Sections

ENGLISH | தமிழ் | বাংলা | മലയാളം | ગુજરાતી | हिंदी | मराठी | BUSINESS | बिज़नेस

Newsletters

Tuesday, Jan 30, 2024
EPAPER TODAY'S PAPER

The Indian EXPRESS
JOURNALISM OF COURAGE

Home Cities India Explained Opinion Business Entertainment Sports Politics UPSC Essentials Lifestyle

TRENDING Get UPSC Express Budget 3 Things Play Premium Health &

News / Business / Market / Overhaul of cybersecurity frameworK: To safeguard cyber infra, Govt may push use of made in India products

Premium

Overhaul of cybersecurity frameworK: To safeguard cyber infra, Govt may push use of made in India products

National Critical Information Infrastructure Protection Centre is behind the framework

Written by **Soumyarendra Barik** Follow
New Delhi | Updated: January 30, 2024 07:24 IST

NewsGuard

Follow Us

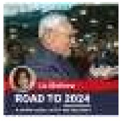
The government has drawn up a guiding policy called the National Cybersecurity Reference Framework (NCRF) in an attempt to provide an implementable measure – with clear articulation of roles and responsibilities for cybersecurity – based on existing legislations, policies and guidelines. (Representational Image)

Asserting that there has been significant progress over the last few years in the development of indigenous cybersecurity products and solutions, the Centre is expected to recommend enterprises – especially those in critical sectors like banking, telecom, and energy – to use only security products and services developed in India, The Indian Express has learnt.

The government has drawn up a guiding policy called the National Cybersecurity Reference Framework (NCRF) in an attempt to provide an implementable measure – with clear articulation of roles and responsibilities for cybersecurity – based on existing legislations, policies and guidelines.

The action comes as India faces a barrage of cybersecurity-related incidents – most recently a high-profile attack on the systems of AIIMS Delhi in 2022– which pose a major challenge to New Delhi's national security imperatives. At least three union ministers told The Indian Express that they feel hamstrung by the lack of an overarching framework on cybersecurity when they are formulating sector-specific legislations. This is what the NCRF is expected to solve.

“In recent years many threat actors backed by nation-states and organised cyber-criminal groups have attempted to target Critical Information Infrastructure (CII) of the government and enterprises. In addition, availability of ‘cyber-attacks-a service’ has reduced the entry threshold for new cyber criminals, thus incre the exposure to individuals and organisations,” the NCRF is learnt to say.



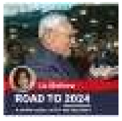
The framework has been drawn up by the National Critical Information Infrastructure Protection Centre (NCIIPC) – which reports to the Prime Minister’s Office – with support from the National Cybersecurity Coordinator (NCSC).

The NCRF was shared privately with companies and other government departments for consultation in May last year, but is yet to be made public. Apart from the main policy document, at least three supporting compendiums detailing global cybersecurity standards, products and solutions have also been formulated.

This paper has also learnt that the NCRF could recommend that enterprises allocate at least 10 per cent of their total IT budget towards cybersecurity. “Adequate resources must be allocated for cybersecurity, and these should be distinct from IT resources… Based on global best practice, it is recommended that at least 10 per cent of the total IT budget should be allocated to cybersecurity. Such allocation should be mentioned under a separate budget head for monitoring by the top-level management / board of directors,” the NCRF is likely to recommend.

Last June, former National CyberSecurity Coordinator Lt. General Rajesh Pant had said that the NCRF will be released for the public soon. The current guiding framework on cybersecurity for critical infrastructure in India comes from an UPA-era measure, the National Cybersecurity Policy of 2013. “It (NCRF) is an important document that supersedes the 2013 policy. From 2013 till 2023, the world has changed as new threats and new cyber organisations have emerged calling for new strategies. The document will be put in public domain after a final check by the committee to ensure that nothing confidential is released,” he said. However, the NCRF is a guideline, meaning that its recommendations will not be binding – although, organisations can use the NCRF to improve their cybersecurity posture, reduce their risk of data breaches or any cybersecurity incidents, ensure compliance with regulations, increase confidence with customers and enhance operational efficiency.

Queries sent to the NCSC's office remained unanswered until publication. Th could also recommend that along with the directions to regulate the operati the critical sector, regulators overseeing and auditing them must also define information security requirements.



"The regulators may also need to access sensitive data and deficiencies related to the operations in the critical sector, and therefore they also would need to have an effective Information Security Management System (ISMS) instance," the policy may recommend.

It could also prescribe that national nodal agencies evolve platforms and processes for machine-processing of data from different entities to carry out sectoral and cross-sectoral analysis of audit compliance, audit effectiveness and grading of auditors.

More Premium Stories

Important to never forget that Ram Rajya was an embodiment

Sachin Pilot at Idea Exchange: 'Raising funds for anybody except

A to Z of Budget

Soumyarendra Barik Follow

Soumyarendra Barik is Special Correspondent with The Indian Express and reports on the intersection of technology, policy and society. With over five years of nev ***... Read More***