infoblox

2023 GLOBAL STATE OF CYBERSECURITY STUDY

UNITED KINGDOM

CRA | Business Intelligence
A CyberRisk Alliance Resource

METHODOLOGY

The data and insights in this CyberRisk Alliance report are based on an online global survey conducted in July/August 2022 with IT and cyber security decision-makers and influencers from 13 countries—including 100 U.K.–based organisations of all sizes. U.K. respondents ranged from chief executives and directors to analysts and consultants. Respondents were employed in various industries, with most from technology (35%), business or professional services (16%), manufacturing (14%) and financial services (12%).

EXECUTIVE SUMMARY

The Russia-Ukraine war continues to impact other nations, including the outlook among U.K. cyber security professionals concerned with economic ramifications, supply chain attacks and state-sponsored threats. “Global conflicts between different countries, especially the Ukrainian war, have greatly increased the likelihood of cyberattacks and have made our organisation more vulnerable to such attacks,” according to a vice president of information technology at a U.K.-based retailer.

As the third anniversary of the COVID-19 pandemic approaches, U.K. organisations continue to adapt to a remote and mobile workforce and online-oriented consumers. They are particularly keen to expand cloud offerings and apply both traditional security controls like DNS security and virtual private networks and newer options, like cloud access security brokers, to various IT environments. This study shows these decision-makers and influencers worry about having enough funding and talent to tackle what they see as the most concerning threats in the coming year: a rise in ransomware, insider threats and state-sponsored attacks.

Training remains a top priority, given how many employees still fall for phishing ploys—requiring more vigilance to prevent both existing and emerging threats from becoming breaches. That said, a majority of participating organisations currently are able to investigate threats in under a day using popular tools like threat intelligence and network traffic analyses. However, more than half (56%) of all U.K. respondents said they suffered one or more breaches in the past 12 months because of a security incident.

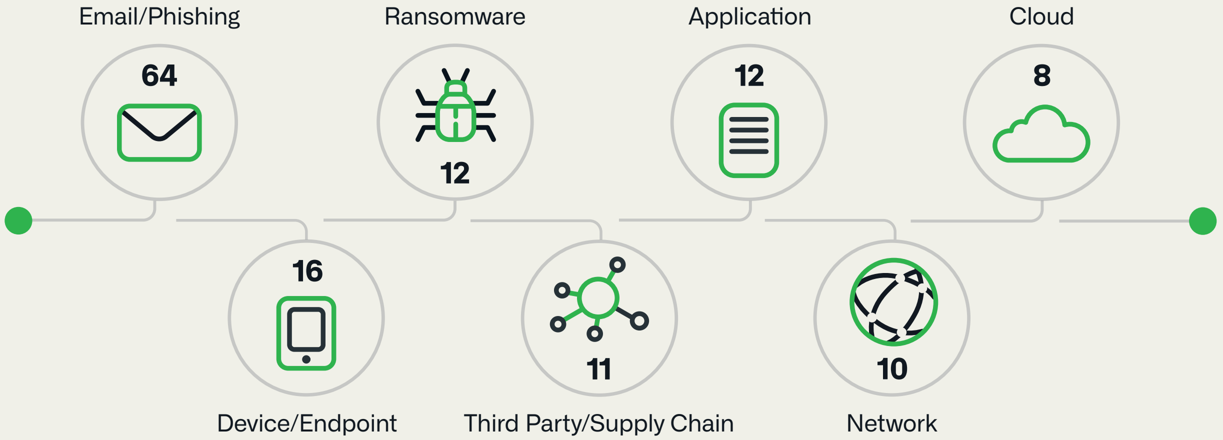
Findings from the 2022 study among U.K. respondents reveal the following trends in the United Kingdom:

47%

of U.K. organisations accelerated digital transformations to support remote workers

1. **Since the COVID-19 pandemic began, many U.K. organisations added network resources, fast-tracked digital transformations to support remote workers and boosted support for customer portals to support their workforces or customers.** Almost half (47%) of all respondents accelerated digital transformations to support remote workers and increased support for customer portals for remote customer engagement. Another 41% moved more applications to third-party cloud providers. Additionally, 37% added resources to networks and databases; 32% focused network and security controls on the edge (such as SASE, secure access service edge); and 29% hired more IT staff. More than a quarter (27%) closed physical offices and 17% reduced IT staff. Least popular actions were switching IT staff to other roles (14%) and decreasing reliance on third-party cloud providers (9%). One in 10 had not made any changes to support their workforces or customers since early 2020.

U.K.: Average Number of Issues Across Various Attack Vectors



2. **In the past year, a large share of U.K. organisations added VPNs, firewalls and cloud-managed DDI servers to protect their networks while managing the proliferation and associated security risks from remote employee-owned devices on the network.** Roughly two-thirds (62%) of respondents reported their organisation added VPNs or firewalls and cloud-managed DNS-DHCP-IPAM—known collectively as DDI— servers (48%) to their networks. The BYOD trend among remote workforces continues to be prevalent, with nearly half (47%) of respondents reporting remote employee-owned devices were also added to their networks.

3. **In the next 12 months, U.K. respondents said their organisation will be most concerned about data leakage, ransomware and attacks through remote-worker connections.** Data leakage (50%) and ransomware (49%) continue to be the most worrisome cyber threats, followed by attacks exploiting remote-worker connections (36%) and direct attacks through cloud services (32%).

4. **U.K. respondents believe their organisation is least prepared for data leaks, ransomware and insider threats, as well as state-sponsored attacks.** Respondents said they felt the least prepared to defend their organisation's networks against data leakage (17%), ransomware (16%), insider threats (15%) and state-sponsored attacks (14%). The lack of technological and human resources alongside growing prevalence of data leakage, ransomware and state-sponsored attacks had participants worried. "They tend to be highly specialized and undertaken by experts with almost unlimited resources," noted one respondent most concerned about threats from nation-states.

5. **On average, U.K. organisations detected at least roughly four times as many issues resulting from email/phishing attacks than any other type, including device/endpoint, ransomware and application attacks.** Respondents estimated their organisation detected issues resulting from roughly 64 email/phishing attacks in the past 12 months, as well as 16 device/endpoint attacks, 12 ransomware attacks and 12 application attacks in the same period.

4x

U.K. organisations detected at least four times as many issues resulting from emails and/or phishing attacks than any other type, including device/endpoint, ransomware and application attacks

£1.5 mil

the estimated average value of U.K. organisational losses

78%

of organisations take 2 hours to 24 hours to investigate a threat

6. **More than half (56%) of U.K. respondents reported one or more breaches to their organisation—most originating from the cloud, Wi-Fi, insiders or Internet of Things (IoT) devices/networks.** Cloud infrastructure or applications accounted for the origin of 39% of breaches to respondents' organisations in the past 12 months, followed by Wi-Fi access points (30%), insiders such as current and former employees (27%) and IoT devices or networks (25%).

7. **Phishing was the most common attack method against organisations that were breached. Phishing accounted for two-thirds of attack methods in the past year, followed by ransomware (41%) and advanced persistent threats (APTs) (38%).** In those attacks, the largest shares of breach victims reported their attackers most often used data exfiltration (50%), credential hijacking (43%) and privilege escalation (38%) against the organisation.

8. **Collectively, the estimated average value of U.K. organisational losses—including direct and indirect financial losses as well as reputational harm and remediation expenses—resulting from those breached in the past year was roughly £1.5 million at the time of the study.** Organisations that were victims of breaches mostly experienced sensitive data exposure/exfiltration or system outages (46% each) and data manipulation (43%). Another 7% said a breach resulted in bodily or psychological injury, and 9% said it led to a loss of life.

9. **U.K. organisations used a variety of controls to protect their networked assets in on-premises, cloud-based and hybrid (on-premises and cloud-based) environments.** Among the various controls used, the most prevalent are VPNs and DNS security for on-premises assets (34%), cloud access security brokers (45%) for cloud-based environments and network security tools, such as firewalls and intrusion prevention systems, (38%) for hybrid environments.

10. **On average, most organisations (78%) take up to 24 hours to investigate a threat, with many relying on third-party threat intelligence platforms or services.** Another 16% said probes took less than an hour. To aid their investigations or threat hunts, security teams rely on third-party intelligence resources (40%), network flow data (39%) and vulnerability information specific to their systems (38%).

> “Ransomware will be the biggest threat because these threats have become a lot more common in recent years, and it can cause major disruption.”
>
> Chief information officer, U.K. business/professional service provider

40%

of U.K. organisations indicated their IT security budgets increased in 2022

11. **The Domain Name System (DNS) provides various security measures to protect organisations and is a key component in virtually all organisations’ security strategies.** Respondents reported their organisation mostly uses DNS in its strategy to help with the following: informing them of devices making requests to connect to malicious destinations (48%); protecting against threats like DNS tunneling, data exfiltration and domain-generating algorithms that other security tools might miss (46%); and helping detect malware activity earlier in the kill chain (40%).

12. **The top anticipated challenges in protecting against attacks relate to limited budgets and the ability to monitor remote worker access.** Forty-two percent of all U.K. respondents reported their organisation struggles with a lack of budget. Monitoring remote worker access and a shortage of IT security skills were also challenges for one-third of respondents, followed by lack of visibility into cloud access and usage, mentioned by 23%.

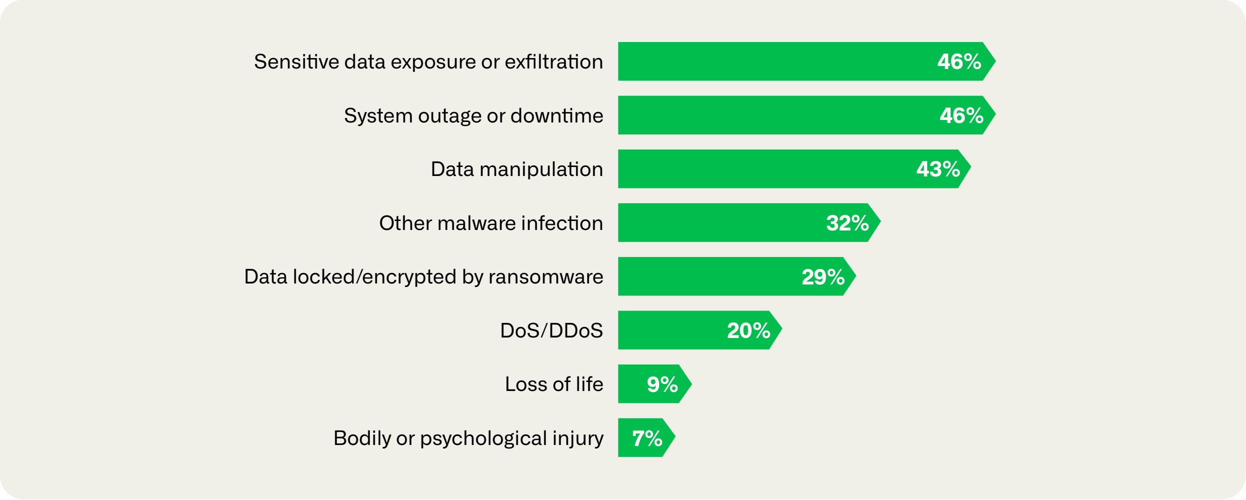
13. **Forty percent of U.K. organisations indicated their IT security budgets increased in 2022, and 52% said they expected bigger security budgets in 2023 to combat known and new threats.** Another 22% expect no change to their budgets, while 24% expect their budgets to shrink next year. Many of the perceived threats in 2023 are influenced by the war in Ukraine and the rise of ransomware and advanced threats in general, according to many respondents. “The biggest threats of cybersecurity will be state-sponsored cyberattacks due to the Russia-Ukraine war; attacks on supply chains; and cyberattacks on remote workers’ devices,” said a director of information technology for a retailer.

14. **The most popular planned technology purchases include data encryption (20%), secure provisioning and deprovisioning (19%) and DNS security, network security and/or VPN/access controls (18%) for on-premises protection; cloud access security broker (CASB) (44%), VPN/access control (36%) and secure web gateways (34%) for cloud-based systems; and network security (firewalls, IPS, etc.) (40%), threat intelligence (37%) and both data encryption and network traffic monitoring/network detection and response (NDR) for hybrid environments (36%).** The highest priorities for improving network protection are generally related to staff training, new or updated equipment and data security.

15. **Throughout 2021 and 2022, phishing continued to persist as the main attack method for at least 8 out of 10 U.K. respondents, a trend they expect to continue in 2023.** Among organisations that were breached in 2022, 39% reported their cloud assets were compromised (compared to 32% in 2021)—replacing Wi-Fi access points as the top attack vector from the previous year.

What were the impacts of the breaches your organisation experienced in the past 12 months?

Select all that apply.



GAIN A MORE COMPREHENSIVE UNDERSTANDING

This report is based on country-level data from a global online survey conducted July/ August 2022. A more detailed global report and a regional report for Europe and UAE are available at Infoblox that provide additional insights about the survey results and offer an invaluable global perspective of the threat landscape that we all face, as well as the technology and security opinions of other security leaders around the world.

infoblox

Infoblox is the company that unites networking and security to deliver better performance and protection. We provide visibility and control over who and what connects to your network and identify threats through intelligent DNS. Learn more at https://www.infoblox.com.

Corporate Headquarters
2390 Mission College Boulevard,
Ste. 501, Santa Clara, CA 95054

+1.408.986.4000
info@infoblox.com
www.infoblox.com