2020 Cyber Risk Overview

Verizon, Purplesec and the Ponemon Institute wrote reports on data breaches in 2020. They analyzed over 150,000 cybersecurity incidents, and 500 companies that suffered breaches. We've distilled some of their insights.

Breach Causes

45% of breaches are due to a **hack**

22% of breaches are due to an **error**

22% of breaches involve **social engineering**

17% of breaches are due to **malware**

8% of breaches are abuse by an **authorized user**

4% of breaches are manipulations of **physical equipment**

The average data breach costs **$3.86 million**.

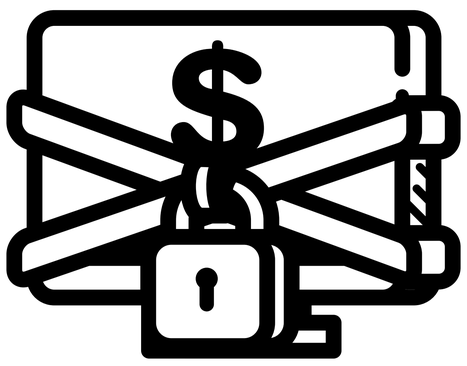
Perpetrators

70% of breaches are by **external actors**

55% of breaches are by **organized crime**

34% of breaches involve **internal actors**

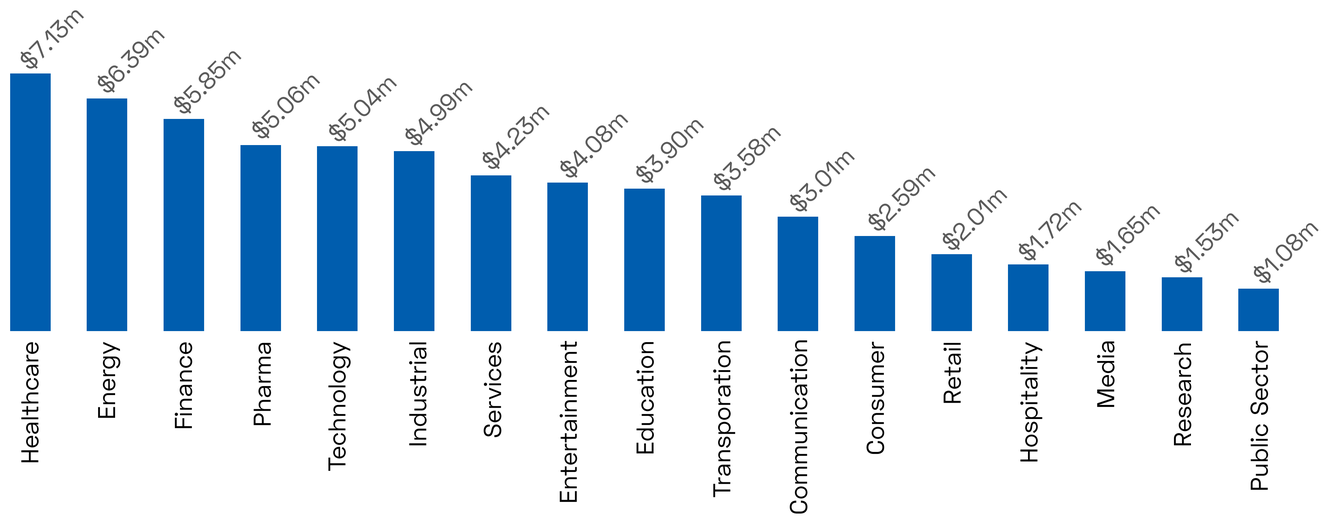
1% of breaches involve **outside partners**



Ransomware claims a new victim every **14 seconds**.

Ransoms are made to be as expensive as you can afford: some companies have paid **$15 million** to restore access to their files.

Data Breach Costs by Industry



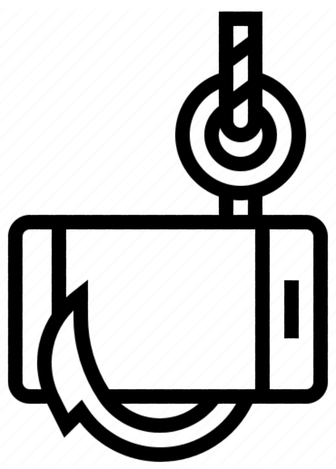
Attack Vectors

94% of malware comes via **email attachments.**

70% of malware contains **ransomware.**

48% of malicious attachments are **Microsoft Office files.**

The average employee receives at least **16 cyberattack emails** per month.



55% of employees click on links they do not recognize.

Funds Transfer Fraud

Also known as **CEO Fraud,** cybercriminals use compromised credentials or complex phishing schemes to impersonate key executives and misdirect payments.

Businesses lost **$26 Billion** to Funds Transfer Fraud just last year.

70% of employees report accidentally deleting data. Only **22%** of data is protected from such accidents.

Cybercrime cost the global economy over $600 billion this year.