



VERIZON 2024 DATA BREACH INVESTIGATIONS REPORT





The Top 4 Attack Types Compromising Organisations in 2024:



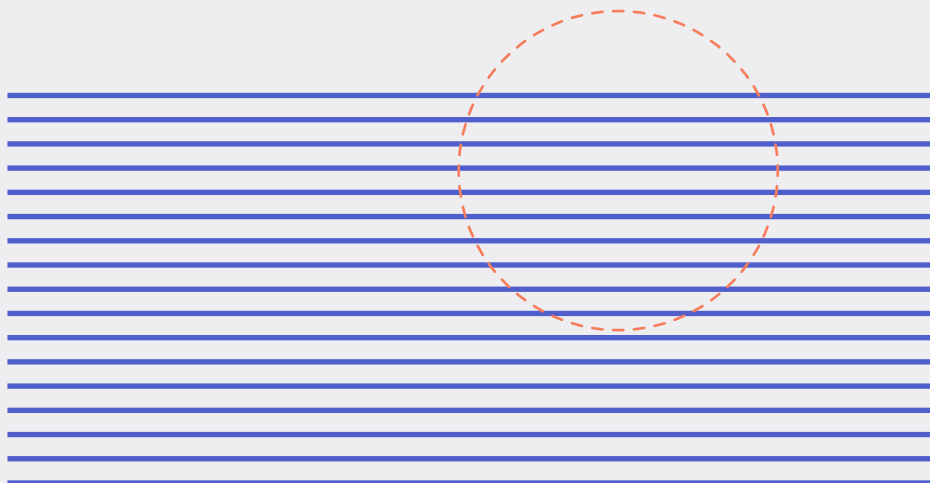


THE HUMAN ELEMENT

For this year's dataset, the human element was a component of **68%** of breaches, roughly the same as the previous period described in the 2023 DBIR.

RANSOMWARE

Ransomware (or some type of Extortion) was involved in just under a third (**32%**) of breaches, and appears in **92%** of industries as one of the top threats.



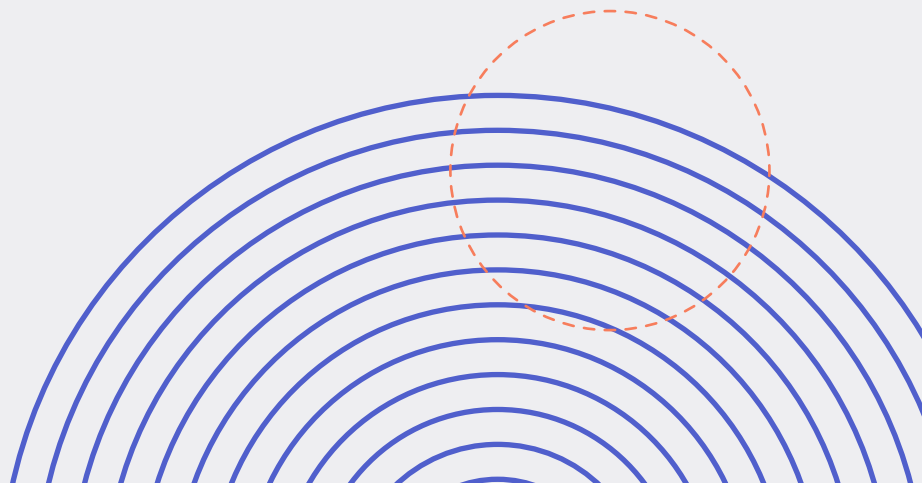


ERRORS

Breaches involving errors reached **28%**. Verizon stated: “This validates our suspicion that errors are more prevalent than media or traditional incident response-driven bias would lead us to believe”.

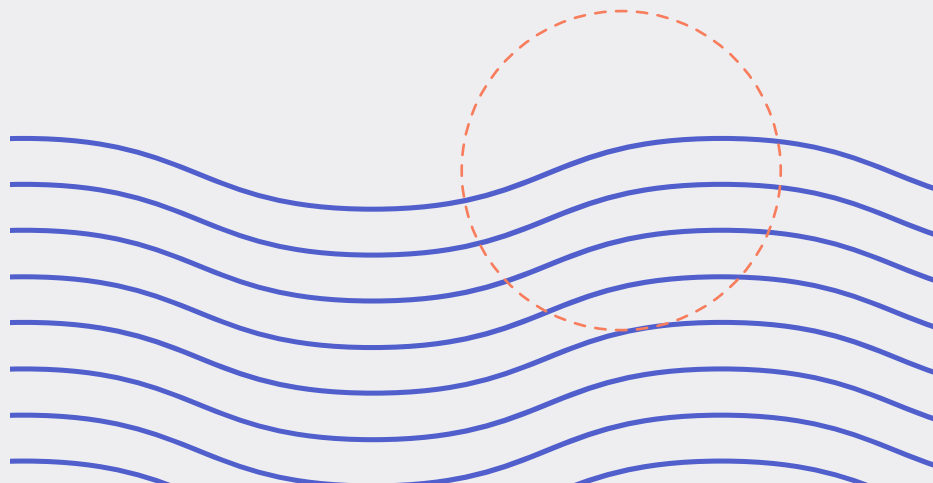
SUPPLY CHAIN

The report includes a calculated supply chain interconnection influence in **15%** of the breaches, a significant increase from **9%** in 2023.





Location Matters: How Your Region Influences Data Breach Patterns





NORTH AMERICA

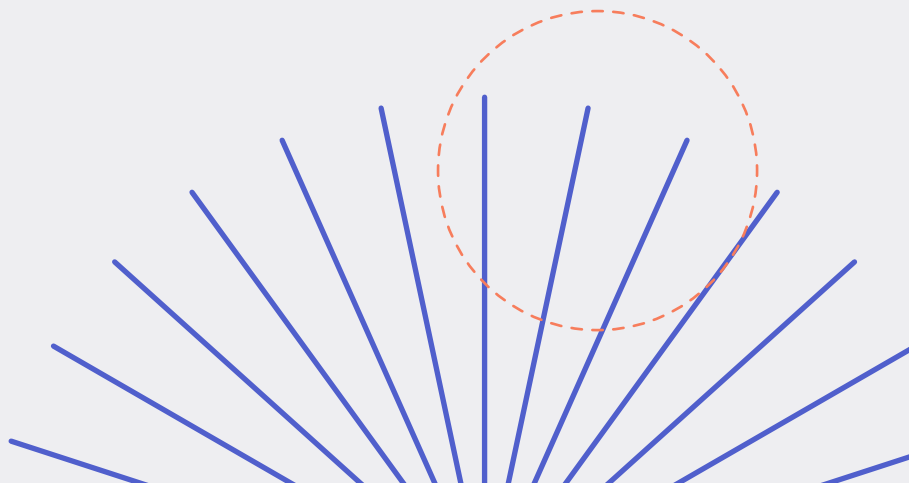
North America sees **97%** of cyber attacks being financially motivated, but this is a decrease from last year's **99%**. Espionage increased from **1%** to **4%**. Personal data was the most compromised this year at **50%**, and credential compromise decreased dramatically from **67%** in 2023 to **26%** in 2024.

MOTIVES

Financial **97%**, Espionage **4%**

TYPE OF DATA COMPROMISED

Personal **50%**, Credentials **26%**,
Internal **19%**, Other **16%**





EMEA

94% of actor motives were financial compared to **91%** in the 2023 report and **79%** in the 2022 report. Miscellaneous errors, system intrusion and social engineering represent **87%** of overall breaches. Internal threats were significantly higher in EMEA than other regions, making up **49%** of incidents as opposed to **2%** in APAC and **8%** in NA, aligning with the prevalence of social engineering attacks.

MOTIVES

Financial **94%**, Espionage **6%**

TYPE OF DATA COMPROMISED

Personal **64%**, Other **36%**,
Internal **33%**, Credentials **20%**





APAC

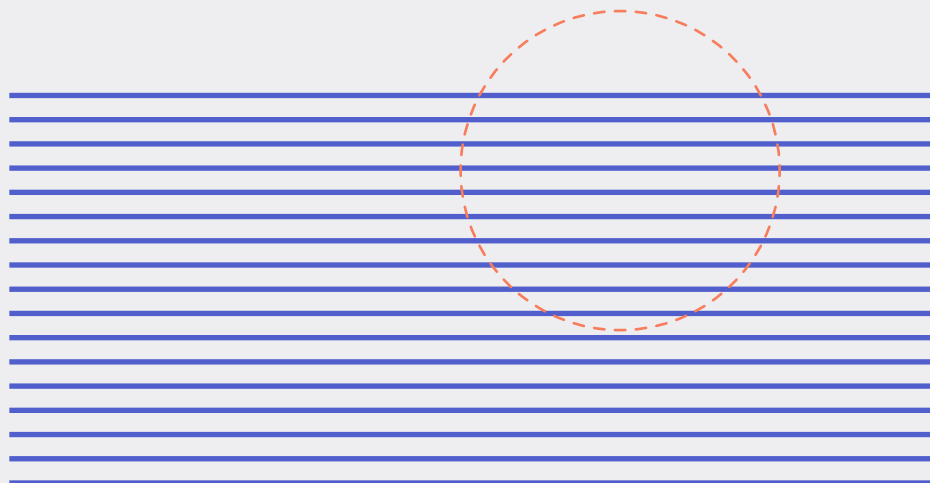
System intrusion, social engineering and basic web application attacks represent **95%** of APAC breaches. Espionage has decreased as a motive for attackers, going from **39%** to **25%**, but remains significantly higher than EMEA (**6%**) and North America (**4%**). Credentials make up a whopping **69%** of compromised data in APAC.

MOTIVES

Financial **75%**, Espionage **25%**

TYPE OF DATA COMPROMISED

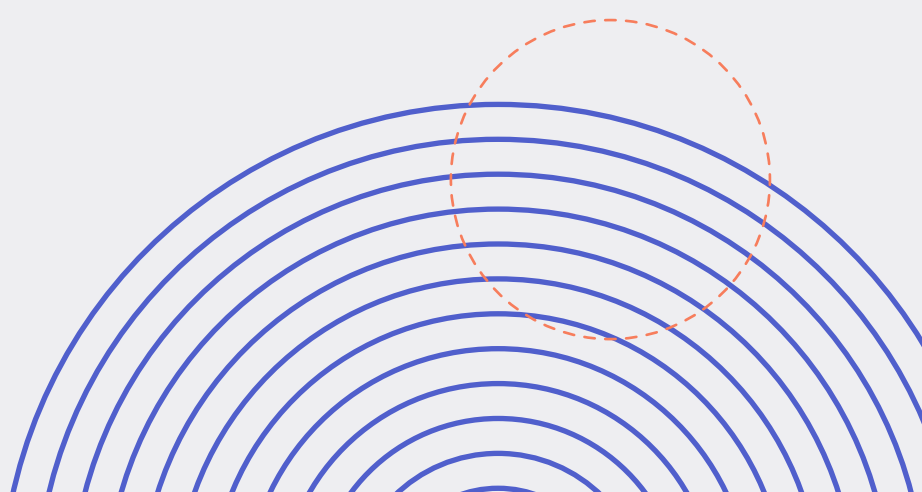
Credentials **69%**, Internal **37%**,
Secrets **24%**, Other **17%**





RISK MANAGEMENT


A robust risk management methodology helps organisations gain full oversight of their risk profile. Undertaking regular risk assessments at a schedule that aligns with a risk's severity ensures existing risks are assessed and updated, while new risks are identified and treated.





SECURITY AWARENESS — TRAINING AND EDUCATION

Ensure that staff, stakeholders and interested parties, including your suppliers, have the appropriate training and knowledge at their disposal to detect and report cyber threats. By doing so, your organisation can identify and mitigate potential incidents and reduce the risk of breaches.



**If you enjoyed this content,
please like, share and
follow for more!**

 **isms**.online

