found to be aware of these topics.

On security aspects related questions, we found 73.4% rejecting unwanted app permission whereas just 35% were aware of setting up the router, MAC filters and WPS disabling.

Similarly, a question was asked to find out if the respondent had been a victim of cyber-attacks such as malware, social site (Facebook, Instagram, etc.) account hacked, data loss, etc., and we found that roughly 54 students out of 124 students have been the victim of cyber-attack.

On the next survey (a survey among students of ICT background students, with the same questions), ironically, no drastic improvement in awareness level is observed despite some marginal improvement.

From the observed data it has been recommended to the respondents and others that for security on an individual level, safe security practices must be followed such as looking for SSL certification while entering sensitive data which can mitigate man-in-the-middle, phishing attacks and cookie hijacking attacks. One should keep the software updated; one must follow the strong password practice (use different passwords for different sites) rather than keeping a common password. Similarly, an individual should enable 2FA, be aware of mal advertising, key loggers, crypto-jacking, DDoS attack, spyware, ransomware, Trojans, etc., and follow strong network practices like disabling WPA, and MAC filters, etc., while setting up wireless LAN.

B. Findings of Survey on Enterprise and ISP level

For knowing the current status of Nepal in the cyber-security field we conducted a questionnaire session with Eminence Ways Pvt. Ltd., a private company that provides security services for different sectors like financial, government, healthcare, ISPs, and education. From the interview with technical heads, we found that some of the enterprises are using their own server with installed security-based programs and operating systems while some are not using their own server-based software. However, interestingly it is observed that most of the enterprises are well aware of cyber security threats and are also following common major preventive majors against possible attacks. From the interview, findings, and field visits, some recommendations have been advised for the enterprises as shown in Table 1.

TABLE I: SUMMARY OF RECOMMENDATIONS FOR ENTERPRISES

Elements	**Without server**				**With server**			
	School	College	Government office	Bank (Branch)	University	Bank (Head office)	Hospital	Government office
Firewall	×	√	√	√	√	√	√	√
VPN	√	√	√	√	√	√	√	√
IDS	×	×	×	×	√	√	√	√
IPS	×	×	×	×	√	√	√	√
DMZ	×	×	×	×	√	√	√	√
UTM	×	×	×	×	√	√	√	√
STP	√	√	√	√	√	√	√	√
Switch port security	√	√	√	√	√	√	√	√
Audit	√	√	√	√	√	√	√	√
MAC filter	√	√	√	√	√	√	√	√
NAC	√	√	√	√	√	√	√	√
Application control	√	√	√	√	√	√	√	√
Antivirus	√	√	√	√	√	√	√	√

The presented table provides recommendations for different types of organizations based on whether or not they have their own server. For institutions such as schools, colleges, government offices, and bank branches that do not have their own server, the main focus can be on maintaining the Virtual Private Network (VPN), Spanning Tree Protocol (STP), and switch port security only. Additional security measures such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Demilitarized Zones (DMZ), and Unified Threat Management (UTM) are considered optional in this case. On the other hand, if the organization utilizes a server, it is recommended to implement all the security parameters including IDS, IPS, DMZ, STP, VPN, and UTM. Regardless of the presence of a server or not, it is highly recommended to perform audits, apply MAC filtering, utilize Network Access Control (NAC), implement application control, and utilize antivirus software.

Similarly, it becomes the matter of open discussion that those organizations should conduct regular security audits to evaluate and identify flaws in their security systems. This should be followed by strict checking and warning from concerned authorities. Concerns including checking security patches, conducting a self-test on existing software to identify vulnerabilities, double-checking access to sensitive data, and implementing the best encryption for it should be considered during the security audit. A scan should also be conducted to identify every network access point, verify wireless

network security, record any previous attacks and how they were mitigated, identify trained employees to detect security threats and ensure all cyber security policies and procedures shall be followed.

Similarly, regular system scanning of the entire network should be performed by the respective technical person. Vulnerability Assessment and Penetration Testing (VAPT) should be carried out to help identify and address cyber security vulnerabilities. Companies can practice awarding individuals who find system issues. Digital forensics is also crucial for law enforcement investigations as it involves identifying, acquiring, processing, analyzing, and reporting electronically stored data, which is involved in almost all criminal activities. Regular malware analysis should be performed by technical personnel specialized in the particular field. Reverse engineering, which can extract the design and origin information of any malicious software or application can be performed if required.

From the survey and site visit of various ISPs in Nepal, we found that ISPs do not employ security management in detail, like those used by banks or other enterprises, but the basic task of access control and proper network management is done through switches and certain firewalls at the time of system configuration. Thus, it is advisable that ISPs should also be working on security aspects such as DDoS attacks and Malware outbreaks. Since ISPs hold a detailed database of user's information, improper security setup within an ISP might lead to a data breach for example Vianet, one of the ISPs, on April 9, 2020, faced a data breach where data belonging to more than 160,000 of its subscribes was leaked [4].

C. Findings of Survey on Cyber Law

While going through the cyber laws and their related areas such as The Electronic Transactions Act, of 2008, The Children's Act of 1992, The Copyright Act, 2002, The Individual Privacy Act, of 2018, and The standard cyber-security by-law as implemented by Nepal Telecommunications Authority (NTA), we found laws has envisioned and incorporated some of the cyber-security related issues but are not at a satisfactory level yet.[5], [6] Also, laws for cyberbullying, cyber terrorism, e-commerce, and digital content protection should be drafted and enforced.

To figure out if cybersecurity-related courses are available or being offered in our curriculum or not; we went through various courses offered in Nepal. In our observation, we found cyber security is not taught in detail in any courses dedicated one. The basic attacks and precautions at the individual level are included in secondary and high school level curricula but this only includes the study of some viruses, attacks, and so on. At the undergraduate level, the specialized course is found to be missing.

III. CONCLUSION

From the study and the observed data, it can be envisioned that the cyber security status of Nepal is in the fair stage. On an individual level, we could see that the educated and active users seem not well aware of cyber security. Enterprises are well aware of the consequences however they are using the common methods and resources against the possible attacks in lack of proper monitoring and enforcement from the authorities.

REFERENCES

[1] 'DIGITAL 2022: NEPAL, 15 FEBRUARY 2022', Accessed on: 23rd March 2023.[Online]. Available: https://datareportal.com/reports/digital-2022-nepal

[2] 'ICT, Telecom Sector In Budget 2078/79: Major Plans/Policies', Accessed on: 23rd March 2023.[Online]. Available: https://www.nepalitelecom.com/2021/05/ict-telecom-sector-in-budget-fy-2078-79.html

[3] '3,906 cases of cybercrime registered in the fiscal year 2020/21', Accessed on: 23rd March 2023.[Online]. Available: https://theannapurnaexpress.com/news/3-906-cases-of-cybercrime-registered-in-fiscal-year-2020-21-4056

[4] 'Hackers leak personal info of Vianet users', Accessed on: 23rd March 2023.[Online]. Available: https://myrepublica.nagariknetwork.com/news/hackers-leak-personal-info-of-vianet-users/

[5] 'Cyber crime and laws in Nepal: An overview' Accessed on: 23rd March 2023.[Online]. Available: https://cyberblogindia.in/cyber-crime-and-laws-in-nepal-an-overview/

[6] 'Cyber Security Byelaw, 2077 (2020)' Accessed on: 23rd March 2023.[Online]. Available: https://nta.gov.np/wp-content/uploads/2020/08/Cyber-Security-Bylaw-2077-2020.pdf