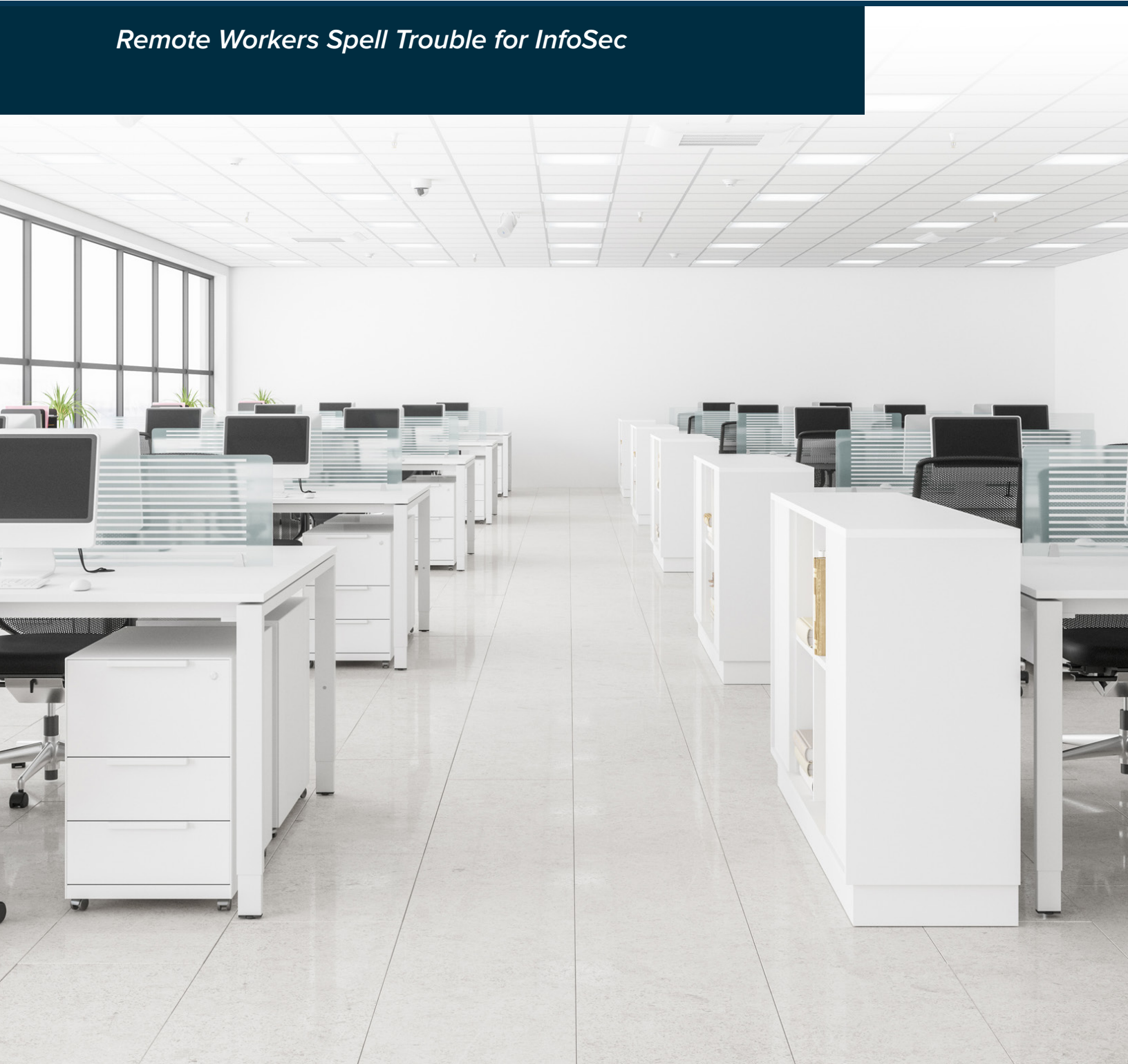


2022 Global State of Security Report

Remote Workers Spell Trouble for InfoSec



Contents

Background	3
Methodology	4
Executive Summary	5
Facing Down the Perils of Remote Work	6
Gaining Control in Chaotic Times	8
Remote Employees + Weak Wi-Fi Security = Big Trouble	9
Current Measures to Counter Threats	11
Anticipated Challenges and Choices for Networks	12
Where Budget Dollars Flow in 2022	13
Growing Popularity of SASE	14
Conclusion	15
About CyberRisk Alliance	16
About Infoblox	16



Background

The past two years have changed how companies and consumers all over the world conduct business. Across countries and industries, employees quit their jobs, leaving organizations vulnerable in their absence. They relocated with little to no notice, creating secure access headaches for IT security teams. They adjusted to digital services that minimize human contact to curb the spread of COVID.

Nearly every nation continues to contend with COVID surges that periodically disrupt daily life due to ongoing supply chain and workforce shortages. Companies now must also question how much to trust third-party partners brought in to fill gaps or foster growth.

In early 2020, the world panicked, then pivoted to survive (both literally and figuratively). Digital transformations accelerated and expectations evolved. So did threats targeting organizations still transitioning to a new way of working. That includes information security specialists responsible for protecting the systems, networks, data centers, and technologies that fuel today's economies.

This global report reflects the state of security at the end of the second year of the pandemic and the measures organizations worldwide took to mitigate risks associated with a remote workforce. While everyone sent staff home, priorities differed. Most countries chose primarily to accelerate digital transformations and build or expand remote-customer portals to help remote workers. Some, like in Germany and Mexico, preferred adding corporate devices over employee-owned ones to their networks. Additional VPNs and firewalls were especially popular in Australia and the United Arab Emirates. Brazil and Spain showed impressive threat response rates, and the Netherlands suffered denial-of-service attacks far more than any other country. Everyone was most worried about phishing, ransomware and cloud attacks. On a positive note, a majority of respondents in all countries anticipated bigger budgets this year to purchase primarily cloud- and hybrid-based IT security solutions – another sign that a majority on-site workforce may be a relic of the past.

At some point we'll experience another global shift when we collectively view COVID as an endemic we live with rather than a pandemic we cope with or conquer. But one thing is certain: information security as it existed before the pandemic isn't coming back.

Methodology

The data and insights in this report are based on an online survey conducted in late 2021 and early 2022 with 1,100 IT and cybersecurity decision-makers and influencers representing 11 countries.

Participants ranged from chief executives to senior analysts or their equivalent across several continents. Roughly 100 participants were selected from each of the following countries: United States, Mexico, Brazil, United Kingdom, Germany, France, the Netherlands, Spain, United Arab Emirates, Australia, and Singapore.

Study participants worked in a wide variety of industries: business, financial and professional services; manufacturing; industrials; retail or ecommerce; IT and technology; healthcare; education; transportation; government; non-profits; media; energy and utilities; and more.

Survey objectives were to gain greater visibility into the global state of security, including the impact remote workers and customers have on organizations forced to adapt to rapid change. Participants were asked about security pain points experienced in the two years since the start of the pandemic, specifically their response to a shifting (and sometimes shrinking) workforce. They also shed insight into current threats and anticipated investments to prevent advanced threats like ransomware. Data was compiled from responses to structured survey questions, and respondents were encouraged to provide corresponding comments where applicable.

The survey, conducted by the Business Intelligence Unit of CyberRisk Alliance, is underwritten by global IT automation and security provider Infoblox, whose products deliver cloud-first services for DNS, DHCP and IP address management and network security.

Executive Summary

Employees aren't coming back. At least not to pre-pandemic levels, before campuses and cubicles were shuttered and half the world locked down to slow the spread of COVID.

Since then, enterprises and government agencies across the globe have entered a state of seemingly perpetual chaos, with uneven re-openings, evolving public health messages, civil unrest and ongoing staffing and supply chain shortages.

Two years into the pandemic, the lack of adequate resources is more than an inconvenience; it's an open challenge to bad actors in search of weakened organizations. But chaotic moves made amid the pandemic have also opened the door to new opportunities for more robust security and business continuity. Among the study's key findings:

- **The surge in remote workers and customers has changed the corporate landscape significantly — and permanently.** Some companies shuttered physical offices for good, and even those still holding on to commercial properties understand they must contend with remote staffs or hybrid workplaces for the time being. As a result, some moved more applications into the cloud and rely on traditional network security like VPNs and firewalls placed on corporate mobile devices. For employees using their own equipment, many companies are deploying solutions to monitor and manage DNS, DHCP and IP traffic moving in and out of servers.
- **The new hybrid workforce reality is causing greater concerns with data leakage, ransomware and attacks through remote access tools and cloud services.** Respondents indicated concerns about their abilities to counter increasingly sophisticated cyberattacks with limited control over employees and vulnerable third-party partners. The sophistication of state-sponsored malware also is a source of worry for many.
- **Organizations have good reason to worry: Most participants experienced up to five security incidents that led to at least one breach.** Attacks tended to originate with WiFi access points, employee-owned endpoints or the cloud. Phishing was a common conduit to gain illegal entry to hijack credentials and steal or lock down data files. These weren't minor events either; the study showed 43% of all organizations surveyed suffered at least US \$1 million in direct and indirect losses.
- **Interest in Secure Access Service Edge (SASE) frameworks is accelerating.** As assets, access and security move out of the network core to the edge with the push for virtualization, 54% have already partially or fully implemented SASE and another 28% intend to do so.
- **Organizations do apply controls for on-premises, cloud and hybrid environments, but there's plenty of room for improvement.** Roughly two-thirds of all participants were less than very satisfied with their organization's ability to respond to an actual attack, such as ransomware, using existing solutions. They also are eyeing solutions for hybrid environments more often than on-prem or cloud only versions.
- **IT security budgets and spending increased for many in 2021, with even more security teams expecting a bump in budgets in 2022.** Many are considering primarily hybrid-oriented solutions that protect assets both on premises and in the cloud. And they are trying a wide variety of solutions — everything from end point and network security to cloud access security brokers, DNS security and threat intelligence services.

These findings point to the current struggles that remain largely unresolved with dispersed workforces and high churn now commonplace.

"Remote working is going to be the norm for the next few years, and we need more security for these remote workers," said an IT security director from a large, UK-based professional services firm.



Facing Down the Perils of Remote Work

In March 2020, citizens around the world were asked or ordered to self-quarantine to stop the early spread of COVID. At that time, employers expected such drastic change to be short-lived.

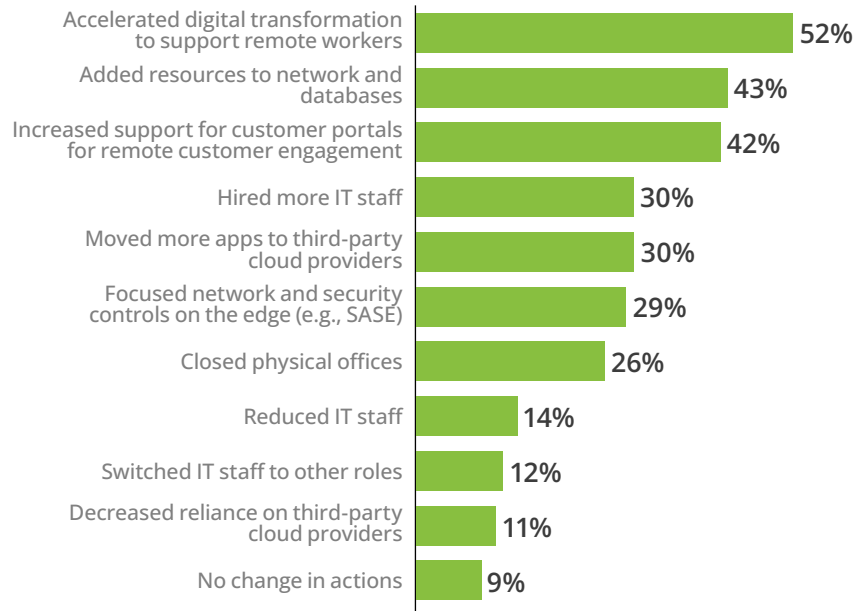
But as days turned to weeks and then months, business leaders realized business continuity plans might be in play longer than expected. They'd need to grant greater autonomy to homebound employees, contractors, and business partners and for an extended period of time. They needed everyone back to work and to convince customers to buy all their goods and services online rather than in-person.

Well-positioned organizations, regardless of industry or location, accelerated their digital transformations to handle higher data workloads and cloud-based applications securely accessed by a wider range of devices. They sped up plans to replace hardware with software-defined networks, which moved more assets to the network's edge. Others at companies with revenue shortages had to contend with new needs supported by stagnant or shrinking security budgets.

As if stabilizing and outfitting an entirely remote workforce wasn't enough of a challenge, by late 2021 employers in almost every industry had another human resource headache: healthy workers quitting in record numbers to protest wages and work conditions, or simply for higher paying jobs, during an ongoing public health crisis. This mass resignation only exacerbated coverage and security gaps yet to be fully resolved.

Since the pandemic began in 2020, which of the following actions has your organization specifically taken to support its workforce or customers? Select all that apply.

Respondents from all regions



Findings from the global survey illustrates how companies around the world responded to the swift shift to remote work. A majority accelerated their digital transformations and nearly half increased support for customer portals to foster engagement. To help keep up productivity and profits, some organizations added resources to networks and databases and shifted applications to external cloud providers. Many also turned their attention to tighter network and security controls.

What companies chose to do were based largely on their resources, expertise, and geography: Some expanded their IT staff. Others reduced their ranks or reassigned IT staff. Some unfortunately closed physical offices permanently as a cost-savings measure, while a lucky few continued with business as usual.

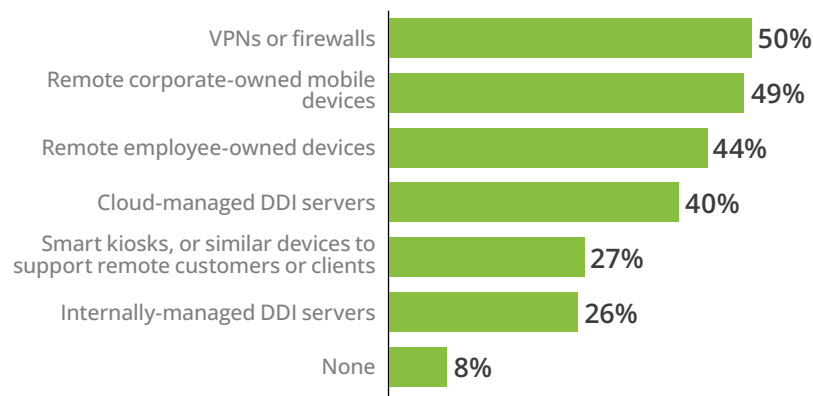
These measures, in part or whole, point to the myriad ways enterprises reacted to a radical decentralization — rapidly reallocating resources and restructuring to meet a new way of working.

To protect critical data from the dangers that come with remote employees using a mix of personal and company devices, some organizations added devices to their equipment fleets, particularly placing corporate-owned mobile devices in the hands of remote employees for slightly more than half of respondents, according to the survey. Just as many added virtual private networks to encrypt transmissions over the internet, especially if a remote worker used public or poorly protected wireless networks. These and other measures were designed to equip employees with secured tools to do their jobs under trying circumstances and without destabilizing the organization.

When looking at responses from different countries, the level of added support is consistent across the board. In Singapore, for example, 57% of organizations accelerated digital transformation timetables to better assist their remote employees while 46% focused on applying network security controls on the edge or increasing support for customer portals. By comparison, 49% of respondents in Australia shortened timetables to modernize their IT infrastructure and improve support for customer portals (46%) to help ease burdens on their workforces. Australian businesses also added resources to networks and databases (45%). Almost a quarter (23%) closed physical offices.

Which of the following types of devices did your organization add to its network in the past 12 months? Select all that apply.

Respondents from all regions



The responses were also consistent when asked about devices added in the last 12 months. In Brazil, for example, 60% of respondents deployed remote corporate-owned devices, compared to 51% who accommodated remote workers' personal devices. Additionally, 44% added virtual private networks or firewalls to protect a more remote workforce. In contrast, 56% of U.K. respondents chose to deploy remote corporate-owned devices (56%) rather than add employee-owned phones, tablets, and laptops by 41%. As a failsafe for all remote devices, 52% in the U.K. added a virtual private network or firewall to protect network traffic moving in and out of those remote devices.

Gaining Control in Chaotic Times

With rapid structural change comes chaos and new concerns. With a decentralized workforce, IT security leaders needed ways to keep production levels up and home networks, corporate and personal devices, and wireless data transmissions away from prying eyes.

It's little surprise that data leakage was the biggest concern last year, given the loosening control over what flowed into and out of corporate or personal devices over remote connections and/or cloud services. There's also growing reliance on cloud-based applications that raise third-party risks should cloud service providers fall short on security controls or fall victim to attacks of their own.

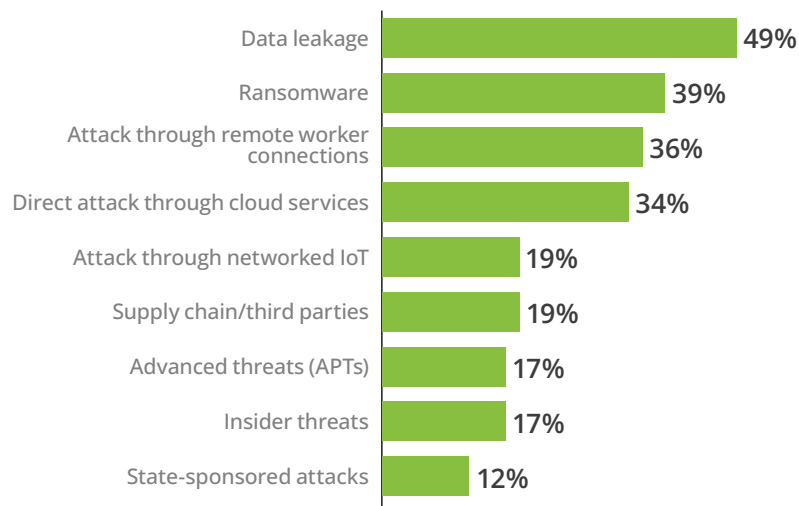
In written comments, professionals expressed frustration with the lack of transparency in knowing what, if any, security precautions and security protections remote employees and third parties with network access use. That lack of visibility has them worried about sensitive information seeping out and ransomware gangs getting in.

Geopolitical tensions also have had an impact, particularly countries known to have fortified their cyber capabilities and launched advanced threats in the past. “Currently, we don’t have the internal systems to protect or restore our IT system if state-sponsored attacks were to take place,” noted a chief executive for an Australian retailer.

Insider threats — whether rooted in maliciousness or misuse — remained an issue too. “It’s practically impossible to control how internal employees handle their information about our systems,” said a chief security officer for a mid-sized German firm.

Which of the following types of cyber threats or vulnerabilities is your organization most concerned about in the next 12 months? Select up to 3.

Respondents from all regions



The level of concern over loss of direct security controls and network visibility was about the same across the 11 countries surveyed. Data leakage, ransomware and remote exploits topped the list of security concerns. In the U.S., 44% of respondents are most concerned about data leakage and up to 39% worry that remote connections will serve as potential entry points for infiltration. That’s compared to French respondents who worry about data leakage (55% of respondents) and vulnerable remote connections (52%).

Remote Employees + Weak Wi-Fi Security = Big Trouble

A consequence of a rapid, mass movement to remote workers and ramp up in consumer digital services is a greater chance of someone or something getting through that shouldn’t. The most successful mode of attack was phishing (58%). Zero-days, among the more difficult to defend, accounted for just under a quarter of all breaches.

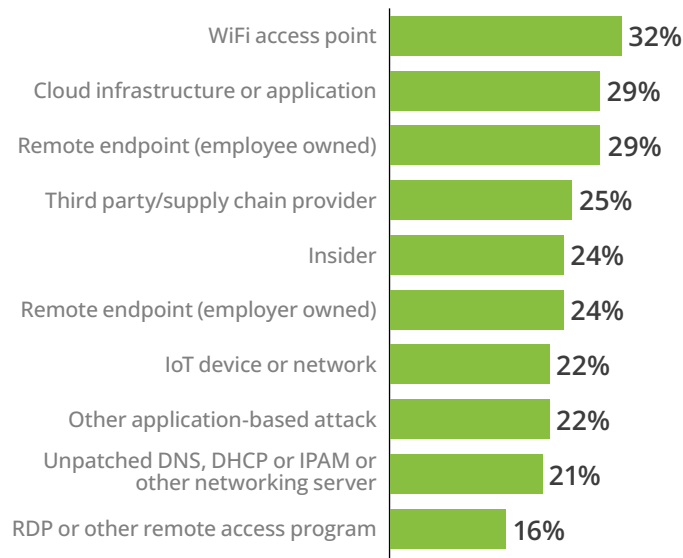
Instead, more than half of all respondents (53%) experienced up to five IT security incidents in 2021, with another one in five grappling with six to 10 events. These events can shatter confidence in internal capabilities and strain vendor relations if the source of compromise turns out to be a third party. It also makes it more difficult to marshal adequate defenses if the defenders themselves lack trust in their own abilities.

Fortunately, some preventative measures are working. Forty-nine percent hadn’t experienced a breach from an incident. Thirty-four percent had one or two, and only 2% had more than 10 breaches.

The two most prominent attack vectors in 2021 were Wi-Fi access points and remote, employee-owned endpoints — two areas in which employers have the least control. The impact from breaches were most likely to be outages or downtime, though compromised data also was significant — whether it was manipulated, stolen, exposed, locked down, or otherwise restricted. Other malware infections hit almost a third of participants.

Which of the following describe where these breaches to your organization originated? Select only those that apply to your actual breaches.

Respondents from all regions



In US financial terms, 43% suffered \$1 million or more in direct and indirect financial damages from breaches. Several respondents described this as the cost of doing business during COVID, where more sensitive information is being shared through multiple channels, some of which are beyond the user's (or their employer's) control. "At this time, we are downloading (and uploading) large amounts of financial data," said the CEO of a U.S. financial service. "We are unsure of the cybersecurity of some of our providers."

Third-party risks were a common theme among respondents. Companies worried that their security measures could prove useless if attackers compromised a trusted supplier or contractor to gain access to sensitive information.

The 11 countries covered in the survey traced breaches they experienced back to such things as weak WiFi security and remote endpoints, third-party suppliers and insecure cloud infrastructures and applications. Respondents in the U.K. said the most likely culprits were insecure WiFi access (47%); a third-party/supply chain provider (35%); cloud services (32%) and employee-owned endpoint (32%). In Germany, the sources of attack were employee-owned endpoints (37%), unpatched DDI or other network equipment (33%), or insiders (24%). In Brazil, attackers were most likely to use a Wi-Fi access point (38%), IoT device or network (29%) or cloud application or platform (27%).

Current Measures to Counter Threats

The survey also asked about security controls being implemented. Respondents leaned toward hybrid versions and their preference for solutions that protect both on-premises to cloud-based IT models with a more fluid workforce. For instance, while somewhat evenly split on on-premises vs. cloud-based vs. hybrid DNS security, there was greater preference for hybrid versions of data encryption and security web gateways

Among the most popular security controls in play:

- Cloud access security brokers (CASB)
- Data encryption
- Data loss prevention
- DNS security
- Endpoint detection and response
- Network security
- Network traffic monitoring/detection and response
- Secure provisioning and deprovisioning
- Secure web gateways
- VPN and other access control tools

Usages of these solutions vary, with the most popular options being DNS security to monitor and manage network traffic and VPNs to control access. Least likely adopted were CASB and provisioning tools.

Only 10% were very satisfied with their ability to respond to an advanced attack, leaving plenty of opportunity to improve cyber defenses — especially given that more than one in four organizations took longer than 24 hours to investigate a threat. When hunting down a threat source, 40% mostly relied on network flow data, systems-specific vulnerability information (39%), DNS queries (39%) and outside threat intelligence services (37%). Some U.S. organizations also relied on CERT alerts (25%) and federal indicator databases (19%), such as those generated by the FBI, Department of Homeland Security and MITRE.

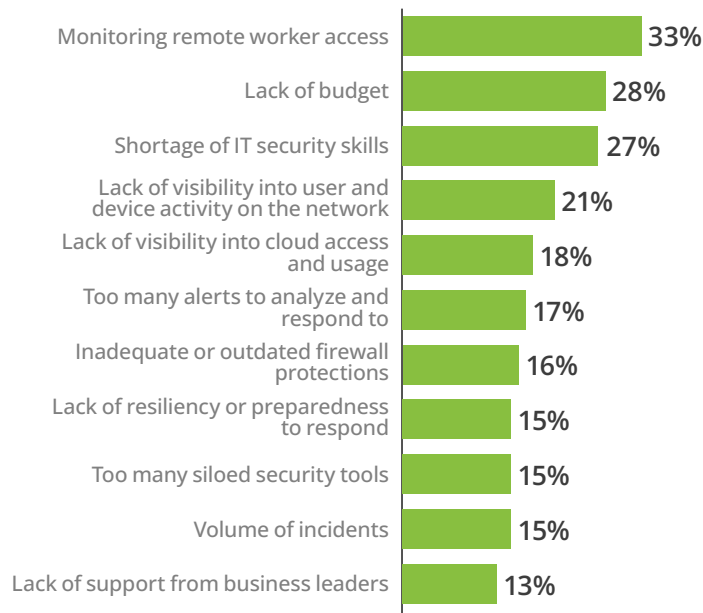
The use of such security controls was about the same across the 11 countries covered in the survey. In Australia, for example, 55% deployed virtual private networks and/or firewalls in response to securing a more remote workforce. Other popular device additions were remote employee-owned devices (48%) and cloud-managed DDI (DNS, DHCP and IP management) servers (41%). Remote corporate-owned devices were added by only 39%. In the UAE, 51% deployed virtual private networks and/or firewalls in response to securing a more remote workforce. Other popular device additions were remote employee-owned devices, cloud-managed and internally managed DDI (DNS, DHCP and IP management) servers (48% each). In Mexico, 67% deployed remote corporate-owned remote devices, and 37% added virtual private networks or firewalls in response to securing a more remote workforce.

Anticipated Challenges and Choices for Networks

Given the resources needed to deploy, outfit, and continually secure remote or hybrid work staff, it makes sense that the top challenge going forward was monitoring remote worker access. Also ranking high was low funding and shortage of skilled labor. All of these top challenges point to consequences of a changing labor market and the ongoing financial impact of the pandemic around the globe.

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

Respondents from all regions



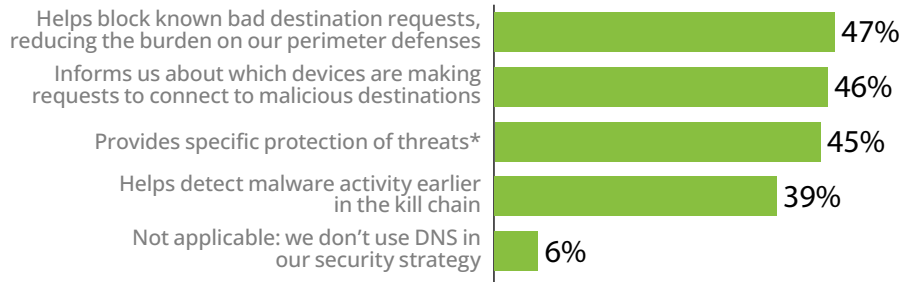
DNS has become a popular component of organizations' overall security strategies. Almost half used it to help block bad destination requests, thereby reducing the burden on perimeter defenses. The same number gathered intelligence from devices making requests to determine malicious destinations.

DNS also was broadly applied to protect against threats like DNS tunneling/data exfiltration, domain generating algorithms, spoofed domains, detect malware activity earlier in the attack kill chain, etc.

DNS is a popular strategy in the U.K. to ease the burden on organizations' perimeter defenses. In exploring the role of DNS (Domain Name System) in a U.K. organization's overall security strategy, 47% reported it is used to block bad traffic and ease burdens on other perimeter defenses. Another 38% used DNS to protect against threats like DNS tunneling. In France, 47% reported using DNS security enhancements to protect against threats like DNS tunneling (47%), and to detect malware activity earlier in the kill chain or detect devices making requests connected to malicious destinations (45%).

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

Respondents from all regions



*DNS tunneling/data exfiltration, domain generating algorithms (DGAs), lookalike domains, etc.

In a nod to the ongoing global transition from on-premises to remote or hybrid workforces, almost 40% of respondents planned to purchase a hybrid version of DNS security in the coming year, with another 27% opting for the cloud only version. In the past 12 months, 40% of respondents had added cloud-managed DDI servers and another 26% installed their own versions. DDI platforms integrate DNS, DHCP (Dynamic Host Configuration Protocol) and IP address management so enterprises can better monitor these core network components. In doing so, they are aware of all devices connecting to the network.

Where Budget Dollars Flow in 2022

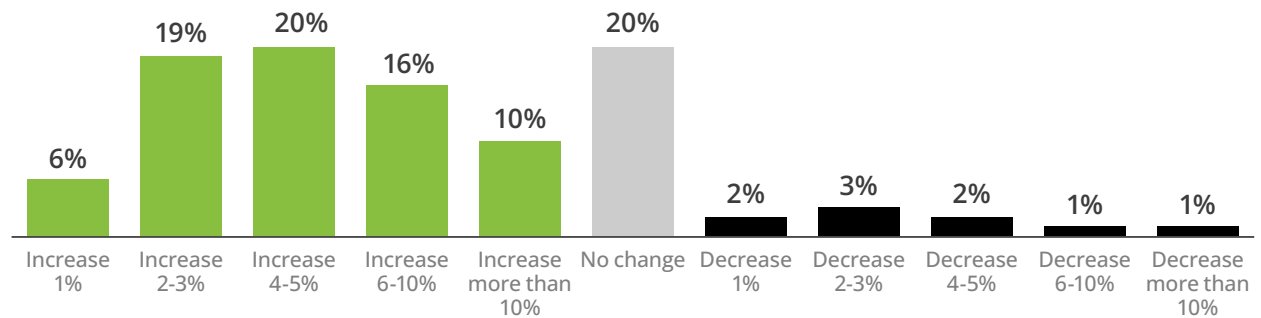
A bright spot for most study participants was greater financial support for cybersecurity programs. Fifty-nine reported their IT security budgets increased in 2021, and almost three out of four respondents expect 2022 IT security budgets to get a boost. The most popular security and data protection technologies are intended for hybrid environments, particularly:

- Data encryption tools
- Traditional network security solutions like firewalls
- Access control products like VPNs
- Network traffic monitoring, detection, and response

Data loss prevention, DNS security, and secure web gateways also ranked high. By placing more controls around the data and network traffic, organizations stand a better chance of keeping out intruders.

How do you expect your IT security budget to change in 2022?

Respondents from all regions



Despite the current shortage of financial resources, a large majority (78%) of U.S. respondents expect their budgets to increase in 2022. Popular purchase options for on-premises investments include network security (31%) and access control and data encryption (29%). Endpoint detection and response (25%), secure web gateways (28%) and threat intelligence solutions (29%) are the most popular cloud-based investments. Those anticipating a hybrid approach are most apt to adopt combo versions of network traffic (32%), secure web gateways (34%), provisioning (32%), and network security tools (36%). A large majority of respondents in Singapore (73%) increased their IT security budgets in 2021, and 69% expect their budgets to increase in 2022. Popular purchase options for on-premises investments include DNS security (28%) and network security (26%). Data encryption (37%) and cloud access security brokers (36%) are the most popular cloud-based investments. Those anticipating a hybrid workforce are most apt to adopt hybrid versions of data loss prevention, network traffic monitoring and VPNs/firewalls, all anticipated by 45% of Singapore participants.

Growing Popularity of SASE

One modern security model gaining traction is Secure Access Service Edge (SASE) that protects remote access from any location. Coined by Gartner analysts in July 2019, an SASE solution replaces the traditional hardware or appliance approach with a cloud-based one. It bundles software-defined networking with network security functions and can be delivered through a single service provider or multiple vendors that specialize in specific components, such as CASBs and firewall-as-a-service. An SASE safely connects devices, applications, and systems using modern security architectures like Zero Trust and secure web gateways.

While only 17% had fully implemented a SASE framework, another 65% were planning or piloting such a program, preferring multiple vendors to a single provider. Only 9% had no plans at present to add the modern IT model to their infrastructure.

Singapore is one country where interest in SASE is accelerating. As assets, access, and security move out of the network core to the edge with the push for virtualization, 61% of Singapore organizations have already partially or fully implemented SASE and another 29% intend to do so, through either one vendor (44%) or many (56%). Meanwhile, 67% of UAE organizations have already partially or fully implemented SASE and another 24% intend to do so, through either one vendor (42%) or many (58%). Sixty percent of Australian organizations have already partially or fully implemented SASE and another 16% intend to do so, through either one vendor (59%) or many (41%), and in the U.S., 58% have already partially or fully implemented SASE and another 20% intend to do so, through either one vendor (55%) or many (45%).

Conclusion

No two countries and companies operate alike, but when it comes to securing IT systems within their businesses and borders, they often share common ground. They worry about human errors and third-party risks. They fear equipment failures and the impact of persistent staff shortages. They wonder if current security controls and planned improvements can keep up with emerging threats, prevent data leakage and ransomware attacks. And if dedicating future security dollars to modern models like SASE and favoring hybrid IT environments will be their savior — or undoing. “We are prepared for any attack, but the cloud is what worries us most,” admitted a financial director for a Spanish wholesaler.

Moving quickly to serve a remote workforce carries risks, but also rewards. Being able to pivot during the pandemic kept economic engines purring during a prolonged period of uncertainty. It may have meant restructuring within IT security ranks to maintain coverage over a decentralized workforce and protect against a new version of “home network invasions.” If this study is any indication, organizations are more willing to invest in cybersecurity solutions to bridge technology and labor gaps and remotely train and monitor employees who may no longer operate in secure areas.

Cybersecurity professionals have learned a great deal since the start of the pandemic, especially their weak spots. Unfortunately, threat actors also are aware of where organizations remain most vulnerable.

“We can only do our best,” said an IT director for a Netherlands retailer, “but the criminals are getting smarter and will keep finding new ways [to get in].”

About CyberRisk Alliance

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. More information is available at <http://cyberriskalliance.com/>.

About Infoblox

Infoblox is the leader in next generation DNS management and security. More than 12,000 customers, including over 70% of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-first world. Learn more at <https://www.infoblox.com>.



Infoblox is the leader in next generation DNS management and security. More than 12,000 customers, including over 70 percent of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-first world. Learn more at 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

© 2022 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).

