infoblox®

2023
GLOBAL STATE OF CYBERSECURITY STUDY

U.S. organizations grappling with a changed **cybersecurity landscape continue to find their way in a hybrid work world**—responding to different consumer demands amid ongoing labor and supply shortages, inflationary pressures and mercurial financial markets. All of these forces will impact a security operations team's ability to protect IT networks and assets from known and emerging cyber threats into 2023.

UNITED STATES

~60%

Of U.S. organizations suffered one or more breaches originating from cloud infrastructure or apps, remote endpoints or IoT devices/networks

AVERAGE NUMBER ATTACKS PER ORGANIZATION BY TYPE

50 email/phishing
23 network
17 application
15 device/endpoint

HOW U.S. ORGANIZATIONS RESPONDED IN THE WAKE OF COVID-19

48% Accelerated digital transformations to support remote workers

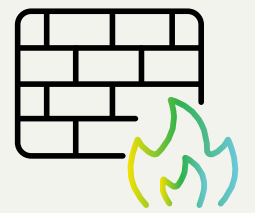**46%** Added resources to their networks and databases

38% Hired more IT staff

TOP SECURITY TECHNOLOGY SOLUTIONS

51% Added new VPNs or firewalls

50% Added cloud-managed DNS-DHCP-IPAM servers to harden security

48% Added remote corporate-owned mobile devices to their networks

---

BIGGEST
CHALLENGES

1. Shortage of IT security skills

2. Monitoring remote worker access

3. Lack of visibility into the user and device activity on the network

---

MOST URGENT THREATS FOR NEXT 12 MONTHS

47% Data leakage

46% Ransomware

42% Attacks exploiting remote-worker connections

37% Direct attacks through cloud services

"As we settle into a new normal, we need to be able to support a remote workforce for the long haul. We need the ability to adapt and change in order to support these teams."

–Director of technology support services, U.S. technology company

---

> GET THE FULL REPORT

2023 GLOBAL STATE OF CYBERSECURITY STUDY
UNITED STATES

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

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