THREAT STATISTICS:

2018 SURPRISING FINDINGS FROM THE 2018 CROWD RESEARCH PARTNERS 'INSIDER THREAT REPORT'

An increasing amount of organizations feel vulnerable to insider threats. The 2018 Crowd Research Partners 'Insider Threat Report' offers statistical insight into the concerns and struggles that many cyber security professionals face. This comprehensive report is comprised of 472 cyber security professionals, the majority (87%) being in leadership roles.The report is extensive, but we've provided you with the most valuable statistics in this graphic.

Don't let these insiders cause your company to be the next data breach victim. Teramind.co monitoring software actively prevents and protects against insider threats.

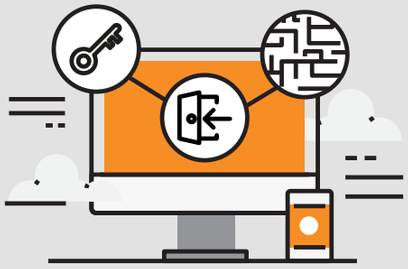
Sources:
https://www.csoonline.com/article/3238867/risk-management/2018-crowd-research-partners-insider-threat-report-hopes-and-fears-revealed.html

http://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf

TERAMIND

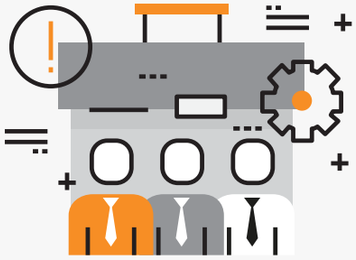
www.teramind.co

90% of organizations felt vulnerable to insider attacks.



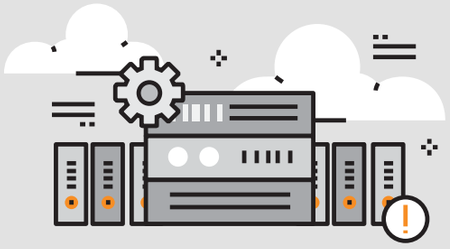
Top three risk factors for insider threats are privileges (**37%**), endpoint access (**36%**), and information technology complexity (**35%**).

53% confirmed that an insider attack happened in their organization during the last year.



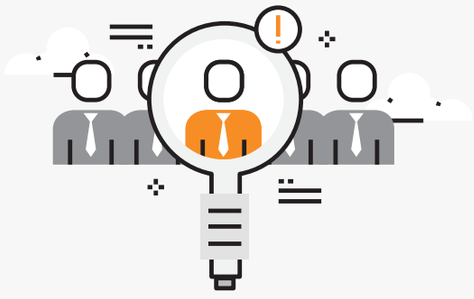
Regular employees (**56%**), privileged users (**55%**), and contractors (**42%**) seem to pose the largest insider threat concern.

Top three types of data vulnerable to an insider attack are confidential business information (**57%**), privileged account information (**52%**), and personal information (**49%**).



The data assets most vulnerable to insider attacks are databases (**50%**), file servers (**46%**), and cloud applications (**39%**).

27% of respondents claimed that an insider data breach could cost them roughly $100K to $500K in US dollars.



More than **88%** of survey respondents believe it's necessary to monitor, profile, and identify insiders based on their behavior with data.