Journal of Applied Engineering, Technology and Management (JAETM)

Navigating Cyber Perils in Bhutan: Challenges and Opportunities

Tashi Wangchuk[1*], Younten Tshering[2], and Pratima Pradhan[3]

[1,2] *Lecturer, Department of Information Technology, Jigme Namgyel Engineering College, Dewathang, Bhutan*

[3] *Bhutan Computer Incident Response Team, Cybersecurity Division, GovTech Agency, Thimphu, Bhutan*

[*] *Corresponding author: Tashi Wangchuk, tashiwangchuk.jnec@rub.edu.bt*

Published: June 2024

DOI: https://doi.org/10.54417/jaetm.v4i1.132

Abstract

Over a decade, Bhutan witnessed massive digital transformation in various sectors offering numerous opportunities, but at the same time, this has also brought in a considerable share of cybersecurity threats and challenges. By reviewing and analysing information related to cybersecurity from various sources, such as journals, news articles, press releases, websites, and annual reports of government agencies related to Bhutan's cybersecurity, this study identified the prominent vulnerabilities, challenges, and opportunities, and explored the mitigation strategies. It was determined that the cybersecurity threat landscape of Bhutan is dynamic and multifaceted, ranging from online scams, phishing attacks, malware infections, vulnerabilities in systems, and a lack of security awareness among the general population. Bhutan has made noticeable efforts towards cyber threat mitigation which includes improving cybersecurity awareness at various levels, collaborating with stakeholders both at national and international levels, and implementing guiding strategies. However, there are still significant challenges being faced in terms of limited allocations of budget for infrastructure and human resource development and management. In addition, penetrating security awareness at the grassroots level is a prominent challenge. There are also opportunities to work towards maintaining and retaining a technical talent pool and implementing the national cybersecurity strategy. This article provides insights into Bhutan's cybersecurity landscape and offers recommendations for addressing current challenges and building capabilities to combat cyber threats effectively.

Keywords— Awareness, Bhutan, cybersecurity, threat landscape, vulnerabilities

1 Introduction

Bhutan is a small, landlocked, and developing country located between the two most populous countries, China and India. The total land area of Bhutan is 38,394 square kilometers and it has a total population of 727,145 people. Bhutan Telecom Limited (government-owned) and Tashi InfoComm Limited (the first private mobile company) established in 2006 are the two companies providing telecommunication services in the country[1]. The vision of Bhutan is to become an ICT knowledge-based information society, where government organizations, businesses, and individuals are leveraging the Internet for day-to-day operations and activities, increasingly depending on information systems, networks, and the Internet.

As the nation embraces digitization to enhance economic, social, and administrative facets, the simultaneous rise in cybersecurity threats has become a serious concern. It was pointed out by Dilipraj that Bhutan's cyberspace is infested with all sorts of malware and spyware, and individual internet users are prone to online scams, social engineering attacks, and phishing [2].

In 2015 the Global Cyber Security Capacity Center (GCSCC), University of Oxford with the World Bank facilitated a self-assessment of Bhutan's Cyber Security Capacity using the Cyber Capacity Maturity Model (CMM) which identifies five distinct dimensions of cybersecurity (policy, culture, legal, skills and technology). The assessment aimed to identify at which stage of maturity Bhutan is in terms of cybersecurity capacity maturity. The stages of maturity consisted of start-up, formative, established, strategic, and dynamic; and in almost all the capacity factors of all the dimensions, the maturity stage was assessed as start-up [3]. This is a serious indication of the dire need for Bhutan to work towards capacity building of Cybersecurity. No further assessments are being initiated and conducted to find out how far Bhutan's Cyber Security Capacity has been developed.

Bhutan's cybersecurity incidents such as online financial scams based on fake emails supposedly sent from the Royal Audit Authority caused the Bank of Bhutan to transfer 16 million (in Bhutanese currency) to three different accounts in India, Malaysia, and Thailand [4] along with the private and government websites defaced, and networks and systems made inaccessible due to malware and physical disruptions clearly shows that Bhutan is not immune to cyber threats [5] and these incidents can be treated as an eye-opening lesson for Bhutan.

The country's recent strides in technological adoption and increased internet penetration have ushered in new opportunities but also have simultaneously exposed it to a myriad of cybersecurity risks. The need to safeguard critical infrastructure, government systems, and individual users from malicious cyber activities is imperative to ensure the sustainable development and security of the Kingdom.

This study took a deeper look into the cybersecurity threat landscape of Bhutan, offering an in-depth analysis of current challenges, identification of prevailing threats and vulnerabilities, and an examination of the strategies implemented to improve the nation's cybersecurity security resilience by the Bhutanese government and relevant agencies. This research contributes valuable insights that can help in making informed key policy decisions, guide strategic planning, and empower cybersecurity stakeholders in Bhutan in successfully navigating the cyber perils in Bhutan.

2 Materials and Methods

The primary objective of this study was to conduct a comprehensive review of Bhutan's cybersecurity landscape, which includes examining current threats, challenges, existing infrastructure, and policies about cybersecurity in the country following the methods and materials adopted below.

2.1 Data Sources

A systematic literature review was conducted to gather relevant information from various sources, including news articles (Kuenselonline, TheBhutanese, BhutanToday, etc.), social media posts, press releases, annual reports of organizations, and research articles related to Bhutan's cybersecurity.

2.2 Data Search and Selection

Keywords such as cybersecurity Bhutan, cyber threats in Bhutan, and Bhutan cybersecurity policies were utilized to ensure comprehensive coverage. In addition, the databases like Google Scholar, and official government websites were searched with filters set to include publications from 2018 to 2023 which were written in English language. The search was conducted from 1st January 2024 to 10 February 2024. The news articles, press releases, annual reports, and papers were selected based on relevance to the study's objectives and for the screening, the titles, abstracts, and full-text reviews were included to ensure the inclusion of relevant information.

2.3 Data Analysis and Extraction

The analysis of data was performed using the thematic analysis approach to identify key trends, threats, and policy measures related to the cybersecurity landscape in Bhutan. The data from selected sources were analysed and synthesised to provide a comprehensive and coherent narrative of the cybersecurity landscape of Bhutan based on the common themes and patterns, and then the relevant and insightful information was extracted accordingly.

3 Results and Discussion

In this section, the findings from the literature review and data analysis are presented and discussed in detail under the following sections.

3.1 Overview of Bhutan's Cybersecurity Landscape

To the outside world, Bhutan is well-known for its Gross National Happiness (GNH) oriented development philosophy and its strong commitment to sustainable development. At the same time, Bhutan's initiative on digital transformation has brought new challenges in safeguarding cyberspace. Bhutan's cybersecurity landscape is presented in the sections (a) Analysis of cyber threats, (b) Cybersecurity infrastructure, (c) Policies and regulatory measures, and (d) Key challenges and opportunities.

3.2 Analysis of Cyber Threats

Bhutan, just like any other country undergoing a rapid process of digital transformation, poses significant challenges to the confidentiality, integrity, availability, and privacy of the general public as well as the digital infrastructure. Bhutan ranks 134th position in the Global Cybersecurity Index (CGI), reflecting its commitment to cybersecurity. It's essential to continue strengthening cybersecurity strategies to protect from evolving threats. The GCI serves as a trusted reference, measuring countries' commitment to cybersecurity on a global scale and evaluates each country's level of development or engagement across legal, technical, organizational, capacity development, and cooperation [6].

According to Kuensel Online News, Bhutan has been facing a surge in cyber threats, particularly phishing attacks and scams. Mobile banking users have been the most affected, losing money to scammers. One common scam involves fraudsters calling locals and asking for their bank details, such as their account number and mobile number, to take control of the mobile banking application. The scammers also convince the victims that they have won a lottery worth millions, and the victims share the OTP and other details. Instead of crediting the amount, the victim's account is debited with the same amount [7]. While specific figures on Bhutan's financial loss due to cybersecurity incidents were not available, there have been several cases of cyberattacks in Bhutan resulting in major damages, in terms of money, data loss, or service disruptions [8]. However, the exact financial loss is not officially recorded.

Phishing attacks and online scams are prevalent in Bhutan and pose a significant threat to individuals, businesses, and government institutions. Cybercriminals often use deceptive emails, messages, or websites to trick users into divulging sensitive information, such as login credentials or financial data. Bhutan's relatively low cybersecurity awareness level makes its general mass particularly vulnerable to these attacks. In the BtCIRT Annual Report, several phishing attacks and scam alerts were documented about Bhutan. These attacks often take the form of links shared through platforms like Facebook, WhatsApp, and WeChat [10], where the cybercriminals or scammers create eye-catching designs and statements to grab users' attention and claim that the users have won an iPhone, a lottery, or a Samsung phone, luring users to click on the links which lead to fake websites that ask for sensitive information or even ask to send money to claim the allegedly won prize.

Malicious software can infiltrate systems, compromise data integrity, and disrupt critical services. In the study conducted by Choejay, the findings suggest that the government organizations in Bhutan are vulnerable to cybersecurity threats such as malware and hacking and that government organizations lack adequate knowledge and awareness on cybersecurity, policies and procedures, technical controls, and incident response capabilities. It also mentioned that the use of pirated software and expired security products in many government organizations was rampant and nullified the effect of technical measures put to provide security [9]. Malware, including viruses, worms, and ransomware, represents another major cyber threat in Bhutan.

3.3 Cybersecurity Infrastructure

As Bhutan continues its journey towards digital transformation, the need for a holistic approach to cybersecurity becomes increasingly imperative. Balancing the promotion of innovation with the protection of critical infrastructure and sensitive data remains a key priority for policymakers. By fostering a culture of cybersecurity awareness, investing in robust infrastructure, and fostering international cooperation, Bhutan can navigate the complexities of cyberspace while upholding its values of Gross National Happiness and sustainable development.

Before 2012: Bhutan's cybersecurity posture was relatively underdeveloped, as is the case with many developing nations. The country lacked comprehensive cybersecurity laws, policies, and strategies to effectively combat cyber threats. There was limited awareness among government agencies, businesses, and the general public about the importance of cybersecurity. Today, only questions such as who could have been interested in peeking into Bhutan's cyberspace; but then it can also be reconciled that limited connectivity could have acted as a barrier to the threat actors. The specific details about Bhutan's cybersecurity initiatives are not readily available. However, it's important to note that like many countries, Bhutan would have faced challenges in the early stages of its digital transformation. To this effect, the following Bhutan's Cybersecurity key milestones are the initiatives taken by the Government of Bhutan in collaboration with international players in the field of cybersecurity to combat cyber threats.

2012: Bhutan's journey towards establishing a robust cybersecurity framework began in early 2012. The International Telecommunication Union (ITU) conducted a readiness assessment to measure the cybersecurity maturity level of Bhutan and its cyber threat landscape. One of the most significant initial challenges faced was explaining the importance of cybersecurity and the necessity for a strategy for non-technical background government and private sector leaders. With the digital transformation underway, the awareness of the importance of cybersecurity remained a bigger challenge where cybersecurity was perceived totally as a technological problem with limited impact on other connected areas.

2016: Following the assessment by the ITU, Bhutan Computer Incident Response Team (BtCIRT) was formally established in April 2016. The BtCIRT operates under the Government Technology (GovTech) Agency, the then Department of IT & Telecom (DITT) of the Ministry of Information & Communications with the mandate of providing both reactive and proactive cybersecurity services to the entire nation, including guiding the development of a national strategy.

2018: By the end of 2018, the development of Bhutan's national Cybersecurity Strategy (NCS) was initiated by ITU and BtCIRT. After several rounds of NCS taskforce workshops in 2020, the first version of NCS was finalized and awaiting approval from the cabinet of Bhutan. BtCIRT engages in conducting various awareness events related to cybersecurity for Bhutan's populace aimed at different levels such as the general public, ICT professionals, and managerial positions. For example, in October 2023 as part of the cybersecurity awareness month, the Capture the Flag (CTF) challenge was conducted for the students of Gyalpozhing College of Information Technology (GCIT), College of Science and Technology (CST), and Jigme Namgyel Engineering College (JNEC) to build knowledge and skills related to the foundations of cybersecurity. Other events include cyber safety programmes for women and children, cyber hygiene information on social media pages for the general population, and technical workshops on network security and domain name abuse for ICT professionals from government, corporate, and private sector organisations [10].

3.4 Policies and Regulatory Measures

Salamzada et al. (2015) evaluated the prevailing cybersecurity status of Afghanistan and proposed a cybersecurity strategy for Afghanistan based on the experiences of developed and developing countries (Malaysia, India, and the US) in terms of cybersecurity. The authors emphasized having a cybersecurity strategy framework to protect government data for the country to systematically address the ever-growing cyber threats [11].

As of today, Bhutan does not have a living National Cybersecurity Strategy (NCS) to guide and combat cyber threats effectively at the national level. While lacking a guiding strategy at the national level, the collaboration of relevant stakeholders and initiatives taken by different stakeholders would remain fragmented with less or no tangible outcomes. As the country faces an increasing number of attacks, a comprehensive strategy is imperative. Bhutan embarked on defining its first NCS in 2012. An initial readiness assessment conducted by the International Telecommunication Union (ITU) measured both the cybersecurity maturity level and the cyber threat landscape in the Kingdom of Bhutan [12]. While the draft NCS is in place, the approval and implementation must be expedited to engage all relevant stakeholders including government agencies, the private sector, and civil society.

Since the establishment of BtCIRT, it has operated under the Government Technology (GovTech) Agency. Their mandate includes providing both reactive and proactive cybersecurity services to the entire nation and guiding the development of a national strategy [12]. BtCIRT plays a crucial role in enhancing cybersecurity in Bhutan. Their efforts include facilitating collaboration, information exchange, capacity building, and sustained advocacy in computer security.

According to the Bhutan Infocomm and Media Authority annual report (2020), since its establishment in 2016 and until May 2020, BtCIRT handled around 655 cyber threat incidents. Seventy-five percent of these incidents were vulnerabilities detected in the systems, 12% were malware or bots, and the remaining 13% comprised other incidents including phishing, ransomware, crypto mining, DDoS, information gathering, spam, and social media cases [13]. More than 90% of the incidents recorded thus far have been detected by BtCIRT with proactive monitoring and security feed analysis, as opposed to only 10% of the incidents being reported by constituents.

In the performance audit report on Preparedness for Cybersecurity of Bhutan, the Royal Audit Authority of Bhutan stated that with the digital transformation, there is an increasing number of organizations collecting and processing personally identifiable information (PII), which demands those entities and organizations to protect information while balancing the need to make information available through digital services. Personal data or information is a growing concern for customers, organizations, and regulators as it might pose data privacy risks such as unauthorized disclosure of data, data loss, phishing, fraudulent activities, and identity theft. Therefore, it is important that entities possessing personal data effectively safeguard from data breaches while using it for the purposes required by the relevant laws and regulations. The report also mentions that Bhutan's cyber landscape is constantly changing and becoming unpredictable as more people, governments, devices, systems, and networks are getting interconnected. While citing the ITU's experience in developing Bhutan's first National Cybersecurity Strategy, the report underscores the lack of sufficient funding, technical and managerial skills, and appropriate structures to deal with cyber incidents in Bhutan [14].

3.5 Challenges and Opportunities

Bhutan's cybersecurity infrastructure is still evolving, with initiatives such as the establishment of the Bhutan Computer Incident Response Team (BtCIRT) aimed at enhancing incident response capabilities and promoting information sharing among stakeholders. However, resource constraints and a shortage of skilled cybersecurity professionals pose significant hurdles to building a robust cyberdefense posture.

The cybersecurity challenges faced by organizations are constantly evolving and the threats come in various forms such as malware, phishing, ransomware, insider threats, and advanced persistent threats. On top of these threats, organizations also face the challenges of securing IT environments and keeping employees trained and aware of cybersecurity. Further, organizations have to comply with cybersecurity regulations and standards such as GDPR and PCI-DSS to avoid legal and financial implications [15].

As opined by Tshering in the Kuenselonline article, the use of pirated software and reassembled hardware, including government institutions poses a significant threat to Bhutan's undermining cybersecurity [16]. To address such challenges, it is crucial that Government agency campaigns educate organizations about the risks of using counterfeit products and emphasize the benefits of genuine hardware and software, increase budgetary allocations for genuine software access with centralized procurement, and enforce strict mechanisms to regulate local suppliers to supply of genuine products. The use of pirated software and reassembled hardware is a double-edged sword. The article emphasizes the risks associated with counterfeit products and it is evident that the use of genuine software and hardware needs to be prioritized for safeguarding Bhutan's digital infrastructure.

According to Ghafoor [17], South Asian countries including India, Bangladesh, Pakistan, Sri Lanka, Nepal, Bhutan, and Afghanistan have limited cyber resilience due to countries' uneven levels of development in their cyber response mechanisms, which is why South Asian region is a prominent target for cyberattacks, ransomware, phishing, and data breaches among others [17]. Dilipraj [2] asserts that the reputation of the South Asian region, especially in the field of security and threats in the physical world as well as in cyberspace is volatile and faces cyber threats like data breaches, hacktivism, and cyber espionage by various countries. This volatile situation is attributed to the minimal penetration rate of cyber technology coupled with limited awareness of cyber security [2].

Cyber incidents in Bhutan are often unreported because of low awareness of cyber threats, and potential disclosure mechanisms not being made clear to the population. If the entities are not encouraged to report cyber incidents, it will be difficult to design better responses and understand the threat and risk profile of the country. Also, the resource allocations, contingency plans and policy development, and building of capacities to mitigate and respond to cyber incidents will be affected thus, affecting the cyber resilience of the country against cybercrime [14]. Increased Cyberattacks on the IT infrastructure is a grave concern for organizations and cyber defense and cyber threat remediation have become the topmost priority of organizations. However, due to the lack of funding, knowledge, and skills, cybersecurity incident monitoring, detecting, and responding mechanisms are not put in place and thus the security incidents of organizations and agencies go undetected. The efforts to promote cybersecurity awareness and education among the public must continue at various levels – grassroots, technical, and managerial.

It is strongly pointed out by Dilipraj that Bhutan's cyberspace is infested with all sorts of malware and spyware, and individual internet users are prone to online scams, social engineering attacks, and phishing [2]. Bhutan faces a shortage of cybersecurity experts, and this void in security has created avenues for all sorts of cyber threats and intrusions into the country's cyberspace without being detected. Bhutan still grapples with key issues including limited human resources trained for cybersecurity coupled with the recent trend of employees resigning and leaving for better opportunities, making the recruitment and retention of skilled experts challenging. To contribute towards building of cybersecurity experts to meet the industry demand, there is a lack of institutions offering comprehensive cybersecurity education. There is a need to incorporate the curriculum and offer it as a viable programme by the Higher Educational Institutions in Bhutan.

The need for a customized National Cybersecurity Strategy (NCS), increased budgetary allocations for genuine software and hardware, enforcing strict regulations against pirated software and counterfeit hardware in all agencies for promoting genuine product usage, and the offering of viable cybersecurity curriculum is necessary for safeguarding Bhutan's digital infrastructure.

4 Conclusion

This study has taken a deep look into various sources of cybersecurity-related information on Bhutan, to analyse and provide an understanding of prevailing threats and vulnerabilities, initiatives, and strategies adopted by Bhutan to mitigate cybersecurity threats and identify challenges and opportunities for mitigating cyber threats. The analysis of the gathered data unfurled a multifaceted cybersecurity threat landscape of Bhutan. The study found that variants of malware, phishing attacks, and online scams in addition to the weaknesses and vulnerabilities of systems add up to the list of challenges that Bhutan faces currently. The human factor was identified as the critical vulnerability leading to the exposure of individuals and organizations for exploitation by the cyber attackers emphasizing the need and importance of cybersecurity education and awareness among the general public. Proactive measures such as strategies and initiatives for mitigation including awareness campaigns, regulatory enhancements, human resource capacity development, and collaboration are taken by the concerned agencies of Bhutan and its stakeholders with a strong commitment towards resilient cybersecurity. However, other challenges such as the lack of a national-level guiding strategy for cybersecurity, sufficient budgetary allocations, and strict enforcement of genuine software and hardware usage are significantly adding to the challenge. The findings of this study put forward valuable insights for policymakers, organizations, and individuals in Bhutan to have a proactive and resilient approach to cybersecurity.

References

[1] NSB, "Statistical Yearbook of Bhutan," National Statistics Bureau, no. October, 2022, [Online]. Available: https://www.nsb.gov.bt/publications/statistical-yearbook/.

[2] E. Dilipraj, "South Asian Cyber Security Environment: An Analytical Perspective Centre for Air Power Studies," in Asian Defence Review, 2014, pp. 161–190. [Online]. Available: https://www.researchgate.net/publication/333262265.

[3] T. Roberts, "Building Cyber-security Capacity in the Kingdom of Bhutan," SSRN Electronic Journal, 2015, doi: 10.2139/ssrn.3658397.

[4] N. Gyeltshen, "BoB transfers Nu 16M based on fake e-mail." [Online]. Available: http://www.bbs.bt/news/?p=59872#:~:text=AccordingtoofficialsfromtheaccountnumberoftheRAA.

[5] P. Choejey, D. Murray, and C. Che Fung, “Exploring Critical Success Factors for Cybersecurity in Bhutan’s Government Organizations,” in Computer Science & Information Technology (CS & IT), Academy & Industry Research Collaboration Center (AIRCC), Dec. 2016, pp. 49–61. doi: 10.5121/csit.2016.61505.

[6] K. Prasain, “Nepal moves up in global cybersecurity ranking,” Kathmandu Post. Accessed: Feb. 08, 2024. [Online]. Available: https://kathmandupost.com/money/2021/07/03/nepal-moves-up-in-global-cybersecurity-ranking.

[7] P. Dem, “Cybersecurity week emphasizes cyber safety,” Kuensel. Accessed: Feb. 08, 2024. [Online]. Available: https://kuenselonline.com/cybersecurity-week-emphasises-cyber-safety/.

[8] P. Seldon, “Securing Bhutan’s Cyber Security – The Bhutanese.” Accessed: Feb. 12, 2024. [Online]. Available: https://thebhutanese.bt/securing-bhutans-cyber-security/.

[9] P. Choejey, “Cybersecurity Challenges and Practices: A Case Study of Bhutan,” no. June, 2018, [Online]. Available: https://journal.scsa.ge/wp-content/uploads/2018/12/07-4.-tinatinmshvidobadze.pdf.

[10] BtCIRT, “National Cybersecurity Awareness Month 2023.” Accessed: Feb. 12, 2024. [Online]. Available: https://www.btcirt.bt/cybersecurity-awareness-month-2023/.

[11] K. Salamzada, Z. Shukur, and M. A. Bakar, “A framework for cybersecurity strategy for developing countries: Case study of Afghanistan,” Asia-Pacific Journal of Information Technology and Multimedia, 2015, [Online]. Available: http://www.ftsm.ukm.my/apjitm.

[12] International Telecommunication Union, “What we learned while developing Bhutan’s first National Cybersecurity Strategy - ITU Hub,” ITU. Accessed: Feb. 09, 2024. [Online]. Available: https://www.itu.int/hub/2020/11/what-we-learned-while-developing-bhutans-first-national-cybersecurity-strategy/.

[13] Bhutan Infocomm and Media Authority, “Study Report on Cybersecurity,” 2020.

[14] Royal Audit Authority, “Preparedness for Cybersecurity,” 2023. [Online]. Available: https://www.bhutanaudit.gov.bt//wp-content/uploads/2023/07/Final-PA-Report-on-Cybersecurity-9.5.23.pdf.

[15] A. A. Mughal and A. A. Mughal, “Building and Securing the Modern Security Operations Center (SOC),” International Journal of Business Intelligence and Big Data Analytics, vol. 5, no. 1, pp. 1–15, 2022, [Online]. Available: https://research.tensorgate.org/index.php/IJBIBDA/article/view/21.

[16] S. Tshering, “Bhutan’s cybersecurity lies in the use of genuine hardware and software,” Kuensel. Accessed: Feb. 07, 2024. [Online]. Available: https://kuenselonline.com/bhutans-cybersecurity-lies-in-the-use-of-genuine-hardware-and-software/.

[17] W. Ghafoor, “Enhancing Cyber Resilience: Challenges and Opportunities in South Asia,” vol. 41, no. 8, 2023.