འབྲུག་གཞུང་འཕྲུལ་རིག་ལས་སྡེ།
GovTech
Bhutan

BtCIRT
Bhutan Computer Incident Response Team

National Cybersecurity Strategy

2024-2029

Table of Contents

Abbreviation

BtCIRT	Bhutan Computer Incident Response Team
CIA	Confidentiality Integrity Availability
CIRT	Computer Incident Response Team
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CTF	Capture the Flag Challenge
COP	Child Online Protection
CSIRT	Computer Security Incident Response Team
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Cybersecurity
GovTech	Government Technology Agency Bhutan
ICMA	Information Communication and Media Act 2018
NCS	National Cybersecurity Strategy
MOU	Memorandum of Understanding
OT	Operational Technology
RGOB	Royal Government of Bhutan
SOC	Security Operations Center

 དཔལ་ལྡན་འབྲུག་གཞུང་།

Royal Government of Bhutan

Foreword

Bhutan is pivoting to a digitally transformed nation and is at a juncture of adopting emerging technologies for the advancement of economy, resiliency, preservation of our culture while navigating digitally originated threats. At this critical juncture, where there is a need to proactively mitigate the growing threats to our critical digital assets, I am honoured to write this forward for the National Cybersecurity Strategy of Bhutan, which cements our commitment to creating a secure and resilient digital ecosystem.

Digital transformation of Bhutan is the cornerstone for taking forward the society into a knowledge based society. The implementation of the National Digital Identity is a significant step toward securing government authentication measures and also ensuring the privacy of the digital citizens. However, the digital world is sophisticated and along with the advancement of technology the threat landscape is ever evolving. As we embrace the Digital Strategy for the Intelligent Bhutan, it is crucial to recognize the evolving cybersecurity threats and not take cybersecurity for granted and prioritise proactive vigilance to ensure the safety and security of digital infrastructure.

The National Cybersecurity Strategy outlines Bhutan's vision, goals and objectives. It will lay the foundation for instituting cybersecurity governance to ensure critical information infrastructure(CII) are safeguarded, timely dissemination of information and robust incident response capability is developed and resilient cybersecurity legislation is enacted to address threats and foster trust among the stakeholders. The Bhutan Computer Incident Response Team (BtCIRT) since its establishment in 2016 has been working to progress the cybersecurity posture of the country. With the Digital Transformation, BtCIRT now under the Cybersecurity Division of the Government Technology Agency (GovTech), will take the lead in the implementation of this Strategy and work with other government agencies, private sector entities and the corporate sector to achieve the goals of the National Cybersecurity Strategy.

As cybersecurity is a shared responsibility among many sectors and stakeholders, collaboration with academia, law enforcement agencies, regulators and all essential sectors is key. Taking a collective approach we will be able to help each other to protect the shared cyberspace of Bhutan to provide a safe and secure environment for many innovative endeavours of Bhutan.

(Tshering Tobgay)

Acknowledgement

The GovTech Agency would like to express its sincere gratitude to all the agencies and individuals who contributed to the development of the National Cybersecurity Strategy. Special thanks to the World Bank for their invaluable advisory support on National Cybersecurity Strategy Development and CII Protection made possible through the Cybersecurity Multi-Donor Trust Fund program.

This collaborative effort would not have been possible without the invaluable support of our key stakeholders, including a dedicated working group of representatives from various government, corporate and private agencies. Additionally, the consultative meetings with key stakeholders allowed us to gather valuable feedback and ensure that the strategy aligns with the needs and priorities of our nation.

We are also deeply grateful to the International Telecommunications Union for their initial support in 2018, which laid the groundwork for the development of this comprehensive cybersecurity strategy.

Contributors
Office of Attorney General
Royal Monetary Authority
Electricity Regulatory Authority
Bhutan Computer Incident Response Team, Cybersecurity Division, GovTech Agency

Executive Summary

The pace of digital transformation in Bhutan is rapid as evidenced by the various online services that have become available in Bhutan and the launch of innovative technology and services such as the national digital identity. The health and education sectors have started transitioning into online platforms. Generally, the use of electronic media and the internet has surged quickly after the Covid-situation. Bhutan's rapid pace of digital transformation is also building a strong foundation for increased digital trade and better integration into the global digital economy. These advancements heighten the nation's susceptibility to digital economy risks, primarily attributed to cross-border data sharing. Further, cyber threats such as phishing, identity theft, and breach of privacy, among others, have been on the rise, putting critical systems and data at risk. As such, the need for a strategic and holistic direction for cybersecurity preparedness of the country is due and urgent.

The National Cybersecurity Strategy (NCS) is the country's first cybersecurity strategy. Its purpose is protecting the cyberspace of Bhutan and preparing the nation to combat various aspects of cybersecurity risks and threats that could adversely affect people, businesses, and the government. The *Information Communication and Media Act* 2018 includes a chapter exclusively on Cybersecurity, and the 2019 eGovernment Policy statement -- "Information Privacy and Security" -- stipulates the development of a national cybersecurity strategy with the objective to secure the internet space.

The cybersecurity strategy envisions: "**To achieve a safe, secure, and resilient cyberspace for resilient Bhutan**" with the help of three guiding principles; 'Inclusiveness', 'Confidentiality', Integrity and Availability' of information (CIA Triad)[1], and 'Alignment with International and National best practices'. The strategy focuses on four strategic goals: 1) Establishment of Cybersecurity Institutional Framework for the Governance and Coordination, 2) Enhancement of Cybersecurity Legislation Framework, 3) Protection of National Critical Information Infrastructure, and 4) Robustness of Cybersecurity Incident Management. The accomplishment of these goals over a period of five years; 2024 to 2029 will lead to the achievement of the overall vision of NCS.

The institutionalisation of the cybersecurity governance framework is essential for seamless implementation of cybersecurity plans and activities. The governance would include the GovTech Commission overseeing the implementation of the Strategy, and the Secretaries of various ministries for cross-sectoral coordination and guidance.

Bhutan has one umbrella act catering to all facets of ICT, the Information, Communication, and Media Act 2018 (ICMA). With the advancement in technology and innovation, the inadequacy of the ICMA can be perceived. An extensive study in identifying the gaps in the ICMA was conducted in 2023 which recommends strengthening cybersecurity legislation. With this strategy in place, Bhutan seeks to strengthen its legislative framework and improve its response to cybersecurity threats.

[1] CIA Triad is a commonly used model that forms the basis of information security development.

The strategy emphasizes the protection of Critical Information Infrastructures of Bhutan, such as those in the Health, Energy, Transportation, Trade, Food, Financial and Telecommunications sectors which are dependent on ICT and the disruption of which would have an adverse impact on the nation.

The Bhutan Computer Incident Response Team (BtCIRT) was established in 2016 with incident management as the principal responsibility among other mandates. However, a number of incidents were not reported due to incognizance of the establishment of CIRT as the national contact for incident coordination and response. NCS identifies approaches to improve incident handling through collaboration among stakeholders, information sharing mechanisms, and awareness creation. In addition, creation of dedicated Security Operation Centers (SOCs) and sectoral CIRTs in critical sectors are perceived to increase protection mechanisms.

The implementation of the National Cybersecurity Strategy (2024 to 2029) will be spread across various Ministries, Agencies, Corporations, and the private sector with the aim to improve the cybersecurity maturity and cybersecurity culture of the country. The NCS will also pave the path for the development of a second comprehensive Cybersecurity Strategy in future.

Part 1: NCS

1. Background

The Bhutan Computer Incident Response Team (BtCIRT) was founded in 2016 to serve as the primary and national body for organizing cybersecurity efforts and acting as a central contact for all cybersecurity issues. Since its inception, the team has managed 1198 cybersecurity incidents till 2023 catering to various constituents, including the government, corporations, private sectors, general public, and international organizations residing in the country.

From the beginning, BtCIRT has prioritized cybersecurity capacity development initiatives for the country. Between 2016-2017, the BtCIRT initiated various awareness programs targeting the government officials. The team also observed ‘national cybersecurity week’ for three consecutive years starting 2021, in collaboration with banks, financial institutions, telecom operators, regulators, private sectors, and international organizations. Besides, the team also organized capacity development events for college students, in the form of Capture-the-flag (CTF) challenge, in 2022 and 2023 with support from the Asia Pacific Telecommunity (APT). The BtCIRT has adopted the CTF challenge as a yearly event alongside the observation of the Cybersecurity awareness week. Further, in collaboration with the International Telecommunication Union (ITU), a tabletop exercise and a cyber drill mirroring real scenarios were conducted in 2018 and 2022 respectively. Yearly, at least two technical workshops catering to various aspects of cybersecurity are conducted - more than 20 such workshops have been conducted till date. As part of a cybersecurity awareness building campaign, cybersecurity content in the form of animation and short videos was also produced and aired on national television.

In addition, the baseline cybersecurity guideline was developed in-house for the government agencies to ensure that minimum required application and network security is implemented to prevent trivial cyber threats. The Child Online Protection (COP) guidelines for various target groups were developed with support from ITU and UNICEF. The COP Guideline is to ensure that children are protected from cyber threats with collaborative approach among parents and educators, policy makers and the industry. BtCIRT became a member of the Forum for Incident Response and Security Team (FIRST) and the Asia Pacific Computer Emergency Response Team (APCERT) in the year 2017. In 2022, the team successfully became a member of the Global Forum on Cyber Expertise (GFCE) and the Cybersecurity Alliance for Mutual Progress (CAMP). BtCIRT is actively involved in all of these forums, including ITU, APT, Asia Pacific Network Information Center (APNIC), and the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC).

In December 2018, the BtCIRT-led team initiated the drafting of the National Cybersecurity Strategy (NCS). The final draft was developed in 2020 with the formation of a taskforce with members from various government agencies and corporations. Unfortunately, due to the unforeseen challenges brought about by the global pandemic and competing priorities, the approval of the NCS faced delays. As the prioritization of cybersecurity in Bhutan has grown over the years and now is one of the top priorities of the government, GovTech Agency renewed its efforts in NCS development in 2022. In order to update the NCS draft to an actionable document it was decided to focus on most pressing cybersecurity issues in Bhutan, prioritizing specific areas that are in most need of improvements, and resulted in this draft of the NCS.

The refined NCS is centered around four specific goals from the initial plan of seven, with a keen focus on expediting the objective of improving Bhutan's cybersecurity maturity level and aligning with available budgetary resources for the 13th Five Year Plan. This targeted approach reflects a strategic commitment to efficiency, ensuring that the NCS Action Plan is implemented in a manner that is financially sound and resource-effective. The narrowed focus on these key objectives underscores a deliberate effort to optimize outcomes and drive success within the established constraints. The four goals emphasize strengthening the cybersecurity ecosystem of the country. Firstly, the Strategy seeks to institutionalize the cybersecurity framework at a national level for seamless and coordinated governance, setting the policy, strategic guidance, its implementation and taking into account the necessity to monitor the changing landscape and providing additional guidance to the cybersecurity direction of the country.

The second is to strengthen the legal instruments by addressing any shortcomings related to cybersecurity of the existing Information, Communication and Media Act, and fulfilling the cybersecurity obligations outlined in the e-Commerce Policy 2023 and eGov Policy 2018. Thirdly, the Strategy seeks to initiate the protection of Critical Information Infrastructure (CII) of Bhutan by defining the necessary CII Identification methodology, designating the list of CIIs and creating CII Protection Roadmap, CII Regulations, and other relevant Guidelines. The fourth goal is to enhance the incident management framework with renewed emphasis on collaboration and cooperation among the incident response teams, police, Competition and Consumer Affairs Authority, and Regulators of finance, electricity, and telecom Service providers, alongside the formation of new governmental and sectoral security operation centers (SOCs).

The three strategic goals: Cybersecurity capacity and capability development; International and Regional collaboration and cooperations; and National Cybersecurity Guidelines that were defined in the earlier draft are already established and represent an ongoing effort with continuous progress. Therefore, they require less immediate national focus, unlike the four goals included in this strategy, the absence of which would significantly hinder progress towards achieving a higher level of Cybersecurity Maturity. In addition, the four prioritized goals build upon and complement those goals, forming a comprehensive roadmap for achieving cybersecurity maturity.

2. Vision

"Towards a safe, secure, and resilient cyberspace for resilient Bhutan."

3. Mission

"To strengthen Bhutan's cybersecurity by establishing a robust cybersecurity ecosystem, and enhancing capabilities to prevent, detect, and respond to evolving cyber threats."

4. Scope

The Strategy encompasses the development of governance and coordination frameworks, strengthening the existing legal frameworks, identification and protection of critical information infrastructure, and enhancement of incident handling capability. As such, the scope of this Strategy extends to all people, businesses, government, and international agencies within the country.

5. Guiding Principles

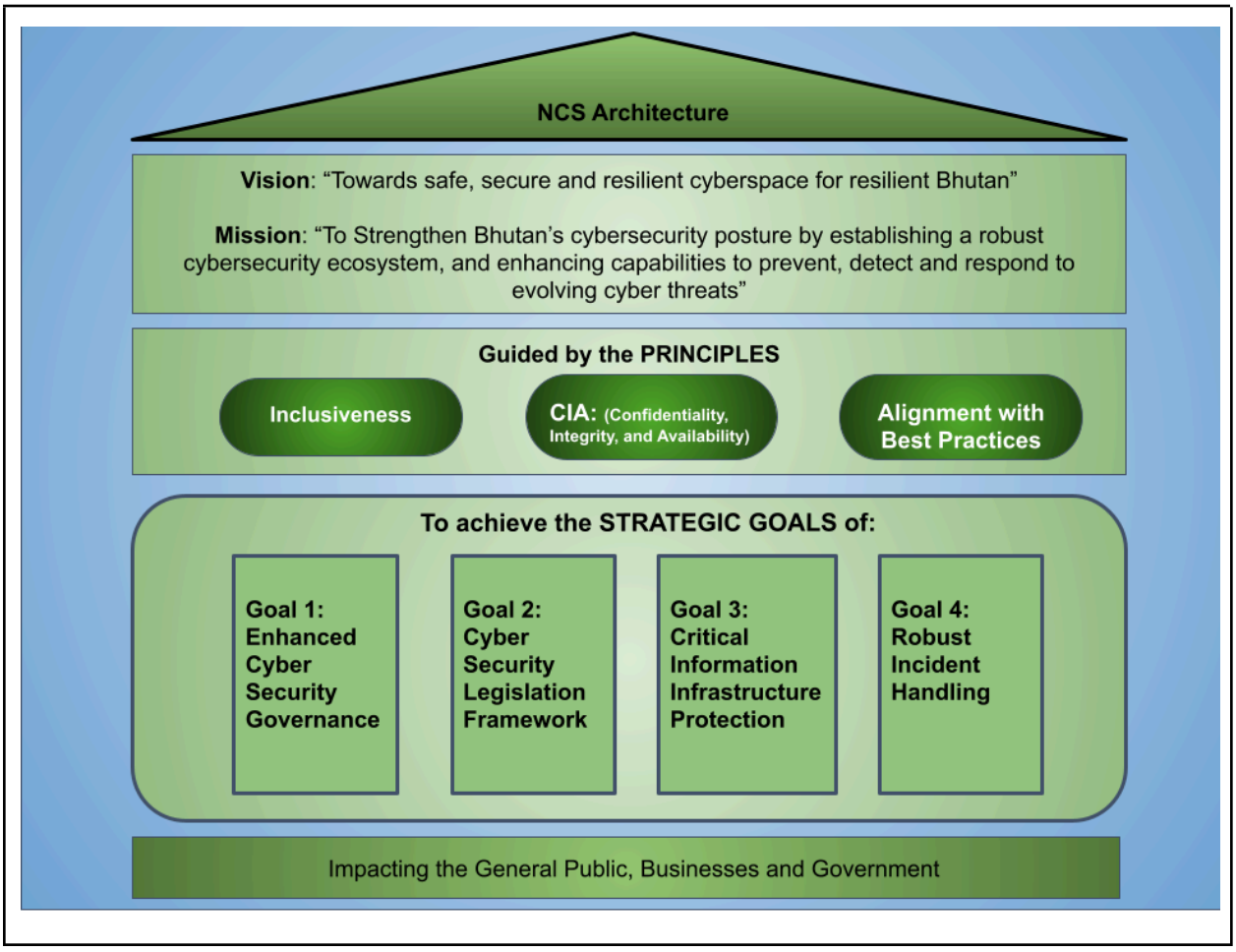


Figure 1: Guiding principles and strategic goals

The initiatives in the NCS are guided by three overarching principles as provided hereunder:

6. Principles

6.1. Inclusiveness

The Strategy embraces inclusiveness as one of its guiding principles. This entails engagement across a spectrum of stakeholders, from government agencies to private entities and other stakeholders. By fostering an inclusive approach, the strategy ensures a comprehensive and robust cybersecurity framework that draws upon diverse perspectives. It ensures stakeholder participation and collaboration across various sectors, fostering a collective responsibility towards building a robust national cybersecurity.

6.2. Ensure Information Security: Confidentiality, Integrity, and Availability (CIA)

In consonance with Bhutan's commitment to safeguarding fundamental rights, the critical triad, encompassing confidentiality, integrity, and availability, forms one of the overarching principles that guide this Strategy. This furthers Bhutan's resolve towards establishing a robust cybersecurity framework and enhancing cyber resilience by upholding the highest standards of cybersecurity, safeguarding the confidentiality of information, maintaining its integrity and ensuring its availability.

6.3. Alignment with International and Regional Best Practices

A fundamental guiding principle of the Strategy is the adherence to international best practices. In recognition of the inherently global nature of cyber threats and vulnerabilities, the Strategy seeks to harmonize its approach with established international standards. By closely aligning with globally recognized best practices, Bhutan seeks to leverage the collective wisdom of the international community in enhancing its cyber resilience. The integration of international best practices underscores Bhutan's dedication to highest standards of effectiveness in fostering a secure cyberspace.

7. National Cybersecurity Strategy (NCS) Governance Framework

A NCS governance framework is crucial for the effective development and implementation of the NCS itself. By establishing a coordinated approach, the framework facilitates collaboration among diverse stakeholders, including government and private agencies.

The NCS Governance Model is created to ensure the successful implementation and monitoring of the four strategic goals. The newly created GovTech Commission via letter number RCSC/LTD/1/COM/2023/1223[2] will be leveraged to govern the NCS lifecycle and the action plans along with any other issues related to cybersecurity. The commission was established as the highest advisory body for the GovTech to provide policy advice to the Royal Government of Bhutan (RGOB) to champion the development and implementation of Whole of Nation/Government ICT and emerging technology policies and programmes. The GovTech Commission will also serve as the highest technical advisory body to manage and guide the GovTech Agency in the implementation of all major technology programs, including Cybersecurity programs of the RGOB. Its functions include reviewing and approving policies relevant to ICTs and emerging technologies, and provide strategic oversight and guidance to GovTech Agency, including the cybersecurity mandate, among other functions. The commission is chaired by the Hon'ble Prime Minister with four permanent members: 1. Coordinating Secretary, Governance Cluster; 2. Representatives from the office of Gyalpoi Zimpon/HMS; 3. Secretary, GovTech; and 4. Chief Technology Officer, Druk Holding and Investment (DHI). The member secretary of the GovTech Commission is the Director of GovTech.

The commission will monitor the implementations of NCS, approve any major deflections of the NCS Action Plan and advise in case of any unforeseen circumstances that might arise during the period of

implementation. The Commission will appoint GovTech as the lead Project Authority for NCS. GovTech is also mandated by the ICMA 2018 and as per the recommendations from the 'Performance Audit of Cybersecurity Preparedness of the country' to coordinate the development of national strategy.

The Advisors are the stakeholders from a spectrum of agencies to support, advise, and assist the Cybersecurity division within the GovTech Agency. The support expertise shall be in the areas of legal advice, government procurement, critical infrastructure regulations, and human resource availability. They will provide recommendations to the GovTech Commission for making necessary decisions.

The Cybersecurity Division under the GovTech Agency will take up the responsibility of planning, stocktaking, risk profiling, and consolidation of the NCS Action Plan, and half-yearly reporting to the GovTech Commission. Three years after the NCS approval, the GovTech in consultation with the Advisory Panel will lead the development of the next cybersecurity strategy.

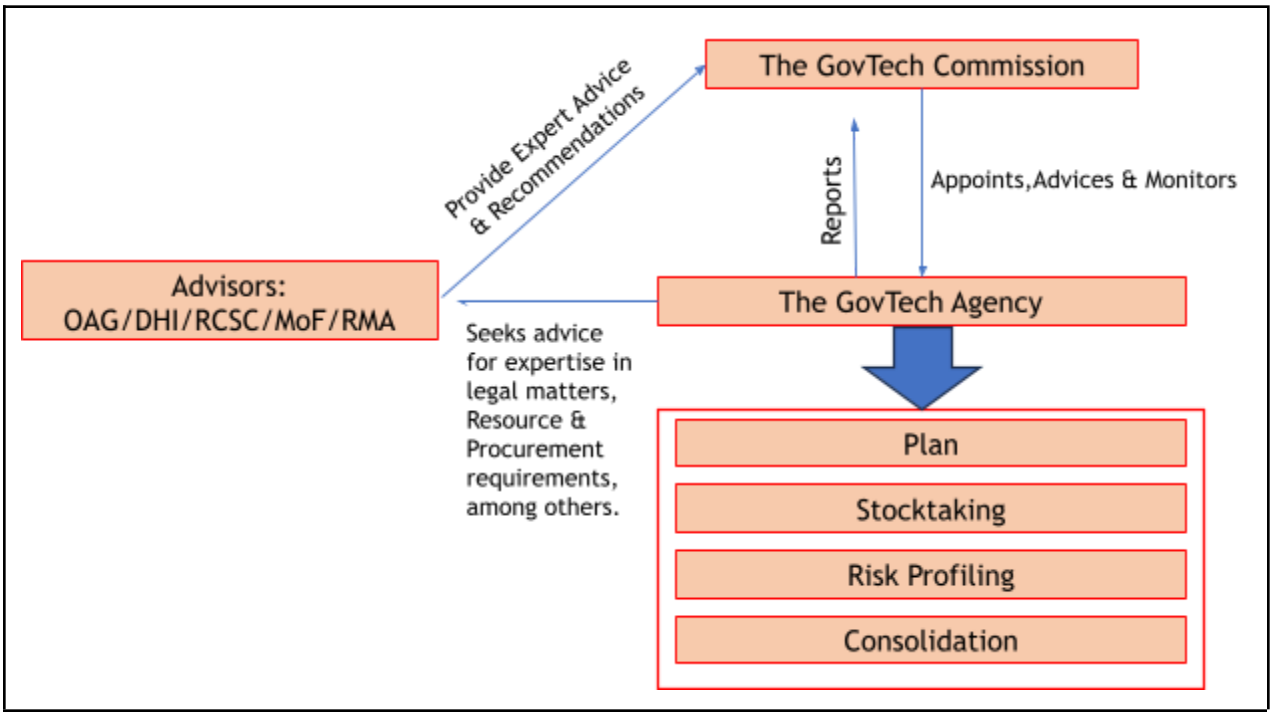


Figure 2: NCS Governance Model

8. Cyber Threat Landscape in Bhutan: A Call for National Strategy

As Bhutan embraces the transformative shift towards a technology-centric future, embracing digital frontier and migrating essential systems online, it has become imperative for Bhutan to acknowledge and address the increasing cybersecurity threats and vulnerabilities that accompany this shift. Bhutan faces increasing regional and worldwide cyber risks despite its distinct cultural and geographical setting.

Developing a successful National Cybersecurity Strategy requires not just an awareness of global trends but also an understanding of the specific issues that Bhutan faces in cyber defence.

8.1. Global Trends in Cyber Threats:

Ransomware attacks against critical information infrastructure are becoming more and more frequent on a global scale. The findings from the ENISA (The European Union Agency for Cybersecurity) Threat Landscape (ETL) report[2] for 2023 underscore a dynamic and evolving cybersecurity landscape where DDoS attacks and ransomware are identified as paramount threats, reflecting a persistent risk to digital infrastructure. Attackers are using cutting-edge techniques to encrypt data and demand astronomical ransom payments, seriously disrupting operations and causing significant financial losses. Ransomware attacks targeting critical information infrastructure have skyrocketed with healthcare facilities experiencing a 75% increase in such attacks in 2023 compared to 2022. Attackers are employing sophisticated encryption algorithms, making data recovery near impossible without the decryption key leaving the victims with a stark choice of paying the ransom or risk facing crippling downtime. The rise of "double extortion" tactics has added another layer of fear as the attackers not only encrypt data but also threaten to leak it publicly, inflicting immense reputational damage. Ransom demands are also reaching staggering heights. For instance, in 2023, a single attack on a U.S. pipeline operator demanded a whopping $4.4 million in cryptocurrency. Many organizations, especially small and medium-sized ones, simply cannot afford such exorbitant sums. Paying up can cripple their finances and even force them to shut down. The disruption caused by these attacks can have cascading effects, impacting entire economies and jeopardizing public safety.

Nation-states are now engaged in a digital cold war where they relentlessly hunt for valuable secrets, stealing confidential data from research institutes and government agencies with alarming frequency across the globe. The prize in this digital war is not oil or gold, but information. However, the ultimate goal is not just information but strategic advantage. Stolen data can influence negotiations, expose vulnerabilities, fuel economic and military dominance, gain insights into scientific advancements and disrupt vital operations and erode trust between nations weakening diplomacy. The 2023 Cyberattacks on Japanese space agency JAXA underscores the continued targeting of critical infrastructure sectors such as space by nation-state actors.

Phishing, social media manipulation, and other social engineering tactics are becoming increasingly sophisticated, tricking users into revealing confidential information or downloading malware. These tactics are slithering through the digital landscape with ever-increasing finesse, leaving a trail of breached data and shattered trust. Deep fakes, spear phishing, fake news have all blurred the lines between reality and fabrication, influencing people's opinion and making it difficult to judge genuine sources of information. The recent The LinkedIn "Deepfake" CEO Scam in 2023 where hackers created a deep fake video of its CEO asking employees to transfer money urgently, highlights how easily people can be tricked into social engineering scams. In this particular incident, the video was so convincing that some of the employees complied resulting in significant financial loss on their part.

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

8.2. Regional Trends

Bhutan might seem like a peaceful haven far removed from the digital shadows of cybercrime. However, its geographical proximity to South Asia, a hotbed of cybercriminal activity, makes it vulnerable to regional threats. Hacking groups operating in neighboring countries have increasingly targeted businesses and government institutions across the region, and Bhutan is no exception.

Cybercrime in South Asia often operates across borders, with hacking groups leveraging shared languages, cultural similarities, and interconnected infrastructure to launch attacks across multiple countries. For instance, there have been cases where Bhutanese people have been tricked by fraudsters and scammers originating from the region.

Bhutan's geographical proximity to South Asia exposes it to regional cybercrime activities. Hacking groups operating in countries in this region have been known to target businesses and government institutions across the region[3].

Several South Asian nations are facing targeted attacks on their critical information infrastructures with instances of hacktivist groups ramping up cyberattacks in the region, motivated by politics and religion. Since June of last year, more than 750 distributed denial-of-service attacks (DDoS), as well as over 70 defacement attacks were reported with Thirty-four percent of those targeting India which is the highest number[4].

8.3. Incidents Reported

While a comprehensive assessment remains crucial for gaining a deeper understanding of the evolving threat landscape, the dynamic threat environment, as evidenced by the diverse incidents and vulnerabilities (1184) handled by BtCIRT from 2016 to 2023, necessitates the immediate development and implementation of a robust National Cybersecurity Strategy (NCS).

Of the total cyber incidents, 839 incidents were vulnerabilities detected in applications systems, which was the highest category every year. It is understood that the vulnerable systems like misconfigurations and use of vulnerable versions of software are widespread. Other incidents are related to phishing and frauds through social media.

[3] https://therecord.media/chinese-military-hackers-redhotel-target-countries-across-asia-north-america-europe
[4] https://therecord.media/bangladesh-hacktivistis-targeting-india

Incident Category	2016	2017	2018	2019	2020	2021	2022	2023	Total
Abusive Content	3	6	4	-	4	2	5	1	**25**
Availability	-	2	-	-	-	-	-	1	**3**
Fraud	-	3	2	4	5	12	31	21	**78**
Information Gathering	5	1	-	-	1	-	1	-	**8**
Information Security	-	14	5	4	8	7	12	14	**64**
Intrusion Attempts	1	4	2	1	-	1	1	-	**10**
Intrusion	4	4	3	4	8	2	11	13	**49**
Malicious Code	18	8	19	23	3	6	3	5	**85**
Vulnerability	150	81	184	45	86	75	113	105	**839**
Infected System	1	1	-	3	18	-	-	-	**23**
Total	**182**	**124**	**219**	**84**	**133**	**105**	**177**	**160**	**1184**

Table 1: Incident statistics from 2016-2023

An analysis of the current threats identified by the BitSight[5] Threat Intel platform reveals that Bhutan's digital infrastructure, mainly the government and education network, remains susceptible to vulnerabilities. These include open ports, ineffective patch management, and reliance on legacy systems. Moreover, our vulnerable internet space makes the netizens of Bhutan a prime target for cybercriminals, particularly those specializing in exploiting outdated infrastructure and weak security protocols. Another critical threat that has been lurking within the cyberspace of the country is fraud, scam and social media related incidents. Over the years, the BtCIRT has recorded more than 100 cases related to scams where some of the reporters were victims of financial loss, defamation, and extortion.

8.4. *Threat landscape of Financial Sector*

The Financial Institution Cyber Response Team (FICRT) was formed in 2020 at an information sharing level. Since then, the banks and Financial Institutions (FIs) have faced various cyber incidents among the customers. The majority of the reported incidents were online investment scams related to Crypto-currency.

[5] Bitsight is the Threat Monitoring and scoring platform provided to the BtCIRT by the International Telecommunication Union through the Cyber4Good program.

8.5. *Threat landscape of Power Sector*

The power companies in the country were also affected by cyber attacks. So far, the impact of the attacks has not been severe due to the existing business continuity plan. However, the companies need to be prepared to withstand the emerging and sophisticated cyber threats. In terms of the overview of cyber incidents, the power sector had two cases of ransomware attack and a case of email accounts of users being compromised resulting in the spamming of the mail server.

The escalating cyber attacks targeting the power infrastructure and the increasing vulnerability of its advanced smart technologies is deeply concerning. These threats pose a real risk of causing widespread blackouts, data breaches, and disruptions to critical services. To safeguard its vital operations and mitigate potential national security risks, the sector urgently needs to adopt proactive measures like implementing robust cybersecurity controls and collaborating with government agencies to develop comprehensive protection strategies.

8.6. Why Bhutan Needs a National Cybersecurity Strategy

A comprehensive strategy will ensure that Bhutan effectively tackles the ever-evolving landscape of cyber threats, taking proactive measures to mitigate both present and future cyber-attacks. As we continue to digitize government as well as other critical services, our reliance on digital technologies necessitates robust protection of critical information infrastructure sectors like ICT, Banking and finance, Health and Energy.

Having a cybersecurity strategy will also foster collaboration with international partners facilitating sharing of intelligence and best practices to combat international cybercrimes. This would result in a resilient and secure cyberspace, cultivating trust and confidence, attracting foreign investment and promoting innovation in Bhutan's digital economy. This also aligns with our GovTech Agency’s vision and mission of creating a safe and thriving digital economy.

8.7. Continuous development of the threat landscape

It is imperative to recognize that the threat landscape is a fluid and constantly shifting environment. As technology advances, threat actors adapt and develop more sophisticated tactics, necessitating a proactive approach to understanding and mitigating emerging risks. To stay ahead of the curve, future strategies will focus on refining our comprehension of incidents through the implementation of a robust incident reporting mechanism. This system will facilitate the collection of real-time data, enabling a swift response to emerging threats.

Additionally, fostering increased cooperation with Critical Information Infrastructures (CIIs) operators will be of prime importance, promoting information sharing and collaborative efforts in enhancing cybersecurity resilience. Concurrently, a dedicated effort towards awareness raising will empower organizations and individuals to recognize and respond effectively to evolving threats, contributing to a more resilient and secure digital landscape. By embracing these proactive measures, we will adapt to the evolving threat landscape and fortify our defenses against the challenges of tomorrow.

Part 2: The Strategic Goals

National Cybersecurity Strategy Goals

The goals of the National Cybersecurity Strategy are:

i. To enhance National Cybersecurity Governance and Coordination through Cybersecurity Institutional Framework

ii. To strengthen the cybersecurity legislation framework in Bhutan while dealing with cybersecurity incidents and cybercrimes.

iii. To protect the Critical Information Infrastructure of Bhutan to prepare them to be resilient.

iv. To enhance Incident Response with better collaboration, cooperation among stakeholder and capabilities.

Goal 1 - To enhance National Cybersecurity Governance and Coordination through a cybersecurity institutional framework.

Objective:

- Strengthen National Cybersecurity governance and coordination to effectively address the dynamic landscape of digital threats. This involves elevating the status of cybersecurity to the highest executive level, underscoring its strategic significance.
- Precise definition of roles and responsibilities, ensuring a coordinated and responsive approach to cyber threats that includes active participation from government agencies, private sector entities, and pertinent stakeholders.
- Implementation of accountability measures within this streamlined framework is essential, providing a systematic approach to monitor and assess the efficacy of cybersecurity initiatives.

To facilitate the establishment of a robust national cybersecurity framework, Bhutan must create an enabling environment for cohesive efforts by integrating diverse stakeholders at different levels of decision making and ensuring their collaboration and coordination. This coordination is vital for efficient resource allocation, enabling decision-makers to prioritize investments based on risk assessments and strategic imperatives. The framework will guide the development and implementation of cybersecurity policies, ensuring their alignment with national objectives and adaptability to the dynamic threat

landscape. Therefore, the development of a cybersecurity institutional framework, with clear roles and responsibilities, in collaboration with stakeholders cannot be overstated.

The Bhutan Computer Incident Response Team (BtCIRT) is the central point of contact for all cybersecurity matters pertinent to national security in the country. However, when it comes to other roles and functions which are beyond the authority of BtCIRT, there is a lack of clarity in determining the responsible authority due to transformation exercises which have resulted in significant restructuring of government agencies, including autonomous bodies. As such, it is necessary to take into account the transformative changes when devising the institutional framework.

i. Establishment of a Cybersecurity Institutional Framework

The cybersecurity institutional framework shall be based on a centralized model, adapting to the overall transformation of the government structure. During the development of the institutional framework the main attention will be placed on clearly defining the roles and responsibilities of each of the entities involved in cybersecurity on different levels (government, strategic, operational and tactical) and on establishment of the working processes for each entity, what concerns cybersecurity, and accountability and coordination mechanisms. Specific considerations will also be made concerning CII protection governance (details in Goal 3) and Incident handling governance mechanisms (details in Goal 4).

At the top government level will be the ***Cabinet***. The Cabinet will provide strategic guidance, mandates, approval of roles and responsibilities of stakeholders, and endorse cybersecurity policies and regulations, specifically the crisis management plan for the nation and resolve high level issues. Right below the government level, the Strategic level body will formulate cybersecurity policy, organize, monitor, and control the implementation of the plans outlined by the government. It will determine the cybersecurity strategic goals, progress, objectives and necessary measures to be achieved. The strategic level entity will be ***the GovTech Commission*** which was established as the governing and advisory body for matters pertaining to ICT. When formulating cybersecurity policies, strategies, and other plans, the GovTech Commission shall work in close consultation with the Secretaries of various ministries.

The implementers shall be at the operational level and shall comprise of all key stakeholders as determined by the GovTech Commission, including ***BtCIRT, Cybersecurity Division-GovTech, Royal Monetary Authority, Bhutan InfoComm & Media Authority, the Electricity Regulatory Authority (ERA), Competition and Consumer Affairs Authority, and Royal Bhutan Police.***

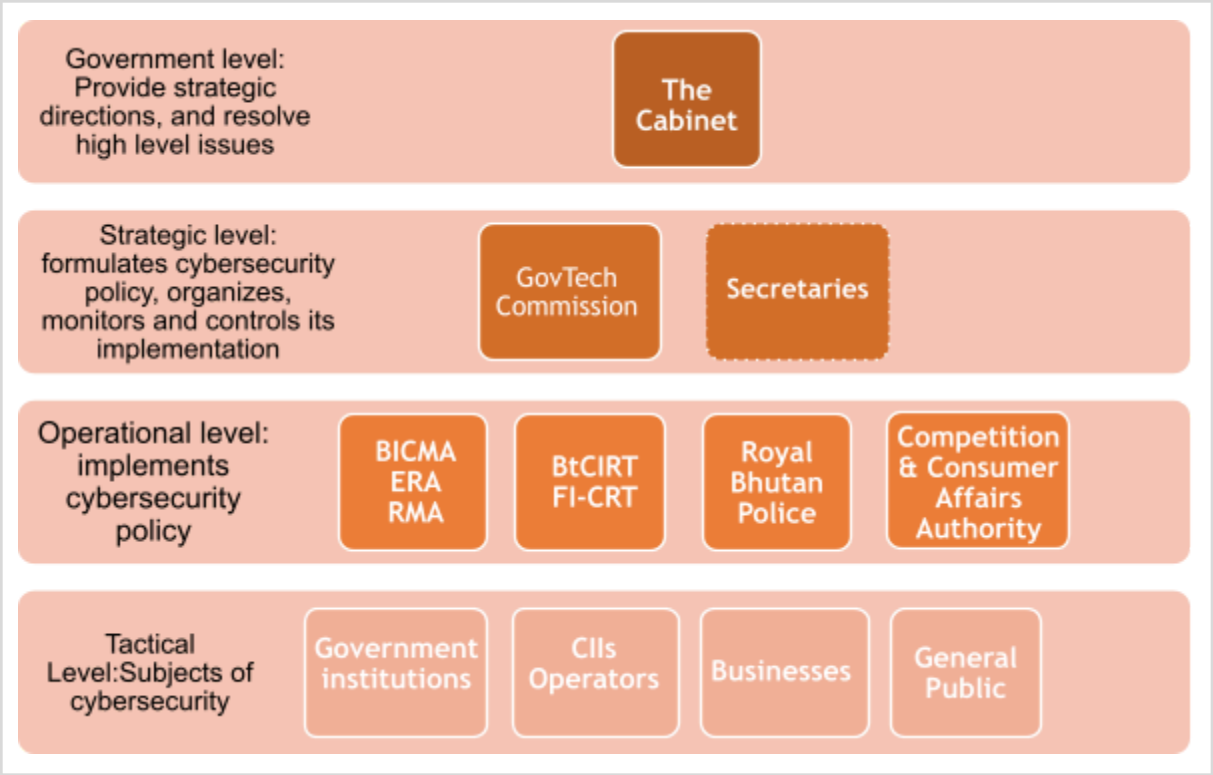


Figure 3: Stakeholders at different levels of the Institutional Framework

At the lowest level shall be the tactical level, comprising the subjects of cybersecurity. At the tactical level, there will be critical information infrastructure (CII) operators, Government institutions, private and corporate entities, and the general public, among others. Where CII operators will have mandatory obligations once the government designates them as CIIs.

For successful development and implementation of the Cybersecurity Institutional Framework with clear roles and responsibilities at operational level, the GovTech Agency shall initiate the formation of a working group which shall be responsible for drafting the Cybersecurity Institutional Framework of Bhutan and developing the Terms of Reference (ToR).

To accelerate the implementation of action plans to achieve the goals of this Strategy, the GovTech Agency shall submit a proposal to the GovTech Commission for the establishment of a Cybersecurity Institutional Framework, through an executive order by the government. The executive order will be then incorporated into the revision of the ICMA 2018 or through new regulations which is provided in detail in goal 2. Cybersecurity legislation.

Similarly, wherever relevant, working groups will be formed to implement the NCS plans such as during the development of CII Protection regulatory framework, legislations projects and incident handling among others. Various Memorandums of Understanding (MoU), or other equivalent documents will be initiated among BtCIRT and other sectoral SOC/CIRTs and law enforcement agencies to ensure seamless handling of incidents. The MoUs will set forth necessary roles and responsibilities to be undertaken during the event of handling incidents.

The **outcome** of this strategic goal will be an approved Cybersecurity Institutional Framework of Bhutan, including definitions of entities, their roles, responsibilities and accountabilities, and work processes and cooperation mechanisms.

Goal 2 - To strengthen Bhutan's cybersecurity legislation framework for dealing with cybersecurity incidents and cybercrimes.

Objectives:

- To establish institutional framework through legislation
- To address prevailing needs and gaps pertaining to cybersecurity and cyber incidents handling
- To establish statutory obligations, standards, and safeguards to protect CIIs, strengthen cybersecurity, and provide incident response services
- To enhance law enforcement capabilities to investigate and prosecute cybercrime and to promote international cooperation
- To address other legal gaps in the existing legislation

Considering the dynamic and evolving nature of cyber threats and vulnerabilities and with critical infrastructures being more interconnected now than ever, creation of an enabling environment that can effectively respond to these emerging risks is imperative. To do so, strengthening the legislative framework and ensuring its agility to address the dynamic landscape of cyber threats is indispensable. A robust cybersecurity legislative framework will not only ensure that legal mechanisms are in place to promptly respond to cyber incidents, but also facilitate law enforcement efforts against cybercrimes, thereby contributing to the overall national cybersecurity and resilience.

In order to strengthen the cybersecurity legislative framework, it is important to understand the limitations within the existing laws and identify gaps that may impede comprehensive cybersecurity efforts. As such, a nuanced examination of the scope and limitations of existing laws is fundamental in determining the areas that need amendment or enhancement for a robust cybersecurity legislative framework.

i. Enactment of a robust legislation on Cybersecurity

While Bhutan lacks a specific legislation dedicated to cybersecurity, existing legislation such as the Information, Communications and Media Act of Bhutan 2018 ("ICMA") provides broad provisions on cybersecurity (through Chapters 20 and 21), thus, establishing the foundation for addressing cyber threats and protecting digital assets. Besides, the National Digital Identity Act of Bhutan 2023 ("NDI Act") also furthers personal data protection and imposes transparency obligations on concerned entities for cybersecurity incidents related to digital identity. The E-Commerce Policy also paves the way for robust consumer data protection requirements.

The ICMA features a comprehensive chapter on cybercrime, enumerating a number of computer-integrity offences, content-related offences, contact-related offences, and computer-related offences. The Act also criminalises acts such as cyberterrorism and unauthorized interception or access to CIIs, among others. However, with the evolving nature of cyber threats, there is a need to reassess and augment the existing legislation to address the emerging challenges.

Concerning the mechanisms for investigation and prosecution of cybercrimes, the ICMA authorizes the police to access computer data for investigation and ensures the admissibility of data messages. The Evidence Act of Bhutan 2005 also provides for legal recognition of electronic records. However, as pointed out by the World Bank in its Report on the Gap-Analysis of the ICMA, the Act is not sufficient in enabling our law enforcement agents to carry out investigations in cyberspace. As such, besides the need to improve communication, collaboration and compliance mechanisms, there is also a need to enhance mechanisms for investigation and prosecution of cybercrimes to enable digital investigation, among others. Besides, there is also a need to strengthen child care and protection provisions pertaining to digital exploitation and address other gaps pertaining to data protection and cybersecurity in the existing legislation.

To address the legal gaps and strengthen the cybersecurity legislative framework, it is crucial to establish a robust cybersecurity legislation. This can be achieved either through amendment of the ICMA or by introducing a stand-alone legislation specifically dedicated to cybersecurity. Regardless of the chosen approach, the GovTech will need to carry out a Legislative Impact Assessment and propose the amendment to the Act or enactment of a new legislation with clear policy guidelines.

ii. Adoption of Regulatory Frameworks to strengthen cybersecurity

Whilst acknowledging the legal gaps that require legislative attention, it is important to note that there are provisions within the ICMA that cater to cybersecurity concerns. Given the protracted procedures and requirements inherent in the amendment and enactment of laws, there should be measures in place to concurrently attend to prevailing needs and gaps. The ICMA and the Civil Service Reform Act of Bhutan 2022 empower the GovTech Agency and the GovTech Commission to develop and adopt rules, regulations, and policies for the purpose of giving full effect to relevant provisions under the ICMA. Accordingly, within the purview of the existing authority, the GovTech will formulate regulatory frameworks to address immediate needs and gaps. One such critical regulatory framework is Critical Information Infrastructure Protection which is the core component of Goal 3, addressing the gap such as the lack of provisions of CII protection in the current legal framework, including the lack of obligations of cyber incident reporting by CII operators covered in Goal 4. Another is the Data Privacy and Protection Framework can be one such measure to address the data privacy and protection, including the handling of sensitive data breaches. Coordinated Vulnerability Disclosure (CVD) Policy can be another, to enable responsible discovery, reporting, and remediation of security weaknesses and other vulnerabilities in software, hardware, or digital systems - a must in the ever-evolving technology landscape. Likewise, the GovTech may adopt other such regulatory frameworks, policies, or regulations consistent with and within

the purview of the existing legislation until such time as the ICMA is amended or a new legislation on cybersecurity is enacted.

The **outcome** of the implementation of this strategic goal will provide Bhutan with clearly defined responsibilities of strengthening the cybersecurity in the country and enable institutions to react to cyber threats and cybercrime in appropriate manner which includes CII Protection regulatory framework and Coordinated Vulnerability Disclosure policy.

Goal 3 - To protect the Critical Information Infrastructure of Bhutan to prepare them to be resilient.

Objectives:

- Identifying the CIIs in Bhutan and developing a robust CII Protection framework in Bhutan.
- Identify and mitigate potential risks and vulnerabilities within the CII.
- Build the capacity and skills of personnel responsible for managing and securing the CII.

As per the ICMA 2018, the Critical Information Infrastructure (CII) is defined as the essential ICT services, infrastructure, and media facilities that underpin Bhutan's society and serve as a backbone of the national security, economy, public health, social welfare, and safety. Therefore, the failure or limited operation of the critical information infrastructure would significantly impact the vast majority of citizens.

With this Strategy, the government will lay the foundation to increase the ability of networks and information systems operated or utilized by CII providers to safeguard against malicious attacks that can compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system.

i. Development of Critical Information Infrastructure Identification methodology and designation of CII

In line with Section 381 of the ICMA which provides for declaration of critical information infrastructure, the identification of CII shall be carried out by the GovTech Commission in consultation with stakeholders, including BICMA. According to this, the BtCIRT, Cybersecurity Division, under GovTech will develop a methodology to identify CII in coordination with the stakeholders.

ii. Establishment of CII Protection (CIIP) Regulatory framework

The GovTech Agency shall initiate the development of a regulatory framework consisting of relevant regulations, policies, and standards to protect critical infrastructure (CII) from cyberattacks, physical threats, and natural disasters. It will help ensure the continued delivery of essential services of Bhutan such as energy, healthcare, financial and telecom systems among others. The framework will introduce the CII governance body to govern the implementation of CII protection plans.

a. CIIP Governance

With the Cybersecurity Institutional Framework establishment, the CII governance will be the responsibility within the framework. Hence, CII governance will be led by the GovTech Commission, as the steering body for the protection of CII. The critical information infrastructure are the concerns at the national level and the task could be performed by both public and private entities in the country. The highest authority for endorsement of CII Identification, review of CII list, endorsement of CII guidelines and regulations will be the Cabinet.

At the operational level, the BtCIRT/Cybersecurity Division will take the responsibility of leading the development and implementation of CIIP Roadmap in close coordination with the regulators of different critical sectors of the country. With the known essential services of the country, regulators: Royal Monetary Authority; Electricity Authority and the Bhutan Infocomm and media authority are the identified key regulators to implement the CIIP. Nevertheless, during the actual CII identification and designation process, any new authority/ regulator identified will be added to the CII governance body. In the CII governing body structure the CII operators are at the tactical level and the beneficiaries for CII obligations and support.

iii. Develop CIIP Guidelines

The CIIP guidelines play a crucial role in proactively protecting CII by enforcing obligations upon CII operators. On the government side obligations will fall upon GovTech which hosts most of the government systems and networks. These obligations ensure they implement and maintain the minimum security standards, procedures and human resource capacity required to safeguard critical infrastructure. Therefore, developing effective CIIP guidelines is key, as it will clearly define cybersecurity requirements and obligations for GovTech and CII operators, along with robust enforcement mechanisms to guarantee adherence to CIIP regulations and protect vital infrastructure.

iv. Capacity Development and Exercises for CII operators

The Identification of CII and designating its operators are to ensure that the assets are properly secured. This goal can be strategically achieved through the provision of necessary training and capacity building including exercises such as Tabletop exercises to manage a crisis or real scenario based cyber drill to prepare the operators for serious attacks. However, before the CII operators take up the technical training it would be paramount to train them on aligning to the CIIP guidelines. The detailed plan will be reflected in the CIIP roadmap.

v. Compliance to CII requirements

To ensure CII operators have implemented the CII requirements, the Cybersecurity division and relevant agencies will develop a Compliance framework and the members of the division will conduct the compliance audit examinations regularly as per the roadmap of CII protection.

The **outcome** of this strategic goal will be identified and designated CII that are aware of the reasons they are designated as such, as well as clear definitions of the governance framework of CII in Bhutan. Clear

policies and guidelines will be introduced to strengthen the security of the CII in Bhutan and all the stakeholders will be socialised with the new regulations in order to be capable and accountable in fulfilling them.

Goal 4 - To enhance Incident Response with better collaboration, cooperation among stakeholders and capability development of incident responders.

Objectives:

- Enhance the overall effectiveness of incident response procedures.
- Encourage and promote better collaboration among stakeholders involved in incident response efforts.
- Develop stronger relationships and communication channels among incident response stakeholders.
- Enhance the skills and capabilities of incident responders to effectively handle and mitigate cyber incidents.

In an era where cyber threats are dynamic and sophisticated, a robust incident response framework ensures that the nation can promptly monitor, detect, respond, mitigate, and recover from cyber incidents. Swift and effective responses not only minimise the impact of attacks but also protect sensitive data, critical systems, and national security interests. It enables the nation to adapt to evolving threat landscapes, facilitates coordination with local and international partners, and ensures compliance with regulatory requirements. Continuous improvement of the incident response framework through regular training, drills, and lessons learned from past incidents strengthens the nation's ability to withstand and recover from cyber threats, ultimately contributing to its overall security and stability.

Creating a resilient and responsive cyber secure environment depends on many factors, including a skilled and coordinated workforce across all stakeholders. While increasing and maintaining skills is a continuous process, achieving a robust cyber defence begins when citizens, businesses, and governments are encouraged to report cyber incidents to BtCIRT. The CII operators, however, are obliged to report incidents and their Incident Response capacity needs to be enhanced. Institutionalization of the incident response framework allows responding to incidents systematically, helps personnel to minimize loss or theft of information and disruption of services caused by incidents, and enables BtCIRT to use information gained during incident handling to better prepare for future incidents.

One of the incident management elements to develop, in the framework of the strategy, is the accountability mechanism. The owners and operators of critical information infrastructure shall be obliged to report every incident in a specific template with necessary timeframe for the CII operators for record keeping and analysis for preparing threat landscape at a national level. The CII Protection

Regulations shall set out obligations for CII operators to ensure effective defence against information security threats.

i. Capacity development for enhancement of Incident Response and Investigation

Enhancement of cybersecurity Incident handling cannot be achieved without the required capacity and capability development among every party involved. This includes the nodal agency BtCIRT/Cyber Security Division, the Royal Bhutan Police, sectoral SOCs/CIRTs. A capacity building plan including the training for key expertise like SOC Tier 1 and 2, Incident Handling, Forensics, Red Teaming and Blue Teaming among other soft skills will be endeavoured, led by the BtCIRT, Cybersecurity Division.

ii. Establishment of Security Operation Center

Cyber threats are evolving, sophisticated and dynamic in nature and at times sector specific. Establishment of Security Operations Center (SOC) serves as the operational arm for continuous monitoring, threat detection, and real-time analysis of the entire ICT infrastructure thereby also playing a proactive role to the incident response framework. A SOC provides a centralized platform equipped with advanced technologies, such as intrusion detection systems and security information and event management (SIEM) tools, enabling the detection of potential threats before they escalate into incidents. Moreover, a SOC operates 24/7, ensuring constant vigilance and rapid response capabilities. By complementing the reactive functions of an Incident Response Team with proactive monitoring and threat intelligence, a SOC fortifies the overall cybersecurity posture. This approach enhances the ability to identify and respond to incidents promptly and also plays a crucial role in preventing and mitigating potential security breaches, thereby safeguarding sensitive data and critical systems.

a. Establishment of Governmental SOC (GSOC)

The GSOC will be a unit within the BtCIRT cybersecurity Division, for monitoring government assets. The GSOC will prioritize the responsibility for ensuring a safe and secure cross-border digital trade ecosystem, as part of the ACCESS project. In this ecosystem, the protection of critical infrastructure starts with securing the Government Data Center and the government networks. The SOC team's developing capabilities will potentially lead to the formation of a National SOC that extends beyond the current NCS plan. The capabilities of the SOC team will potentially lead to establishing a National SOC in the next NCS plan.

b. Establishment of EduSOC

As there are dedicated Research and Education Network for Bhutan’s schools, universities and health facilities, there are incidents reported from these networks and systems. Web defacement and botnet infections are common cases in the Education Sector with very limited capability for resolutions. Formation of Education SOC/CSIRT will enable threat information sharing among the colleges, and schools within the country and with the capability development among these teams will prevent such

incidents and enhance the capability in containment. The Ministry of Education and Skills Development (MoESD) will lead the formation of Education CIRT/SOC in collaboration with GovTech along with Royal University of Bhutan (RUB) and Khesar Gyalpo University of Medical Sciences in Bhutan (KGUMS). BtCIRT will facilitate and support the ministry during the conceptualization and implementation.

d. Establishment of Power SOC/CSIRTs:

Operational Technology (OT) is crucial for the functioning of critical infrastructure specially for the power sector of Bhutan. OT encompasses the hardware and software systems that monitor and control physical processes, playing a vital role in ensuring the reliability, efficiency, and safety of industrial operations. As Bhutan's power sectors are increasingly integrated with digital technologies, the need for robust cybersecurity measures to protect OT systems has become important.

By concentrating on monitoring and securing industrial control systems, it can uncover anomalies or cyberattacks often overlooked by conventional IT-centric security setups. The intrinsic nature of OT demands specialized expertise in both cybersecurity and industrial processes. An OT-related SOC/CSIRT, staffed with professionals possessing domain knowledge, facilitates a more effective response to threats affecting critical infrastructure. Additionally, in the realm of OT, rapid incident response is necessary due to the immediate and severe real-world consequences of cyber incidents. The OT SOC/CSIRT enables swift detection, analysis, and mitigation of threats specific to industrial environments, thereby minimizing downtime and reducing the potential for cascading disruptions. In essence, the creation of an OT-related SOC/CSIRT is essential for safeguarding critical infrastructure and ensuring the resilience of essential services against evolving cyber threats.

iii. Threat Information Sharing among the CIRTs and SOC

Bhutan Computer Incident Response Team (BtCIRT), since 2016 has been functioning as the national competent authority responsible for transmitting accurate and actionable information among the national Cybersecurity community including the public and private sectors.

With the formation of the GSOC and the sectoral level Security Operation Centers, the BtCIRT will lead the information compilations related to threats, indicators of compromises and incident reports from each sectoral entity. Through timely and efficient threat information sharing, organizations in Bhutan can improve their ability to detect, protect and respond to cyber threats swiftly and effectively.

iv. National Risk Assessment and Cyber Threats Landscape report

In the absence of a national cyber threat landscape, the nation faces difficulties in planning and prioritizing actions to implement cybersecurity measures and processes. The national cyber threat landscape should identify and rank actual threats in the country based on the information from every relevant institution. The findings would increase the awareness of institutions and citizens about the cybersecurity threats and would help inform the actions to counter them. Although the identification of the threat landscape is a very lengthy process, the yearly Cyber Threat Landscape report consolidating the main cyber threats for the year will promote awareness on the key cyber threats in Bhutan.

The **outcomes** of this strategic goal will be a robust incident response mechanism empowered by enhanced capacity and capability, and strong partnership with the Regulators, Police and new cybersecurity bodies, and development of the Threat Landscape of Bhutan.

Part 3: Implementation

i. Implementation of the NCS

The success of any strategic document lies in its effective implementation, where the execution of actions takes precedence over the strategies themselves. An implementation plan is essential to translate strategic visions into tangible outcomes. Prioritizing the execution of well-defined actions ensures that the outlined strategies are not merely theoretical constructs but practical and impactful initiatives. An essential part of an effective NCS is the implementation phase through the NCS action plan which will be monitored by the NCS governance body. Therefore, the Action plan of the NCS is a crucial element with each action having an "owner" will ultimately be responsible for the activities' implementation and be accountable for reaching the Key Performance Indicators (KPIs) agreed by all stakeholders. In addition, each of the actions must have an approximate budget that would be necessary to implement each activity in the action plan and the timeline for implementation of each activity will be clearly defined to ensure the action is completed within the specified timeline.

ii. Monitoring and review of the NCS

A dedicated monitoring framework for the strategy will involve the continuous collection and analysis of KPIs assessing each outcome against the strategic goals. The division will conduct half-yearly reviews starting from the first year of implementation, engaging stakeholders from relevant sectors. The review will be aligned with the regular budget review and progress review processes. These reviews will ensure a comprehensive examination of the strategy's impact on various facets of the society, the economy, and national security.

The monitoring and review process creates an opportunity for feedback and collaboration, fostering engagement among governmental agencies, private sectors, and civil society. The BtCIRT, Cybersecurity division will document emerging challenges, assess the strategy's adaptability to evolving threats, and incorporate the lessons learned for future iterations. The results will be reported to the GovTech, for critical concerns and the report will be presented to the GovTech Commission for resolution.

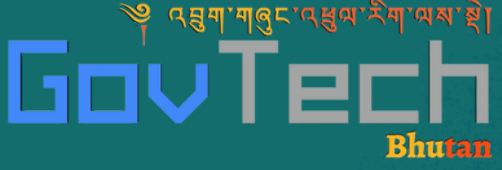
The insights gained from the review reports will inform the next cycle of the strategy, maintaining transparency and accountability through regular reporting to stakeholders and the public. This ensures that the strategy remains aligned with the evolving needs of the nation.

9. Conclusion

The National Cybersecurity Strategy, spearheaded by GovTech Agency outlines the national priorities, goals and actions to secure Bhutan's cyberspace in the next five years. The strategy aims to proactively secure Bhutan's cyberspace with focus on cybersecurity governance, a robust cybersecurity legislation framework, critical information protection and robust incident handling. Through this strategy, all stakeholders are invited to join GovTech Agency in implementing this strategy and building a secure and resilient cyberspace for Bhutan.

10. References

https://www.rcsc.gov.bt/wp-content/uploads/2022/10/Press-Release-Oct-2nd-2022-2.pdf
https://www.rcsc.gov.bt/wp-content/uploads/2023/01/Enactment-of-CSR-Act.pdf
https://www.rcsc.gov.bt/wp-content/uploads/2022/12/Civil-Service-Reform-Act-of-Bhutan-2022.pdf
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
https://www.dsci.in/resource/content/india-cyber-threat-report-2023
https://therecord.media/bangladesh-hacktivistis-targeting-india
https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/
https://therecord.media/chinese-military-hackers-redhotel-target-countries-across-asia-north-america-europe
https://www.aljazeera.com/news/2023/3/21/saudi-iran-deal-view-from-yemen
https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/



Bhutan Computer Incident Response Team

GovTech Agency

Royal Government of Bhutan