BtCIRT Annual Report
(2021-2022)

Table of Content

Highlights of 2021-2022 financial year

a. Summary of major activities

The annual report covers all the major activities, initiatives and incidents handled by the Bhutan Computer Incident Response Team (BtCIRT) for the 2021-2022 financial year (FY), from July 2021 till June 2022.

In 2021, although the COVID pandemic continued and the nation experienced a few lock downs and restrictions, BtCIRT was able to meet some critical targets for the year. The country's first ever "Cybersecurity Week" was successfully conducted. Articles and alerts on latest cyber trends, threats, vulnerabilities and best practices were also published. Majority of the workshops and training were carried out online due to the pandemic.

b. Milestones in brief

There were many milestones that were achieved, including the first ever Bhutan Cybersecurity Week.

- First ever "Bhutan Cybersecurity Week" observed from 20-25 December
- Production and airing of awareness videos on national television and online platforms
- 4 advisories published on latest scams and threats
- 4 alerts issued on scams and threats
- 85 alerts on security patches and updates issued
- 156 incidents handled

1. About BtCIRT

Bhutan Computer Incident Response Team (BtCIRT) is a division under the Department of Information Technology and Telecom, Ministry of Information and Communications. The overall mission of BtCIRT is to enhance cyber security in the country by coordinating cybersecurity information and establishing computer security incident handling capabilities in the country.

BtCIRT was formally established on 20 May 2016 as the central agency for cybersecurity activities and initiatives in the country and is responsible for everything related to cybersecurity in the country.

The overall BtCIRT mandate include:

i. Conducting end-user awareness at national level and disseminates information on threats and vulnerabilities, and conducts security workshops related to various cyber security domains.

ii. Monitoring systems hosted in the Government Data Center (GDC) for attacks and vulnerabilities, and provides timely reports to the GDC operating team along with system administrators.

iii. Carrying out periodic security assessment of government systems and on a request basis for non-government organizations.

iv. Representing the country in international forums.

v. Developing strategies, policies, standards, guidelines and baseline documents.

BtCIRT constituents are all government institutions which use government network infrastructure to host their IT resources and services. While BtCIRT services like awareness and reactive services are extended to all users within the country.

2. Achievements and Milestones

a. Incident Handling Report

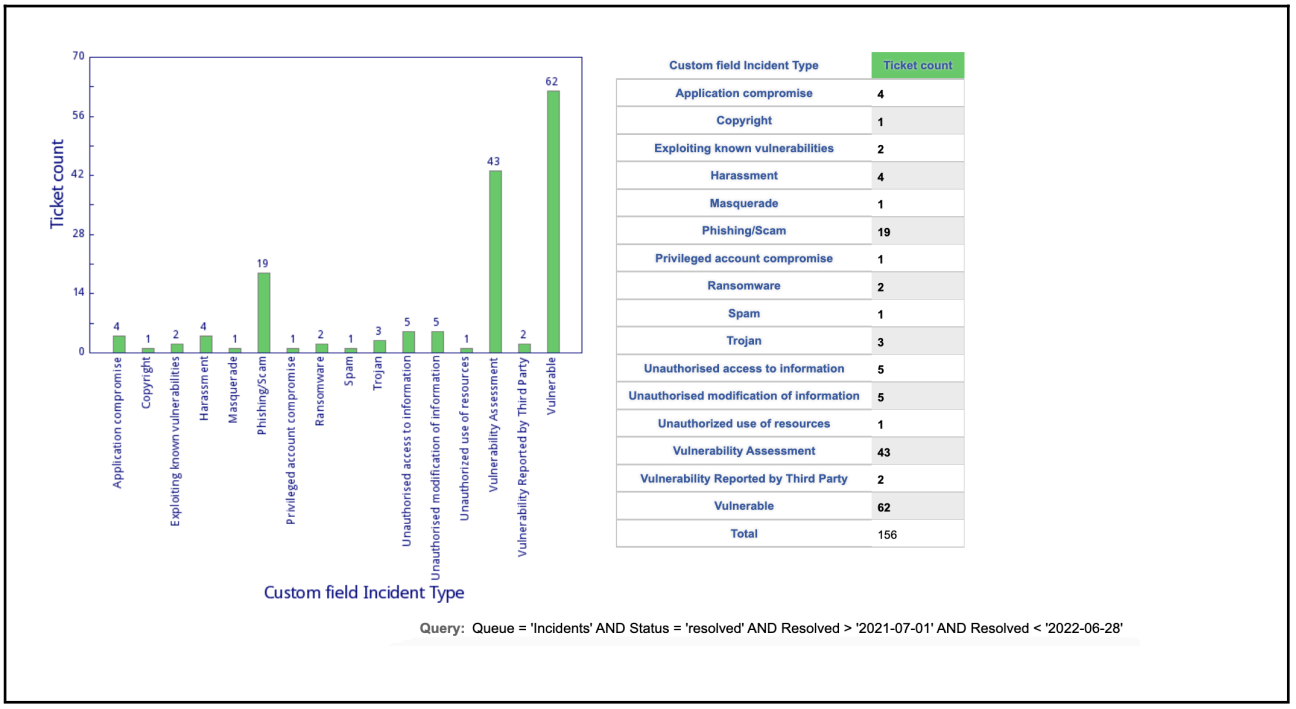
There are two situations which invoke potential action by the BtCIRT – security events and security incidents.As per the *BtCIRT Incident Handling Procedure* the definitions of these two are:

> **Security events** – any situation reported by a computer system or human being to the BtCIRT – no matter where it comes from – internal or external sources, which is a potential cyber threat or potential cyber-related law breach for the constituency covered by the BtCIRT.
>
> **Security incident** is a single or series of security events that violates cyber-related law or have significant probability of adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.[1]

An incident will also constitute an occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.[2]

156 incidents were handled in 2021-22, majority of which were vulnerabilities related, followed by scam incidents and malware. The following graphs provide a number of incidents resolved on a monthly basis in the FY 2021-22:

[1] Information source: https://niccs.us-cert.gov/glossary
[2] Information source: https://niccs.us-cert.gov/glossary



Custom field Incident Type	Ticket count
Application compromise	4
Copyright	1
Exploiting known vulnerabilities	2
Harassment	4
Masquerade	1
Phishing/Scam	19
Privileged account compromise	1
Ransomware	2
Spam	1
Trojan	3
Unauthorised access to information	5
Unauthorised modification of information	5
Unauthorized use of resources	1
Vulnerability Assessment	43
Vulnerability Reported by Third Party	2
Vulnerable	62
Total	156

Figure 1: Number of Incident types by Incident Category

[The Incident types and classification details are provided in Annexure 1.]

b. Advocacy and Awareness

- As a part of the Bhutan Cybersecurity Week, an Open Awareness Program was conducted in two local banks targeting the general public and a Cyber hygiene awareness program with high school students was also conducted.

- In collaboration with the Tech Industry Development Division, a total of three animation videos were developed. The animation videos covered Online Banking security, How to Protect Online Accounts and Online scam related advisory and safety measures. The contents were aired on national television and shared through various social media platforms. A comic was also published highlighting cyberbullying issues in schools and the importance of providing support by parents, teachers and peers in helping students address such issues.

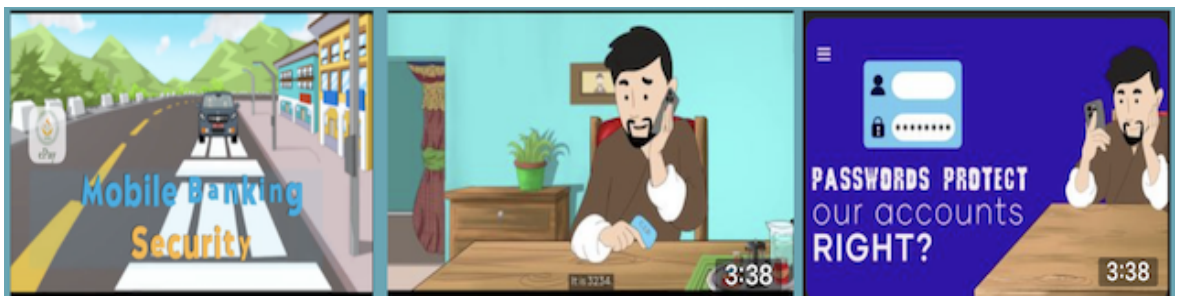


Figure 2: Awareness Videos produced

- The BtCIRT developed a digital comic book for children focussed on online privacy, cyberbullying and role of parents and guardians.
- Social Media Activities such as quizzes and featuring cybercrime victim stories were also conducted as part of the Cybersecurity Week event.
- Basic Cyber hygiene awareness workshops were conducted in two colleges (Royal Thimphu College) and (Khesar Gyalpo University of Medical Science, Faculty of Traditional Medicine).
- Advocacy on cyber hygiene was conducted at National Scout Center, Paro for class 12 graduates on 22nd June, 2022.

Figure 3: Advocacy at National Scout Center, Paro

- Participated in Lap Go Mi Logu (Youth-Talk) organized by RENEW on 11th June,2022.

c. 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 85 alerts were released to address critical patches and updates released by software vendors to fix the vulnerabilities such as Cisco, Microsoft, Apple, Mozilla etc and 4 Alerts were issued focussed on different scams. 4 Advisories were issued. Advisories include researched analysis of computer incidents/scams along with mitigation and recommendations.

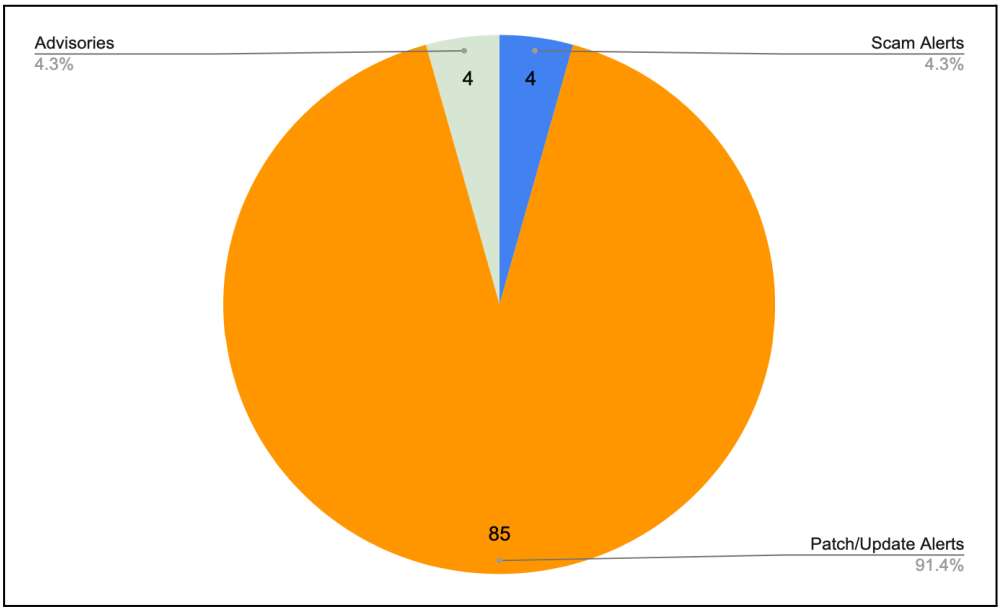


Figure 4:Number of Incident types by Incident Category

To provide an overview of the kind of alerts and advisories published, the following table depicts the details of alerts and advisories issued between June 2021 - July 2022:

Table 1: Details of Alerts/Advisory issued

Sl. No	Alerts/Advisory issued	Date of Issuance	Details
1.	Coca Cola welfare fund	7th June, 2021	Scam Alert issued
2.	Canada Visa lottery scam	8th November,2021	Scam Alert issued
3.	WhatsApp link	17th December,2021	Phishing/Scam Alert
5	Digital Investment Scheme and re Scams	27th Jan,2022	Advisory on Digital Investment Scheme and re Scams
6	Emotet Malware	4th February,2022	Advisory on Emotet Malware
7	Facebook Phishing Alert	22nd March,2022	Advisory on links being automatically shared through Facebook Messenger
8	US Visa Lottery Scam	16th June,2022	Scam Alert issued
9	Instagram Scam	20th June, 2022	Advisory on Instagram Scam

3. Events organized

a. Bhutan Cybersecurity Week 2021

The national Cyber Security Week was observed with the theme "Be Cyber Safe - A step towards building the human firewall", to achieve cybersecurity awareness among the general public, educate and inspire students in the cybersecurity field and upskill ICT Professionals to secure their work space. Several activities were conducted over week-long events from 20th to 25th of December, 2021, targeting students, non IT professionals, ICT officers and the general public.

The cybersecurity week campaign began with online workshops on Basic cybersecurity practices, Network Security, MANRS for Network Operators and Web Applications security which ran for the first three days. They were followed by the cybersecurity conference that was presided by international and national speakers sharing their experiences on cyber attacks, policies and strategy development, risk assessment, awareness survey reports. The one day conference was closed with a panel discussion on "Emerging Cybercrimes and Cybersecurity Risks, and the State of Bhutan's Preparedness" with panel members representing BtCIRT, RBP, RENEW, BNBL and TTPL. The week of programs came to a close with cyber hygiene screenings in the Bank of Bhutan and the Bhutan National Bank on the 5th day and an awareness program for school students on the sixth day.

Figure 5: Bhutan Cybersecurity Week Opening

As part of the cybersecurity week parallel social media activities were also conducted partnering with social media influencers "Denkers getaway" to conduct daily cybersecurity quiz nights and "Humans of Thimphu " for story covers of victims of cyberbullying and cyber crimes. A selfie challenge in BtCIRT facebook page was also conducted to engage young social media audiences.

The cybersecurity week was conducted with kind support and sponsorship from sponsors APNIC, Internet Society, Team CYMRU, Bank of Bhutan, Bhutan National Bank, Royal Monetary Authority, Thimphu Techpark, Tashi Bank, NGN Technologies, and Yangkhor IT Solutions, RGoB, Bhutan Broadcasting service, btNOG, Center for Bhutan Studies.

Details of the training/workshops are covered under Capacity Building.

Figure 6: Bhutan Cybersecurity Week Conference Local Speakers

b. Child Online Protection(COP) workshop

The BtCIRT in collaboration with ITU and UNICEF Bhutan, organized a kick-off, virtual information session on the 7th April, 2022. The ITU presented on the COP Asia-Pacific project and shared the work plans, activities, and the expected next steps with the relevant stakeholders, while raising awareness on the increased importance of COP globally and in Bhutan due to COVID and the importance of identifying collaboration opportunities for the objective of developing localized COP guidelines for Bhutan.The BtCIRT, National Commission for Women and Children (NCWC), UNICEF Bhutan and Bhutan Telecom presented on the various initiatives undertaken so far and the future plans on COP. Various challenges and concerns pertaining to child online protection were also raised. Participants included officials from Civil Society Organizations dealing with child protection, RBP, YDF, MoE, Telcos, UNICEF, Dratshang Lhentshog, NCWC, Department of Information and Media (DoIM), Bhutan Nun Foundation, BICMA, Women Children and Youth Committee from the National Assembly and OAG.

Figure 7: COP Workshop participants on Zoom

4. International Collaborations

BtCIRT maintains relationship and membership with Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Information Response Security Teams (FIRST). In addition to existing memberships and collaborations, BtCIRT also collaborated with the following forums/memberships and organizations:

a. GFCE (Global Forum on Cyber Expertise)

BtCIRT initiated membership to the GFCE. The GFCE is a multi-stakeholder community of more than 140 members and partners from all regions of the world, aiming to strengthen cyber capacity and expertise globally. The GFCE endeavors to be a pragmatic, action-oriented and flexible platform for international collaboration, reducing overlap and duplication of efforts in the cyber capacity building (CCB) ecosystem to ensure an open, free, peaceful and secure digital world.

b. The Cybersecurity Alliance for Mutual Progress (CAMP)

BtCIRT initiated membership to the CAMP. The Cybersecurity Alliance for Mutual Progress (CAMP) is initiated by the Korean government with the purposes of achieving sustainable benefits and serving as a platform where members prepare themselves with collective actions to keep cyberspace safe. CAMP was officially launched on July 11, 2016 in Korea with 40 organizations from 29 countries to serve as a platform for the members to enhance their cybersecurity capacity.

c. Asia Pacific Network Information Center (APNIC)

The APNIC has been a key stakeholder in the workshops conducted by the BtCIRT in 2021 in terms of technical support for the workshops as well as financial support for the cybersecurity week.

d. Nanyang Polytechnic International (NYP) and Temasek Foundation, Singapore

The BtCIRT in collaboration with NYP International and Temasek Foundation,

conducted a "Cybersecurity Programme for Leaders" , a 5-day online training programme for executives, chiefs from various government Ministries and agencies. The objective of the program was to cultivate cybersecurity leadership in the ministries/agencies and educate leaders on cybersecurity.The details of the training are mentioned in the Training section.

e. Sri Lanka CERT and Singapore Cybersecurity Agency (CSA)

The Sri Lanka CERT and CSA Singapore graciously agreed to talk on cybersecurity and share their experiences during the Bhutan Cybersecurity Week Conference on 23rd December, 2021.

f. International Telecommunication Union (ITU)

The BtCIRT team attended a series of meetings and workshops including a Cyber Drill conducted by the ITU in 2021 that enhanced the capabilities of the team both technically and on a policy level. ITU has also been collaborating with the BtCIRT in the initial planning and implementation of Child Online Protection (COP) guideline in Bhutan.

5. Local collaborations

The BtCIRT has collaborated with the following external agencies in the capacity of sponsors and support for the Bhutan Cybersecurity week, speakers for the workshops and other initiatives on cybersecurity:

a. Bank of Bhutan (BOB)

b. Royal Monetary Authority (RMA)

c. Bhutan National Bank (BNB)

d. GIC Bhutan Reinsurance Co. Ltd.

e. Royal Bhutan Police (RBP)

f. National Commission for Women and Children (NCWC)

g. Renew Educate Nurture Empower Women (RENEW)

h. Thimphu TechPark Ltd (TTPL)

i. UNICEF

6. Capacity building

Since the inception, BtCIRT has conducted various capacity development programs in order to build the capacity of ICT professionals. In 2021-2022 FY various cybersecurity trainings were conducted by BtCIRT.

a. The following training/workshops were carried out as a part of the Bhutan Cybersecurity Week from 20-22 December, 2021:

- 20-21st December, 2021 : Network Security Workshop

- 20-21st December, 2021: Web Application Security Webinar
- 21st December, 2021: Mutually Agreed Norms for Routing Security (MANRS)
- 20-21st December, 2021 : Cyber Security Awareness Workshop
- 25th December, 2021: School cyber hygiene workshop

b. In collaboration with NYP International and Temasek Foundation, a "Cybersecurity Programme for Leaders" conducted a 5-day online training programme for executives and chiefs from various government Ministries and agencies. The objective of the program was to cultivate cybersecurity leadership in the ministries/agencies and educate leaders on cybersecurity.

The details of the training are as follows:

- 4th January 2022: Overview of Singapore's Cybersecurity Landscape, Strategy, Legislation and Policies. Sharing and Dialogue session with National Agency
- 6th January, 2022: Managing Cybersecurity in Public Agency - sharing and dialogue session with invited agencies.
- 11th January, 2022: The cost of Cybersecurity incidents - impact on financial industry and businesses
- 27th January, 2022: Manpower development and training for Cybersecurity competencies
- 28th January, 2022: Closing Dialogue with Participants

c. An email security and SSL Certificate workshop at MoIC conference Hall from 24-25 May 2022. The training included discussion of common vulnerabilities and vulnerability management. The participants were ICT officials from various government agencies.

Figure 8: Email security and SSL certificate workshop

a. Trainings Attended

BtCIRT has participated and benefited from various online trainings as presented in the table below:

Table 2: Details of trainings attended

Date	Title	Organizer/Trainer
15-19 June 2021	Hands on Training on Fundamental Web and Application Security Issues for NREN Professionals	Institute of Information Technology (IIT) University of Dhaka Bangladesh
6 – 10 September 2021	Second Workshop under the Asi@Connect- “Identity access management and monitoring of the network performance and its security" Network Security & Performance Workshop.	Lanka Education and Research Network (LEARN)
6 - 10 September 2021	Online programme on Integrated Management Systems (IMS) – IT Service Management (ITSM) of ISO/IEC 20000-1, Information Security (ISMS) of ISO/IEC 27001 and Business Continuity (BCMS) of ISO 22301 Management Systems.	Malaysian Technical Cooperation Program
22 -26 November 2021	Integrated Cybersecurity for Safer Digital Worlds	Singapore Cooperation Program
29 - 3 December 2021	Third Workshop under the Asi@Connect "Uplifting Resources to DNS/DNSSEC”	Lanka Education and Research Network (LEARN)

b. Drills and exercises

APCERT Annual Drill 2021

The Asia Pacific Computer Emergency Response Team (APCERT) successfully completed its annual drill to test the response capability of leading Computer Security Incident Response Teams (CSIRT) within the Asia Pacific economies on 25th August,2021.The theme of the 2021 APCERT Drill was "Supply Chain Attack Through Spear-Phishing - Beware of Working from Home" The exercise reflected real incidents and issues that exists on the Internet. The participants handled a case of a supply chain attack triggered by spear phishing. This drill included the need for the teams to interact locally and internationally, with CSIRTs/CERTs and targeted organizations, for coordinated suspension of malicious infrastructure, analysis of malicious code, as well as notification and assistance to affected entities. This incident response exercise, which was coordinated across many economies, reflects the collaboration amongst the economies in mitigating cyber threats and validates the enhanced communication protocols, technical capabilities and quality of incident responses that APCERT fosters in assuring Internet security and safety.

Bhutan participated in the drill with 24 other CSIRTs from 19 economies of APCERT (Australia, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Malaysia, Myanmar, Philippines, Singapore, Sri Lanka, Thailand, Tonga, and Vietnam).

Global ITU- Cyber Drill 2021

BtCIRT participated in Global ITU-Cyber Drill 2021, which was held from September to November, 2021.

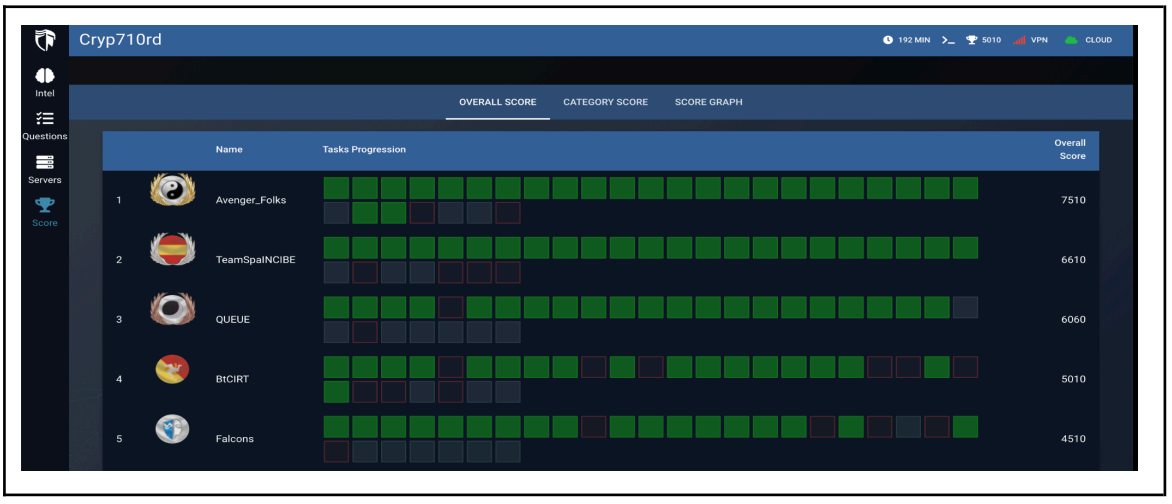


Figure 8: Cyber Range platform showing the Leaderboard

7. Future Plans

There are many plans and programs planned for the year and beyond to continue fulfilling our mandates towards achieving a cyber safe Bhutan. The activities include, but are not limited to, the following:

- Building Capable human resources
- Protecting Critical Information Infrastructure
- Enhancing Cyber Incident Handling and Response
- Creating Awareness through continuous awareness and advocacy programs

8. Conclusion

The BtCIRT will continue to focus on improving its visibility in the country and to create awareness on the importance of cybersecurity. Importance will be given to training and human resource development of ICT officials in the government and critical sectors to improve our cyber threat resilience.

Annexure 1 : Incident classification

The incidents are classified in types with further breakdown of type of incidents, as provided in the table below (*Source: BtCIRT Incident Handling Procedure*)

Classification	Type	Description
Abusive Content	Spam	Or 'unsolicited bulk e-mail', meaning that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having identical content.
	Harassment	Discrediting or discriminating against somebody (i.e., cyberstalking).
	Child/sexual/violence	Child pornography, glorification of violence, ...
Malicious Code	Virus Worm Trojan Spyware Dialler Rootkit	Malicious Code or Malware is a software that is intentionally included or inserted in a system for a harmful purpose - for causing damage to systems, computers, computer networks or users/clients. A user interaction is normally necessary to activate the code. There are different variants of Malware - Virus, Worm, Trojan, Spyware, Dialler and Rootkit serving different intentions of harm.
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This also includes some kinds of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, …).
	Sniffing	Observing and recording network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g., lies, tricks, bribes, or threats).

Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g., buffer overflow, backdoors, cross site scripting, etc.).
	Login attempts	Multiple login attempts (guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions		A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by unauthorized local access.
	Unprivileged account compromise	
	Application compromise	
	Bot	Compromised computer connected to the botnet and controlled by the botnet operator.
Availability	DoS	In this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYN- a. PING- flooding or e-mail bombing (DDoS: TFN, Trinity, etc.). However, availability can also be affected by local actions (destruction, disruption of power supply, etc.).
	DDoS	
	Sabotage	
Information Security	Unauthorized access to information	Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.
	Unauthorized modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (e.g., the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	Attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.[3]
Vulnerable	Detected vulnerability	Detected security weakness in the system.
Other	Other	Other incidents that do not fall into any class above.

[3] Information source: https://en.wikipedia.org/wiki/Phishing