

Looking within:

The Hidden Costs of Insider Threats

Most organizations understand the challenge of external cyber attacks. But many of today's biggest threats come from within. Whether it's careless users, disgruntled employees or compromised accounts, the cost of insider threats is on the rise.

Here's a closer look at this little-known, but growing challenge, adapted from the Ponemon 2020 Cost of Insider Threats Global Study.

More Incidents, Higher Costs

The number of insider-caused cybersecurity incidents jumped 47% since 2018, with the average cost up 31% to \$11.45 million.

Cybersecurity incidents increased by:

47%



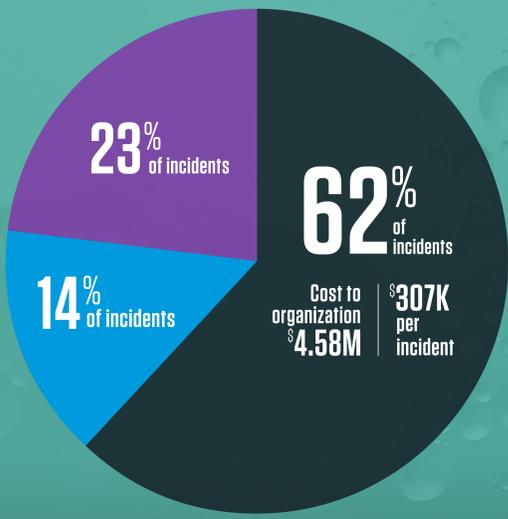
Cost of insider threats rose:

31%



Three Kinds of Insider Threats

Insider threats are not created equal. Here's a breakdown of the three main types of insider threats.



NEGLIGENT INSIDERS are careless and distracted users who unintentionally expose data. They account for the largest share of incidents by far and highest total cost. But the per-incident costs from these insider threats are much lower.

CRIMINAL INSIDERS are malicious insiders who deliberately expose the organization's data for financial gain or out of spite. Though they account for the smallest share of incidents, they cost organizations more than twice as much per incident as negligent insiders.

CREDENTIAL INSIDERS, or credential thieves, take over insiders' accounts and use them to steal data and money, spread within the organization, and launch more insider attacks. Though they represent less than a quarter of all incidents, they do much more damage per incident than the other two types of insider threat.

How Organizations are Fighting Insider Threats

Spending to stop insider threats is up 60% from just three years ago and 25% from 2018. The bulk of that goes to detection and investigation efforts. Insider threat investigation costs alone have jumped 86% in just three years.

60%

Increase in insider threat spend, compared to 3 years ago

25%

Increase in spend since 2018

86%

Overall, investigation costs have increased by 86% in only 3 years

The Clock is Ticking

The cost of an insider threat rises exponentially as it lingers:

■ Incidents that were resolved in less than 30 days cost victims \$7.12 million.¹

■ Incidents resolved in 90 days or longer cost victims \$13.71 million.



¹ Costs are calculated on an annualized basis.

Insider incidents take an average of

77 DAYS to contain

Industry Matters

The cost of insider incidents varies according to organizational size according to the study:

- Organizations with a headcount of between 25,001 and 75,000 people spent an average of \$17.92 million to resolve insider incidents.
- Those with a headcount of 500 or fewer spent an average of \$7.68 million to resolve insider incidents.

Here are some industry-specific statistics over the past two years:

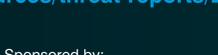


Get the full report to see how your industry compares and view more data from around the world. proofpoint.com/us/resources/threat-reports/2020-cost-of-insider-threats

Independently conducted by:



Sponsored by:



SHARE NOW:

