infoblox

2023 GLOBAL STATE OF CYBERSECURITY STUDY

THE NETHERLANDS

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 Netherlands-based organisations of all sizes. Dutch respondents ranged from chief executives and directors to analysts and consultants. Respondents were employed in various industries, with most from manufacturing (17%), technology/telecom and retail/ecommerce (15% each) and financial services (11%).

EXECUTIVE SUMMARY

With a broadband connection in nearly every household, The Netherlands is regarded as one of the most wired countries in the world. But that ubiquitous connectivity also makes the nation a bigger target for malicious cyber activity. In July 2022, the National Coordinator for Counterterrorism and Security and National CyberSecurity Center for The Netherlands issued a joint statement warning of "industrial scale" cyber attacks. The alert came after Russian forces were said to have launched cyber attacks against numerous nations in the wake of its invasion of Ukraine. The agencies, according to the NL Times, also noted that Dutch organisations should follow best practices—like backing up data and requiring multi-factor authentication—with their growing use of cloud services.

These concerns were also revealed in the CyberRisk Alliance study conducted around the same time as those warnings were publicized. "Usually, countries like Russia and China have extensive or even unlimited resources to perform a hack. From the saying 'a broken clock is right twice a day,' it is plausible that one only has a very small chance, but there is a chance that the hack will succeed at some point," noted one Dutch participant most concerned about state-sponsored attacks.

Those aren't the only sources of anxiety for organisations operating in The Netherlands. Data leaks and data lockdowns (via ransomware) are also worrisome, according to the study. The number of breaches originating from unpatched networking equipment and the proliferation of remote devices latching on to networks reflect the unsettling environment in which Dutch cyber security professionals now operate.

The organisations fortunate enough to gain more budget in the coming year intend to boost network traffic monitoring and detection capabilities, as well as install data loss prevention and VPN/access controls to mitigate the growing cyber threats posed by external sources—and their own employees and contractors.

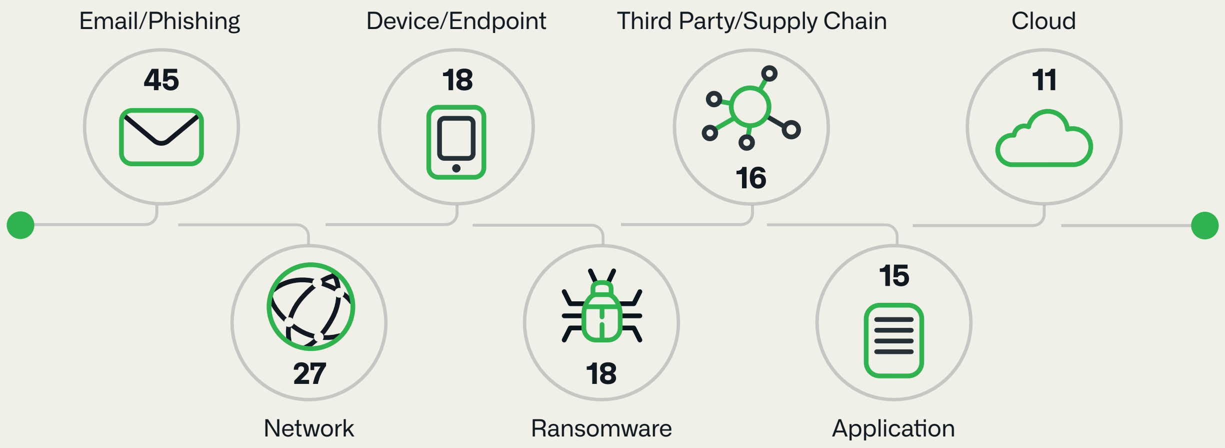
Findings from the 2022 study among Dutch respondents reveal the following trends in The Netherlands:

46%

of Dutch organisations accelerated digital transformations to support remote workers

1. **Since the COVID-19 pandemic began, many Dutch organisations fast-tracked digital transformations to support remote workers, added network resources and expanded IT staffs.** Almost half (46%) of all respondents accelerated digital transformations to support remote workers, while 36% added resources to networks and databases and 32% hired more IT staff. Almost a third (31%) closed physical offices—among the highest percentage to shutter offices among Europeans included in the study. Another 28% increased support for customer portals for remote customer engagement and nearly as many (27%) moved more apps to third-party cloud providers. A quarter focused network and security controls on the edge (such as SASE, secure access service edge), and one in five switched IT staff to other roles or reduced IT staff altogether.

The Netherlands: Average Number of Issues Across Various Attack Vectors



55%

of respondents reported their organisation added VPNs or firewalls

2. **In the past year, a large share of Dutch organisations added VPNs and firewalls while managing the proliferation and associated security risks from remote employee-owned devices on the network.** More than half (55%) of respondents reported their organisation added VPNs or firewalls to their networks. The BYOD trend among remote workforces continues to be prevalent, with nearly half (49%) of respondents adding remote employee-owned devices (compared to 37% adding remote corporate-owned mobile devices) to their networks. Forty percent reported adding cloud-managed DDI (DNS-DHCP-IPAM) servers, compared to 32% that added internally managed DDI servers. Smart kiosks or similar devices to support remote customers or clients accounted for another 30% of added devices.

3. **In the next 12 months, Dutch respondents said their organisation will be most concerned about data leakage, ransomware and attacks through cloud services.** Data leakage (39%) and ransomware (37%) continue to be the most worrisome cyber threats, followed by direct attacks through cloud services (33%) and exploiting remote-worker connections (32%).

4. **Dutch respondents believe their organisation is least prepared for data leaks, ransomware and insider threats and attacks through remote worker connections.** Respondents said they felt the least prepared to defend their organisation's networks against data leakage (18%), ransomware (13%) and insider threats (12%). The shift from temporary to permanently remote workers also continues to take its toll. "With more and more employees working from home, more weak points are being introduced to the network," noted an application development manager at a business services firm concerned about threats posed by insecure remote connections.

2–3x

Dutch organisations detected at least twice as many issues resulting from emails and/or phishing attacks than any other type, including application, network and cloud attacks

5. **On average, Dutch organisations detected roughly two to three times as many issues resulting from email/phishing attacks than any other type, including network attacks, ransomware or endpoint attacks.** Respondents estimated their organisation detected issues resulting from roughly 45 email/phishing attacks in the past 12 months, as well as 27 network attacks, 18 ransomware attacks and 18 device/endpoint attacks in the same period.

6 in 10

Dutch respondents reported one or more breaches to their organisation from cyber attacks

6. **Nearly two-thirds (63%) of Dutch organisations suffered one or more breaches to their organisation from cyber attacks—most originating from unpatched DNS, DHCP or IPAM networking servers; remote, employee-owned endpoints; or IoT devices or networks.** Unpatched networking servers including DNS, DHCP or IPAM accounted for the origin of 40% of breaches to respondents' organisations in the past 12 months, followed by remote employee-owned endpoints (33%) and IoT devices or networks (30%). Another 27% suffered attacks originating from cloud infrastructure or applications; insiders, such as current and former employees or contractors; or Wi-Fi access points.

7. **Phishing was the most common attack method against organisations that were breached.** Phishing accounted for 56% of attack methods in the past year, followed by ransomware (46%) and advanced persistent threats (APTs) (41%). In those attacks, the largest shares of breach victims reported their attackers most often used credential hijacking (49%), data exfiltration (46%), command-and-control communications (38%) and privilege escalation (32%) against the organisation.

€2.2 mil

the estimated average value of Dutch organisational losses

8. **Collectively, the estimated average value of Dutch 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 €2.2 million.** That amount is higher than other EU companies taking part in the study. Organisations that were victims of breaches mostly experienced sensitive data exposure or exfiltration (41%), data lockouts due to ransomware (also 41%) and system outages or downtime (37%). Among other consequences: 17% of Netherlands respondents said a breach led to bodily or psychological injury; 11% said it led to a loss of life.

9. **Dutch 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 network security (firewalls, intrusion prevention, etc.) and VPNs and access controls (both 34%) for on-premises assets, cloud access security brokers (41%) for cloud-based environments and network traffic monitoring and network detection and response (37%) for hybrid environments.

> “I believe our biggest threat is the amount of people that have no idea how cyber security works.”
>
> IT security consultant, Dutch technology provider

10. **On average, most (68%) organisations take up to 24 hours to investigate a threat, with many relying on network flow data or third-party threat intelligence platforms or services.** To aid their investigations or threat hunts, security teams mostly rely on network flow data (39%), third-party threat intelligence platforms or services (35%), vulnerability information specific to their systems (34%) and CERT alerts (31%).

68%

of organisations take up to 24 hours to investigate a threat

11. **The Domain Name System (DNS) provides various security measures to protect organisations and is a key component in almost all organisations’ security strategies.** Respondents reported their organisation most typically uses DNS in its strategy to help with the following: protecting against threats like DNS tunneling, data exfiltration and domain generating algorithms that other security tools might miss (44%); informing them of devices making requests to connect to malicious destinations (43%); and blocking known bad destination requests to reduce the burden on perimeter defenses (42%). Almost as many (40%) use DNS to detect malware activity earlier in the kill chain.

12. **The top anticipated challenge in protecting against attacks is a cyber security talent shortage.** Thirty percent of Dutch respondents reported their organisation struggles with a shortage of IT security skills to protect their networks from threats. Another 28% mentioned difficulty monitoring remote worker access, while 26% had too many siloed security tools. Additionally, 25% mentioned the lack of visibility into user and device activity on their networks.

49%

of organisations indicated their IT security budgets increased in 2022

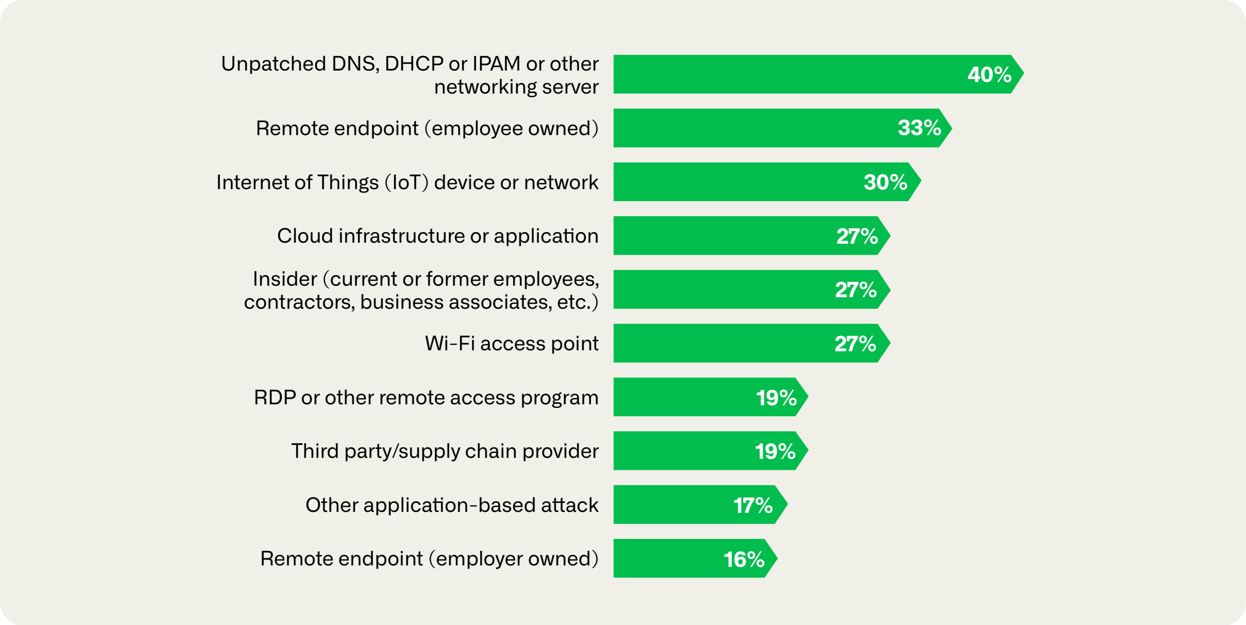
13. **Forty-nine percent of Dutch organisations indicated their IT security budgets increased in 2022, and 54% said they expected bigger security budgets in 2023 to combat known and new threats.** Another 21% expect no change to their budgets, while 24% expect their budgets to shrink next year. Many of the perceived threats in 2023 are influenced by both financial and talent constraints as threats like ransomware march on. “The amount of emails with phishing content is increasing. Only one email needs to slip through to cause major problems,” said the owner of a technology company.

14. **The most popular planned technology purchases include network traffic monitoring and network detection and response (32%) for on-premises protection; data loss protection (41%) and data encryption (39%) for cloud-based systems; and threat intelligence (36%) as well as network security, VPNs and other access controls (34%) for hybrid environments.** The highest priorities for improving network protection are generally related to better security awareness training for employees to mitigate phishing and replacing or updating old equipment, such as firewalls.

15. **Dutch respondents continued to worry about data leakage and ransomware threats in 2022 and indicated that concern will continue through 2023.** Four in 10 respondents reported these types of cyber threats among their main concerns in both 2022 and 2021. Fears about cloud attacks also persisted in 2022 and were reported by one-third of respondents in 2022 and 2021. Among Dutch organisations that were breached in 2022, 40% said the top attack vector was an unpatched networking server, compared to remote endpoints mentioned by 31% as the top attack vector in 2021. Additionally, Dutch respondents noted IoT networks and devices became a more common attack vector in 2022, as indicated by 30% compared to 22% in 2021.

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

Select only those that apply to your actual breaches.



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