infoblox

2023 GLOBAL STATE OF CYBERSECURITY STUDY

The United Arab Emirates as a nation has **shifted more resources toward cybersecurity since seeing a sharp rise in cyber attacks in recent years**, particularly multi-vector distributed denial of service (DDoS) attacks. But there's a great deal more that needs to be done to gain ground on malicious hackers—those residing both within and outside of the UAE.

66%

Of UAE organisations suffered a data breach by remote endpoint, IoT device, Wi-Fi or cloud

AVERAGE NUMBER ATTACKS PER ORGANISATION

27 email/phishing

15 device/endpoint

15 network

14 application

HOW UAE ORGANISATIONS RESPONDED IN THE WAKE OF COVID-19

61% Accelerated digital transformations to support remote workers

41% Added resources to their networks and databases

37% Added new VPNs or firewalls

37% Hired more IT staff

TOP SECURITY TECHNOLOGY SOLUTIONS

59% Added remote corporate-owned mobile devices to their networks

59% Added cloud-managed DNS-DHCP-IPAM servers to harden security

37% Added new VPNs or firewalls

BIGGEST CHALLENGES

1. Monitoring remote worker access
2. Keeping up with alert analysis and response
3. Shortage of IT security skills

MOST URGENT THREATS FOR NEXT 12 MONTHS

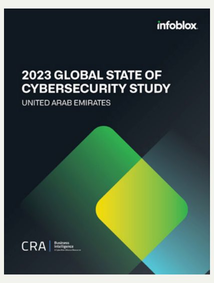
48% Data leakage

27% Ransomware

40% Direct attacks through cloud services

27% Attacks exploiting remote-worker connections

> "The greatest threat comes from insufficient internal security."
>
> –VP, IT security UAE manufacturer



infoblox

2023 GLOBAL STATE OF CYBERSECURITY STUDY

UNITED ARAB EMIRATES

CRA

> 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: UAE**

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