TTX for Network/System Engineers and ICT Officers

SANOG43, btNOG-12

You may connect with me

Pratima Pradhan

Linkedin:
https://www.linkedin.com/in/pratima-pradhan-957bb821/

Lead CIE , Thimphu TechPark

Deputy Chief ICT Officer , BtCIRT
Cybersecurity Division, GovTech

Go to Menti meter and Enter the Code 5629 3386

https://www.mentimeter.com/app/presentation/alz9zvd1354uwndwigpzkyggcj9857fj/edit?question=i4v5g9uobim9

House Rules

Observers : Observe and take note. (Comment only at the end)

Players: Must be willing to play, take up role and get involved.

What is TTX (Table Top Exercise)

- Proactive Approach for checking our Preparedness

A **Tabletop Exercise** - TTX is an informal, discussion-based session in which a team discusses their roles and responses during an emergency, walking through one or more example scenarios. It's a totally safe way of practicing the policies and procedures around a table not touching any systems

It is not a **Test** but more of experience sharing, communications and leverage skills in the room.

It is an **Incident Role Play!**

It’s **low-stress** and discussion-based to prepare for: **Cybersecurity incident response,Disaster recovery (natural or technical), Business continuity or Crisis communications**

Why we need Tabletop Exercise?

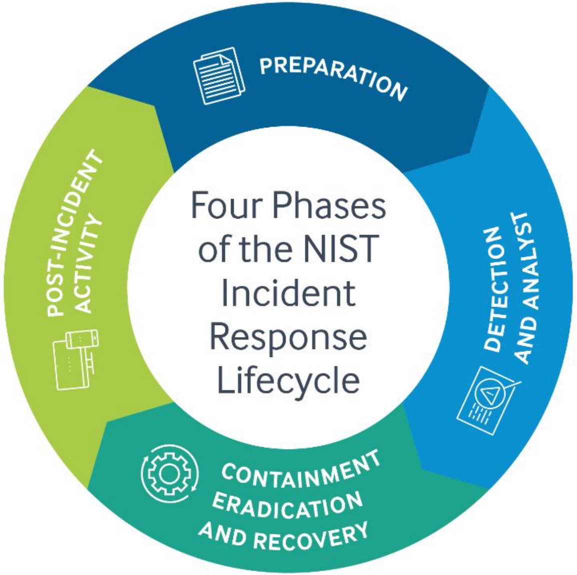
- Spot weaknesses early
- Boost Team Coordination
- Sharpen decision making
- Meet Compliance
- Essential training

Incident Response

“Incident Response is like a fire drill for ICT systems – detect the fire, contain it, put it out, and learn how to prevent it next time.”

“Incident response is the mitigation of violations of security policies and recommended practices. An incident response capability includes the ability to detect incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore IT services.”

-NIST


Four Phases of the NIST Incident Response Lifecycle
PREPARATION
DETECTION AND ANALYST
CONTAINMENT ERADICATION AND RECOVERY
POST-INCIDENT ACTIVITY

Exercise Let's Start

Title: ISP Under Siege: Coordinated Cyber Attack on Bhutan’s Largest Internet Service Provider

Company - ISP (GNH Infocom Ltd)

Country - Bhutan

Objectives:

- Creating Awareness on Table Top Exercise
- Evaluate ISP-wide incident response and business continuity
- Test coordination across national players and Assess regulatory communication and customer notification protocols

Group Set Up **Participants can assume the Roles**

Mix Up Different Organizations

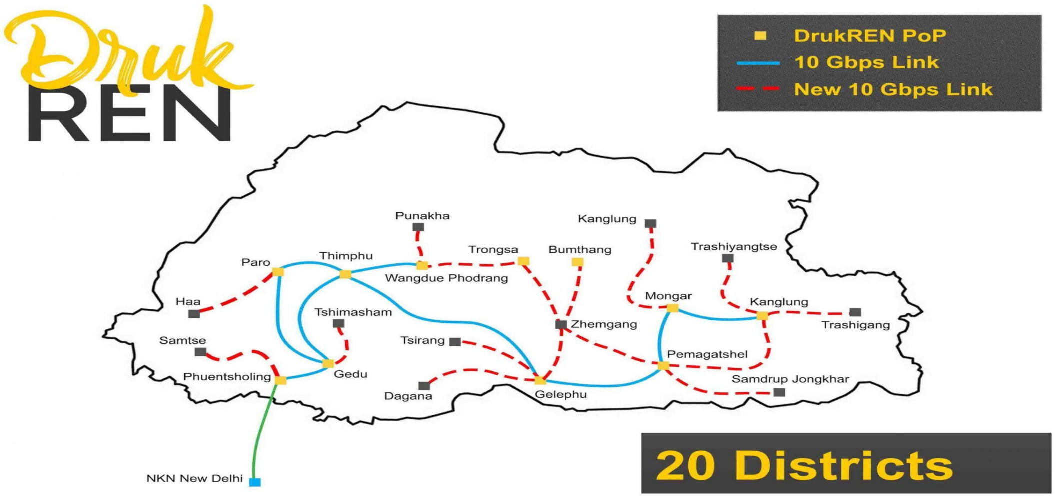
- Appoint Note taker
- Appoint Speaker
- Incident Responder,
- Customer Care
- Network engineer
- legal/ Regulatory Liaisons
- Communications Team
- C-Suite Roles.

Scenario Overview

You are an employee of country’s largest ISP and is facing a sophisticated, multi-vector cyberattack. The attack begins with a DDoS flood on regional DNS servers and escalates to internal network compromise via zero-day exploitation.

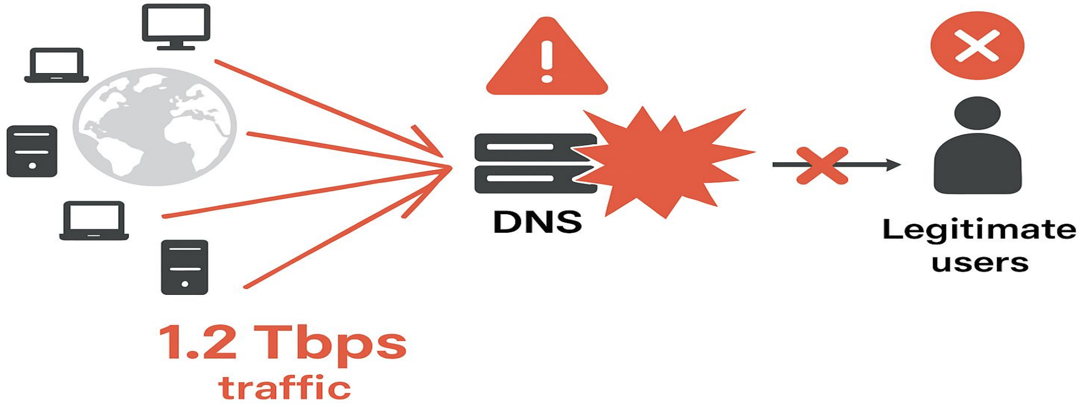
PHASE I - DISRUPTION and INVESTIGATION

INJECT 1: Customer service reports that thousands of users in the central and eastern region are unable to access any govt and banking sites.



src:DrukREN

INJECT 2 : Internal monitoring shows a massive DDoS attack targeting your public DNS servers (over 1.2 Tbps).

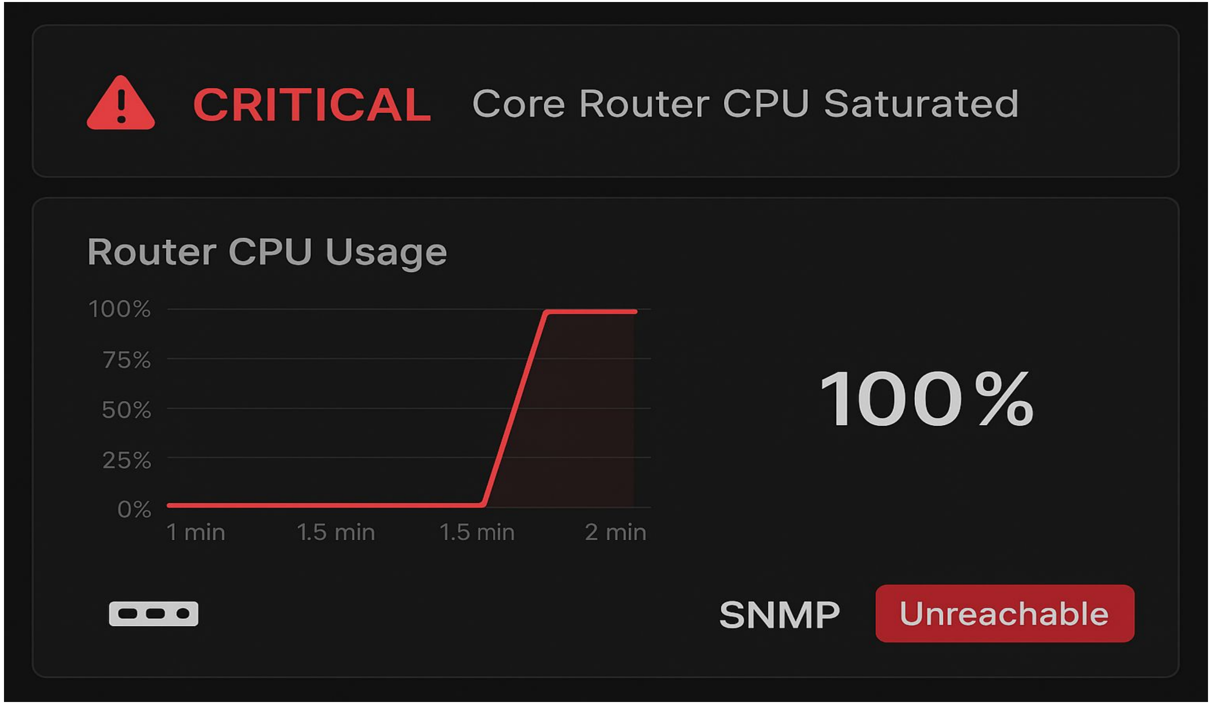


Task: **Discuss in your group**

- What is the potential impact of the incident?
- What would be your action?
- Who do you involve?
- What information be shared and when should you be sharing ?

PHASE II - ESCALATION and THREAT IDENTIFICATION

INJECT 3: Traffic anomaly alerts from a GNH data center core router CPU at 100% and SNMP disabled.



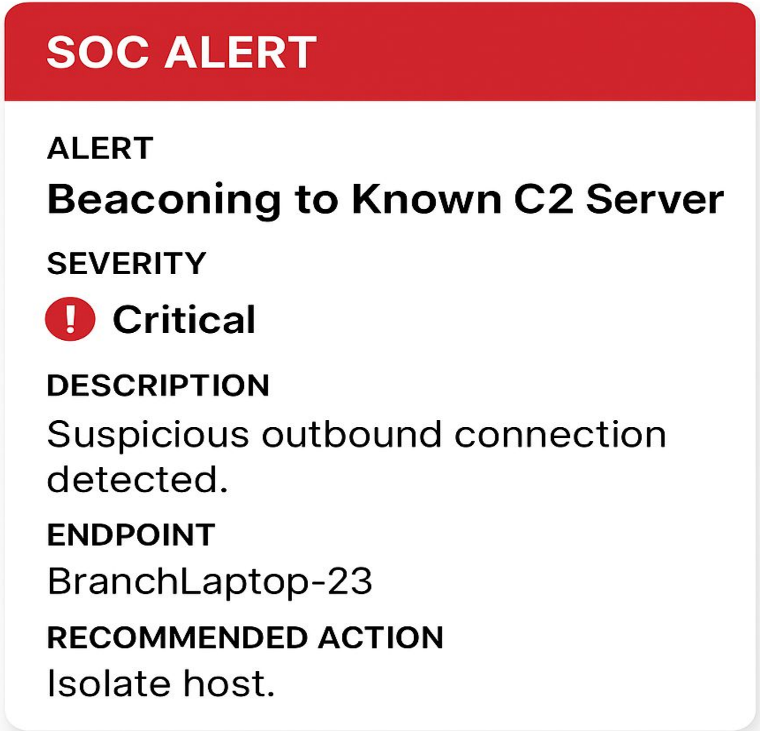
⚠ CRITICAL Core Router CPU Saturated

Router CPU Usage

100%

SNMP Unreachable

INJECT 4: A staff laptop in a branch office is found beaconing to a known C2 server.



SOC ALERT

ALERT

Beaconing to Known C2 Server

SEVERITY

❗ **Critical**

DESCRIPTION

Suspicious outbound connection detected.

ENDPOINT

BranchLaptop-23

RECOMMENDED ACTION

Isolate host.

INJECT 5 : The BICMA AND GOVTECH AGENCY requests an urgent briefing.

འབྲུག་གཞུང་འཕྲུལ་རིག་ལས་སྡེ།

GovTech

Bhutan

༄། འབྲུག་བརྡ་དོན་བརྒྱུད་འཕྲིན་དང་བརྡ་བརྒྱུད་དབང་འཛིན། ༎

BICMA

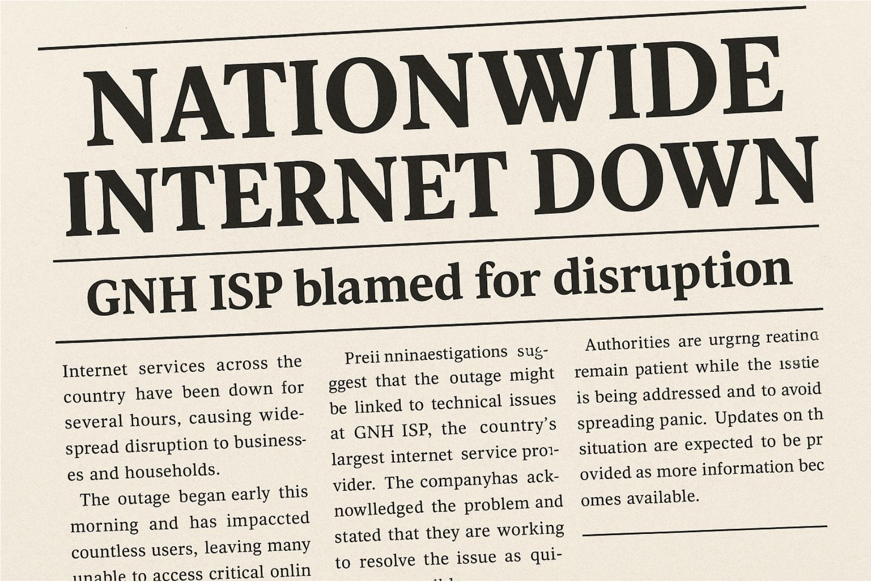
Bhutan InfoComm and Media Authority

Task: **Discuss in your group**

- What is the potential impact of the incident?
- What would be your action?
- Who do you involve?
- What information be shared and when should you be sharing ?

PHASE III -
SERVICE RECOVERY AND FALLOUT

INJECT 6 : Local news reports claim the "Nationwide internet is down" and blames GNH Infocomm Ltd.



NATIONWWIDE INTERNET DOWN

GNH ISP blamed for disruption

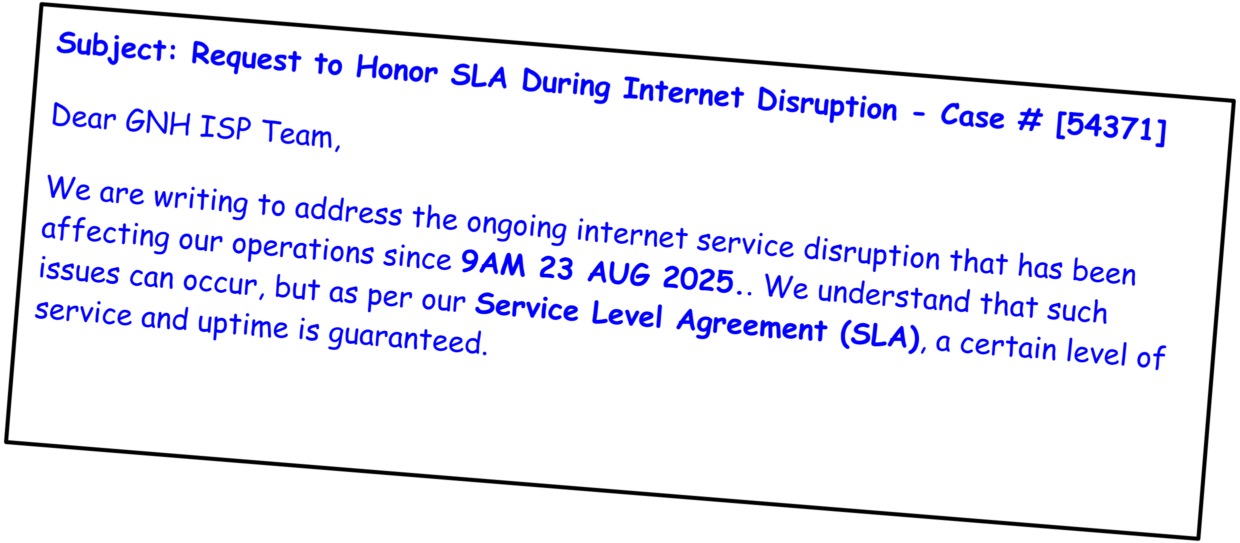
Internet services across the country have been down for several hours, causing widespread disruption to businesses and households.

The outage began early this morning and has impaccted countless users, leaving many unable to access critical onlin

Preii nninaestigations suggest that the outage might be linked to technical issues at GNH ISP, the country's largest internet service proıvider. The companyhas acknowlledged the problem and stated that they are working to resolve the issue as qui-

Authorities are urgrng reatinα remain patient while the ıssie is being addressed and to avoid spreading panic. Updates on th situation are expected to be pr ovided as more information bec omes available.

INJECT 7 : Cloud and enterprise customers demand SLAs be honored.



Subject: Request to Honor SLA During Internet Disruption - Case # [54371]

Dear GNH ISP Team,

We are writing to address the ongoing internet service disruption that has been affecting our operations since **9AM 23 AUG 2025**.. We understand that such issues can occur, but as per our **Service Level Agreement (SLA)**, a certain level of service and uptime is guaranteed.

INJECT 8: Logs show exfiltration attempts targeting customer data.

```
Aug 23 14:23:11 fw01 kernel: [UFW ALLOW] OUTBOUND
SRC=1XX.168.10.45 DST=2XX.0.113.55 PROTO=TCP DPT=443 LEN=1200
BYTES=5242880 SESSIONS=1 NOTE="Large outbound transfer"
```

Task: **Discuss in your group**

- What is the potential impact of the incident?
- What would be your action?
- Who do you involve?
- What information be shared and when should you be sharing ?

DEBRIEF AND WRAP UP

REFLECTION

- What went well?
- What were the gaps and delays?
- What improvement and tools is needed?
- Were we well-prepared for DNS-level attacks?
- Was internal escalation fast enough?
- Were customer communication protocols effective?

https://thegfce.org/wp-content/uploads/Deliverable-1-Intro-to-TTX-Final-Version.pdf

https://www.youtube.com/watch?v=-ZjOxks33Mc&t=62s

END of Exercise