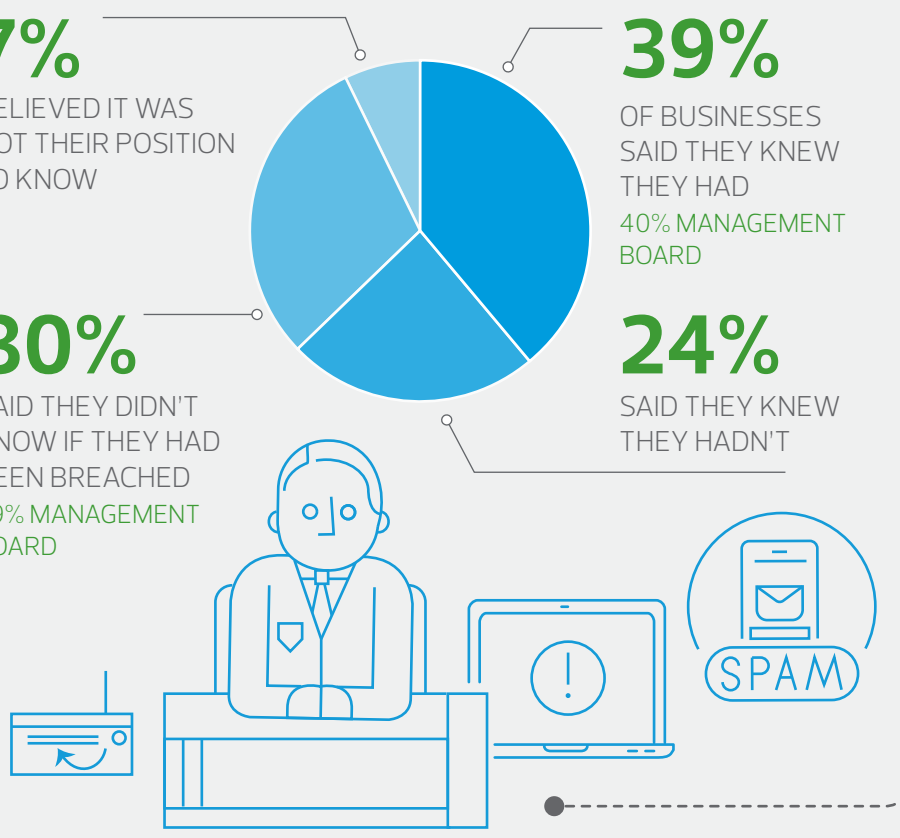
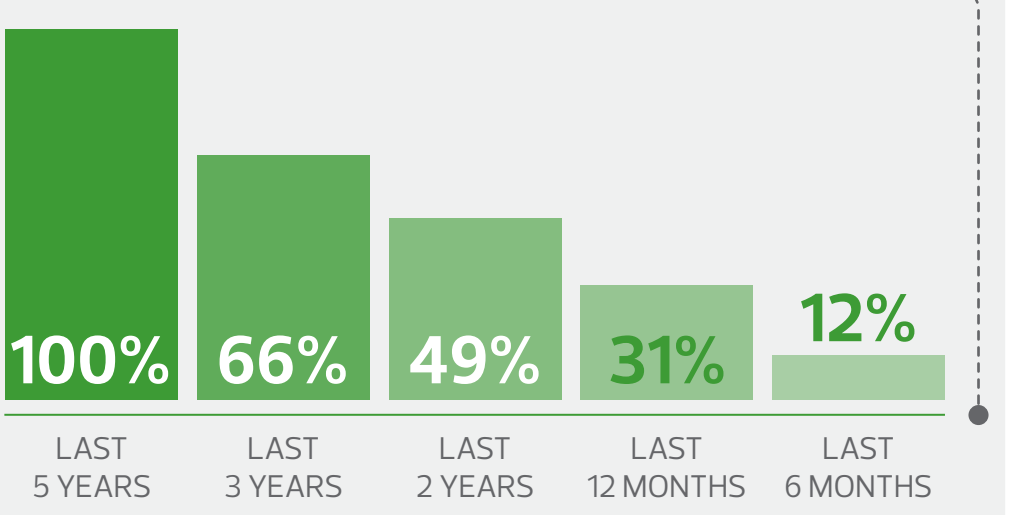
REPORTING CYBERCRIME
TO INCREASE AWARNESS AND FIND SOLUTIONS

RSM

When directly asked if they knew if their company has ever had a **security breach**:



Details of the businesses admitting a breach. The breach took place in:

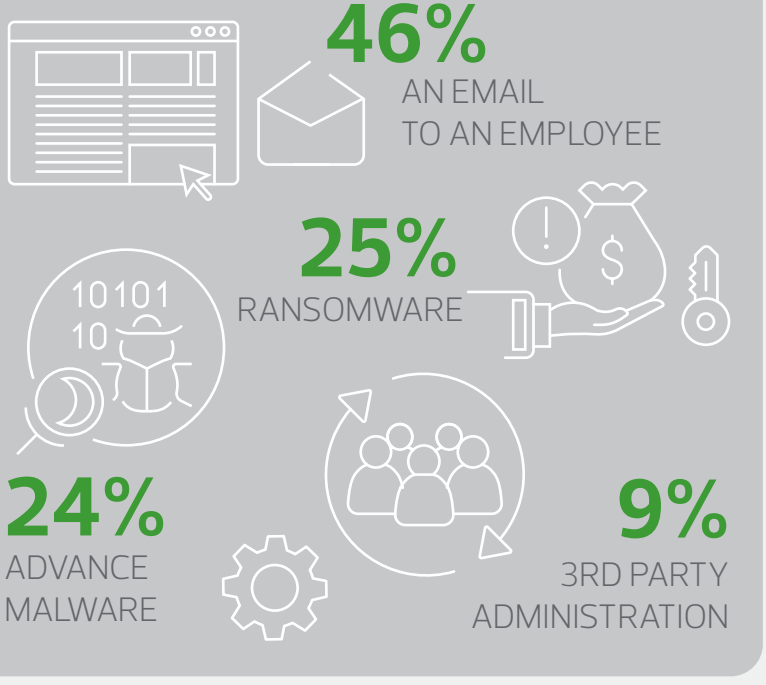


77% of the breaches were identified by an internal member of staff

9% come from the hacker (ransom demand)

7% were alerted by an external client or customer

CYBERCRIMINAL GAINED ACCESS THROUGH:



In **50%** of cases the company was made aware of the breach within the **first 2 hours** of the attack, **28%** were alerted **within 24 hours**, **9%** within **less than a week** and **3% in 1–2 weeks**

THE KEY IMPACT

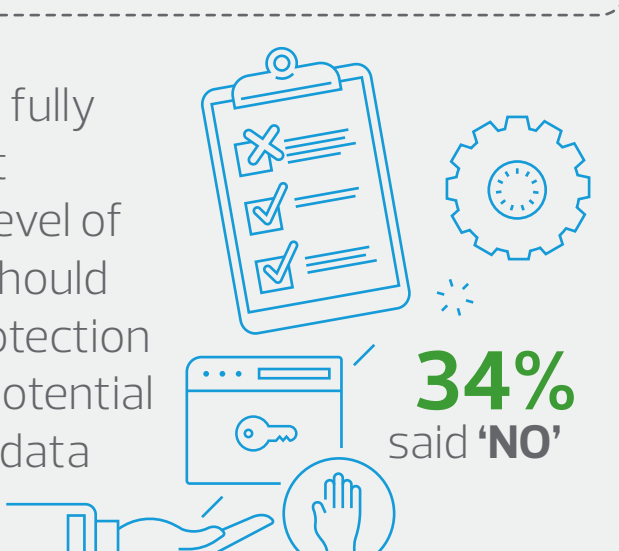
54% data loss/leakage or system damage

19% didn't know

In **75%** of the businesses the breach **DID NOT** become **public knowledge** (in only **19%** of businesses **it did**)

In **10%** of businesses, cybersecurity did not become more of a priority for senior management even after the breach

When asked if they fully understood in what circumstances, or level of data breach, they should inform the Data Protection Authority when a potential breach of personal data has been detected



34% said **'NO'**

SHORT TERM RESPONSE OF BUSINESSES:

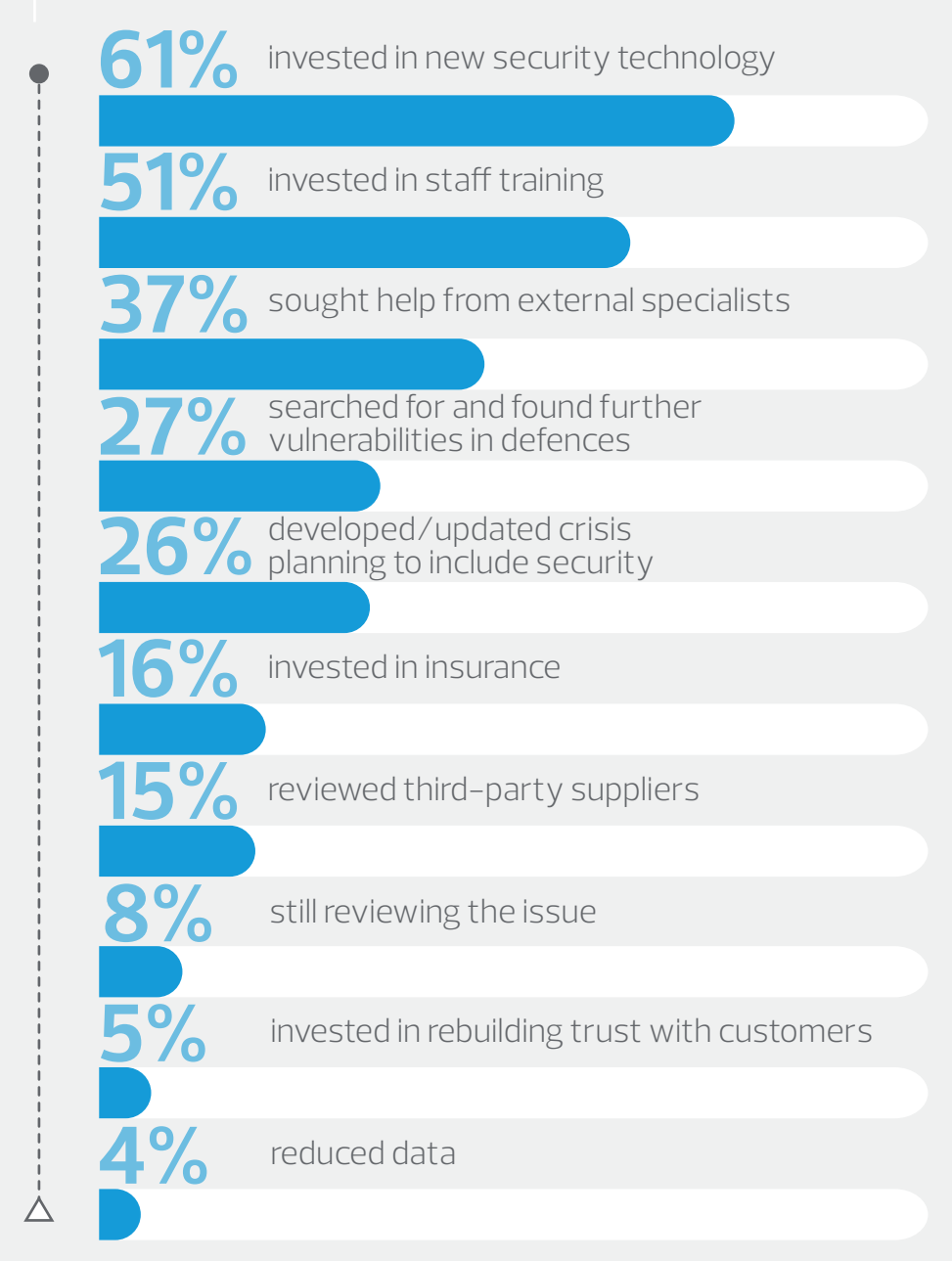
23% INFORMED THE REGULATOR

21% INFORMED CUSTOMERS

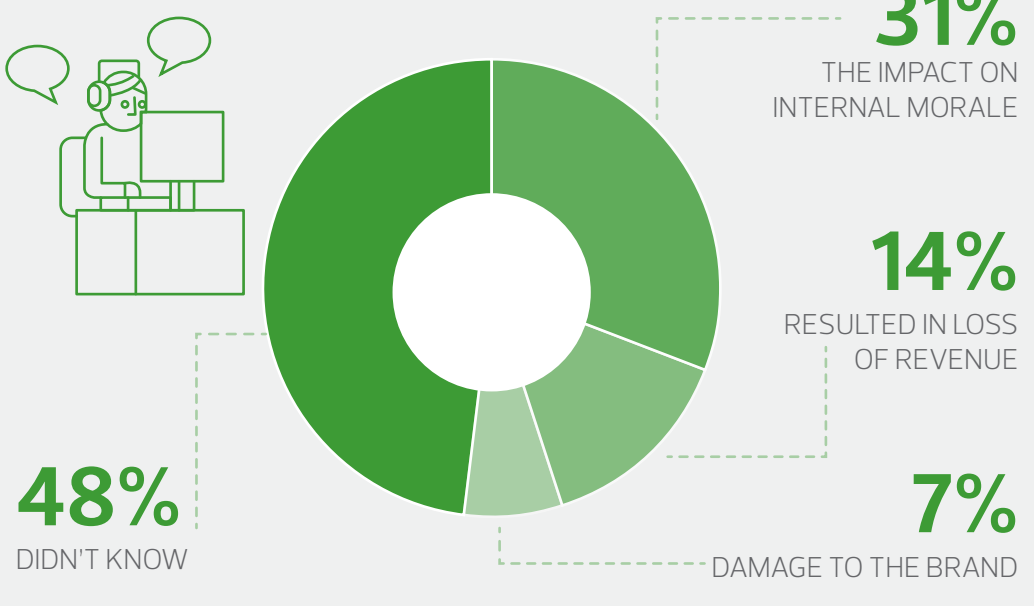
66% INTRODUCED IMMEDIATE COMMUNICATION TO STAFF

4% PAID A RANSOM

LONG TERM RESPONSE OF BUSINESSES:



THE OVERALL EFFECT OF THE DATA BREACH ON THE COMPANY



The most positive outcomes cited from the breach by businesses was an **increased awareness of threats company-wide** (**60%**) and a **necessary review of systems** (**49%**)