netwrix

2024

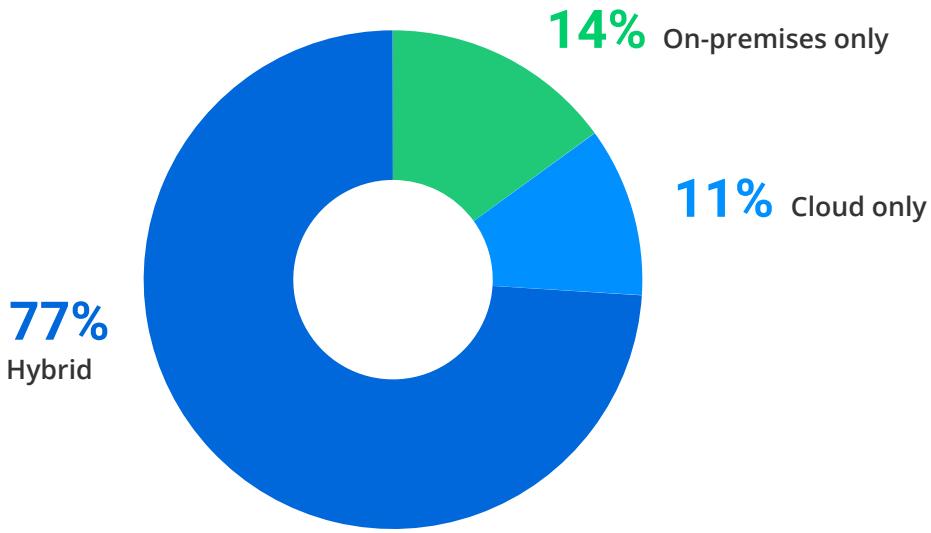
Hybrid Security Trends Report

Additional Findings for the Managed Service Provider (MSP) Sector

CLOUD ADOPTION

Managed service providers adopt cloud technologies at a pace similar to that of the rest of the market. About 3 in 4 MSPs have a hybrid IT architecture, and 11% are cloud-only.

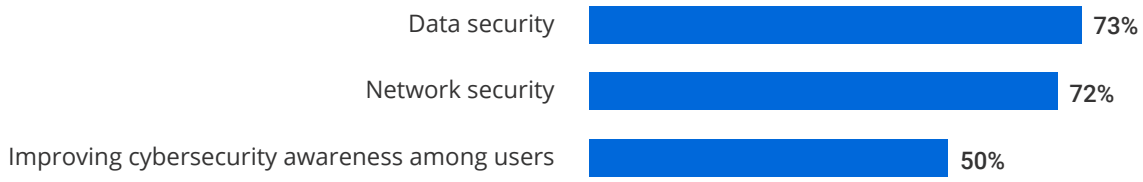
IT architecture of MSPs



IT PRIORITIES

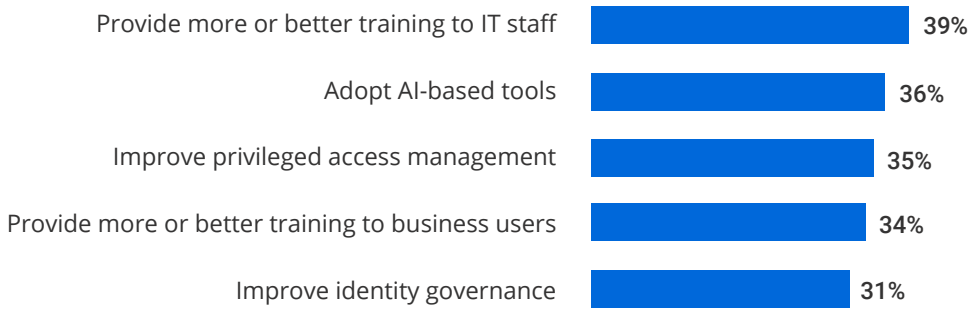
Like in 2023, the top IT priorities for the MSP sector are data security and network security, both of which were named by 7 in 10 MSPs.

Top organizational IT priorities for MSPs



We also asked our respondents what enhancements they would implement if they could choose how to improve their organization's security posture. The most desirable changes lie in the training area for IT staff and regular users. Surprisingly, implementing AI-based tools ranked second, while in the other industries, it was in seventh place.

Cybersecurity measures that IT pros working for MSPs would prioritize



AI technology promises the most desirable outcome for every MSP: Augment of the human talent resulting in better service at a lower cost to more clients. While operating within numerous IT environments, one of the most time-consuming tasks is the analysis of incoming signals. Delegating the navigation of benign notifications, false positive alerts, and actual attack patterns to an AI tool sounds promising. Still, only time will show when this scenario becomes feasible.

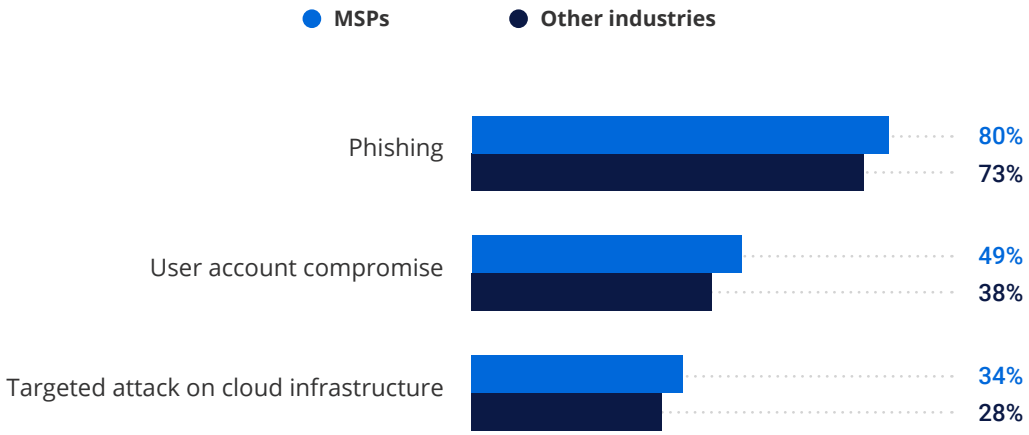
Dirk Schrader

VP of Security Research at Netwrix

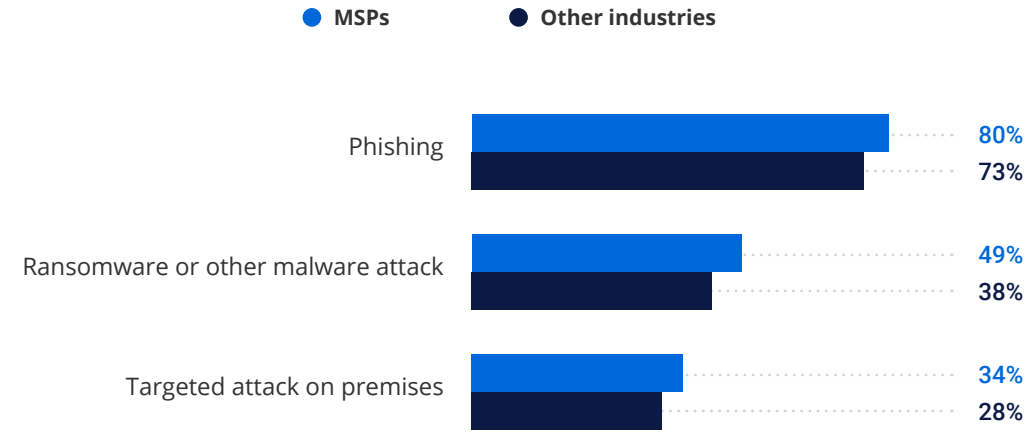
SECURITY INCIDENTS

76% of MSPs spotted a cyberattack on their infrastructure within the last 12 months, similar to the results among organizations overall (79%). For the MSP sector, each second security incident in the cloud was associated with user account compromise, while 46% of attacks on premises were ransomware or other malware attacks. In contrast, these types of attacks were less common among other industries.

Most common security incidents in the cloud for MSPs



Most common security incidents on premises for MSPs



MSPs largely rely on software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) solutions. These are usually accessible to both MSPs and their clients, significantly limiting the implementation of network-based restrictions like IP address filters. As a result, attackers target such cloud-based solutions because they might be easier to infiltrate, and one successful breach gives keys to many kingdoms.

Dirk Schrader

VP of Security Research at Netwrix

The service provider is a promising target for ransomware gangs. On one hand, MSPs can hardly afford downtime and would be more eager to have the operations back up and running, which increases the chances for ransom payout. On the other hand, breaching a service provider can be just a step toward the real target in a supply chain attack. MSPs should adequately assess the risks and rely on threat intelligence to make their security decisions.

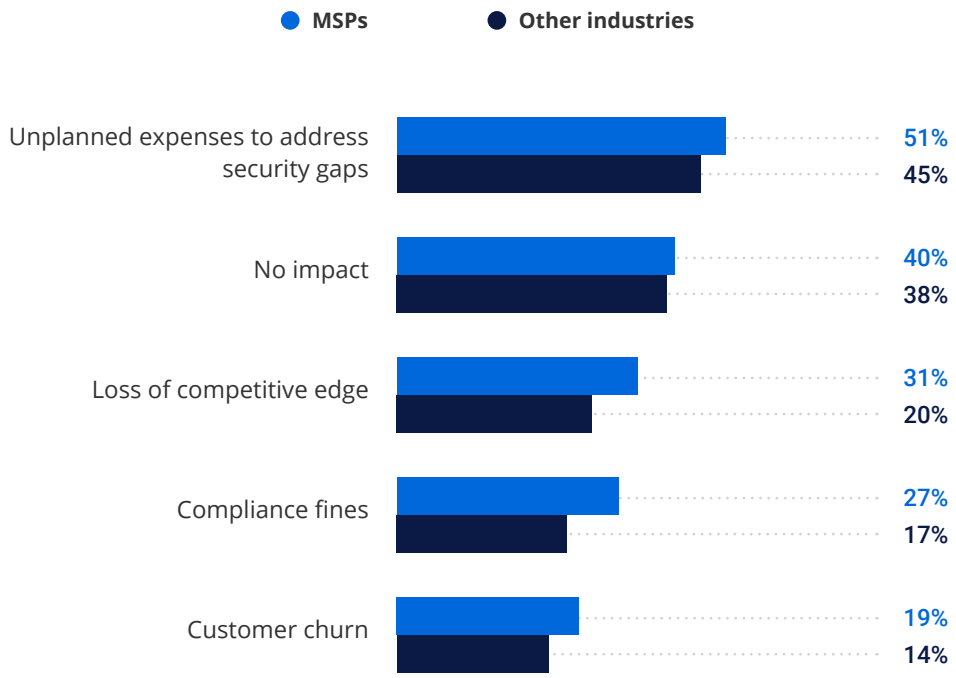
Ilia Sotnikov

Security Strategist at Netwrix

CYBERATTACK CONSEQUENCES

The survey reveals that the MSP sector suffers from cyberattack consequences more often than other industries. Among those that were attacked, every second MSP (51%) had to deal with unplanned expenses to fix the security gaps. Moreover, 31% experienced a loss of competitive edge, and 27% faced compliance fines compared to 20% and 17% across all other industries.

Cyberattack consequences for MSPs



ABOUT THE REPORT

The report is brought to you by Netwrix Research Lab, which conducts industry surveys among IT pros worldwide to discover important changes and trends. For more reports, please visit www.netwrix.com/research

ABOUT NETWRIX

Netwrix champions cybersecurity to ensure a brighter digital future for any organization. Netwrix's innovative solutions safeguard data, identities, and infrastructure reducing both the risk and impact of a breach for more than 13,500 organizations across 100+ countries. Netwrix empowers security professionals to face digital threats with confidence by enabling them to identify and protect sensitive data as well as to detect, respond to, and recover from attacks.

For more information, visit www.netwrix.com

Corporate Headquarters:
6160 Warren Parkway, Suite 100, Frisco, TX, US 75034
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

www.netwrix.com/social