infoblox

2023 GLOBAL STATE OF CYBERSECURITY STUDY

Economic and geopolitical fears shaped the IT security landscape for organizations across the globe over the past 12 months. Survey findings reveal what types of attacks were most prominent, how organizations responded and what will be top of mind as 2023 unfolds.

>60%

Of organizations globally suffered at least one data breach

$2M

Average cumulative losses for each organization suffering breaches

TOP ATTACK VECTORS

Percent among organizations with one or more attacks

81	email/phishing
56	cloud
56	application
55	device/endpoint
54	ransomware
50	third party/ supply chain
49	network

HOW GLOBAL ORGANIZATIONS RESPONDED IN THE WAKE OF COVID-19

52% Accelerated digital transformations to support remote workers

45% Added resources to their networks and databases

44% Boosted support for customer portals

DNS IN CYBER DEFENSE

How organizations globally used DNS in their security strategies

51%

Protected against DNS tunneling and DGAs

48%

Blocked DNS requests to bad destinations to ease perimeter defense burdens

49%

Flagged devices connecting to bad destinations

40%

Located malware early in the cyber kill chain

BIGGEST CHALLENGES

1. Monitoring remote worker access

2. IT security skills shortage

3. Lack of budget

MOST URGENT THREATS FOR NEXT 12 MONTHS

50%

Data leakage

36%

Direct attacks through cloud services

22%

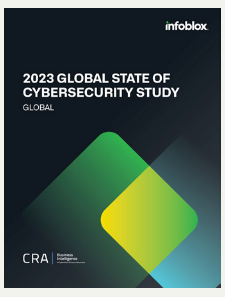
Advanced persistent threats

40%

Ransomware

33%

Attacks exploiting remote-worker connections



> GET THE FULL REPORT

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

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