infoblox

2023 GLOBAL STATE OF CYBERSECURITY STUDY

GLOBAL

CRA | Business Intelligence
A CyberRisk Alliance Resource

NO RELIEF IN SIGHT FOR CYBER SECURITY TEAMS IN 2023

Findings from the CRA Business Intelligence 2023 Global State of Cybersecurity Study

BACKGROUND

If 2022 is any indication, the current year will resemble recent years: fraught with employees and contractors unintentionally or willingly leaking data and difficult to monitor remotely. COVID-19 may now be an endemic, but other, potentially destructive forces are poised to replace it as a preoccupation among global cyber security operations.

Instead of fearing the spread of a deadly virus, organizations continued to negotiate rough economic waters due to growing geopolitical tensions—particularly arising from cyber powerhouses China and Russia. A looming global recession was increasingly expected, keeping anxiety levels high. Russia's war in Ukraine (the "breadbasket" of Europe and perhaps the world) continued to disrupt global markets, force painful rations and leave organizations vulnerable to the growing sophistication of cyber gangs and nation-states trolling networks to steal, expose and sell sensitive data for financial gain.

Such economic and geopolitical fears factored into results of the CRA Business Intelligence 2022 Global State of Cyber Security Report conducted as the pandemic was winding down and issues like inflation and war dominated news coverage. Cyber security teams hoping to catch their breath after a few years of pandemic-driven decisions didn't always get the relief they expected, especially on the threat front.

"Hackers are using more and more attacks that are not so easy to detect with antivirus or security programs," said a Brazilian respondent from the retail sector. Many from the study expressed concerns about the growth in cyber attack opportunities due to remote workers and demanding customers. By accelerating digital transformations to remain in business during the COVID-19 crisis, organizations also made themselves more vulnerable to cyber criminals.

In the past 12 months, many organizations worldwide also contended with ongoing labor shortages and inflation, forcing security operations to handle more incidents with fewer resources. Some filled talent or technology gaps through outsourcing, which generated new cyber risks; others moved more assets and applications to the cloud, spurring complaints of poor visibility into access as usage rose.

"Cloud-based attacks are more sophisticated as security has evolved and improved over the COVID period with people working from home," stated a respondent from an Australian healthcare organization.

The pandemic may no longer be a prime concern, but organizations worldwide remain on high alert for security incidents that develop into breaches. They continue to find the best path forward to remain competitive and secure, knowing the rough patches could be quite rocky.

METHODOLOGY

The data and insights in this report are based on a July/August 2022 global study conducted by CRA Business Intelligence and sponsored by global IT automation and security provider Infoblox. The survey for India was conducted in December 2022 and January 2023.

CRA conducted an online survey among 1,300 professionals in multiple languages across 13 global markets, with 100 respondents from each of the following countries: United States, Mexico, Brazil, United Kingdom, Germany, France, The Netherlands, Spain, United Arab Emirates, India, Australia, Singapore, and Japan.

Respondents were technology and business professionals, including chief executives, VPs, directors, managers, and senior analysts who worked in fields such as high-tech/technology; business, financial and professional services; manufacturing; retail and ecommerce; healthcare; education; transportation; government; non-profits; media; energy and utilities; and more.

Survey objectives were to gain greater visibility into the global state of cyber security, including the ongoing impact remote workers and customers have on organizations as well as security challenges experienced since the start of the pandemic in 2020. Respondents also shed insight into current threats and anticipated investments to prevent attacks from becoming breaches. Data was compiled from responses to structured survey questions, and respondents were encouraged to provide corresponding comments where applicable.

EXECUTIVE SUMMARY

Key findings from this study include the following:

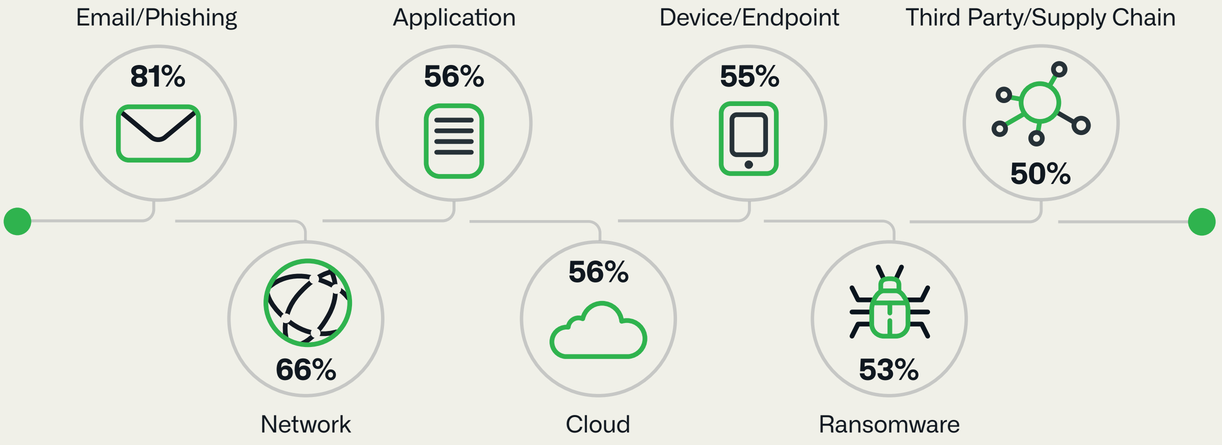
52%

of global organizations accelerated digital transformations to support remote workers

1. **Since the start of the pandemic, approximately half of all organizations globally responded to the needs of their remote workforce and customers by fast-tracking digital transformations** (52%)**, adding resources to networks and databases** (45%) **and increasing support for customer portals** (44%). Roughly one-third of respondents said their organization hired more IT staff, moved more apps to third-party cloud providers and placed network and security controls on the edge. One in five closed physical offices, and some switched IT staff to other roles, reduced IT headcounts or decreased their reliance on third-party cloud providers.
2. **Data leakage, ransomware and cloud attacks were chief concerns for many organizations globally for the coming year.** Many were also concerned about their remote worker connections, APTs, attacks through networked IoT, insider threats, supply chains or third parties and state-sponsored attacks.

Global: Percentage of Attacks Across Various Vectors

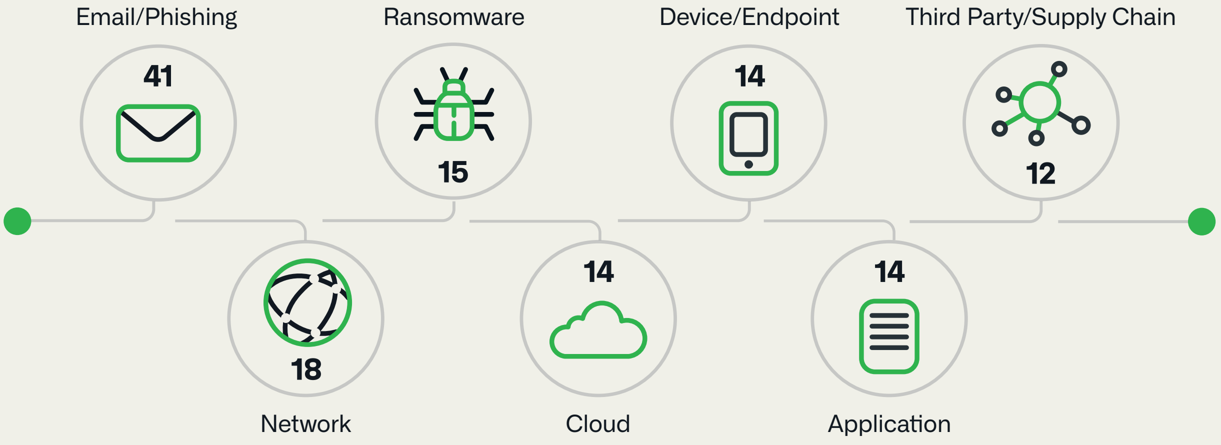
Percentage that experienced one or more attacks in the past 12 months



3. **Globally, organizations were much more likely to have experienced a phishing attack in the past 12 months, compared to ransomware, network, cloud, application, endpoint and third-party attacks.** A large majority (81%) indicated they experienced one or more email/phishing attacks in the past 12 months, with an average of roughly 41 issues from this attack vector. Additionally, two-thirds of respondents said they experienced at least one network attack, on average, during this time period resulting in roughly 18 network issues. At least half of all respondents said their organization also suffered cloud, application, device/endpoint, ransomware and third-party/supply chain attacks, resulting in an average of roughly 12 or more issues from these attack vectors.

4. **Wi-Fi access points** (**34%**) **and cloud platforms or applications** (**33%**) **were prime sources for organization breaches in the past 12 months.** Other vectors included IoT devices or networks (29%), remote employee-owned (29%) and employer-owned (24%) endpoints, insiders (26%) and unpatched DDI servers (25%). Other, less common breach sources were third parties or supply chain providers (24%), non-cloud applications (20%) and remote access programs (17%).

Global: Average Number of Issues Across Various Attack Vectors



5. **Among the organizations that were breached, respondents said their attackers were most likely to steal data or hijack credentials, while some victims experienced system outages and data manipulation.** Attackers favored data exfiltration (51%) and credential hijacking (50%), along with command-and-control communications (38%) and privilege escalation (34%). Almost a quarter (24%) also used lateral movement to infiltrate networks. Organizations that were breached suffered system outages or downtime (48%) and data manipulation (41%) more often than sensitive data exposure (38%), data lockouts (35%), other malware infections (26%) or distributed denial of service (23%).

$2 mil

the estimated average value of global organizational losses

6. **The cumulative value of losses in the past 12 months from these breaches averaged USD$2 million, but damages sometimes went far beyond that figure.** In addition to direct financial losses as well as downtime, reputational harm and response expenses, there were more troubling costs of a compromise. Globally, 10% suffered a loss of life, and another 12% reported bodily or psychological injury among a breach's impacts.

7. **Traditional network security tools like firewalls, intrusion prevention systems (IPSs) and virtual private networks (VPNs) remain popular security controls to protect on-premises networked assets; cloud access security brokers (CASBs) topped preferred controls for cloud-based environments.** Those with hybrid environments favored both network security tools and data encryption. Other common choices for on-premises and cloud-based environments were secure web gateways and DNS security. For hybrid settings, network traffic monitoring, detection and response (NDR), VPNs and data loss protections were the most common.

8. **A large majority of respondents (74%) took 2 to 24 hours to investigate a threat, most often using network flow data, vulnerability information or DNS queries and response to conduct probes.** A full third (33%) took 2 to 5 hours, and another quarter (26%) took 6 to 24 hours. Another 15% took an hour or less, compared to 3% that took seven or more days.

9. **Monitoring remote worker access (33%) is expected to be the top challenge in the coming year, as well as a shortage of IT security skilled labor (27%) and lack of budget (26%).** Other primary challenges include lack of visibility into user and device activity on a network (22%) or cloud access (20%); too many alerts to respond to (20%); inadequate firewall protections (18%); volume of incidents (17%) and number of siloed security tools (also 17%). Least anticipated challenges are lack of resiliency or preparedness to respond to an attack (15%) and lack of business leadership support (14%).

10. **DNS is part of almost every organization's security strategy for protection against threats like DNS tunneling and domain generating algorithms (51%), as well as to flag devices trying to connect to malicious destinations (49%).** Other strategic purposes include blocking known bad destination requests to ease perimeter defense burdens (48%) and help locate malware activity earlier in the kill chain (40%).

11. **Most organizations (61%) globally expect more budget in the coming year—a significant increase over the 51% that received more funding in 2022.** The most popular anticipated data protection purchases across the globe were VPNs/access controls and network security (firewalls, etc.) for on-premises; CASBs and secure web gateways for cloud-based environments; and network security and DNS security for hybrids.

12. **Organizations' increasing reliance on their remote global workforces in 2023 continues to have profound impacts on cyber security that were laid bare in 2022.** The acceleration of digital transformations, additional resources for networks and databases and increased support for customer portals remained the top three activities in supporting workforces and customers throughout 2021 and 2022. Accordingly, about half of all respondents worldwide remain concerned about the threat of data leakage in the coming year. Likewise, respondents' top fears—ransomware, attacks through remote worker connections, and cloud services attacks—continued to persist in 2022 and have carried into 2023. While there was no/little change in the primary sources of breaches (i.e., Wi-Fi access points, cloud infrastructure and remote endpoints), there were indications that attacks originating from IoT devices/networks became more prevalent in 2022 (as reported by 29%) compared to 2021 (22%). For two consecutive years, at least one in four organizations worldwide still believes that monitoring remote worker access, a lack of budget and a shortage of IT security skills are their top challenges in protecting their networks against threats and attacks for the foreseeable future.

THE HIGH COSTS OF WORKING FROM HOME

When the pandemic hit in 2020, 52% of organizations responded primarily by fast-tracking digital transformations, adding resources to networks and databases (45%) or increasing support for customer portals (44%). Another 34% chose to hire more IT staff, as opposed to 14% forced to reduce theirs and 16% that switched IT staff to other roles. Almost a third moved apps to third-party cloud providers (31%) or focused network and security controls on the edge (such as with SASE, secure access service edge) (30%). One in five closed physical offices.

These structural changes also required new or additional means of protecting and securing critical assets now residing or transmitted from home networks. Even more than a year into the pandemic, organizations were still playing catch-up. Between mid-2021 and mid-2022, a majority (54%) were still adding VPNs and firewalls to networks a year or more into the pandemic, while 48% added remote employee-owned devices and/or remote corporate-owned mobile devices to meet demands of a remote workforce. Global organizations also preferred cloud-managed DDI (DNS-DHCP-IPAM) servers over internally managed ones by 43% to 30%. Some respondents (28%) also added smart kiosks and similar devices to support remote customers or clients.

DATA LEAKAGE IS MAJOR CAUSE FOR CONCERN

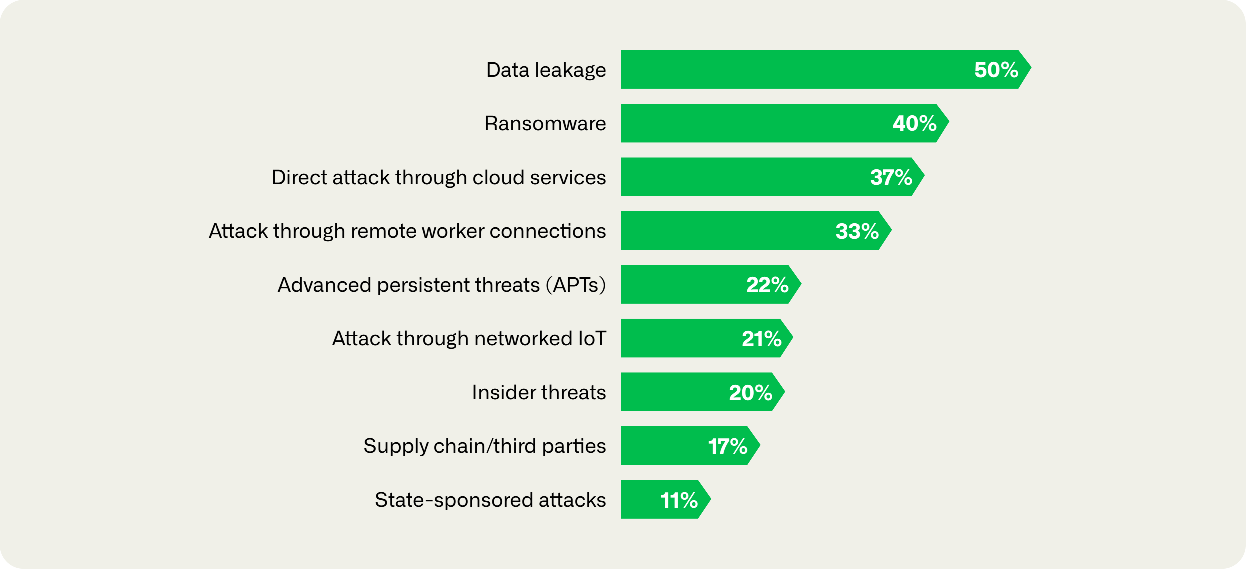
Half of all organizations worldwide were most concerned about data leakage, in which data is exposed due to internal errors like poorly trained employees or outdated systems. Ransomware also remains a top concern for many (40%), followed by direct attacks through cloud services (37%) and attacks through remote worker connections (33%). Data leakage and ransomware are closely related because poor cyber hygiene provides an ideal entry point for ransomware.

These top concerns reflect ongoing struggles resulting from accelerated digital transformations to support remote workers and customers. By quickly digitizing more assets and moving assets and applications to the cloud, cyber security professionals broadened attack surfaces.

Compared to most other countries surveyed, Brazil and Singapore had significantly larger shares of respondents concerned about advanced persistent threats (APTs), cited by 34% and 29%, respectively. At 34%, France had the largest proportion of respondents most concerned about insider threats. And, given cyber superpower Russia's ongoing war to take control of Ukraine, those most concerned about state-sponsored attacks—United Kingdom (14%), Germany (14%) and France (16%)—were located closer to battlegrounds. "State-sponsored attacks seem to have unlimited resources as well as people who can focus on looking for loopholes and access to our servers in the cloud or at physical locations," said a U.K. respondent most concerned with state-sponsored attacks.

Which of the following types of cyber threats or vulnerabilities is your organization most concerned about in the next 12 months?

Select up to three.



Globally, phishing continues to be the primary attack vector creating issues for organizations, accounting for at least three times more than network, cloud, application, endpoint and third-party attacks. Even ransomware, considered a prime concern globally, was linked to an average of 15 attacks compared to 41 for phishing.

ORGANIZATIONS MOST VULNERABLE TO UNSECURED WI-FI AND CLOUD SERVICES

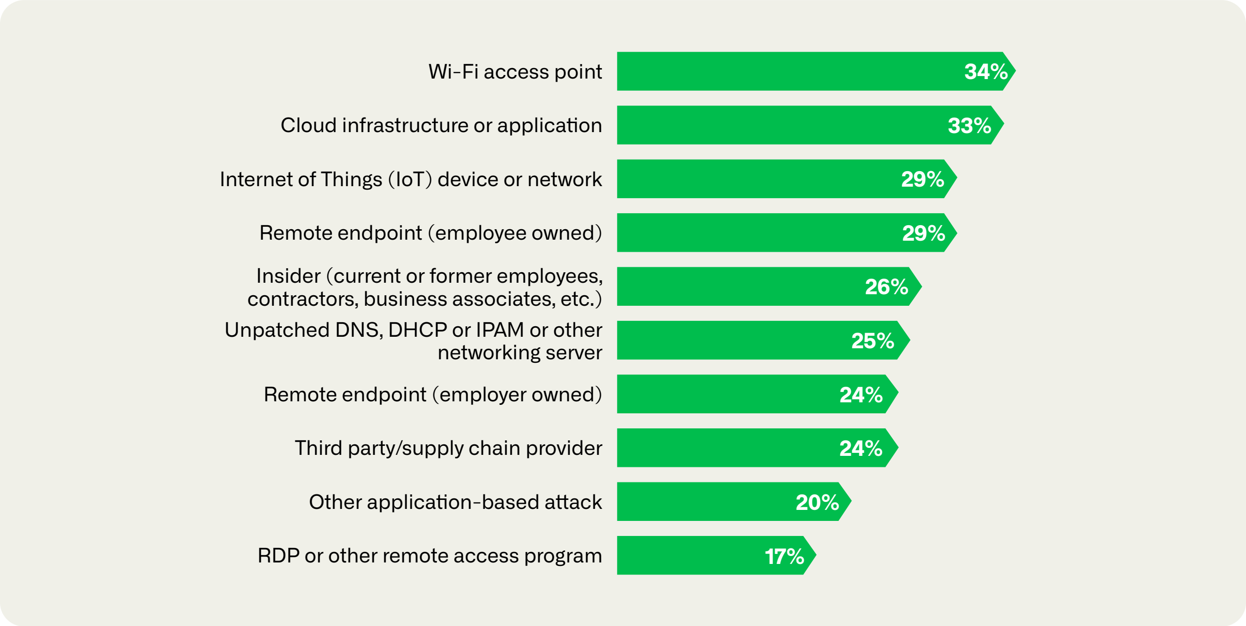
On average, 62% of all respondents reported their organization experienced an IT security incident in the past 12 months that resulted in a breach. Most handled between one to five breaches while another 8% contended with six or more.

Globally, the top attack vectors used in successful breaches were most likely to be Wi-Fi access points, cloud infrastructure or applications, IoT devices or networks and remote employee-owned endpoints as a result of remote workers using unprotected (or under-secured) wireless networks, cloud services and networked devices beyond the organization's full control. Insiders also posed a significant threat, as well as unpatched DDI or other networking servers.

The increase in IT and security budgets and a focus on hiring may be related to an effort to address these identified risks because many popular breaches in these areas have been linked to configuration errors or unpatched devices. So an investment in better network discovery and visibility tools, along with an increased focus on security hygiene and maintenance appear to be in the works for 2023 for many organizations.

Which of the following describe where these breaches to your organization originated?

Select only those that apply to your actual breaches.

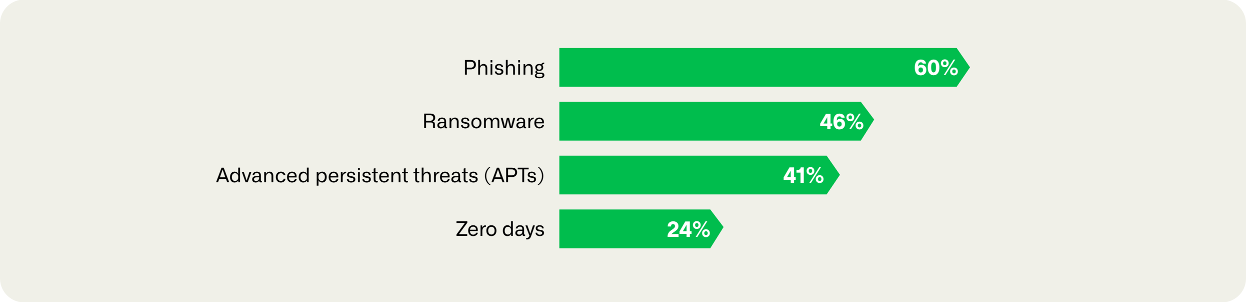


For 6 out of 10 respondents whose organization was breached, phishing was the attack method, while nearly half indicated ransomware (46%) and advanced threats (41%) were to blame. And there is likely overlap since phishing is often used as the attack vector to deliver ransomware and other advanced threats.

Once attackers gained illegal access, they were most likely to exfiltrate data (51%), steal credentials (50%), establish command-and-control communications (38%) or escalate privilege (34%). About one in four (24%) respondents indicated these attackers moved laterally within their compromised systems.

Which of the following attack method(s) were used in these breaches your organization experienced in the past 12 months?

Select all that apply.

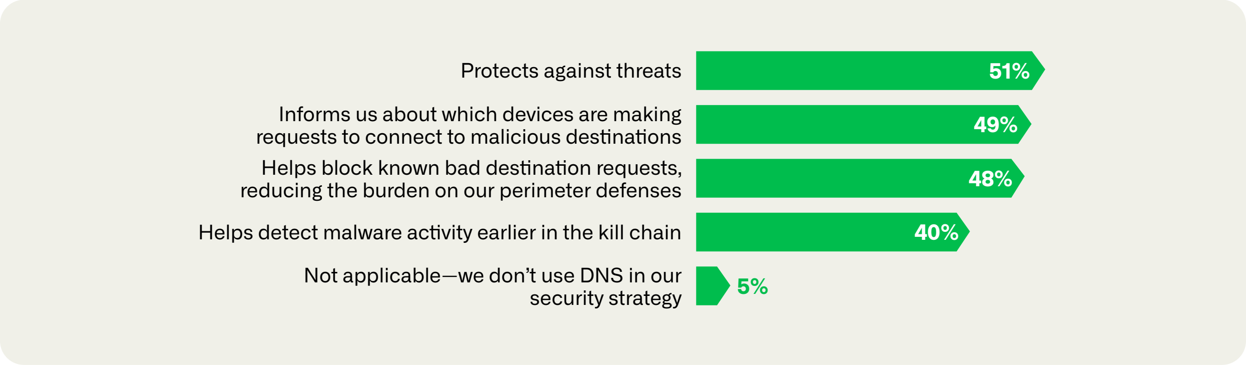


To find the source of their attacks, organizations relied on network flow data (42%), systems-specific vulnerability information (39%) and DNS queries and responses (38%) in their probes. They also incorporated third-party threat intelligence (36%), packet and network traffic captures (29%), open-source intelligence (28%) and CERT alerts (27%). About one in five also used federal indicator databases, such as those supplied by equivalents of the U.S. Federal Bureau of Investigation or Department of Homeland Security.

The Domain Name System (DNS) is part of all organizations' overall cyber security strategies. Organizations leverage DNS to find threats like DNS tunneling and data exfiltration and detect malware activity earlier in the kill chain. They also use DNS to reduce the burden on perimeter defenses by blocking bad destination requests and helping find devices making requests to connect to malicious or suspicious destinations.

Which of the following best describes how the Domain Name System (DNS) is used in your organization's overall security strategy?

Select all that apply.



THE HIGH COST OF A BREACH

For respondents who reported their organizations were victims of a breach, the approximate cumulative value of losses resulting from these breaches amounted to roughly USD$2.0 million. That includes direct financial losses as well as indirect losses due to downtime, reputational, harm and response expenses. In some countries, including those in Europe, Brazil, Australia, Mexico, and UAE, monetary losses are positively correlated to the size of the organization.

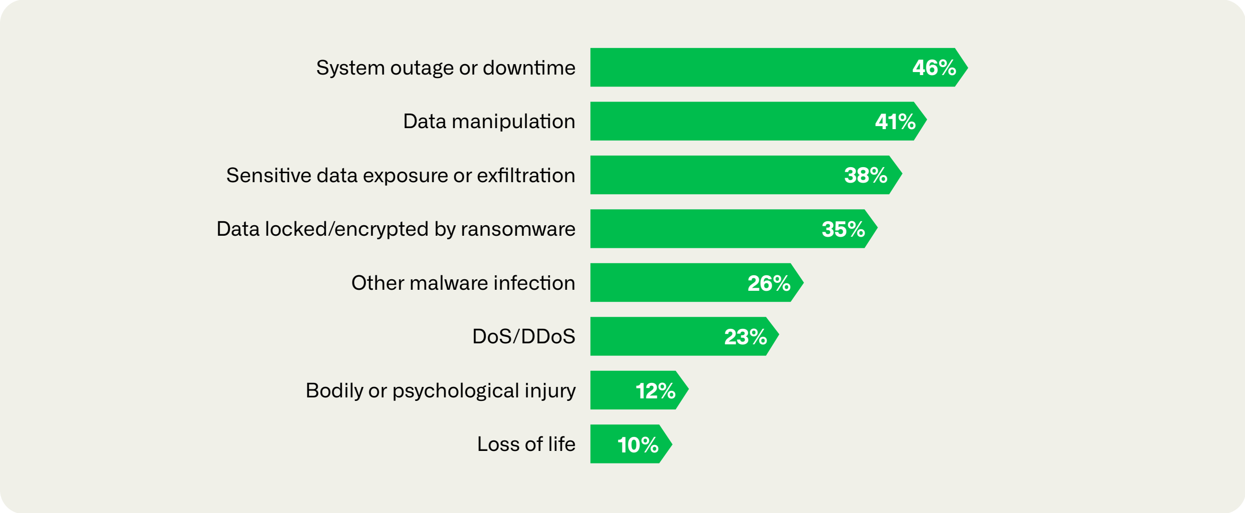
Those losses, however, are only part of the story. Organizations globally also reported another impact of a breach: bodily or psychological harm, even death. Particularly EMEA countries like France (21%), UAE (18%) and The Netherlands (14%) reported someone hurt as a result of a successful attack. France and the UAE also reported the highest percentages of breach-related deaths associated with a compromise. By industry, professional services were most apt to report some type of human harm, while energy and electronics-based manufacturing were more likely to report a loss of life.

These results point to both the enormous stress for today's cyber security professionals as well as potentially devastating consequences when an organization fails to protect itself—and those it serves—from threat actors.

Almost half of the organizations that were breached were likely to have experienced system outages or downtime. Many respondents (41%) also reported their data was manipulated. Some also had sensitive data exposed or stolen (38%) or locked/encrypted by ransomware (35%). Others suffered malware infections and denial of service attacks that temporarily shut down operations.

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

Select all that apply.



CYBER DEFENSES LIMITED BY BUDGETS AND SHORTAGE OF IT SKILLS

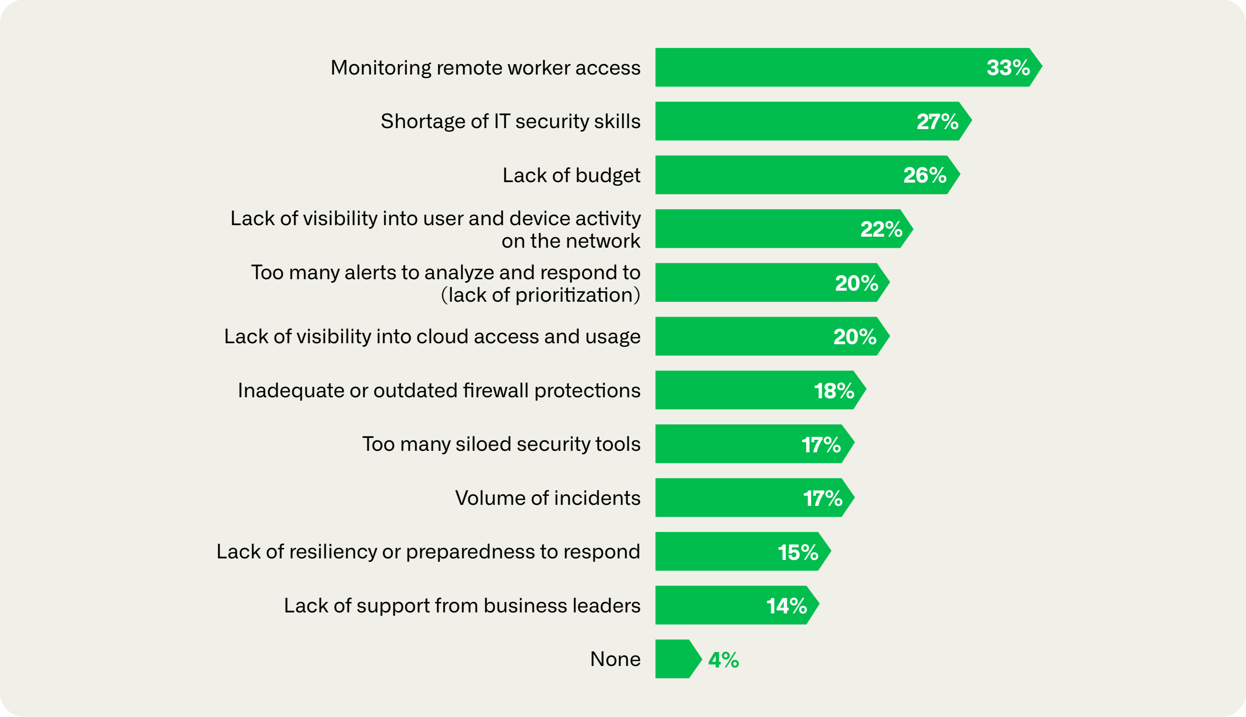
While 51% of all organizations saw their IT security budgets increase in 2022, 61% anticipate more funding in 2023. Another 19% do not expect their budgets to change in the coming year.

Globally, the biggest challenges that respondents said they expect to face in the coming year involve monitoring remote worker access and having enough skilled staff and funds to provide adequate network protections. A shortage of IT security skills was most prevalent in Japan (38%), Australia (34%) and the United Kingdom (34%). Singapore (28%) and Mexico (27%) had the highest proportions of respondents who believed their organization lacked resiliency or preparedness to respond to threats and attacks. Other areas of concern in the coming year involve poor visibility into device and user activity both on a network and within the cloud; outdated equipment no longer up to the task; and capacity issues with too many siloed security tools prompting too many alerts in need of a response.

Only 14% of respondents said they lack support from business leaders, which suggests that executives now take cyber security seriously, even if these same business leaders aren't willing or able to devote more funds to their organizations to stay protected against cyber threats.

What are your organization's top challenges in protecting its network against threats or attacks in the next 12 months?

Select up to three.



GAIN A MORE COMPREHENSIVE UNDERSTANDING

This global survey report is based on aggregated data from a global online survey conducted July/August 2022. For more insights, readers may also want to review the country-level summaries available for the United States, Mexico, Brazil, United Kingdom, Germany, France, The Netherlands, Spain, United Arab Emirates, India, Australia, Singapore, and Japan.

CONCLUSION

The past few years have brought new troubles for organizations forced to pivot once workers and customers were sent home to limit the spread of a deadly virus. The sudden shift to a virtual workforce caused numerous problems still being felt on various fronts today.

One senior official from a U.K. manufacturer summed up current frustrations on numerous fronts: “Company expansion is bringing in more users—and vulnerabilities. Larger databases to manage and back up safely. As cloud use increases and projects grow, so does collaboration with third parties, which are harder to trust.”

Though issues and priorities may vary by country, this study also points to a global shared experience. The pandemic may have sped up digital transformations and shifted security controls to manage and monitor remote employees and devices. But more established threats like ransomware and data leakage were already prompting change well before COVID-19 provided the push.

The research indicates which nations grappled more than others with modernization plans—and still do. And it highlights where organizations are most concerned and how they are focusing their budgets and uplift efforts. This is the dynamic nature of cyber security. Today, economic forces such as inflation and geopolitical tensions, like the war in Ukraine, influence an ever-changing threat landscape and the risks to a rapidly expanding attack surface. As such, continuing to find ways to overcome IT security struggles today will perhaps future-proof organizations for the turbulent times ahead.

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

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).