netwrix

**2024**
**Hybrid Security Trends Report**

# Additional Findings for the Healthcare Sector

# CLOUD ADOPTION

Almost one-quarter (24%) of healthcare organizations are fully cloud-based, compared to only 11% in other industries. Moreover, while 74% of respondents overall have a hybrid infrastructure, this number is lower for the healthcare sector (64%).

*IT architecture: Healthcare*

**12%** On-premises only

**24%** Cloud only

**64%** Hybrid

"
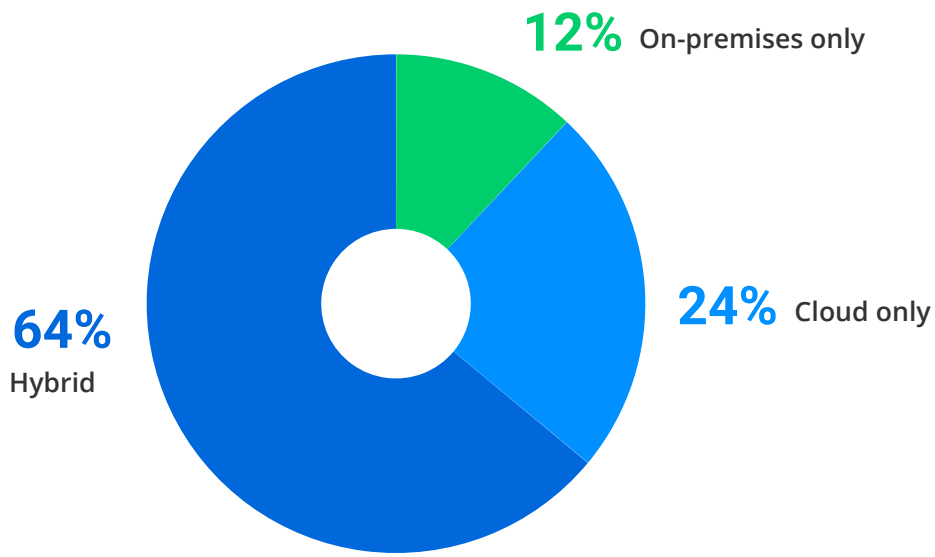
**The effort and cost of managing an on-premises infrastructure are higher in the healthcare sector, due in part to stringent regulatory standards around the handling and storage of patient and research data. In order to focus on their core healthcare mission, these organizations often offload significant parts of the security and compliance burden to software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) providers, which drives higher cloud adoption rates in this sector.**

**Ilia Sotnikov**
Security Strategist at Netwrix

# IT PRIORITIES

The two main IT priorities are the same for organizations across all sectors: data security and network security. Automation of manual IT processes ranked third for the healthcare sector, compared to just fifth place for respondents overall. Indeed, nearly half (46%) of healthcare organizations respondents picked it as one of their top priorities for 2024.

*Top IT Priorities: Healthcare*

| | |
|---|---|
| Data security | 64% |
| Network security | 54% |
| Automating manual IT processes | 46% |

"

**Healthcare organizations traditionally deal with many processes that require manual input of information like treatment protocols, administered drugs, procedures performed — basically, everything that happens to a patient. Automating these processes saves the valuable time of healthcare professionals, so it's no wonder that automation is a high priority for this sector.**
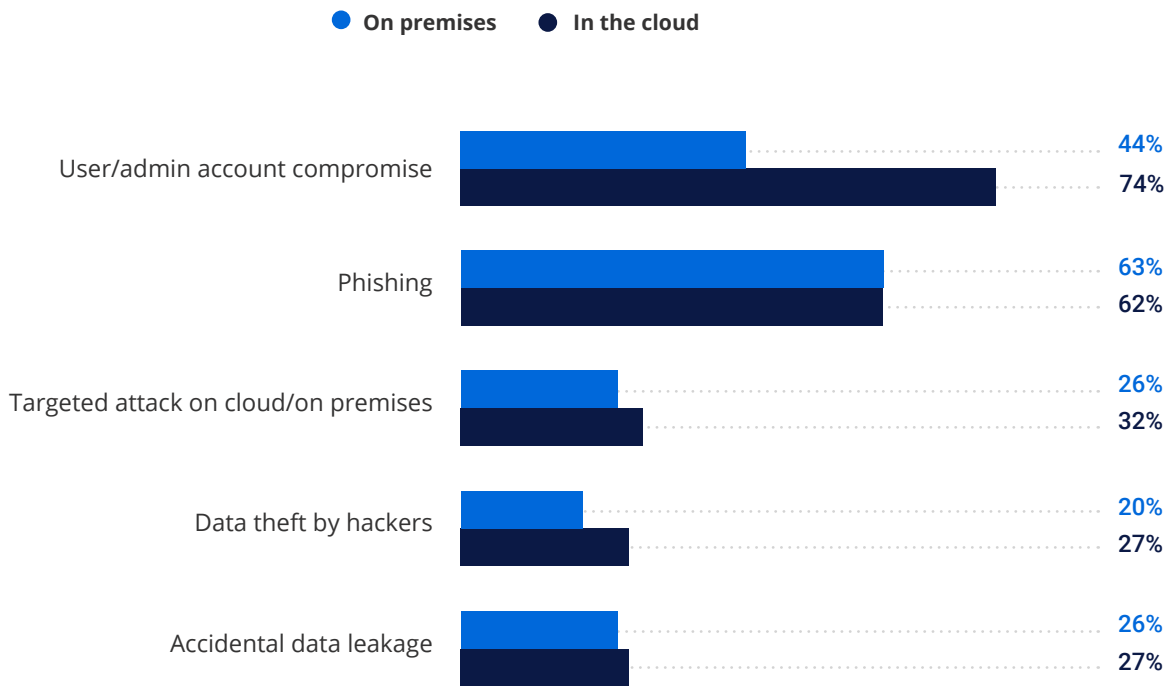
**Dirk Schrader**
VP of Security Research at Netwrix

# SECURITY INCIDENTS

84% of organizations in the healthcare sector spotted a cyberattack within the last 12 months. Phishing was the most common type of incident experienced on premises, similar to other industries. Account compromise topped the list for cloud attacks: 74% of healthcare organizations that spotted a cyberattack reported user or admin account compromise.

*Most Common Security Incidents: Healthcare*

● **On premises**    ● **In the cloud**

| Incident | On premises | In the cloud |
|---|---|---|
| User/admin account compromise | 44% | 74% |
| Phishing | 63% | 62% |
| Targeted attack on cloud/on premises | 26% | 32% |
| Data theft by hackers | 20% | 27% |
| Accidental data leakage | 26% | 27% |

"

Healthcare workers regularly communicate with many people they do not know — patients, laboratory assistants, external auditors and more — so properly vetting every message is a huge burden. Plus, they do not realize how critical it is to be cautious, since security awareness training often takes a back seat to the urgent work of taking care of patients. Combined, these factors can lead to a higher rate of security incidents.

**Dirk Schrader**
VP of Security Research at Netwrix

"

Protected health information (PHI) is one of the most expensive types of data sold on darknet forums, which makes healthcare organizations a top target for cybercriminals. A core defense strategy is to minimize standing privileges by using a privileged access management (PAM) solution. Another is to implement identity threat detection and response (IDTR) tools to quickly block malicious actors using compromised credentials.
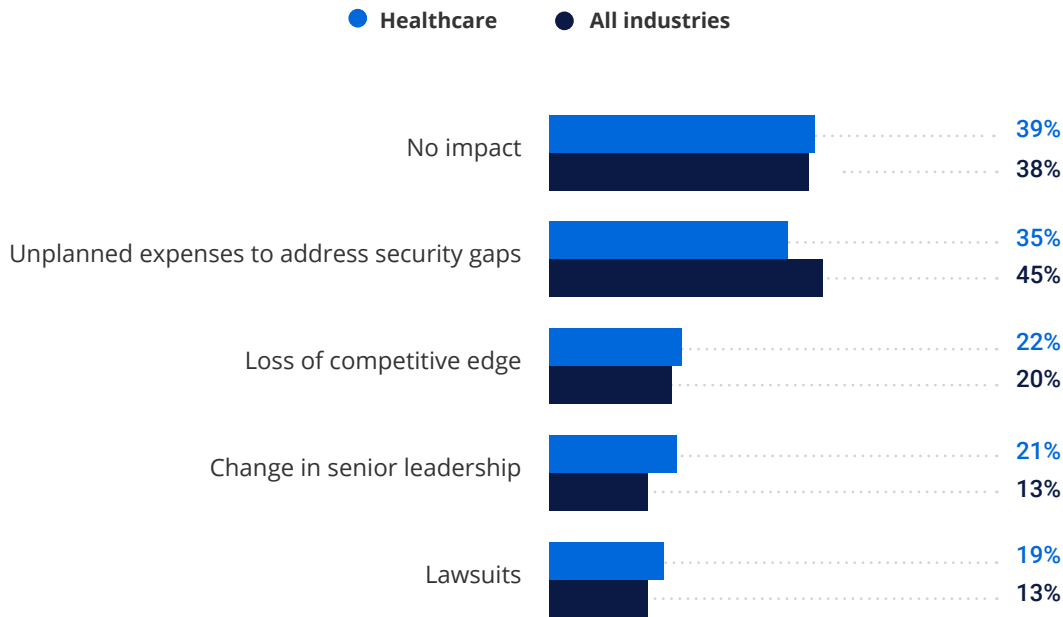
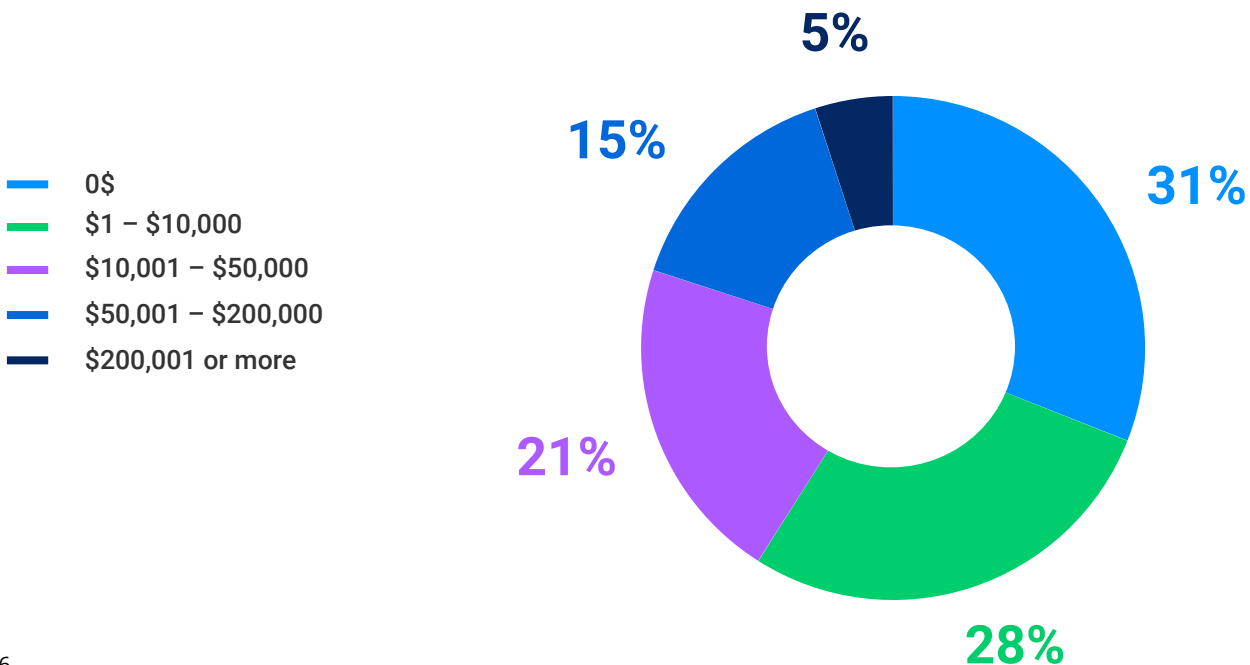**Ilia Sotnikov**
Security Strategist at Netwrix

# COST OF CYBERATTACKS

A cyberattack resulted in financial damage for 69% of healthcare organizations, compared to 60% among other industries. One in five healthcare organizations that suffered an attack experienced a change in senior leadership (21%) or lawsuits (19%) as a result, compared to 13% for each of these outcomes among all industries surveyed.

*Cyberattack Consequences: Healthcare*

● **Healthcare**    ● **All industries**

| Consequence | Healthcare | All industries |
|---|---|---|
| No impact | 39% | 38% |
| Unplanned expenses to address security gaps | 35% | 45% |
| Loss of competitive edge | 22% | 20% |
| Change in senior leadership | 21% | 13% |
| Lawsuits | 19% | 13% |

*Estimated Financial Damage due to Cyberattacks: Healthcare*

— 0$
— $1 – $10,000
— $10,001 – $50,000
— $50,001 – $200,000
— $200,001 or more

- 31%
- 28%
- 21%
- 15%
- 5%

# 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