netwrix

2023
Hybrid Security Trends Report

Additional Findings for the Finance & Banking Sector

CLOUD ADOPTION

The financial sector is adopting cloud technology at a slower pace compared to other industries. While, on average, 73% of respondents report having a hybrid infrastructure, the financial sector lags slightly behind at 62%. However, 89% of those currently relying solely on on-premises systems have plans to embrace cloud technologies.

IT Architecture: financial sector

32% On-premises only

62% Hybrid

6% Cloud only
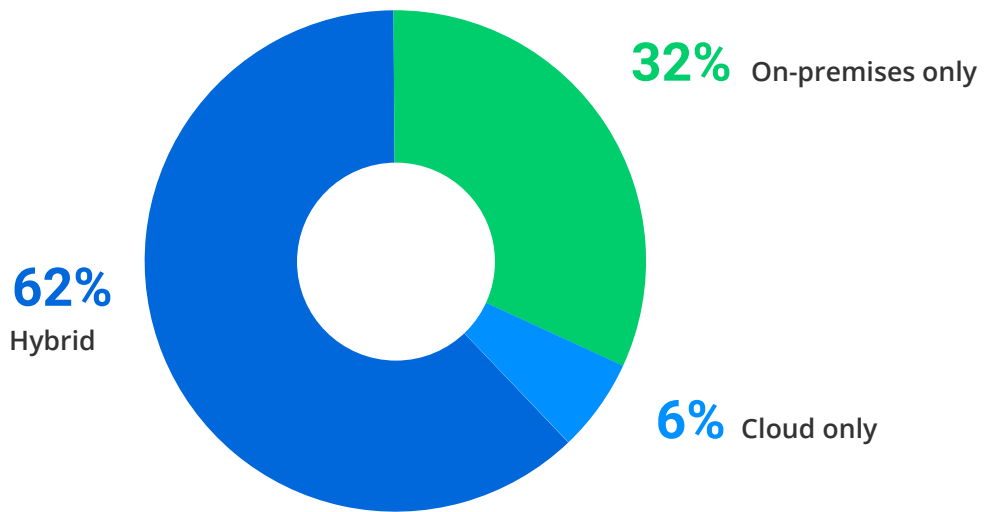
Legislative compliance likely impedes the financial sector's swift transition to the cloud. The intricacies mainly revolve around shared responsibilities between organizations and cloud providers, especially when complying with mandates such as security audit site visits.
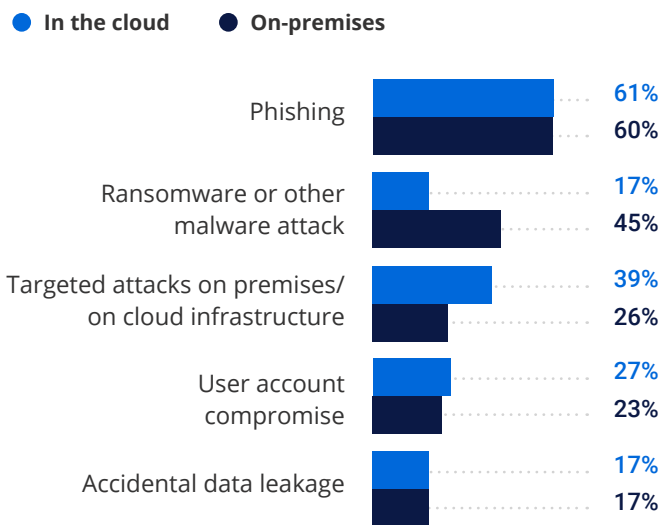
Dirk Schrader
VP of Security Research at Netwrix
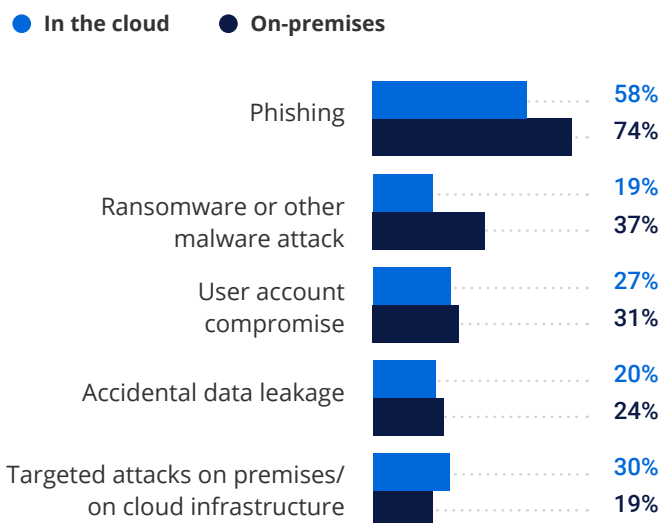
SECURITY INCIDENTS

Within the last 12 months, 77% of financial organizations detected a cyberattack, compared to 68% among other industries. The most common security incidents were phishing, ransomware, and targeted attacks on both cloud infrastructure and on-premises systems.

Among respondents in the financial sector, 39% encountered targeted attacks on their cloud infrastructure, higher than the 30% reported among organizations overall. Conversely, the financial sector experiences user account compromise less frequently compared to the market's average rate.

Most common security incidents *in the financial sector*

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

	In the cloud	On-premises
Phishing	61%	60%
Ransomware or other malware attack	17%	45%
Targeted attacks on premises/ on cloud infrastructure	39%	26%
User account compromise	27%	23%
Accidental data leakage	17%	17%

Most common security incidents in organizations *overall*

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

	In the cloud	On-premises
Phishing	58%	74%
Ransomware or other malware attack	19%	37%
User account compromise	27%	31%
Accidental data leakage	20%	24%
Targeted attacks on premises/ on cloud infrastructure	30%	19%

"

Along with healthcare, the financial sector holds access to some of the most critical data concerning citizens and organizations, managing banking information and access to funds. Any operational disruption proves highly problematic, increasing the likelihood of substantial ransom payments to attackers. Moreover, the sector's heavy reliance on digital assets amplifies vulnerability; virtually every banking or financial transaction involves a computer. This dependency on technology, while providing agility and speed, introduces a multitude of attack vectors, where a single flaw can allow an attacker to infiltrate the system.
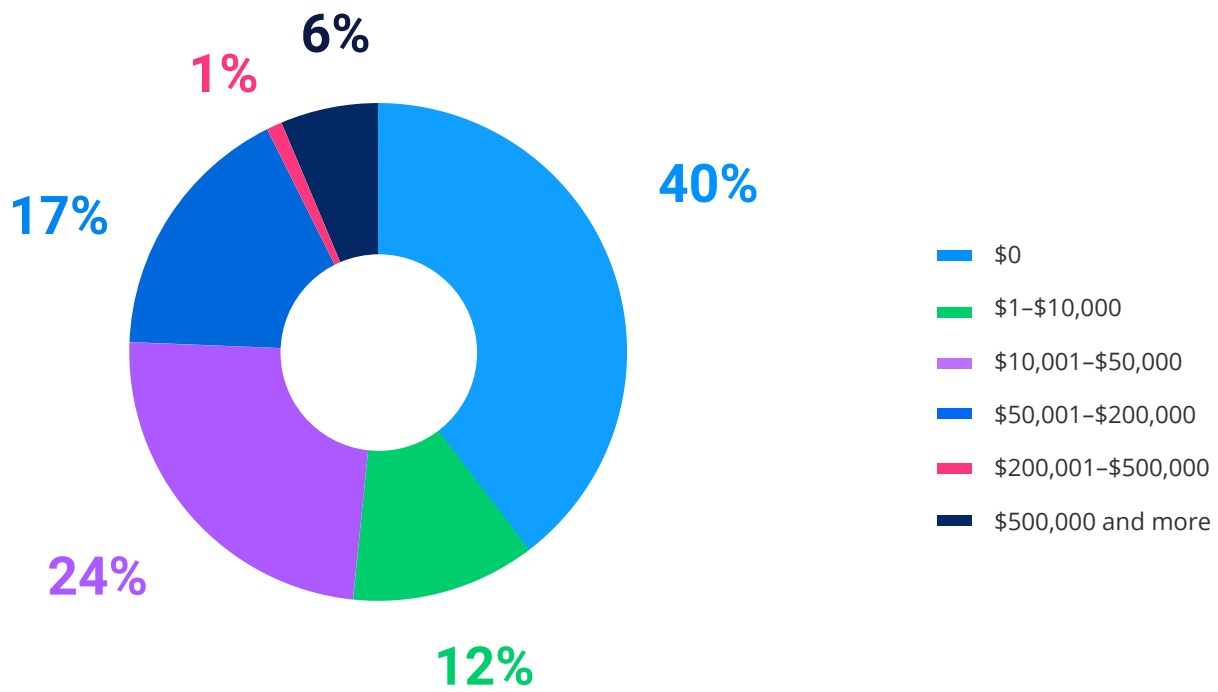
Dirk Schrader
VP of Security Research at Netwrix

COST OF CYBERATTACKS

The financial sector also reports larger expenses as a result of cyberattacks than other industries. Indeed, 24% of financial organizations estimated their financial damage from cyberthreats to be at least $50,000, compared to just 16% among organizations overall.

Estimated financial damage due to cyberthreats in the financial sector

6%

1%

40%

17%

24%

12%

- $0
- $1–$10,000
- $10,001–$50,000
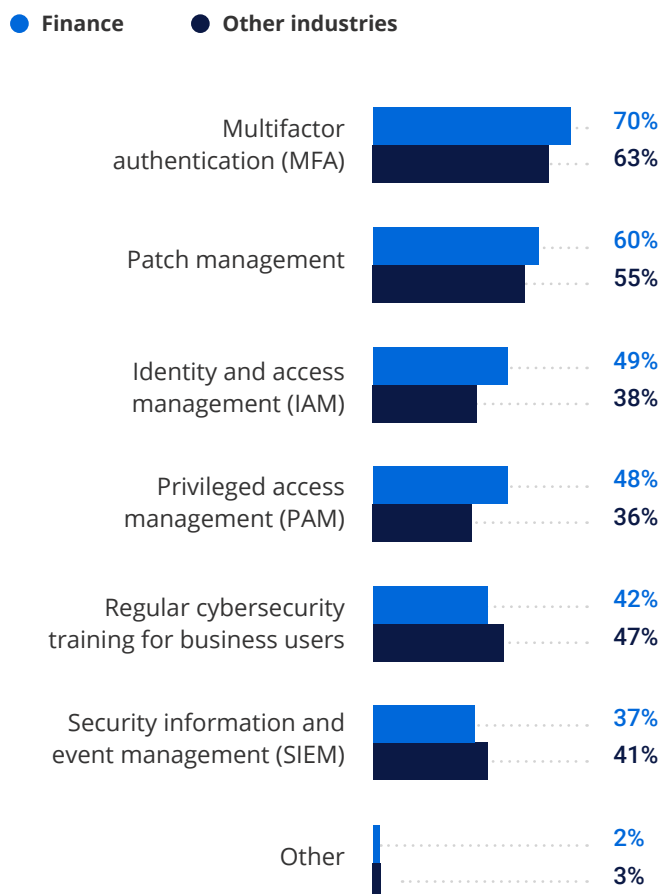- $50,001–$200,000
- $200,001–$500,000
- $500,000 and more

60% of financial organizations face financial consequences due to cyberattacks even if they do not result into a data breach.

CYBER INSURANCE

Organizations with the financial sector consider purchasing a cyber insurance policy more often than other industries. 73% of respondents either have such a policy or plan to acquire one within the next 12 months, whereas among organizations overall, this stands at 59%. Given the sector's risk profile, insurance companies impose stricter security requirements on financial organizations: 49% of respondents needed an identity and access management (IAM) solution, contrasting with 38% in other industries, and 48% had to comply with privileged access management (PAM) requirements, compared to 36% in other sectors.

What requirements did your organization have to meet in order for the insurance company to issue a policy?

● **Finance**   ● **Other industries**

Requirement	Finance	Other industries
Multifactor authentication (MFA)	70%	63%
Patch management	60%	55%
Identity and access management (IAM)	49%	38%
Privileged access management (PAM)	48%	36%
Regular cybersecurity training for business users	42%	47%
Security information and event management (SIEM)	37%	41%
Other	2%	3%

"

Two primary drivers compelling the financial sector to mitigate the impact of breaches through cyber insurance are forensic risk analysis and the high cost of compliance violation fines. However, while a policy can assist financially, it cannot restore the reputation, a core element of successful financial business. Therefore, this sector stands out as one of the most mature industries in terms of cybersecurity.

Dirk Schrader

VP of Security Research at Netwrix

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 makes data security easy. Since 2006, Netwrix solutions have been simplifying the lives of security professionals by enabling them to identify and protect sensitive data to reduce the risk of a breach, and to detect, respond to and recover from attacks, limiting their impact. More than 13,000 organizations worldwide rely on Netwrix solutions to strengthen their security and compliance posture across all three primary attack vectors: data, identity, and infrastructure.

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