CyberSafe BY THE

INSIDER THREATS

WHAT ARE INSIDER THREATS, AND WHY DO THEY HAPPEN?

INSIDER threats are cybersecurity risks that originate from inside an organization.

- Employees
- Partners
- Contractors

EXTERNAL threats originate from sources that are not affiliated with a business.

- Organized crime
- Cybercriminals
- Nation-state–sponsored hackers

HUMAN ERROR, INCLUDING MISUSE AND SUSCEPTIBILITY TO SOCIAL ENGINEERING, CONTRIBUTED TO 74% OF DATA BREACHES IN 2023. *Verizon 2023 DBIR*

THERE ARE TWO KINDS OF INSIDER THREATS:

PURPOSEFUL AND ACCIDENTAL

***Purposeful** insider threats originate from people working alone or with a third party to harm a company for personal or financial gain.*

Employee retaliation: Disgruntled insiders who harm a company due to a personal grudge.

Data exfiltration: Unauthorized copying or transferring of sensitive data by an insider.

Cybercrime conspirators: Insiders who steal data or intellectual property from a company to sell to hackers or other malicious actors.

***Accidental** insider threats result from negligent insiders who inadvertently allow security risks.*

Careless staff: Insiders who disregard cybersecurity protocols out of convenience or lack of consideration.

Compromised accounts: Oblivious insiders with access to sensitive information whose credentials have been stolen by malicious actors.

Social engineering victims: Insiders who have been manipulated into unknowingly sharing information, downloading malware, or otherwise acting against a company's interests.

Reyes Holdings · REYES · MB · REYES Coca-Cola Bottling