BtCIRT Annual Report
(2023-2024)

Bhutan Computer Incident Response Team

Table of Content

1. Highlights

1.1 Summary of major activities

The third edition of the "National Cybersecurity Week" was conducted successfully in October 2023 as a part of the Cybersecurity Awareness Month of October with two technical workshops and a conference. The National Cybersecurity Strategy and Critical Information Infrastructure (CII) Identification methodology along with the CII Protection roadmap, were drafted for approval and implementation from 2024-2029. A CIRT maturity assessment and a few capacity development workshops and awareness programs were also conducted.

1.2 Achievements & milestones

Key activities included:

- Organized the third "Cybersecurity Week" from 25-27 October, covering various programs; a full day Conference, Application Security, Network security and Domain abuse workshops, and an Open Awareness program with awareness content published on BtCIRT Facebook page promoting cyber hygiene best practices.
- Conducted Capture the Flag (CTF) challenge in three ICT colleges in Bhutan in partnership with Asia Pacific Telecommunity (APT) where 138 students participated from 3 technical colleges.
- Published Child Online Protection (COP) related posters and drafted COP Guidelines.
- Drafted the National Cybersecurity Strategy and Critical Information Infrastructure (CII) Identification methodology.
- Published 86 Alerts and advisories on the latest scams and threats.
- Handled a total of 183 incidents in the fiscal year June 2023 to July 2024.
- Conducted CIRT maturity assessment, a malware analysis workshop and a tabletop exercise in collaboration with ITU.

2. About BtCIRT

The Bhutan Computer Incident Response Team (BtCIRT) was formally established on 20th May 2016 as the national focal point for coordinating and implementing cybersecurity activities and initiatives for Bhutan. BtCIRT is part of the GovTech Agency under the Cybersecurity Division. The overall mission of BtCIRT is to enhance cyber security in the country by implementing relevant cybersecurity plans and programs, including coordinating cybersecurity information and establishing computer security incident handling capabilities in the country. It is also mandated to proactively monitor government systems for attacks and vulnerabilities.

BtCIRT constituents are all government institutions under the Royal Government of Bhutan (RGOB) utilizing government network infrastructure to host their IT resources and services. Services like awareness and reactive services are extended to all users within the country.

3. Activities & Operations

As the main body for cybersecurity in the country, BtCIRT is responsible for identifying and carrying out relevant cybersecurity plans and programs that contribute towards achieving the vision of safe and secure Bhutan.

The specific mandates of BtCIRT are as follows:

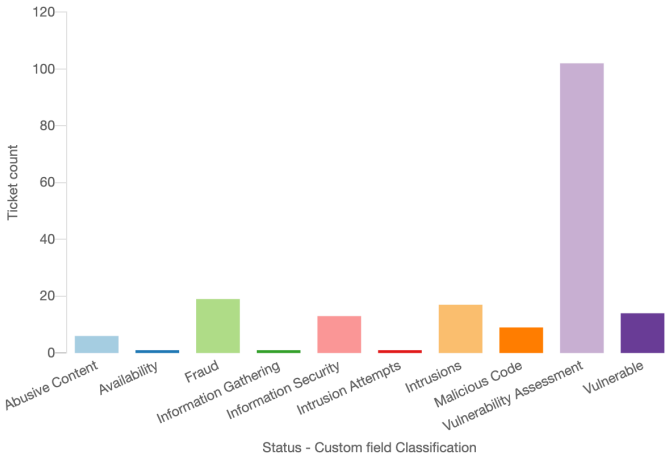
- Operate as a national contact in relation to coordinating and implementing all cyber security issues, plans and programs.
- Conduct end-user awareness at the national level and disseminate information on threats and vulnerabilities, and conduct security workshops related to various cyber security domains.
- Actively monitor systems hosted in the Government Data Centre (GDC) for attacks and

vulnerabilities, and provide timely reports to the GDC operating team and the system administrators.

- Conduct periodic security assessments of government systems and provide services to non-government organizations on request.
- Represent Bhutan in international forums.
- Develop relevant strategies, policies, standards, guidelines and baseline documents.

3.1 Incident Handling Report

A total of 183 incidents were handled in 2023-2024 FY, majority of which were vulnerability Assessment (102), followed by fraud related incidents like phishing and scams (19), intrusions (17), and other incidents as depicted in the bar graph below.



Status	Custom field Classification	Ticket count
resolved	Vulnerability Assessment	102
	Fraud	19
	Intrusions	17
	Vulnerable	14
	Information Security	13
	Malicious Code	9
	Abusive Content	6
	Intrusion Attempts	1
	Information Gathering	1
	Availability	1
	Total	183

Figure 1: Number of Incidents handled by Incident Classification type (July 23 to June 24)

3.2 Awareness creation programs

Awareness and advocacy is a very important mandate of BtCIRT. A number of awareness programs were implemented in 2023-2024 FY, as described in the following:

3.2.1 Drafting Child Online Protection (COP) Guidelines

In collaboration with ITU and UNICEF a localized version of the COP guidelines 2020 by ITU were drafted taking into consideration the existing COP measures and the lack thereof. The guidelines are very prescriptive and outline the necessary steps that the respective COP targets; Parents & Educators, Policy Makers, and Industry should take to help children to be safe online and to ensure that they are adequately protected. Online safety related Posters for children and young individuals were also published to be distributed to schools around the country.

3.2.2 Awareness Content Pamphlets

An awareness pamphlet covering cyber hygiene tips was published to be showcased and distributed during the cybersecurity awareness month in October. The topics covered were safeguarding against social engineering and phishing scams, safeguarding accounts and data through password security, updating systems and encrypting data.

3.2.3 Open Awareness Program

As a part of Cybersecurity Awareness month and Cybersecurity Week programs, an open cybersecurity awareness program was conducted targeting the general public to help with their understanding of prevalent cybersecurity threats and cybersecurity best practices in the online world. Awareness content was also published in the BtCIRT Facebook page throughout the week promoting cyber hygiene best practices.

3.3 Security Advisory and Alerts

BtCIRT publishes latest cyber security news and vulnerabilities to keep the constituents well informed about the latest development in the area of cybersecurity on its website and facebook page. A total of 86 alerts and advisories were published, out of which a significant proportion were released to address critical patches released by software vendors to fix vulnerabilities.

4. Events organized / hosted

4.1 Workshops/ Training

Capacity development is another important mandate of BtCIRT to ensure that all the stakeholders in the cybersecurity ecosystem are prepared to meet the challenge of the ever changing cybersecurity threat landscape. In that note, several capacity development activities have been carried out to strengthen the capabilities of all stakeholders.

4.1.1 ITU expert led workshop (15-17 August)

As a part of the ITU-CIRT assessment mission, the ITU expert conducted several hands-on exercises on Digital Forensics, Web Server compromise case analysis, Malware Analysis, Reverse Engineering, Log analysis and Designing through introduction of relevant tools.

Figure 2:Participants during the ITU Workshop

4.1.2 National Cybersecurity Week (25-27 October)

The 3rd edition of the National Cybersecurity Week was observed from 25-27 October, whereby several training programs and a conference were conducted. It was observed as a part of Cybersecurity Awareness Month of October.

4.1.3 Technical workshops (25-26 October)

The Cybersecurity technical workshop was conducted on Domain Name Abuse and Network Security for more than 50 participants including Network Engineers, System Administrators, ICT officers and Data Protection related officers from Private, Corporations and Government agencies.

4.1.4 Cybersecurity conference (27th October)

More than 75 participants participated in the Cybersecurity conference, where the program included a Panel of experts from various agencies and institutions within the country engaged in discussions on critical cybersecurity issues, including data privacy, ransomware attacks, National Digital Identity and the role of artificial intelligence in cybersecurity. The interactive session covered a diverse range of perspectives surrounding the theme 'Trust in the Digital Age'. There were also presentations by various stakeholders on the state of cybersecurity in their respective organizations.

Figure 3:Participants during the Cybersecurity Conference

4.1.5 Security Workshop on OpenSource firewall/IDS/Network Incident response (29th April-1st May)

Given the importance of implementing security tools to protect the networks of critical organizations, a Technical workshop was conducted with the help of APNIC. Tools such as the Open Source firewall, Intrusion detection System (IDS) were conducted to provide the participants with the best practices on handling network incidents and cleaning up malware infection

Figure 4:Participants during the Security workshop

4.2 Drills/Exercises

The following drills and tabletop exercises were conducted:

4.2.1 Cybersecurity Capture The Flag Challenge (16 - 17 October)

The Cybersecurity CTF 'Capture the Flag' challenge took place at three colleges: College of Science and Technology, Jigme Namgyel Engineering College and Gyalpozhing College of Information Technology. It consisted of a hands-on workshop on introducing the basics of cybersecurity on Day 1 and Capture the Flag competition among the students on Day 2. The objective of the program was to develop the future cybersecurity workforce of Bhutan.

Figure 5:Participants during the CTF challenge in 3 colleges

4.2.2 Tabletop Exercise (15th August)

As a part of the CIRT assessment and training session, a tabletop exercise on Cybersecurity Crisis management was conducted by the ITU experts for the critical agencies. The exercise helped the participants understand the role of different team members in responding to incidents.

5. International Collaboration

BtCIRT has been a member of FIRST and APCERT since 2017. The newest memberships were established with Cybersecurity Alliance for Mutual Progress (CAMP) and Global Forum for Cybersecurity Experts (GFCE) in 2022. BtCIRT have also received support from the International Telecommunication Union (ITU) and World Bank in various initiatives till date; including establishing BtCIRT, the drafting of National Cybersecurity Strategy, conducting cybersecurity drills, developing the Critical Information Infrastructure Protection Roadmap, among other important

initiatives. Beside this the Asia Pacific Network and Information Center (APNIC) has been an important partner for building the cybersecurity capacity of IT and security professionals in Bhutan since 2016.

The BtCIRT members have availed a number of skills development opportunities from various international partners through training, workshops, conferences which have helped the members to upskill their knowledge and skills. These have also provided opportunities to network with a number of international and national Cybersecurity/CIRT communities and experts. BtCIRT is grateful to all the organizers for providing these various capacity building opportunities.

5.1 International Training/Workshops/Meetings/Conferences

BtCIRT participated and benefited from the following international events that included training, workshops and conferences.

Event	Organizer/Trainer	Region	Date
8th Annual CAMP Meeting	CAMP	South Korea	11-13 July, 2023
Training on CyberSecurity Ecosystem in Indonesia	JICA	Indonesia	21-25 August, 2023
Annual APCERT Drill themed "Digital Supply Chain Redemption"	APCERT	Virtual	16th August, 2023
APT Training Course on "Empowerment of Blockchain, Cyber Security & Cyber Forensic	Asia Pacific Telecommunity	India	1-6 September, 2023
GFCE Annual Meeting, GC3B Conference	GFCE	Ghana	26th December, 2023 27 - 28 December, 2023
ITU Interregional CyberDrill for Europe and Asia-Pacific	International Telecommunication Union	Cyprus	28th Nov to 1st Dec, 2023
Global CyberDrill	United Arab Emirates Cyber Security Council (CSC) with ITU	UAE	23-25 April, 2024
Defense practice against cyber attacks	Knowledge Co-Creation program by JICA	Japan	19 May - 1st June, 2024
APC-HUB event on Cybercrime Capacity Building	Asia-Pacific Cyber Crime Capacity Building Hub secretariat with the Supreme Prosecutors' Office of the Republic of Korea (KSPO)	South Korea	28-31 May, 2024

36th FIRST Conference	FIRST	Fukuoka, Japan	11 to 14 June, 2024

BtCIRT also had the opportunity to present the best practices of Network Security during btNOG-10 in Paro in June 2023 and sharing of the national cyber crisis response plans and insights on the experience with intersectoral coordination in Bhutan during the ITU Interregional CyberDrill for Europe and Asia-Pacific on 28th November 2023.

6. Future Plans

As BtCIRT continues to work towards improving incident handling capabilities and work on areas to improve the overall cybersecurity maturity of Bhutan, the immediate plan is to kick-start the implementation of the National Cybersecurity Strategy (NCS) from 2024 through to 2029. As a part of the strategy, various initiatives will be carried out to enhance national cybersecurity governance and Coordination, strengthen cybersecurity legislation, protect critical information infrastructure and enhance incident response capabilities.

In addition, BtCIRT will continue to conduct cybersecurity awareness and capacity development activities for various stakeholders, including leaders, critical operators, small and medium Businesses, and the general public. Further, strengthening cooperation and collaboration with more organizations internally and internationally will be another priority for BtCIRT.

7. Conclusion

In 2023-2024 FY, BtCIRT handled a total of 178 incidents and carried out various cybersecurity programs inline with the various cybersecurity mandates of BtCIRT which included various capacity development and awareness programs covering a broad range of target groups. In future, BtCIRT will continue to focus on improving its visibility in the country and to create awareness on the importance of cybersecurity. In addition the implementation of the National Cybersecurity Strategy and the protection of Critical Information Infrastructure protection will be key priorities for the 2024-2025 FY.