

2022

INSIDER THREATS ARE ORGANIZATIONS' BIGGEST CYBERSECURITY RISK

External attacks aren't the only cyber threats today's organizations need to consider. Malicious, negligent and compromised users are a serious and growing risk.

Insider threats have become more frequent and costly—and affect organizations in ways that go well beyond direct financial losses.

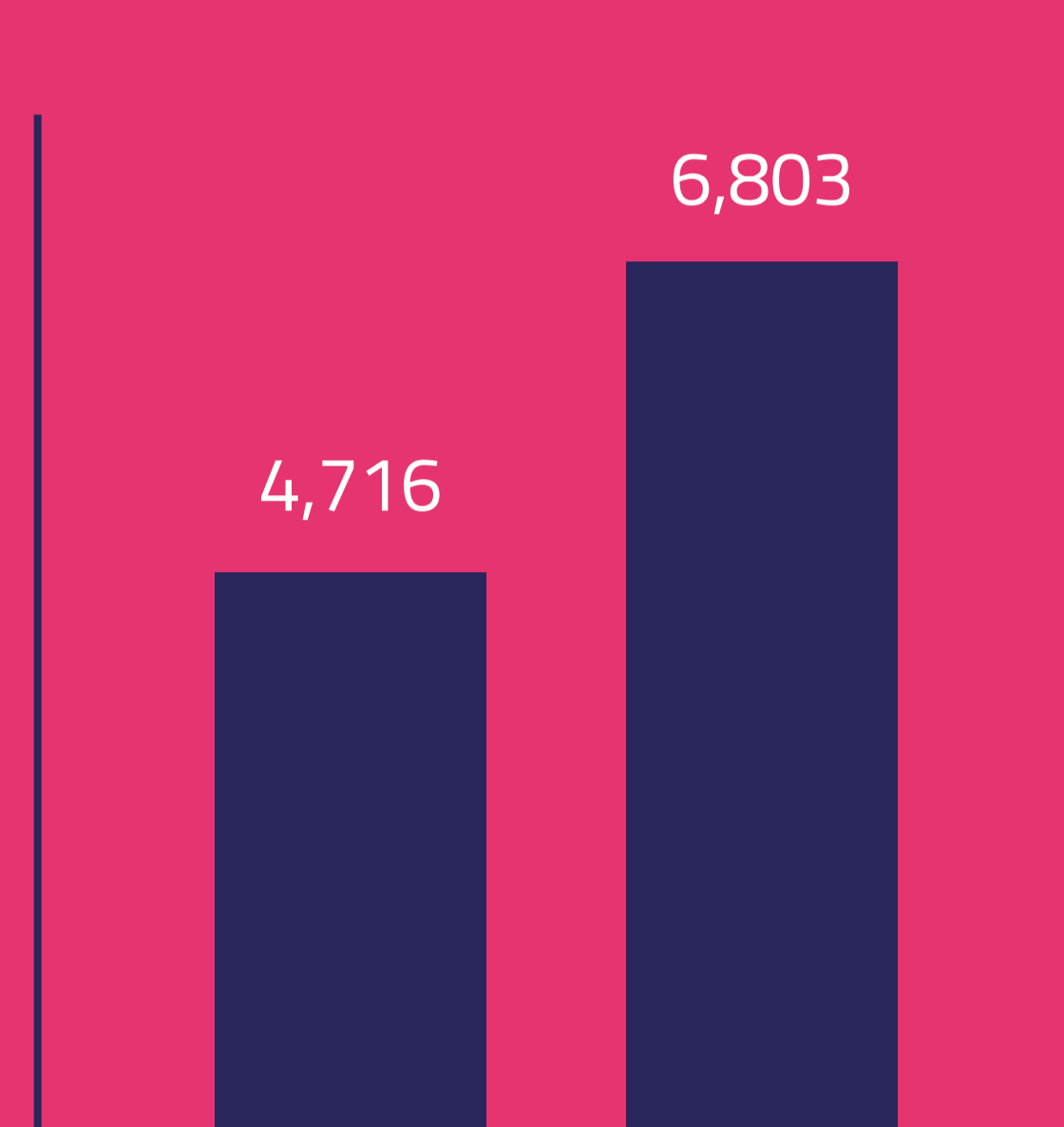
Here are some key findings from the 2022 Cost of Insider Threats Report independently conducted by

DATAPATROL



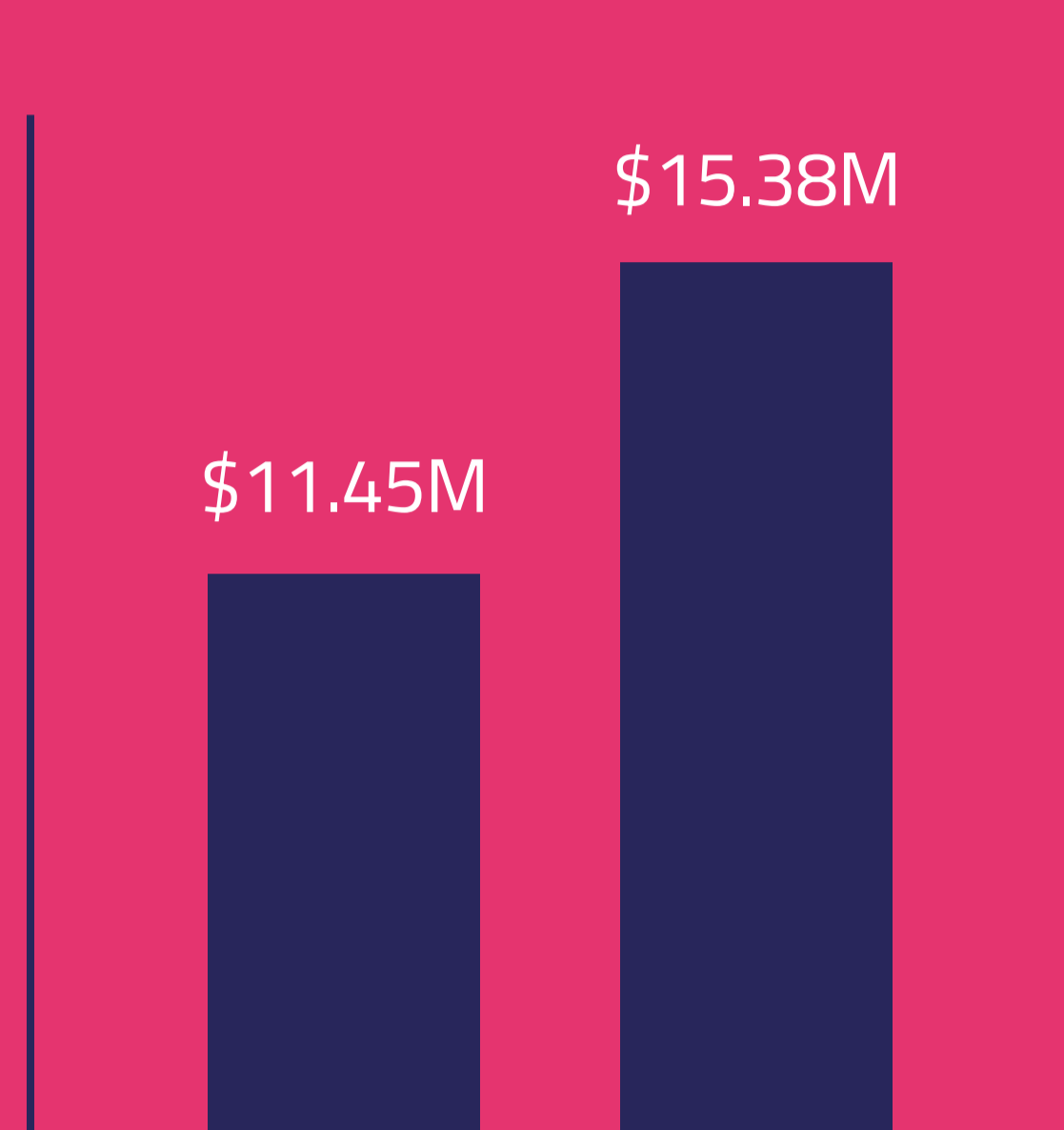
UP AND UP: THE COST OF INSIDER THREATS IS GROWING

The number—and costs—of insider-led cybersecurity incidents has soared over the last two years.



Insider-led cybersecurity incidents

44% increase



Total annual cost of insider threats

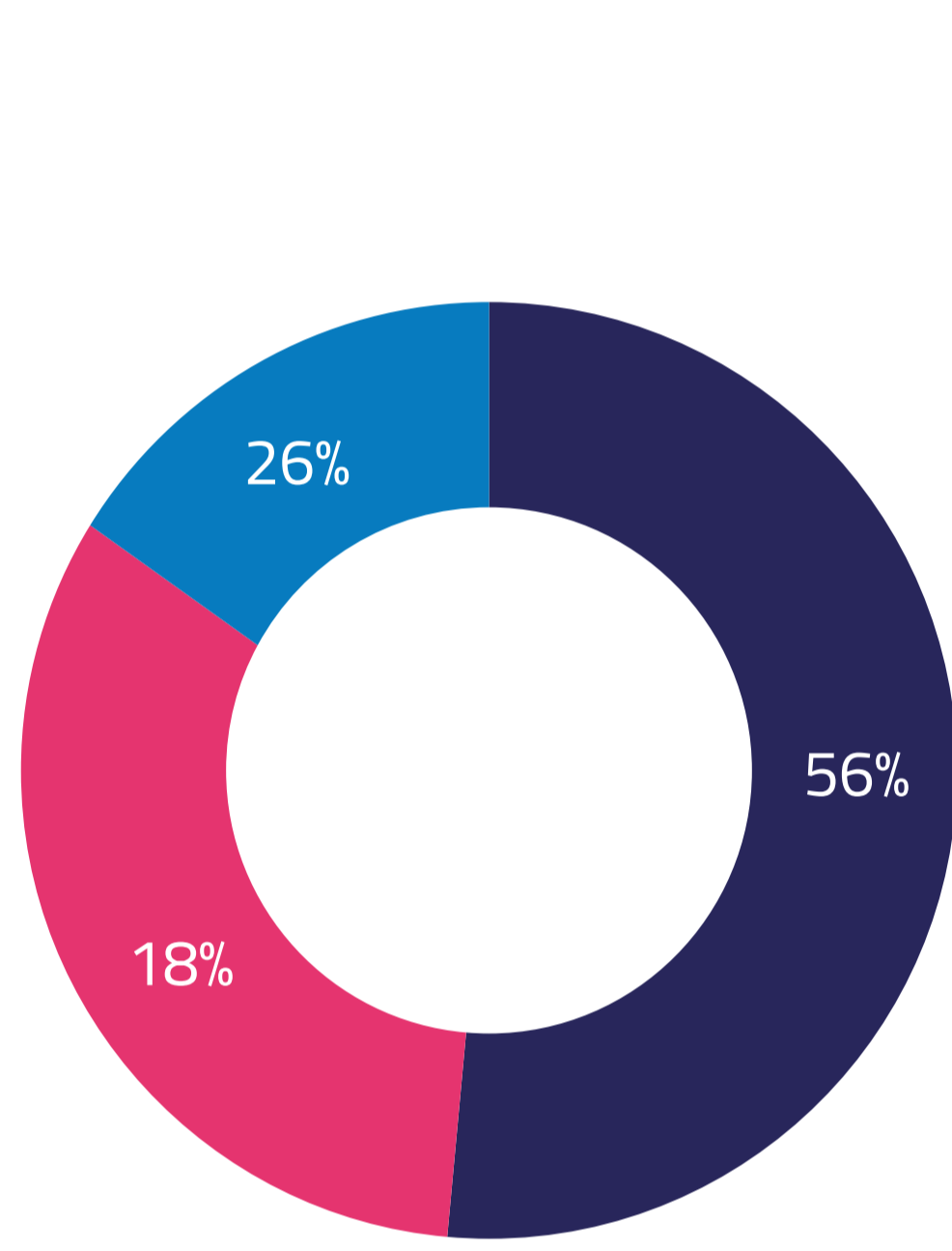
34% increase

TRIPLE THREAT: THREE TYPES OF INSIDER THREATS

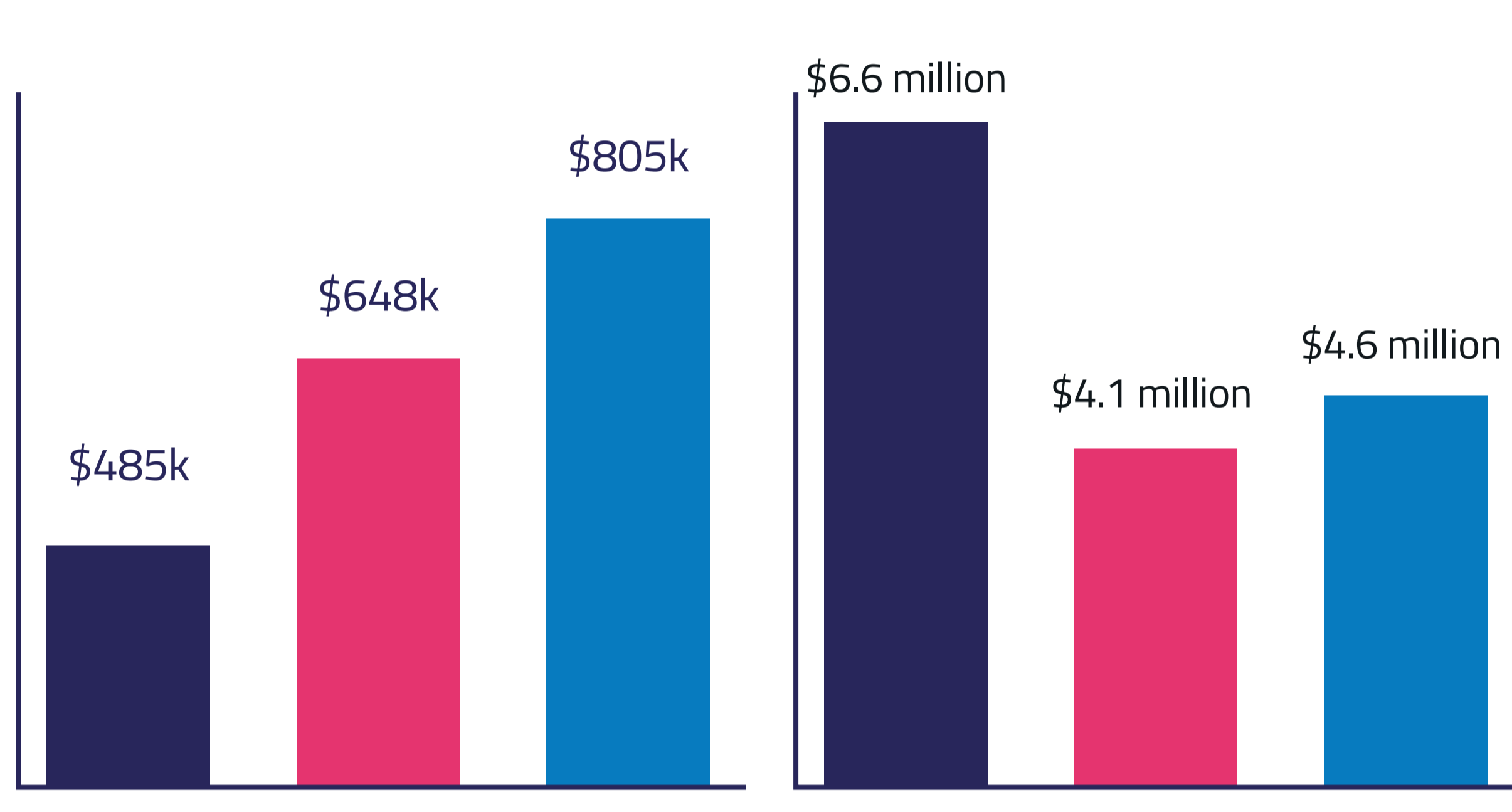
Not all insider threats are alike. Here's a breakdown of the three main types—and what they're costing organizations.

TYPE OF INSIDER

- Negligent insiders
- Malicious insiders
- Credential insiders



% OF INCIDENTS



COST PER INCIDENT

TOTAL COST TO ORGANIZATIONS

80% INCREASE IN INSIDER THREAT SPEND VS. 2016

Average costs per security incident in 2022 in USD:



Detection

\$35k



Investigation, Escalation, Response

\$280k



Containment, Analysis, Remediation

\$331k



Total

\$646k

TIME IS MONEY

When it comes to insider threats, time is money. Yet it's taking companies longer than ever to contain incidents when they occur.

Annualized cost

≤30 DAYS
\$11.23M

(up from \$7.12 million in 2020)

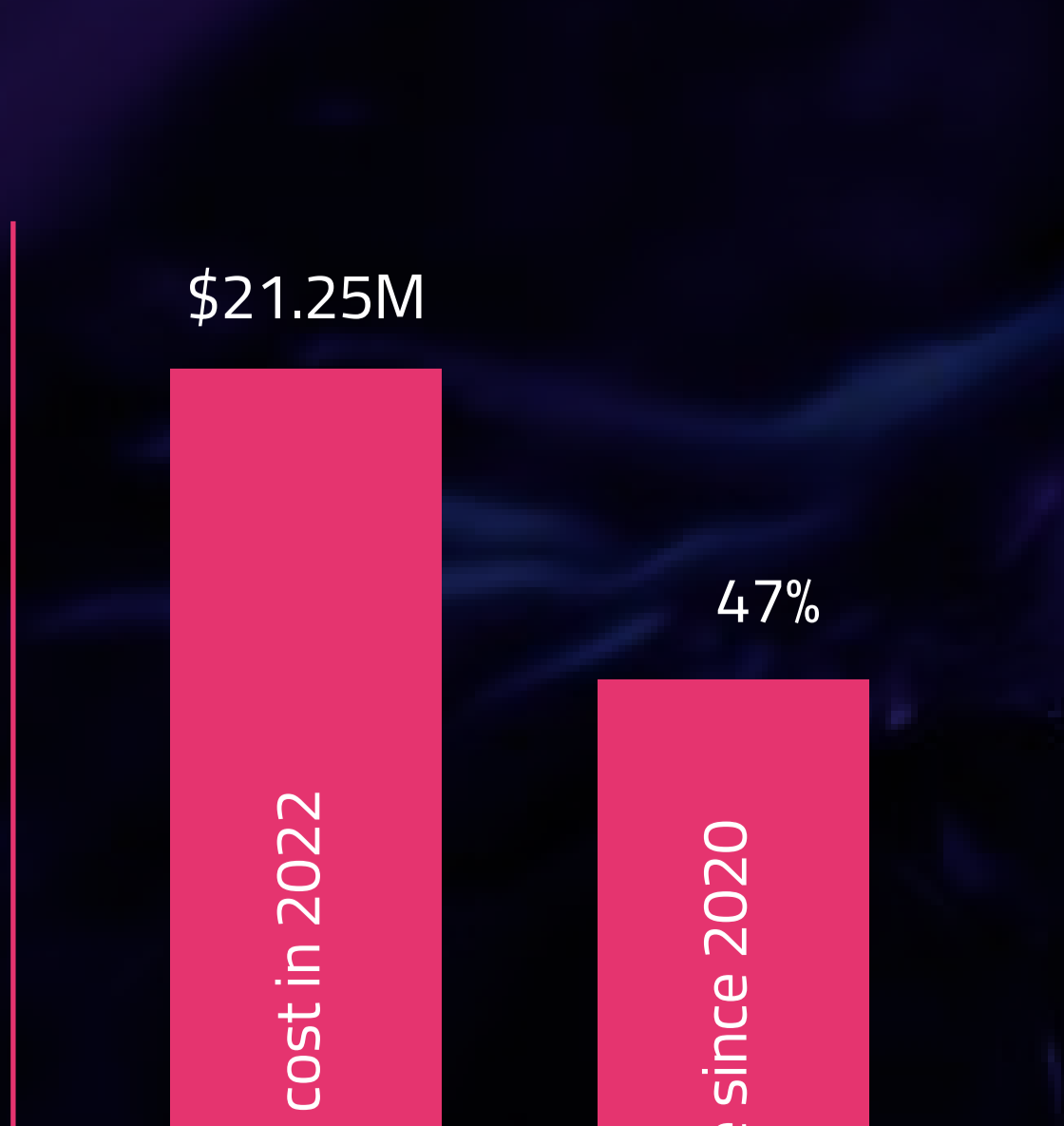
≥90 DAYS
\$17.19M

(up from \$13.71 million in 2020)

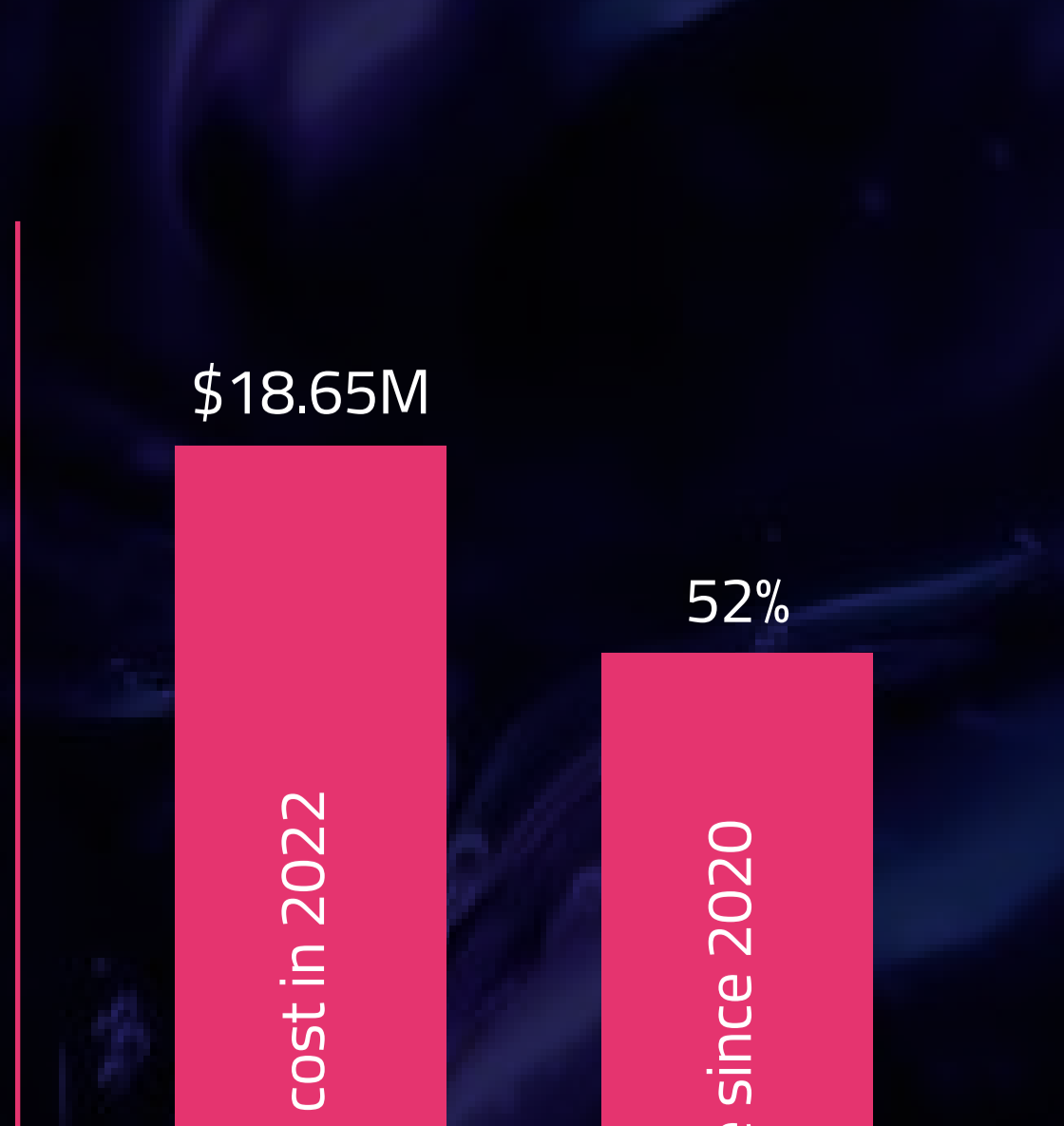
MOST AFFECTED INDUSTRIES



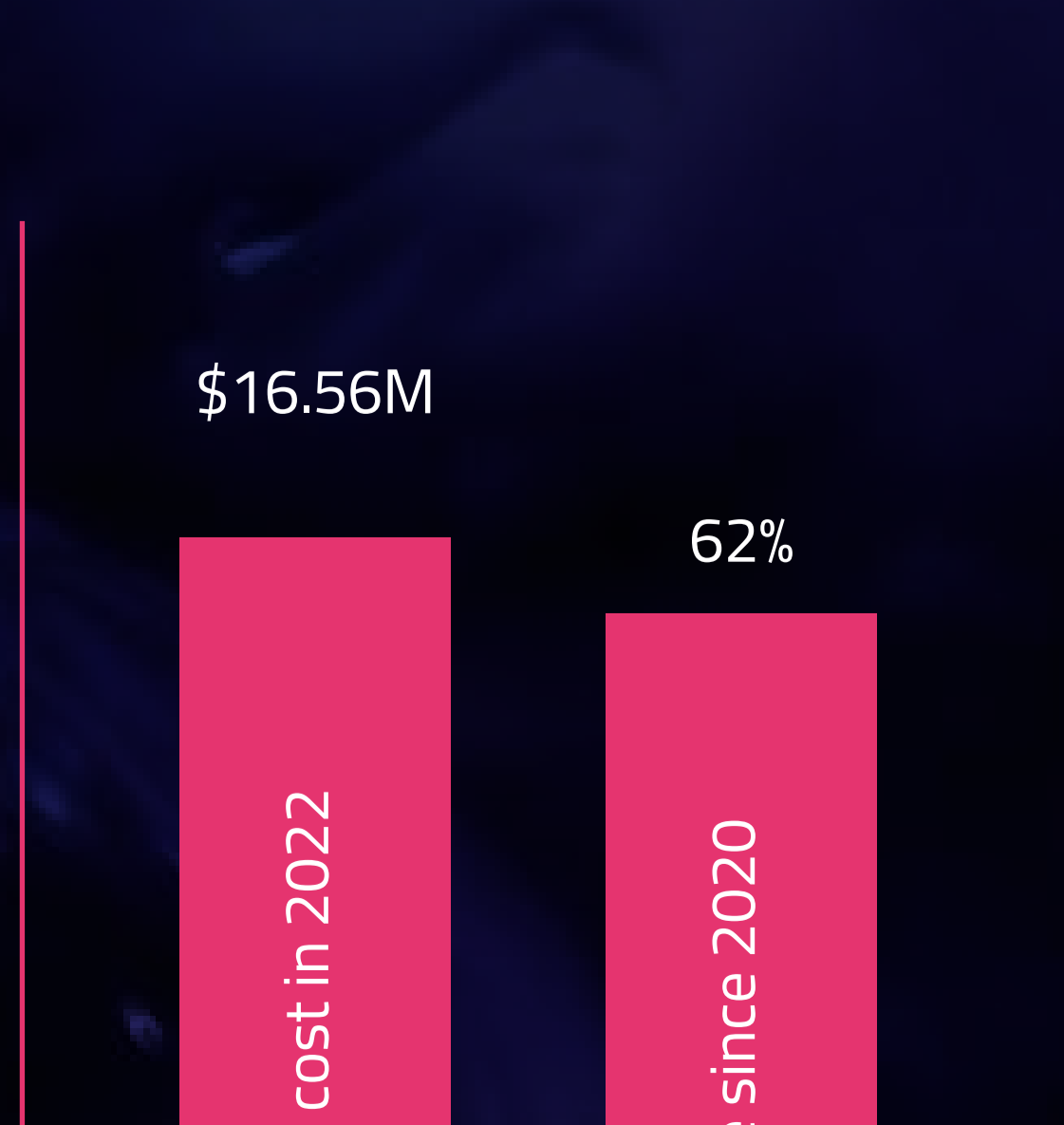
Financial services and services organizations bear highest average costs managing insider threats



FINANCIAL SERVICES



SERVICES



RETAIL