

National Cybersecurity Framework

NEED OF SMART SOCIETY

ABOUT ME

Bijay Limbu Senihang

Co-Founder and Chief Technology Officer of Rigo Technologies Pvt. Ltd.

We provide Information and Cybersecurity Service

Rigo Cyber Threat Monitoring System

Security Operation Center as a Service

Vulnerability Assessment and Penetration Testing

Information System and Security Audit

CLIENTELE



OBJECTIVES

01.

Nepal to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace.

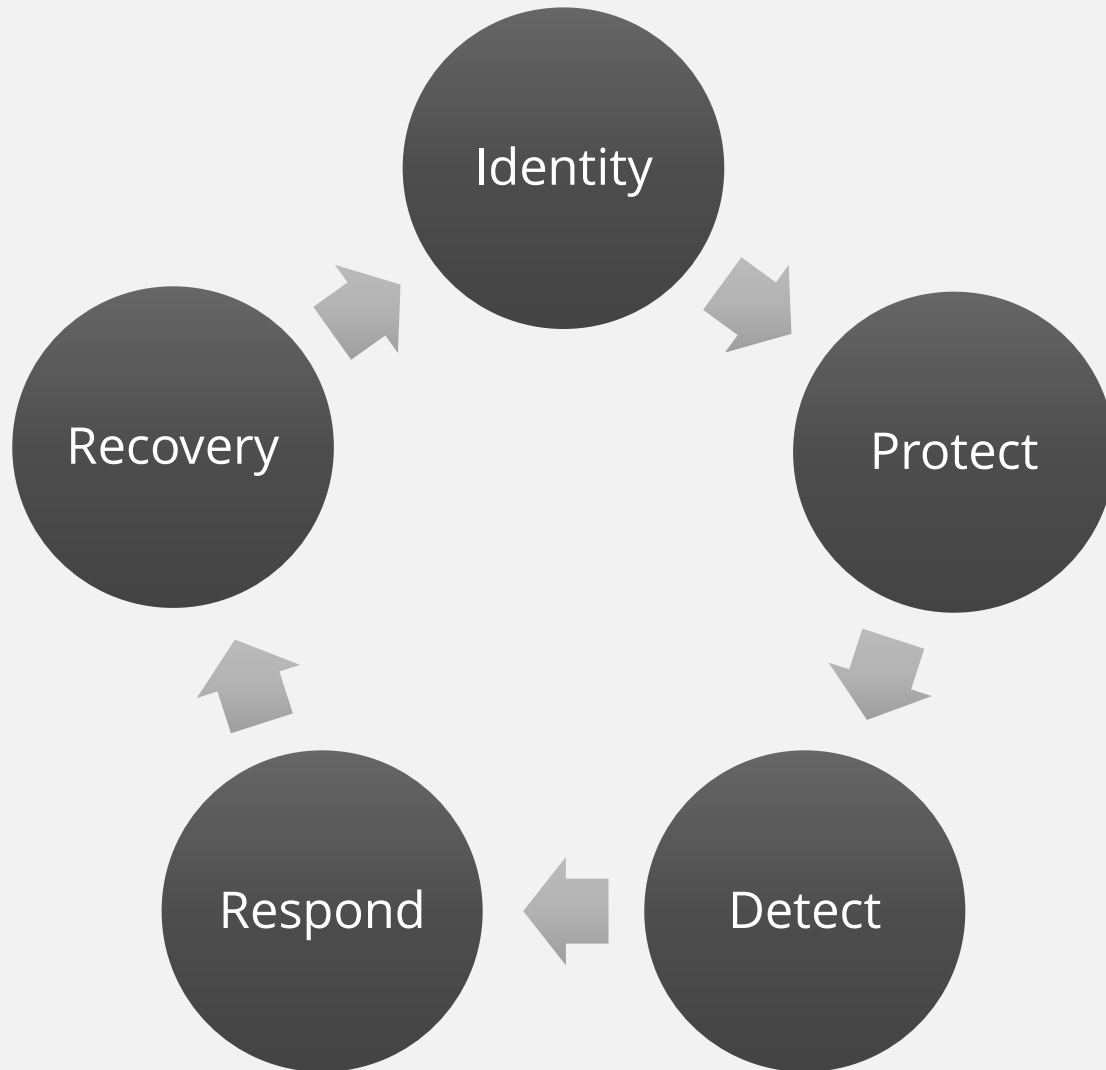
02

Nepal to be more resilient to cyber attacks and better able to protect our interests in cyberspace.

03.

Nepal to have helped shape an open, stable and vibrant cyberspace which the Nepal public can use safely and that supports open and smart society.

NATIONAL CYBERSECURITY FRAMEWORK



Cybersecurity framework comprises of risk based compilation of guidelines that can help to Identify, Implement and Improve cybersecurity practices and create a common platform for internal and external communication of cybersecurity issues.

IDENTIFY



- Classification of Industries
- Data and Information Classification
- Define Critical Infrastructure
- Inventory of System and Software used in Critical Infrastructure
- Cyber Security Act
- Data Protection Act
- Privacy Act
- Consumer Data Security and Breach Notification Act
- Business Impact Analysis
- Threats and Vulnerabilities Likelihoods and impact analysis

— PROTECT



- National Cybersecurity Policy and Guidelines
- Cybersecurity Regulation as per the industry
- Cybersecurity Guideline as per the industry
- National Plan for Cybersecurity awareness training
- Establishment of National Cybersecurity Defense Unit
- Establishment of Cyber Bureau at Nepal Police
- Establishment of Cyber Intelligence Unit at Nepal Army

DETECT



- Establishment of National Cyber Security Operation Center
- Initiation of National Honeypot Project
- Monitoring Activities of Cyber Terrorist, Cyber criminals
- Continuous Vulnerability Scanning of Critical Infrastructure and Government Infrastructure.

RESPOND



- Establishment of National Computer Emergency Response Team
- National Cyber Incident Submission and Sharing platform
- Enhancement of Cyber Forensic Lab
- Notification channel of Cyber Incidents

RECOVERY



- National Business Continuity and Disaster Recovery Plan
- National Public Relation Management
- Cybersecurity friendly environment for Judiciary
- Reporting mechanisms to all stakeholders
- Recovery plans incorporate lessons learned



Co-ordination with other International CERT,
Cybersecurity Community, Cybersecurity
Service Provider and International
Cybersecurity Regulatory Bodies

NEED OF NATIONAL CYBERSECURITY FRAMEWORK





THANK YOU!