INDIALAW



CIVIL

Understanding Computer Emergency Response Team (CERT-In) : India’s Cybersecurity Response Framework

AUTHOR Rahul Sundaram

PUBLISHED 25 November 2024

Introduction

The Computer Emergency Response Team (CERT-In) is a vital component of India's cybersecurity infrastructure, established under the Information Technology (IT) Act, 2000. This article sets out the legal provisions, functions, responsibilities, and operational framework of CERT-In, and its role in protecting the country's digital infrastructure.

Table of contents

- Introduction
- Legal Provisions Under the IT Act
- Definitions and Key Terms
- Functions and Responsibilities of CERT-In
- Role of CERT-In in International Coordination
- Stakeholders and Collaboration
- Reporting Requirements
- Review Committee
- Conclusion

Legal Provisions Under the IT Act

CERT-In was formally established through Section 70B of the IT Act, which empowers the government to designate a team to respond to cybersecurity incidents and protect critical information infrastructure. The following sections of the IT Act are particularly relevant to CERT-In's operations:

Definitions and Key Terms

The framework governing CERT-In includes several key definitions:

Cybersecurity Incident: An event that compromises the integrity, confidentiality, or availability of information.

Director General: The head of CERT-In, responsible for overseeing its operations.

Critical Information Infrastructure: Systems essential for the functioning of the economy and society, which CERT-In aims to protect.

Functions and Responsibilities of CERT-In

CERT-In is tasked with a broad range of responsibilities aimed at enhancing cybersecurity resilience in India. These include:

1. Incident Response: Providing timely responses to cybersecurity incidents to mitigate damage.

2. Prediction and Prevention: Identifying potential threats and vulnerabilities to prevent incidents before they occur.

3. Analysis and Forensics: Conducting detailed investigations into cybersecurity incidents to understand their nature and impact.

4. Information Security Assurance: Offering audits and assessments to ensure the security of information systems.

5. Training and Awareness: Educating stakeholders about cybersecurity best practices and emerging threats.

CERT-In (Computer Emergency Response Team, India) is central to coordinating with emergency response teams of other countries to enhance global cybersecurity measures. Here's a breakdown of its functions and responsibilities in this area:

Role of CERT-In in International Coordination

1. Information Sharing:

CERT-In collaborates with international counterparts to share information regarding emerging threats, vulnerabilities, and malware. This exchange of data helps in identifying global trends in cyber threats and developing strategies to combat them.

2. Collaborative Incident Response:

In the event of significant cyber incidents that cross national borders, CERT-In works with other countriesâ?? CERTs to respond effectively. This includes joint investigations, sharing resources, and implementing coordinated responses to mitigate impacts.

3. Capacity Building:

CERT-In engages in capacity-building activities, where it shares its expertise and best practices with other nations. This may include training programs, workshops, and collaborative research initiatives aimed at strengthening national and regional cybersecurity frameworks.

4. Participation in International Forums:

CERT-In actively participates in global and regional cybersecurity forums such as the Global Forum on Cyber Expertise (GFCE) and ASEAN Ministerial Conference on Cybersecurity (AMCC). These platforms allow for dialogue, exchange of ideas, and collaborative efforts among various nations.

5. Bilateral and Multilateral Agreements:

CERT-In may engage in bilateral and multilateral agreements with other countries to enable cooperation in cybersecurity. These agreements outline the framework for collaboration, including information sharing, joint exercises, and mutual assistance during cybersecurity incidents.

6. Awareness and Training Programs:

Through collaborations, CERT-In also conducts awareness campaigns and training programs, helping other countries develop their capabilities in responding to cybersecurity threats.

7. Incident Reporting and Alerts:

CERT-In is a point of contact for receiving and disseminating information about threats and vulnerabilities from international sources, ensuring that Indian stakeholders remain informed about global cybersecurity issues.

Stakeholders and Collaboration

CERT-In collaborates with various stakeholders to strengthen its cybersecurity efforts, including but not limited to:

Sectoral Computer Emergency Response Teams: Specialized teams focusing on specific sectors.

Intermediaries: Entities that enable communication and data exchange.

Internet Registries and Domain Registrars: Organizations that manage domain names and IP addresses.

Industry and Academia: Collaborating with businesses and educational institutions for research and development in cybersecurity.

Law Enforcement Agencies: Working together to address cybercrime and enhance security measures.

Reporting Requirements

CERT-In mandates the reporting of specific types of cybersecurity incidents, which include:

– Targeted scanning or probing of critical networks.

– Unauthorised access of IT System/data

-Defacement of website or intrusion into a website and unauthorised change such as inserting malicious code, links to external websites

– Compromise of critical systems or unauthorized access to IT systems.

– Malicious code incidents and phishing attacks.

– Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

– Identity theft, spoofing, and other cyber threats

– Attacks on application such as e-governance, e-commerce etc.

– Attacks on critical infrastructure , SCADA System and Wireless networks

– Attack on servers such as databases, mail and DNS and network devices such as routers

Review Committee

To ensure effective governance, a Review Committee oversees CERT-In's operations. This committee includes but is not limited to representatives from various government ministries, such as:

– Ministry of Law and Justice

– Department of Telecommunications

– Ministry of Home Affairs

– Group Coordinator for Cyber Law and e-Security

The committee meets regularly to assess CERT-In's performance and provide strategic direction.

Conclusion

The role of CERT-In in coordinating with emergency response teams from other countries is critical to creating a strong international cybersecurity framework. By encouraging collaboration, sharing knowledge, and responding to incidents collectively, CERT-In enhances the ability of nations to combat cyber threats effectively. This cooperation safeguards national interests and contributes to global stability in cyberspace.

CERT-In also is central to India's cybersecurity framework, providing essential services to mitigate risks and respond to incidents. Its establishment under the IT Act ensures a structured approach to managing cybersecurity threats, backed by legal provisions that enable cooperation among various stakeholders. As cyber threats continue to evolve, CERT-In's proactive measures and collaborative efforts will be vital in safeguarding India's digital infrastructure.

For more information write to contact@indialaw.in