

# Stack your cybersecurity knowledge—and watch attacks topple

## Key findings from Verizon's 2025 Data Breach Investigations Report

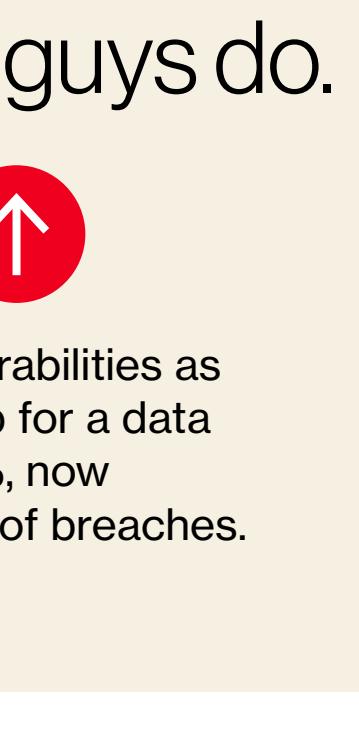
It's time to shine a light on shadow actors. In the 2025 Data Breach Investigations Report (DBIR), we decoded 12,195 data breaches across 139 countries. Here's a snapshot of our most critical findings.



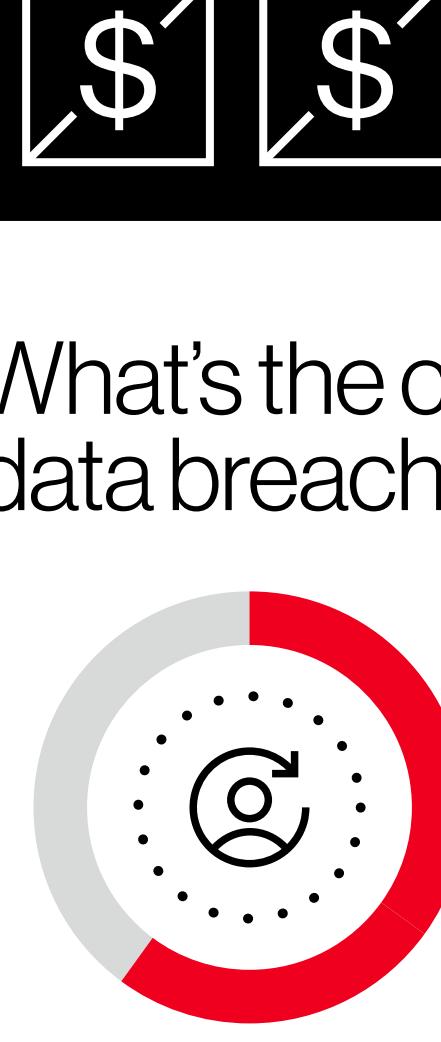
### Unwitting partner in crime?

**15% → 30%**

The percentage of breaches where a third party was involved doubled from the previous year, highlighting the importance of choosing partners and suppliers carefully.

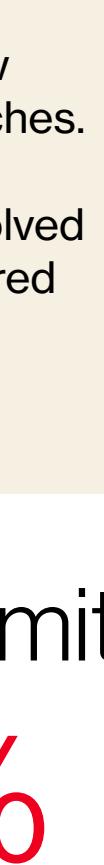


### Do you know where your weaknesses are? The bad guys do.



**34%**

Exploitation of vulnerabilities as an initial access step for a data breach grew by 34%, now accounting for 20% of breaches.



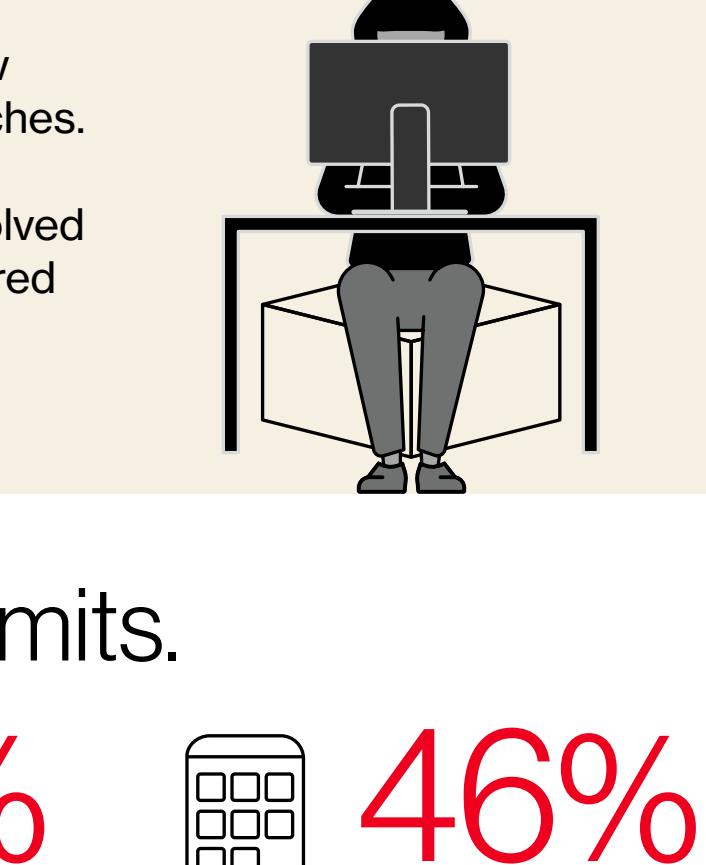
**34%**

Developing a unified cybersecurity posture with partners and suppliers can help reduce vulnerability.

### Criminals hope you will respond slowly—or stall out entirely.

**32 days**

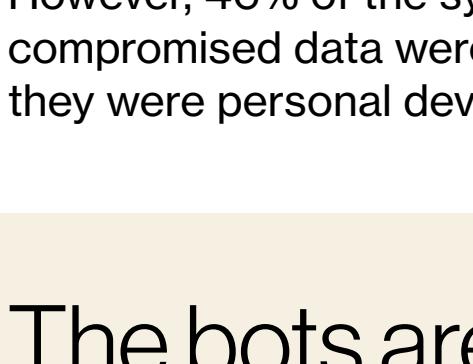
Our analysis shows only about 54% of perimeter device vulnerabilities were fully remediated, and it took a median of 32 days to do so.



### More organizations are being held hostage.

**44%**

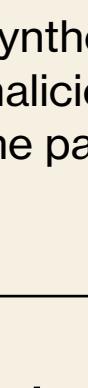
of cybersecurity breaches involved ransomware, up 37% from the previous year.



### "Pay up or else."

**\$115,000**

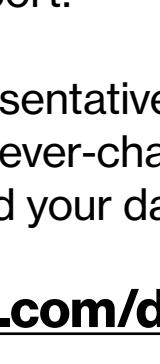
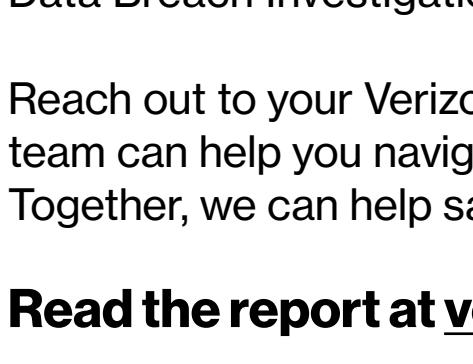
Ransomware attacks can take a costly toll on organizations. The median amount paid to ransomware groups was \$115,000.



### What's the common link in most data breaches? The human element.

**60%**

Human involvement in cybersecurity breaches remained about the same as the previous year – 60%.



Credential abuse and social actions – like phishing – were major factors in these types of breaches.

Credential abuse and social actions – like phishing – were major factors in these types of breaches.

But there's good news, too. The majority of victim organizations – 64% – did not pay the ransoms.

But there's good news, too. The majority of victim organizations – 64% – did not pay the ransoms.

### State eyes are on the dollar signs.

**28%**

Espionage-motivated attacks now account for 17% of security breaches. But espionage isn't the only thing state-sponsored actors were involved in – roughly 28% of state-sponsored incidents had a financial motive.

