truadvantage
award-winning • IT & Cybersecurity

# 2024 Cybersecurity and Breach Stats for SMBs

## Stat and Source:

1. Stat: A cyberattack takes place roughly once every 39 seconds.
·Source: Exploding Topics
·Link: https://explodingtopics.com/blog/cybersecurity-stats

2. Stat: Cybercrime rates up by 600% since the start of the Covid-19 Pandemic
·Source: Exploding Topics
·Link: https://explodingtopics.com/blog/cybersecurity-stats

3. Stat: More than 2, 200 cyberattacks occur each day.
·Source:
·Link: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

4.Stat: The global average cost of negligence (insider threat) is $11.45M and negligent employees or contractors were the root cause of 2,962 of the 4,716 incidents reported.
·Source: IBM Security – Cost of Insider Threats
·Link: https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/?_ga=2.81919894.1813358506.1610826674-1323527553.1610826674#/

5.Stat: Data breaches initiated by malicious insiders were the most costly—USD 4.90 million on average, or 9.5 percent higher than the USD 4.45 million cost of the average data breach.
·Source: IBM Security – What are insider threats?
·Link: https://www.ibm.com/topics/insider-threats#:~:text=According%20to%20IBM's%20Cost%20of,of%20the%20average%20data%20breach

6. Stat: A recent survey conducted by Spiceworks finds that only 18 percent of IT budgets are allocated to managed services
·Source: Spiceworks' 2023 State of IT Report
·Link:https://swzd.com/resources/state-of-it/

7. Stat: The Identity Theft Resource Center tracked 2,116 data compromises in the first three quarters of 2023, breaking the all-time high of 1,862 compromises in 2021.
·Source: Cybernomics 101
·Link: https://www.barracudamsp.com/resources/reports/cybernomics-101

8. Stat: Remote working had led to 47% of cyberattack victims falling for a spear-phishing attack
·Source: Exploding Topics
·Link: https://explodingtopics.com/blog/cybersecurity-stats

9. Stat: The global average cost of a data breach is $3.9 million across SMBs
·Source: Cyber Security Facts and Stats through Juniper Research
· Link: https://www.cybintsolutions.com/cyber-security-facts-stats/

10. Stat: 84 percent of 1,050 survey respondents in 15 countries said that their organization had experienced at least one successful email-based phishing attack during 2022.
·Source: IT World Canada
·Link: https://www.itworldcanada.com/article/employees-still-too-gullible-for-phishing-lures-report/530090

11. Stat: International research commissioned by Barracuda in 2023 found that roughly half (46%) of organizations say they are already using AI in cybersecurity, and a further 43% plan to start adopting it in the near future. Only 2% say that they have no plans to start using AI.
·Source: Securing tomorrow: A CISO's guide to the role of AI in cybersecurity
·Link: https://www.barracudamsp.com/resources/ebooks/ciso-guide-ai-cybersecurity-ebook

12. Stat: 2022 Study: 50% Of SMBs Have A Cybersecurity Plan In Place
·Source: UpCity
·Link: https://upcity.com/experts/small-business-cybersecurity-survey/

13. Stat: The cybersecurity market size is set to be $203.78 USD Billion in 2024
·Source: Mordor Intelligence
·Link: https://www.mordorintelligence.com/industry-reports/cyber-security-market

14. Stat: The United States cybersecurity market size revenue in 2023 was 73.41 USD Billion.
·Source: Mordor Intelligence
Link: https://www.mordorintelligence.com/industry-reports/cyber-security-market

15. Stat: Digital ad fraud is rising sharply. The ad industry loses approximately $51 million per day due to ad fraud and by 2023 that number will skyrocket to $100 billion annually, according to an estimate featured in Bloomberg Law.
·Source: Cybercrime Magazine
·Link: https://cybersecurityventures.com/cybersecurity-almanac-2022/

16. Stat: Phishing attacks account for 31% of all cyberattacks
·Source: Exploding Topics
·Link: https://explodingtopics.com/blog/cybersecurity-stats

17.  Stat: The sheer number of ways in which an organization may be exposed to threats is daunting; for example; at least one open-source vulnerability was found in 84% of codebases in 2023.
·Source: Gartner report
·Link: https://www.gartner.com/doc/reprints?id=1-2G6U1RDP&ct=240109&st=sb

18. .Stat: 83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.
·Source: Verizon 2023 Data Breach Investigations Report
·Link: https://www.verizon.com/business/resources/reports/dbir/2023

19. Stat: The average cost of a data breach is 4.24 million dollars.
·Source: IBM
·Link: https://www.ibm.com/downloads/cas/OJDVQGRY

20. Stat: The average number of days to identify and contain a data breach is 287.
·Source: IBM
·Link: https://www.ibm.com/downloads/cas/OJDVQGRY

**Additional stats:**

Source: Exploding Topics: The Ultimate List of Cyber Attack Stats (2024)
Link: https://explodingtopics.com/blog/cybersecurity-stats

·Remote working lead to 47% of cyberattack victims falling for a spear-phishing attack
·Remote work has resulted in a $137, 000 increase in the average cost of a data breach
·85% of phishing schemes target login information
·Hackers breach an average of 30, 000 websites daily
·More than $17, 000 is lost every 60 seconds due to phishing
·On average, data breach incidents cost companies more than $3.9 million
·Small businesses account for 43% of cybercrime
·Only 5% of organizations' storage folders have adequate protection

Source: Verizon Data Breach Investigations Report 2023
Link: https://www.verizon.com/business/resources/reports/dbir/2023

·74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.
·The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.
·Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.