A Literature Review on Threats and Countermeasures of Cybersecurity: A cross-industry analysis in Kathmandu

Neelima Shahi (NP000461)
Lord Buddha Education Foundation
Asia Pacific University of Innovation and Technology
Masters in Information Technology Management
neelima.shahi@study.lbef.edu.np

Abstract— As technology progresses and the world moves towards the new era of information technology and internet, the importance of cybersecurity in corporate and individual spaces grows exponentially. The term "cybersecurity", in a broad sense, refers to the protection of networks and individual machines from potential malwares, attackers, and hackers, while also enhancing the security of any devices and constantly studying the historical attacks to understand and mitigate potential future threats. In the current situation, as the number of corporate organizations grow in Kathmandu-Nepal, the likeliness of organizations getting targeted by attackers increases. In this case, the corporates must always be ready for potential attacks like malwares, phishing, insider threats, and so on. This paper primarily reviews different journals and publications developed in the cybersecurity domain to understand cyber threats and cybersecurity trends. Then, it attempts to map those understandings in the context of Kathmandu to derive a generic theory for strengthening their cybersecurity capabilities and tackling the present cyber threats.

Keywords— cybersecurity, security threats, human psychology, privacy concerns, information security, e-governance

I. Introduction

Globally, businesses have seen a big jump in Information Technology (IT) usage in their processes in the last couple of years. The progression of humanity is directly attributed to the advancement in technology. In the last couple of decades, we have leapt through the advancement in information technology – particularly, internet. As countries continue to fight COVID-19, it has changed our social environment and existing social structures. (Hakak, Khan, Imran, Choo, & Shoaib, 2020). COVID has forced people to leave with restraints like staying at home and socially distancing themselves. A large percentage of the population moved to such a social system has resulted in a massive surge of internet usage. People rely on online methods for their day-to-day needs like banking, bills, entertainment, business, government services, etc. (Ma & McKinnon, 2021).

As COVID-19 hit the world and half of the global workforce started working from home and through the internet, the cyber-attacks also increased (Hakak, Khan, Imran, Choo, & Shoaib, 2020). The attacks have grown substantially compared to the past few years. The attacks have been targeted towards everyone, from big corporations and governments to individuals, resulting in financial loss, data breaches, disruption of significant services, etc. (Ma & McKinnon, 2021).

The internet usage statistics from April 2020 show that the world has seen a global digital growth of 7.1% compared to April 2019 - 301 million people started using the internet. In addition, mobile phone usage increased by 2.5% compared to April 2019, and the number of active social media users increased by 8.7% (Kemp, 2020). Comparing this growth to the data from April 2021, internet users increased by a whopping 60.1%, active social media users grew by 55.1%, and the global number of internet users reached 4.72 billion (Kemp, 2021).

Every year, corporations – big or small, collectively lose billions of dollars to cyber-attacks. In the last year alone, examining the reported losses, 95% of BEC (Business Email Compromise) reported the loss between $250 and $985,000 with $30,000 being the median, and CDB (Computer Data Breach) ranging from $148 to $1.6 million. (Verizon, 2021). This shows that, no matter the size of businesses, they are gravely affected by the uprising in cyber-attacks. Here are some findings from (Verizon, 2021):

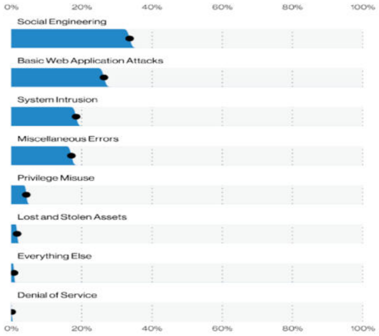

Figure 1: Patterns of security breaches (Verizon, 2021)

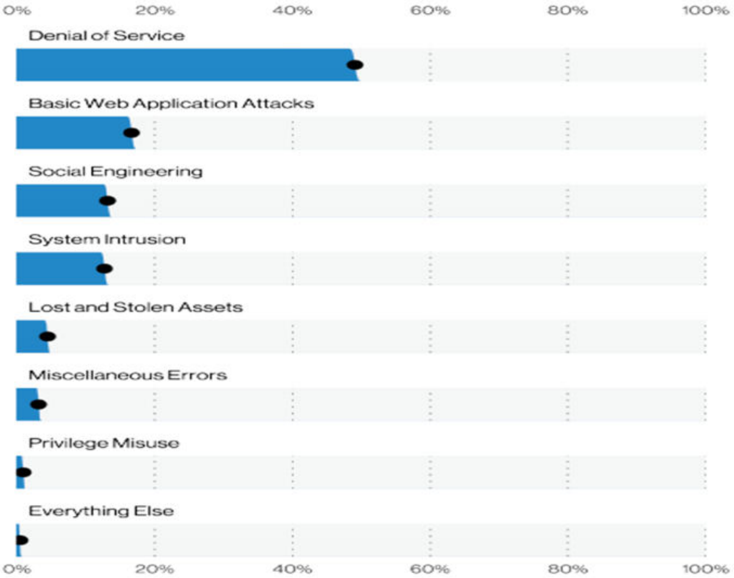

Figure 2: Patterns in incidents (Verizon, 2021)

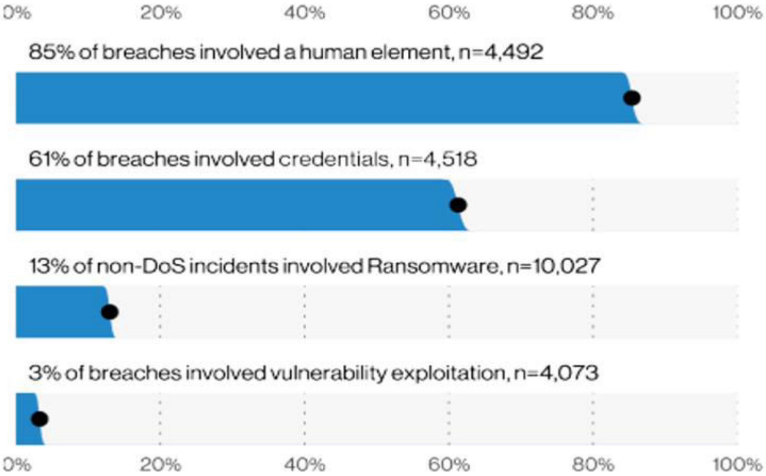

Figure 3: Action Varieties(Verizon, 2021)

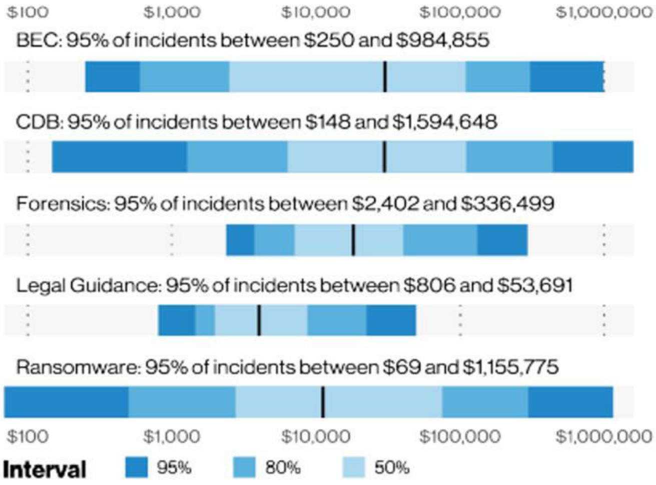

Figure 4: Impacts of Incidents(Verizon, 2021)

As we can see from Figure 1, the most common form of attack being used is social engineering, followed by basic web application attacks, system intrusion, and so on.

The Global Cybersecurity Index (GCI) is an initiative of the International Telecommunication Union (ITU). With a state score of only 0.260, Nepal ranks poorly compared to other countries concerning cybersecurity. From 2016 to 2019, Nepal has seen a 37% growth in cybercrime - from 1318 cases filed in 2016 to 2209 cases filed in 2019. Amongst different forms of cybercrime, Nepal has particularly suffered from hacking. Government services, businesses, and individuals have been the victims of hacking (Giri & Shakya, 2020).

The importance of cybersecurity is highlighted in the current situation where no corporation or individual is safe from cyber attacks. Cybersecurity in short, can be described as a process of keeping your information, assets, networks, and applications safe from outsider and insider threats.

This paper studies the emerging cybercrimes as we see significant changes in our social and work environment. It explores the nature of current cybercrimes globally and in Nepal, their results, and suggestions on mitigating them. The knowledge from these reports are then used to solve the explored problems.

II. Concepts and Taxanomies

A. *Social Engineering*

Social engineering attacks refer to attackers using baits to manipulate people into providing them with sensitive and personal information (Ramadan, et al., 2021). The information that the attackers seek can range from personal and bank details to the person's social media credentials. Social engineering attacks are popular because it relys on people's vulnerabilities rather than a system's vulnerabilities. It is relatively easier to trick people into making decisions based on their natural instinct rather than find a way to hack the system or the network.

Following forms of social engineering attacks are predominantly used:

- Phising : The attackers send you an important looking email or a message which prompts you to download a seemingly harmless software or a file. This can lead to you downloading a malware and installing it on your system, potentially compromising it (Hakak, Khan, Imran, Choo, & Shoaib, 2020).

- BECs (Business Email Compromises): In a BEC attack, an attacker uses spearphising tactic to specifically target individuals, tricking them to believe that the malicious emails/texts are from their friends. This can lead to the victim downloading malicious programs into their systems (Verizon, 2021).

B. *Basic Web Application Attacks*

When attackers get initial access through the web application compromises, they use basic web application attacks to get access to different commodities like emails, passwords, personal information, application data. These kinds of access help the attackers to leverage the system to further perpetuate attacks on bigger systems, distribute malwares, or future DDoS attacks (Hakak, Khan, Imran, Choo, & Shoaib, 2020). These attacks mainly target web servers, users/developers, networks, terminal, media, and so on.

C. *System Intrusion*

System intrusion is one of the new attack being employed by attackers. This attack can consist of a complex series of different kind of attacks. While the usage of ransomwares is the most common form of system intrusion, attackers have also been seen using the magecart attack to target payment card data in web applications. Attackers also used hacking as one of the steps of system intrusion (Barona & Mary, 2017).

D. *Miscellaneous errors*

Miscellaneous errors deal with the case of human errors instead of attackers deliberately targetting a system. Humans are prone to making mistakes. Accidentally sending information to a wrong/vulnerable address, misconfiguring databases, etc. are some of the few examples of miscellaneous errors that can lead to system and network compromise. Interal actors for miscellaneous errors include system admins, developers, end-users, etc (Barona & Mary, 2017). The error varieties include, misconfiguration, misdelivery, publishing errir, development error, loss, etc.

E. *Privilege Misuse*

One of the insider threat type, privilege misuse is a kind of attack carried out by abusing the privileges given to the individual/insider (Srinivas, Das, & Kumar, 2019). Majority of the attackers misuse their privileges for financial gain while others can do it because of personal vendettas. With personal information as the most stolen data from privilege misuse, the current situation (remote working) showed to have no effect on this attack type (Ramadan, et al., 2021).

F. *Lost and Stolen Assets*

Although low, lost and stolen assets also add to a certain percentage of breaches every year. This breach type also stems from the fact that humans are prone to making mistakes. People can lose their devices (computers, cellphones) which leads to the comprmise of things like personal and organizational information, application data, work documents, etc .

In the current world of advanced cyber-attacks and equally advanced protection systems, most of the organizations and individuals need to understand the scale of the problem (Barona & Mary, 2017). In doing so, they need to accumulate the knowledge required to become better at protecting their information, and subsequently implement different measures to mitigate the risks.

(Hakak, Khan, Imran, Choo, & Shoaib, 2020) explains following security goals should be kept in mind by any informed individual or an organization:

- Confidentiality: Information should be accessed by authorized individuals only.
- Integrity: The integrity of information should be maintained. Unauthorized individuals should not be able to change the information.
- Availability: The information must be readily available to the authorized individuals.
- Authenticity: The information should be exchanged between the verified source and the verified destination.

III. Relevant Theories

A. *Anomie Theory*

(Ma & McKinnon, 2021) have emphasized that one of the explanations to the current rise in cyber fraud and crimes can be explained through the Anomie theory. In this theory, the rapid social changes (like the results of COVID) in any traditional communities can lead to anomie.

This theory classifies the society's ability to normalize an individual's native drives during rapid social change (Ma & McKinnon, 2021). This can lead to abnormality in individuals' social behavior. In a society of current times, people lack guidance, discipline, and regulations. When these things are not in place and in proper order, people become confused and frustrated. This allows the cyber attackers to easily prey on these people and exploit and abuse them. New norm of working from home, and constantly using online services allows people to become a subject of attacks like social engineering attacks, malware attacks, and so on.

B. *Strain Theory*

(Ma & McKinnon, 2021) also attribute the current uprising of cyber-attacks to the Strain theory. Strain theory takes off from where the Anomie theory stops. Robert Merton (1957) develops the Anomie theory by suggesting that even the stable social conditions allow for more crimes because of the social structural strain. Each community has a different definition of what's successful and what's not. They have their own goals and what the individuals must strive for to get these goals. For example, in American and many other societies, accumulating money is seen as climbing up the social hierarchy and this leads people to go out of their ways to commit crimes to accumulate the said wealth. The strain theory can be used to explain the monetary motives of the cybercriminals. In the current setting, the Strain theory can be used to explain why cyber-attacks have increased – from social strains to the insecurity of jobs, food, and scarcity of safe and secure shelter.

C. *Socio-technical Systems (STS) Theory*

(Malatji, Solms, & Marnewick, 2019) defines STS as a unified system theory that combines human, business processes, organizational structure, technology, and external acting environment to fulfill intended functions. It gives a broad overview of people using technical resolutions to perform activities by applying different processes within an organizational boundary to achieve planned goals. They argue that deploying any new information system in the organization will only succeed if they consider the system's impact on strengthening human factors and eliminating the social constraints. Hence, the synergy of all three components improve the cybersecurity performance in any sector.

(Kumar, Biswas, Bhatia, & Dora, 2020) also praises the STS theory in his work and cite it as the HOT theory- human(H), organization(O) and technology(T). They suggest that an organizations' technical capabilities and employed human resources uniformly govern its cyber-security. He advocates the importance of senior management in promoting cyber-security in the orgnization.

Table 1: Analysis of Different Related Papers on Threats and Countermeasures of Cybersecurity

Article #	Full Reference (APA Referencing Style)	Main Research Questions/ Objectives	Main Result/Issues	Why is this paper relevant?	Other Remarks
1.	(Wang, Nnaji, & Jung, 2020)	What are the cybersecurity threats and fundamental security practices employed in the Nigerian banking industry? What is the level of security capabilities of the Nigerian banking industry?	As per the survey, the top cyber threats in the Nigerian banking industry are malware, spam emails, hacking, and cyberstalking. Nigerian banking industry practices adequate management support and training for handling security breaches. To strengthen the security capabilities, both socio-technical and socio-legal approaches should be applied.	This paper studies the current state of cybersecurity in the banking industry. It suggests a holistic approach to minimize the gaps between detecting and dealing with cybersecurity breaches.	The researchers conducted an online survey with 100 qualified experts working in 15 Nigerian banks and 27 banking security services. 80% of the sample population faced one or more cyber threats at work. This paper includes research from limited literature and sample size.
2.	(Mbelli & Dwolatzky, 2016)	To examine various cyber threats associated with cyberbanking in South Africa. To introduce a path to cyberbanking security, including network and application security. To propose a cybersecurity framework that financial institutions can adopt.	The researchers recommend firewall, authorization, and authentication techniques to defend banking premises for boundary security. They also suggest input validation, output validation, parameterization, attack surface identification, and reduction during system development for application	The paper discusses the threats to information system and network boundary and propose different techniques to defend them.	The researchers limit the scope of this paper to the South African banking industry. They pinpoint that regular investment in advanced security technologies and measures can prevent massive monetary and data losses from cyber-attacks.

			security. They propose a cybersecurity framework that includes different controls for entry points, operations, propagation techniques, and threats validation.		
3.	(Nurse, 2018)	What are the significant cybercrimes conducted against individuals? What are the critical human and psychological factors that make cybercrimes successful?	This paper appraises trickery and social engineering, harassment through online means, hacking, identity-thefts, and (DOS) denial of services and information as the major types of cybercrimes conducted against individuals. It shows how cyber attackers exploit an individual's ignorance, oversharing and trusting nature, need for love and affection, understanding of essential data to make cybercrimes successful.	This paper portrays the real-life cases of different cybercrimes attacking individuals. It advocates how the human factor impacts the successful execution of such crimes.	This report applied a thorough and methodical review of case studies, and articles about online crimes in academic, industry, and government circles across the world. It does not describe how to defend and resolve the cybercrimes.
4.	(Ma & McKinnon, 2021)	To identify, propose and develop new links amid COVID-19, digital users, and cyber fraud. To unite existing criminological theories, associate practice across disciplines,	The researcher claims that cyber attackers aim individual's socio-psychological vulnerabilities that might be extra prominent in the COVID- 19 period. They use Anomie	It illustrates cyber fraud trends, causes, and countermeasures in the current pandemic setting.	This paper is a general review of COVID-19 related information security counterfeits through empirical to conceptual reports from different agencies and institutions.

		and present multiple insights in the pandemic setting.	and Strain theory to analyze and understand the causes of COVID-19 themed cyber frauds and introduce four dimensions of cyber fraud based on authorization, financial information theft, identity theft, and fraudulent intent.		This research paper only collects data from secondary sources, i.e., it does not include any quantitative or qualitative analysis of its own.
5.	(Hakak, Khan, Imran, Choo, & Shoaib, 2020)	To understand the influence of Covid-19 on cyber-attacks and security. To generate a novel taxonomy of cyberattacks and their consequences on cybersecurity goals. To address the possible countermeasures to cyber threats.	This research categorized cyberattacks with covid-19 theme into four major headings: interrupting services, monetary profits, information stealing, and fearware. It also presented possible alleviation solutions like using secure and updated system.	This research paper explores potential cybersecurity vulnerabilities in various sectors and explain how cybercrimes disrupt the security goals.	It does not examine the emerging technologies for predicting, observing and diagnosis of cyber threats.
6.	(Ramadan, et al., 2021)	What kind of cybersecurity attacks are happening during the COVID-19 pandemic? What are the recommendations and countermeasures for different types of cybersecurity attacks?	The researchers classified work-from-home threats, phishing, unethical attack, ransomware attack, social engineering, physical attacks, and denial of service attacks as the significant cybersecurity attacks faced during the pandemic. They explore the reasons behind it in-depth and provide countermeasures	This paper explores the cybersecurity attack culture in the pandemic era. It explains how network vulnerabilities are exploited, how individuals fall victim to social engineering attacks, so on.	The researchers accumulated data from trusted organizations- World Health Organization (WHO), news portals, national statements, and existing articles. Although the cybersecurity attack data is explored thoroughly, this paper lacks slightly on exploring the countermeasures.

			to these attacks.		
7.	(Bechara & Schuch, 2021)	Why is cybersecurity important in the context of current global governance? What are the initiatives being taken in international cooperation to mitigate cybersecurity issues? What factors are the most important in international cooperation that help mitigate the said issues?	This paper also explores the regulatory approach by which governments and organizations have tried to counter the cybersecurity threats. It explores the positive initiatives in international cooperation and highlights the importance of harmonization as cybersecurity issues have been getting political.	This paper explores the importance of regulations to resolve the cybersecurity issues, the policies to create an international cooperation and, the harmonization amongst different nations to implement these policies.	While this paper gives a great insight into the importance of regulations and international cooperation, it lacks further research into what are the current ideas implemented to counter these cooperation issues. It also falls short in providing detailed and thought-out recommendations.
8.	(Srinivas, Das, & Kumar, 2019)	To address the threats, strategies, and regularity challenges in cybersecurity. To examine the national standards and government strategies to guard cyberspace.	A minimum collection of cybersecurity standards is required to attain a strong security approach. Lack of awareness, agility, coverage, economic and organizational considerations as the challenges for cybersecurity standardization.	This report discusses about the legal standards and challenges for cybersecurity. It also presents a framework for incident management that empowers organizations to prevent, respond and identify cyber threats.	This is a general review that covers the importance of government regulations, national standards, and framework in cybersecurity.
9.	(Giri & Shakya, 2020)	To study the current scenario of cybercrime and determine the top cyber threat risks in Nepal. To examine the future cybercrime challenges in Nepal.	The researchers claim that cybercrimes are exponentially increasing in Nepal; most cases include social media as the medium and female as the victim. All the sectors of	This paper studies about cybersecurity state, its causes and recommend measures to control cybercrimes in the context of Nepal.	This study applies the report analysis method using global surveys and in-depth interviews with subject experts.

			Nepal should use updated technologies, enforce security training programs, perform security audits, and prioritize cybersecurity to enhance their capabilities and fight against cybercrimes.		
10.	(Barona & Mary, 2017)	What are the principal data breach and cyber threats existing in the cloud infrastructures? What are the best security practices that cloud service providers can follow to prevent a data breach?	The researchers identified malicious users, cloud configurations, broken binaries, firewall, vulnerable browser, multi-tenancy, and mobility as the major causes of a data breach. They discovered the security deficiencies in transparency, data protection methods, encryption, and coordinating data privacy and origin.	This report presents the fundamental data security goals, causes of a data breach, and security approaches to guard data against those violations.	This research mainly studies the challenges of cloud data security faced in client-server infrastructure; the researchers aim to conduct a detailed study in different cloud computing models, including more diverse security goals in the future.
11.	(Malatji, Solms, & Marnewick, 2019)	To find out the gaps between an organization's social and technological system that impacts cybersecurity practices. To develop a socio-technical security framework that can adequately address an organization's security goals.	The implementation of socio-technical framework optimized the organization’s cybersecurity performance. Organizations need to invest tremendous amount of time resource to continuously monitor their accuracy in initial stage.	This report presents the implementation of two major determinants of cybersecurity – social and technological system.	The researchers employ a socio-technical practice to generate a conceptual framework, implement it in selected security frameworks, and continuously observe their performance.

12.	(Chen, Beaudoin, & Hong, 2017)	To recognize probable online victims based on different theories like routine activity, self-control, and fear-based theory. To develop a new model for analyzing the consequence of online scams on privacy concerns and cybersecurity behaviors.	The researchers develop a conceptual, structured equation model by combining routine-activity theory, self-control theory, and extended parallel process model to address the influence of a victim's experiences on privacy concerns. They claim that privacy concerns are directly related to the privacy defending activities.	This paper links the routine behavior, self-control activities to the cyber victimization. It shows how the cyber victims tend to follow privacy protection activities and be more concerned about their privacy.	The researchers surveyed 11,534 online users to develop a structural equation model for identifying the indicators to predict scam victims.
13.	(Barton, Tejay, Lane, & Terrell, 2016)	To examine the influence of external pressures in motivating cybersecurity participation to senior managers by applying neo-institutional theory.	This report demonstrates the importance of senior management support for the success of security programs. The external factors like national policy, government regulations, moves of competitors and benchmark industries motivates the senior management participation in cybersecurity.	This report focusses on the factors that influence senior management and employees to participate and comply with the cybersecurity practices in the organization.	The researchers conducted an online survey with a sample population of 167 who work in different-sized companies in the central-south United States.
14.	(Ekelund & Iskoujina, 2019)	What is the optimum level of investment in cybersecurity? How can it be accomplished?	The researchers advocate the use of computer simulation and risk cost functions to analyze the historical incidents and determine the	This paper discusses on the organization's need for cybersecurity investment for the safety of critical assets.	The researchers perform a case study exploration supplemented by cybersecurity economic theories and techniques to review a financial institution and its security

			optimal level of investment for those assets.	It guides the security practitioners to decide on the cybersecurity investments against the cyber risks.	investment determinants. It includes a single case study and a limited number of observations to conclude the research work.
15.	(Kumar, Biswas, Bhatia, & Dora, 2020)	To identify the organizational level antecedents of an improved cyber-security. To examine cybersecurity's technical and human perspective using human–organization–technology theory.	The researchers claim that organizations should adopt legal policies and technical models, followed by management roles and proactive cybersecurity to enhance their level of information security.	This paper aims at enhancing the cybersecurity levels by combining organizational, human, and technological perspectives.	The researchers conducted a study on 151 cybersecurity specialists working in different sectors of India.

IV. Conlusion and future work

As Nepal sees a vast growth in the IT industry, it is essential for each organization to constantly study the current global state of cybersecurity – its trends, new breaches, new counter measures and so on. Just like the rest of the world, COVID-19 has forced Nepali corporate industry to work from home. In a indistrial culture of working from office only, this sudden change has impacted the organizations in both, better and worse ways.

Many organizations are realizing that it is actually viable to run a company where people can work online. On the other hand, some organizations suffer from lack of monitoring and human supervision.

Desregarding the advantages and disadvantages, the current situation has forced all the corporate organizations to seriously consider their stand in regards to cybersecurity as the cyber-attacks are increasing. At the same time, the digization of the workplace has led unware individuals and even organizations to become potential cybercrime victims.

Hence, it is consiquential for Nepali corporate industry to take a good look at the current status of cybersecurity in Nepal, what are the new challenges faced by the Nepali corporate industry, and what can be done to mitigate these ever-looming cyber threats.

Bibliography

1. Barona, R. and Mary, E.A. Anita, 2017. A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats. *International Conference on circuits Power and Computing Technologies [ICCPCT].,* 1-8. doi: 10.1109/ICCPCT.2017.8074287
2. Barton, Kevin A., Tejay, Gurvirender, Lane, Michael and Terrell, Steve, 2016. Information system security commitment: A study of external influences on senior management. Elsevier Ltd., *59*9-25. doi: https://doi.org/10.1016/j.cose.2016.02.007
3. Bechara, Fabio Ramazzini and Schuch, Samara Bueno, 2021. Cybersecurity and global regulatory challenges. *Journal of Financial Crime, 28*2359-374. doi: 10.1108/JFC-07-2020-0149
4. Chen, Hongliang, Beaudoin, Christopher E. and Hong, Traci, 2017. Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior, 70*291-302. doi: https://doi.org/10.1016/j.chb.2017.01.003
5. Ekelund, S. and Iskoujina, Z., 2019. Cybersecurity economics – balancing operational security spending. *Information Technology & People, 32*51318-1342. doi: https://doi-org.ezproxy.apiit.edu.my/10.1108/ITP-05-2018-0252

6. Juneja, S., Gahlan, M., Dhiman, G., & Kautish, S. (2021). Futuristic cyber-twin architecture for 6G technology to support internet of everything. Scientific Programming, 2021.

7. Giri, Shailendra and Shakya, Subarna, 2020. High Risk of Cybercrime, Threat, Attack and Future Challenges in Nepal *International Journal of Computer Sciences and Engineering, 8*246-51. doi: https://doi.org/10.26438/ijcse/v8i2.4651

8. Hakak, S., Khan, W. S., Imran, M., Choo, R. and Shoaib, M., 2020. Have you been a victim of COVID-19-related Cyber incidents? Survey, taxonomy, and mitigation strategies. *IEEE Access, 8*124134-124144. doi: 10.1109/ACCESS.2020.3006172

9. Kumar, Saurabh, Biswas, Baidyanath, Bhatia, Manjot Singh and Dora, Manoj, 2020. Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management,* 1-33. doi: 10.1108/JEIM-06-2020-0240

10. Ma, K.W.F. and McKinnon, T., 2021. COVID-19 and cyber fraud: emerging threats during the pandemic *Journal of Financial Crime,* 1-14. doi: 10.1108/JFC-01-2021-0016

11. Malatji, Masike, Solms, Sune Von and Marnewick, Annlizé, 2019. Socio-technical systems cybersecurity framework *Information and Computer Security, 27*2233-272. doi: https://doi-org.ezproxy.apiit.edu.my/10.1108/ICS-03-2018-0031

12. Mbelli, Thierry Mbah and Dwolatzky, Barry, 2016. Cyber Security, a Threat to Cyber Banking in South Africa An approach to Network and application security. *3rd International Conference on Cyber Security and Cloud Computing* 1-6. doi: 10.1109/CSCloud.2016.18IEEE Computer Society

13. Nurse, Jason R. C., 2018. Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit *The Oxford Handbook of Cyberpsychology,* 1-23. doi: https://dx.doi.org/10.1093/oxfordhb/9780198812746.013.35

14. Ramadan, Rabie A., Aboshosha, Bassam W., Alshudukhi, Jalawi Sulaiman, Alzahrani, Abdullah J., El-Sayed, Ayman and Dessouky, Mohamed M., 2021. Cybersecurity and Countermeasures at the Time of Pandemic, *Journal of Advanced Transportation,* 1-19. doi: https://doi.org/10.1155/2021/6627264

15. Reyana, A., Kautish, S., Vibith, A. S., & Goyal, S. B. (2021). EGMM video surveillance for monitoring urban traffic scenario. International Journal of Intelligent Unmanned Systems.

16. Sandhya Sharma, Sheifali Gupta, Deepali Gupta, Sapna Juneja, Gaurav Singal, Gaurav Dhiman, Sandeep Kautish, "Recognition of Gurmukhi Handwritten City Names Using Deep Learning and Cloud Computing", Scientific Programming, vol. 2022, Article ID 5945117, 16 pages, 2022. https://doi.org/10.1155/2022/5945117

17. Srinivas, Jangirala, Das, Ashok Kumar and Kumar, Neeraj, 2019. Government regulations in cyber security: Framework, standards and recommendations, *Future Generation Computer Systems, 92*178-188. doi: https://doi.org/10.1016/j.future.2018.09.063

18. Verizon, *2021. Data Breach Investigations Data Breach Report (DIBR). Avialable from: https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf*

19. Wang, Victoria, Nnaji, Harrison and Jung, Jeyong, 2020. Internet banking in Nigeria: Cyber security breaches, practices and capability, *International Journal of Law, Crime and Justice, 62*1-11. doi: https://doi.org/10.1016/j.ijlcj.2020.100415

20. Kemp, Simon, 2020. *DIGITAL 2020: APRIL GLOBAL STATSHOT,* DataReportal. Available From: https://datareportal.com/reports/digital-2020-april-global-statshot

21. Yasser Alharbi, Ali Alferaidi, Kusum Yadav, Gaurav Dhiman, Sandeep Kautish, "Denial-of-Service Attack Detection over IPv6 Network Based on KNN Algorithm", Wireless Communications and Mobile Computing, vol. 2021, Article ID 8000869, 6 pages, 2021. https://doi.org/10.1155/2021/8000869