2023 GLOBAL STATE OF CYBERSECURITY STUDY

Fallout from the COVID-19 crisis continues to fundamentally **reshape the IT security landscape** in India. Survey findings over the past 12 months reveal what types of attacks Indian organisations faced, how they responded and what will be top of mind as 2023 unfolds.

7 out of **10**

Organisations in India suffered at least one data breach

134 AVERAGE NUMBER ATTACKS PER ORGANISATION IN PAST YEAR

- **26** email/phishing
- **22** network
- **20** application
- **18** ransomware
- **17** device/endpoint
- **16** cloud
- **15** third party/supply chain

HOW INDIAN ORGANISATIONS RESPONDED IN THE WAKE OF COVID-19

68% Accelerated digital transformations to support remote workers

63% Boosted support for customer portals

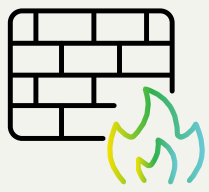
58% Added resources to their networks and databases

TOP SECURITY TECHNOLOGY SOLUTIONS

73% Added cloud-managed DNS-DHCP-IPAM servers to harden security

62% Added remote corporate-owned mobile devices to their networks

55% Added new VPNs or firewalls



BIGGEST CHALLENGES

1. 
IT security skills shortage

2. 
Poor visibility into cloud usage

3. 
Monitoring remote worker access

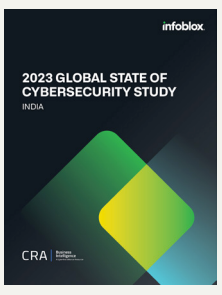
MOST URGENT THREATS FOR NEXT 12 MONTHS

57% Data leakage

40% Direct attacks through cloud services

39% Attacks through networked IoT devices

> "The biggest threats we will face in 2023 are malware, the economy and the lack of skills and equipment we need [to counter] it."
>
> –Senior manager, Indian manufacturing company



> GET THE FULL REPORT

Complete insights and top cyberssecurity issues and priorities for the coming year are available in the full **2023 Global State of Cybersecurity Study: India**

Survey findings were conducted by the CyberRisk Alliance and underwritten by Infoblox.