INTERSET

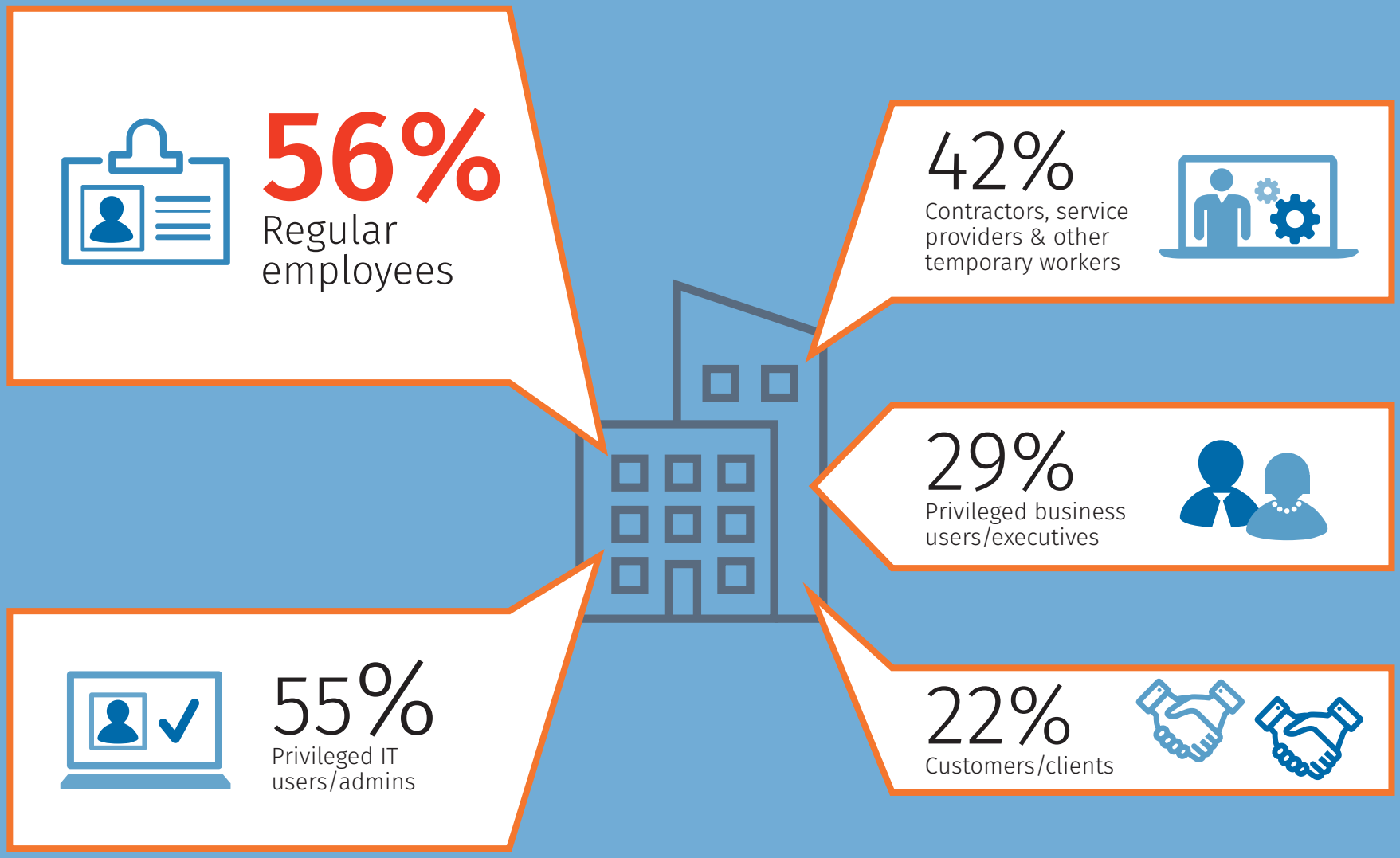
The 2018 Insider Threat Report

More than half of all enterprises have experienced an insider attack, according to new research from Cybersecurity Insiders (co-sponsored by Interset). In the study, security professionals—90% of whom admit their companies are still vulnerable to insider threats—candidly detail concerns related to these attacks, and how they plan to stop them.

Note: *Because security-team risks, challenges, and solutions are multifaceted, participants were asked to select all applicable responses. As such, survey results may not add up to 100%.*

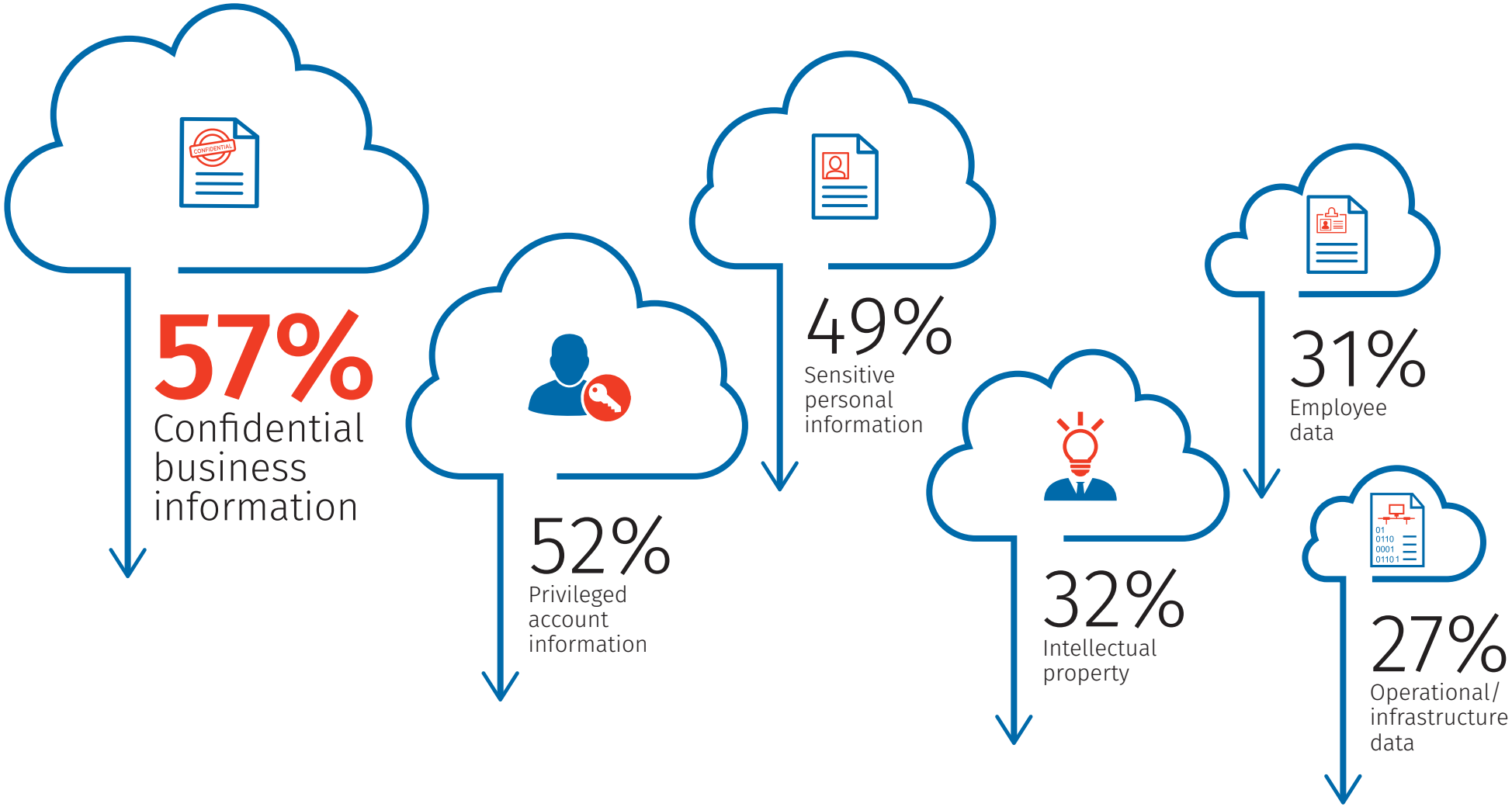
Riskiest Insiders

Which types of insiders pose security risks to organizations?



Most Vulnerable Data

Which data types are most vulnerable to insider attacks?



Infiltration Methods

What are the biggest enablers of accidental insider threats?

56%
Weak/reused passwords

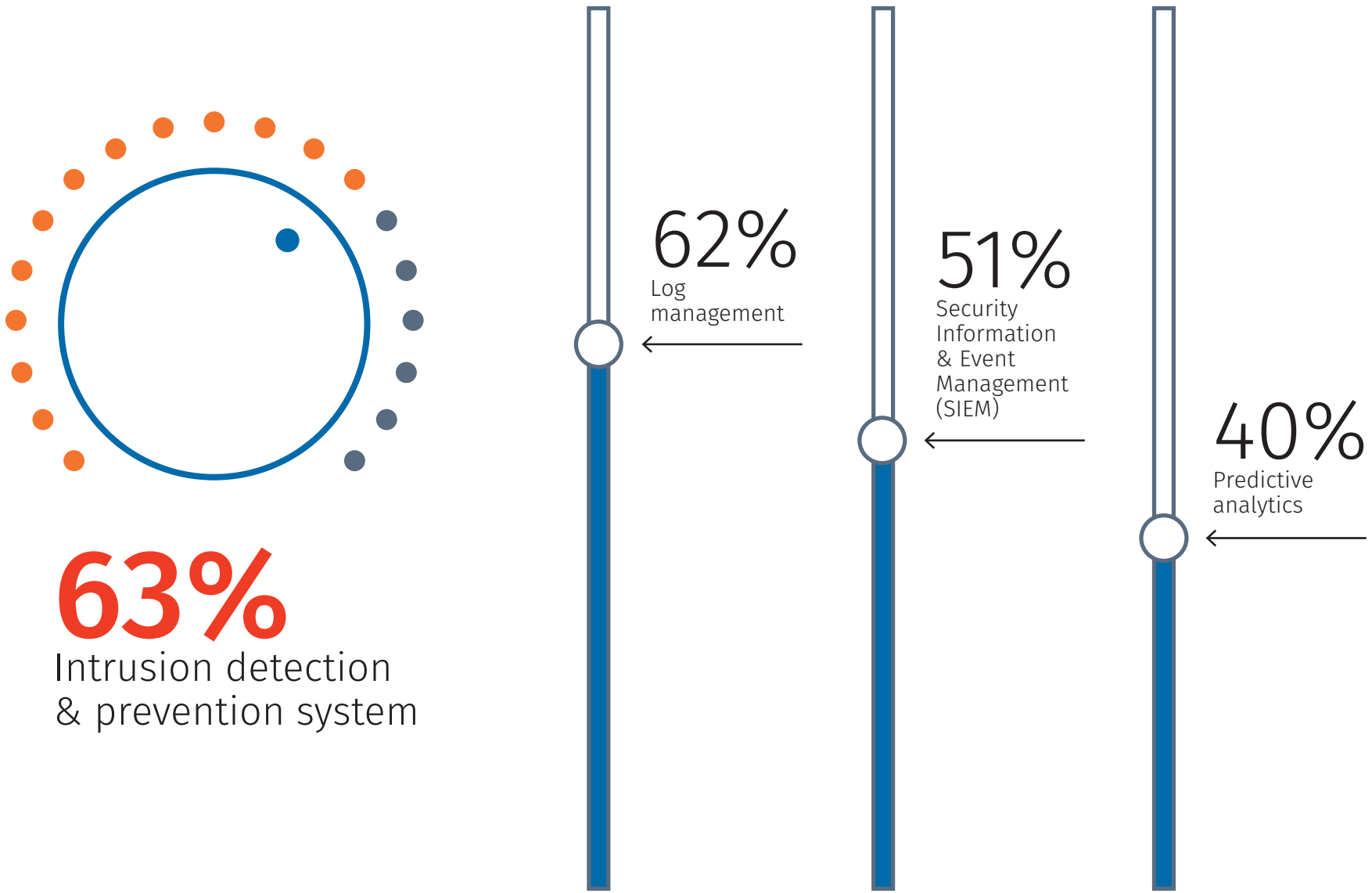
44%
Unlocked devices

44%
Bad password sharing practice

32%
Unsecured WiFi networks

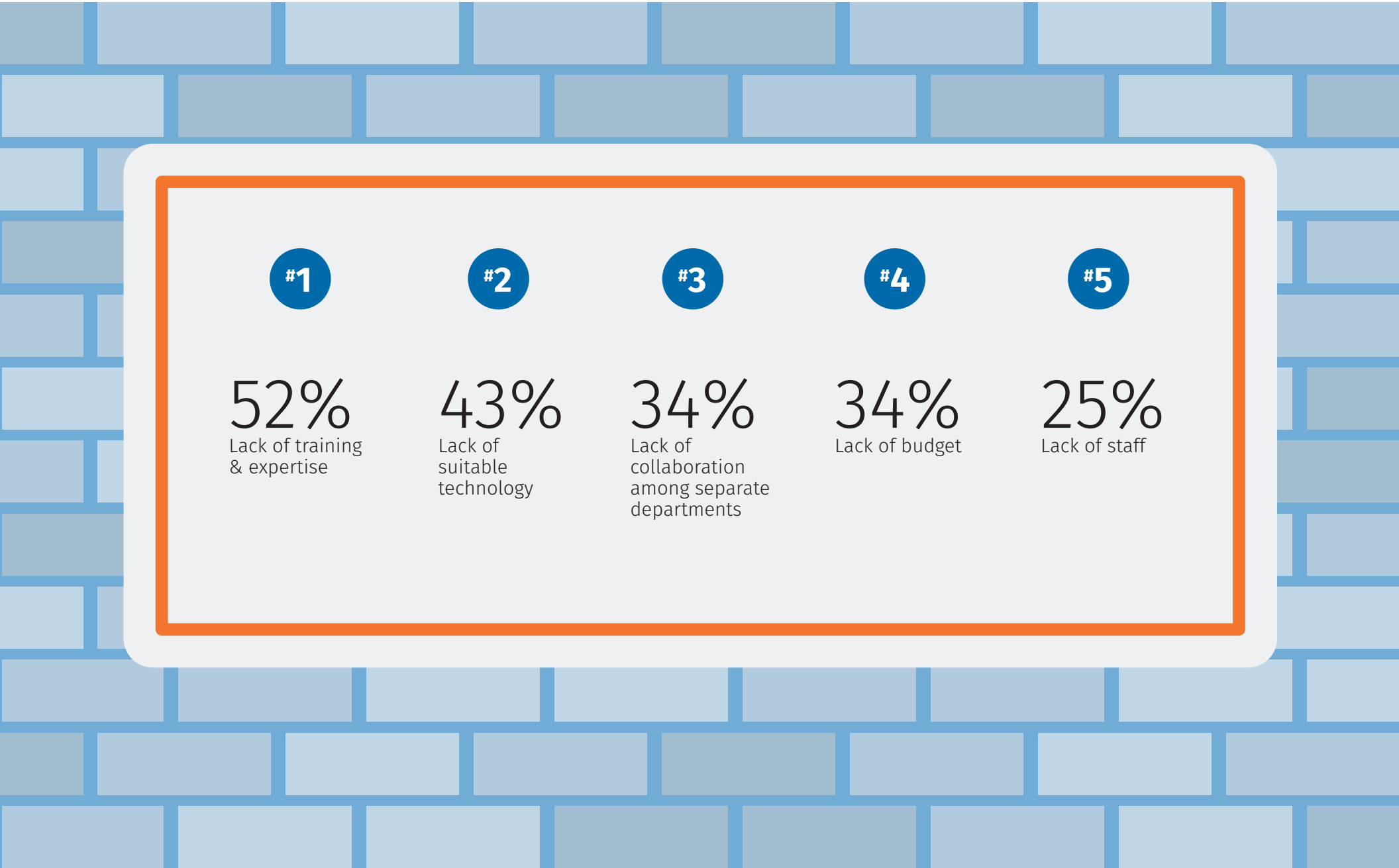
Current Cybersecurity Tools

Which controls do you have in place to detect and analyze insider attacks?



Threat Management Obstacles

What are the biggest barriers to better insider-threat management?



How to Fill the Security Gap

Do you think it's necessary to monitor and profile how insiders are accessing your sensitive data?

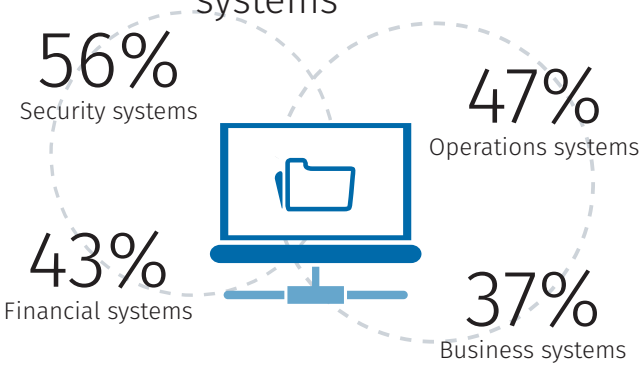
90%
Yes

3%
No

7%
Not sure

Which company information does your insider-threat detection program leverage?

75%
IT infrastructure systems



56%
Security systems

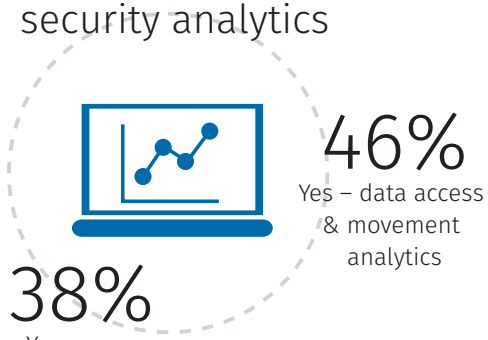
47%
Operations systems

43%
Financial systems

37%
Business systems

Does your organization leverage analytics to determine insider threats?

55%
Yes – security analytics



46%
Yes – data access & movement analytics

38%
Yes - user behavior analytics