isms.online

CYBERSECURITY AWARENESS MONTH

Verizon 2022 Data Breach Investigations Report

What are the main attack types compromising organisations in 2022

HUMAN ERROR

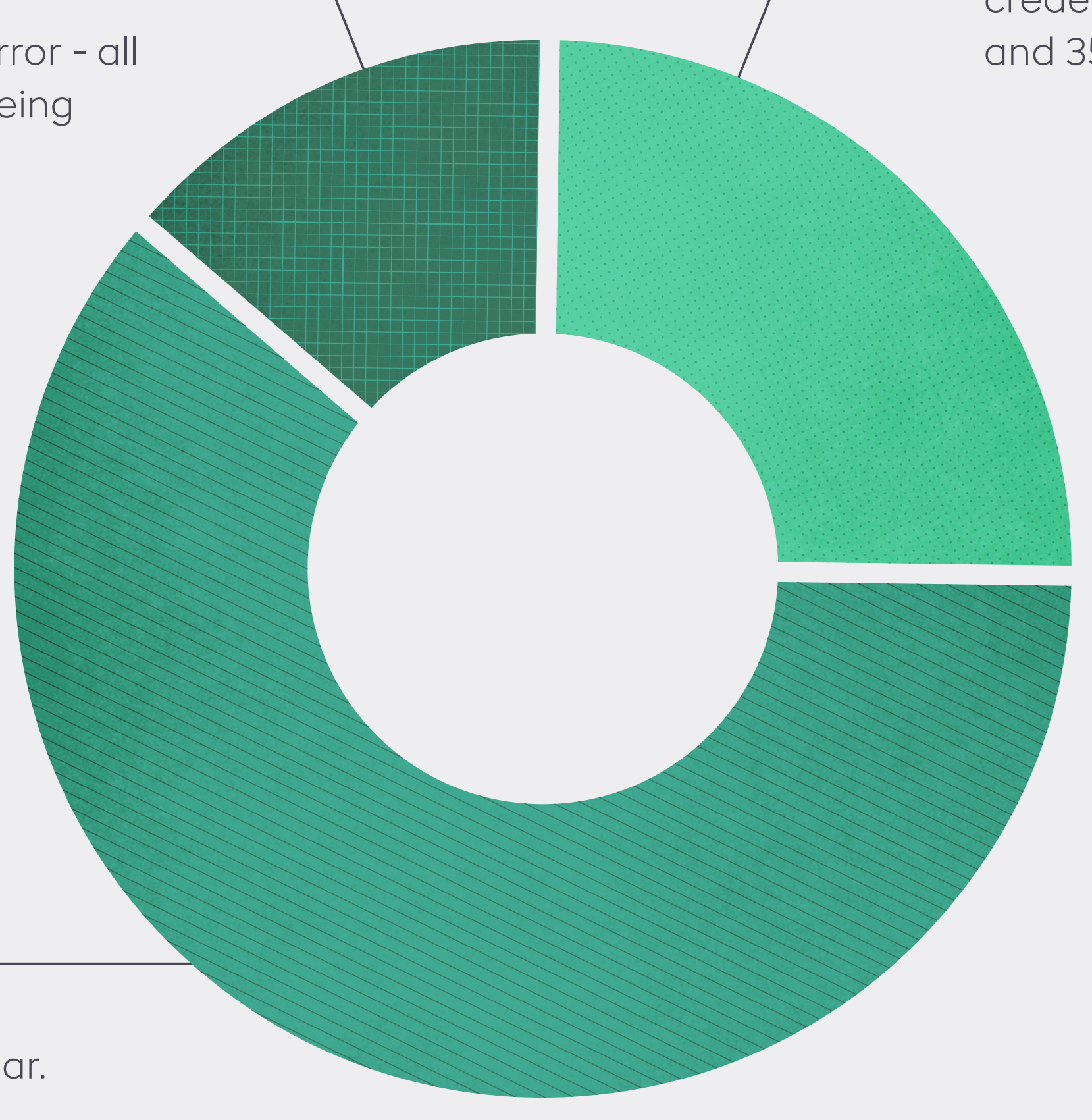
In the last year, 14% of breaches were because of human error.

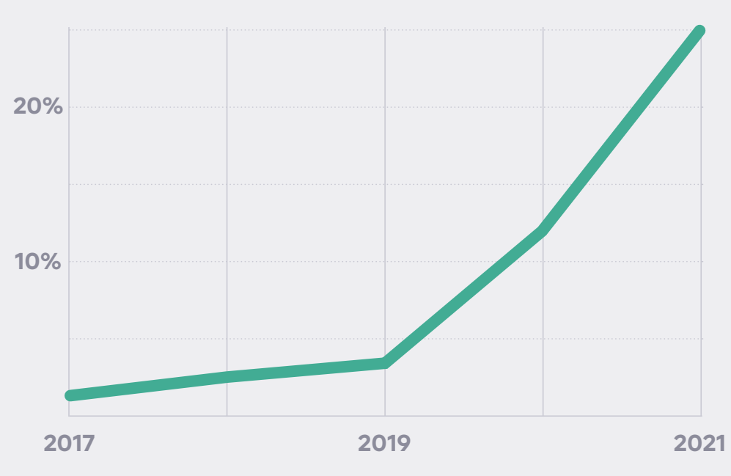
82% of breaches involved stolen credentials, phishing attacks, access misuse or simply an error - all coming back to the human being compromised to gain access.

RANSOMWARE

25% of breaches came from ransomware.

Looking at the pathways in for these ransomware attacks, 40% involve stolen credentials via desktop sharing software and 35% used email compromise.



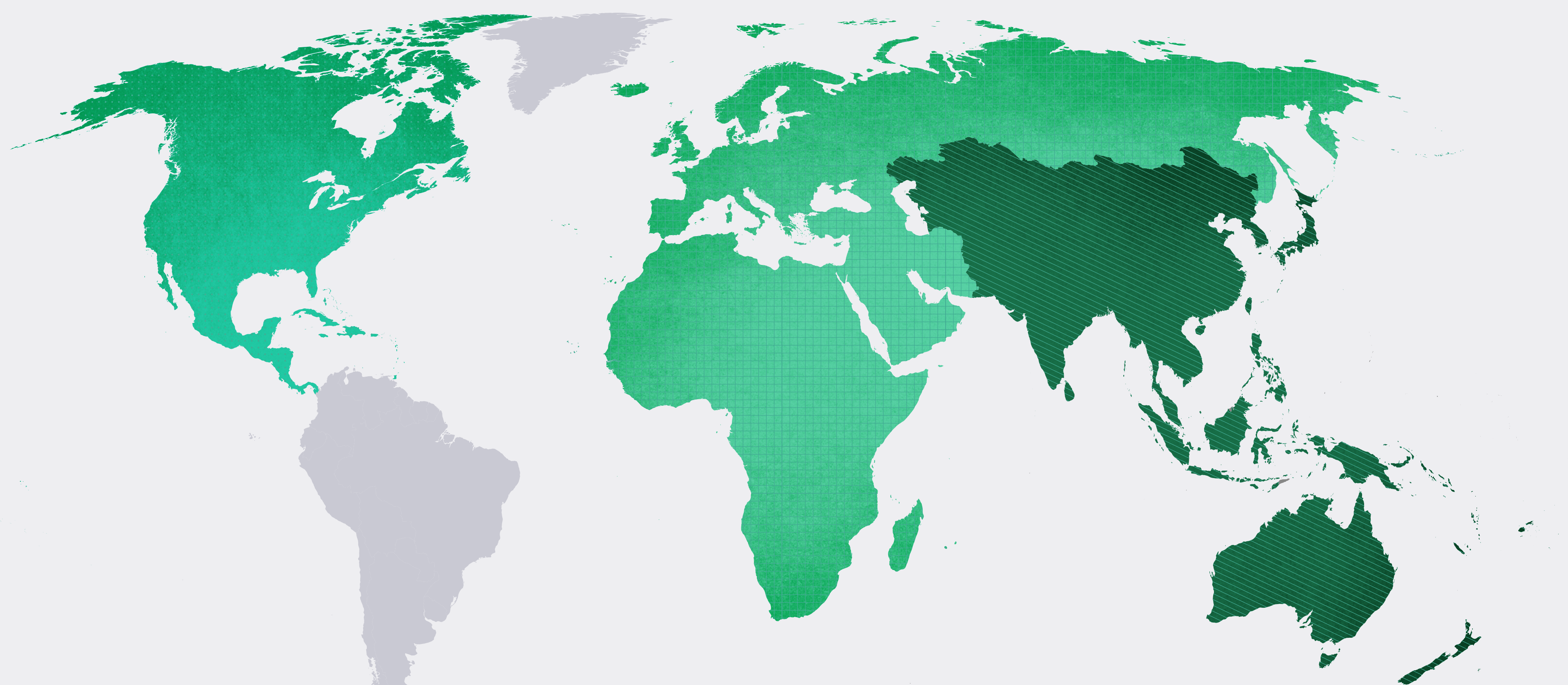


RANSOMWARE HAS HAD A 13% YEAR-ON-YEAR INCREASE – A RISE AS BIG AS THE PAST FIVE YEARS COMBINED

SUPPLY CHAIN

Supply chain was involved in 61% of cyber incidents this year.

Data breach patterns: where you are influences the attack methods used



NORTH AMERICA

North America sees almost 96% of cyber attacks being financially motivated; attackers know the value of data and brand reputation for organisations, therefore, how lucrative a breach can be.

The last year has seen system and network intrusion surpass social engineering attacks as the dominant attack pattern. However, there also remains a significant problem with social actions such as phishing and business email compromise

EMEA

The EMEA region sees highly financially motivated attacks, with 79% of attackers looking to monetise their activities.

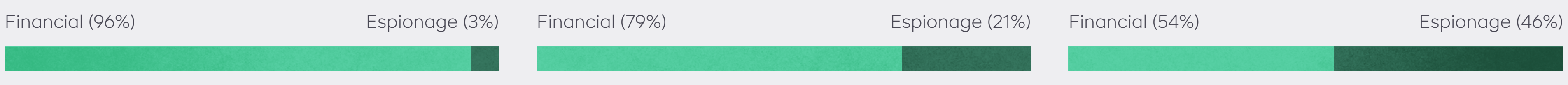
The most popular attack vector, social engineering, illustrates the need for controls to detect this type of attack quickly. Credential theft remains a significant problem, with basic web application attacks seemingly pervasive in the EMEA region.

APAC

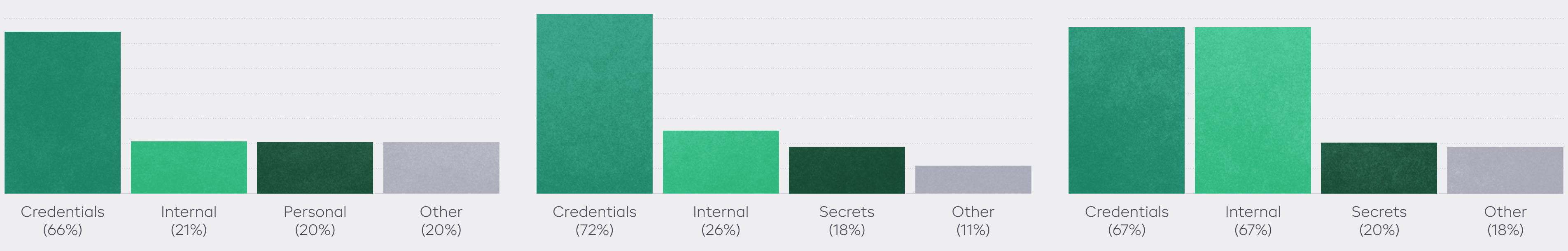
APAC experiences many social media and hacking-related attacks but has a much lower number of ransomware cases than other areas.

These attacks are driven primarily by financial motives (54%), but espionage comes a very close second (46%).

MOTIVES



TYPE OF DATA COMPROMISED



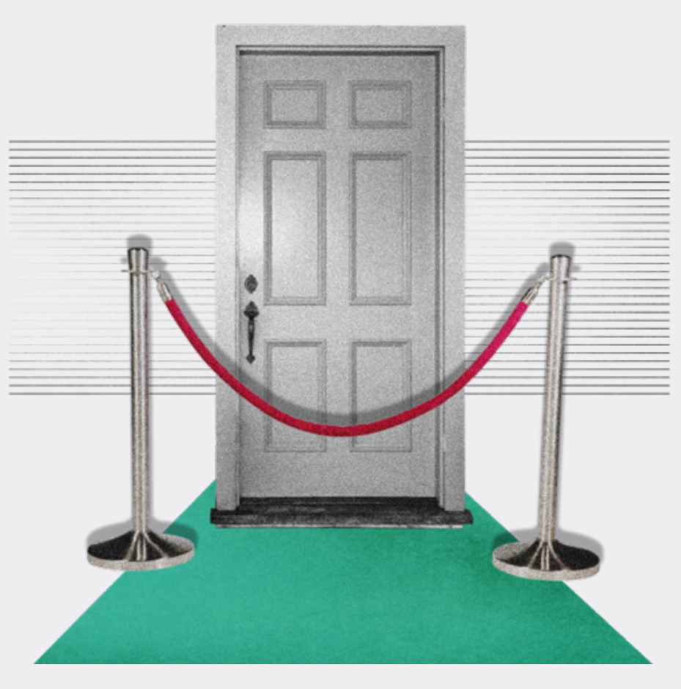
How can organisations defend against data breaches

DATA PROTECTION

Appropriate processes and technical controls to identify, classify and securely handle organisational data in all its forms are essential. Tools such as information management systems or frameworks can help organisations to prevent accidentally exposing their data through email, misconfigurations, and poor security behaviours.

SECURITY AWARENESS TRAINING PROGRAM

A classic and one that hopefully does not require a great deal of explanation. With human error and social engineering two of the most significant attack vectors being leveraged in the last 12 months, ensuring your people have the training, systems and knowledge to detect and respond to cyber threats means organisations can more meaningfully defend themselves.



ACCESS MANAGEMENT

Effective management of the rights and privileges of users and the use of controls such as multi-factor authentication can be a critical defence against the use of stolen credentials and unauthorised access.

SECURE CONFIGURATION

Where possible, organisations should focus on engineering solutions that are secure from the outset, as opposed to tacking them on later. This approach offers substantial benefits in reducing error-based breaches such as misconfiguration.

isms.online