

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?



56%
Regular employees

42%

Contractors, service providers & other temporary workers



29%

Privileged business users/executives



55%
Privileged IT users/admins

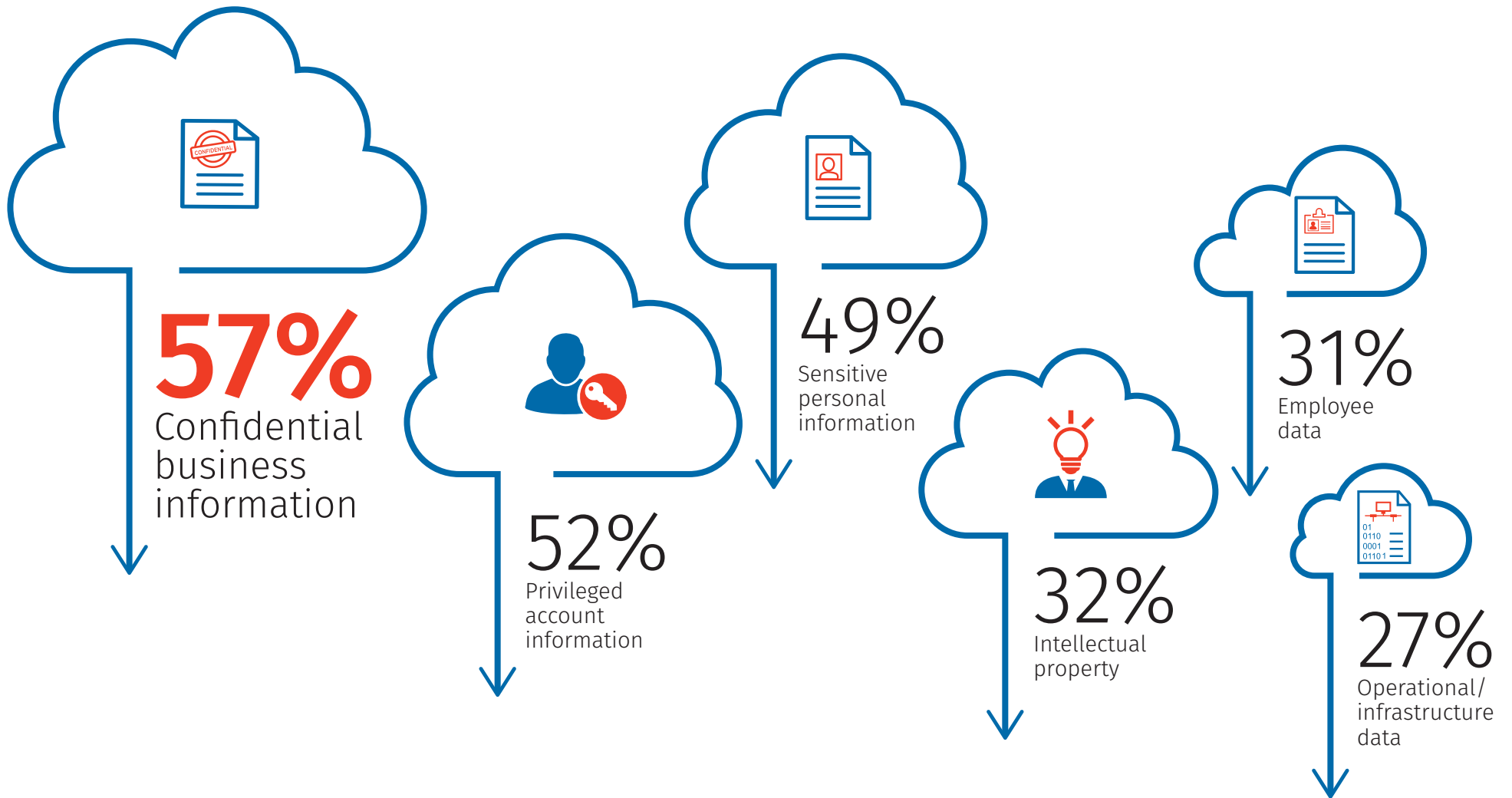
22%

Customers/clients



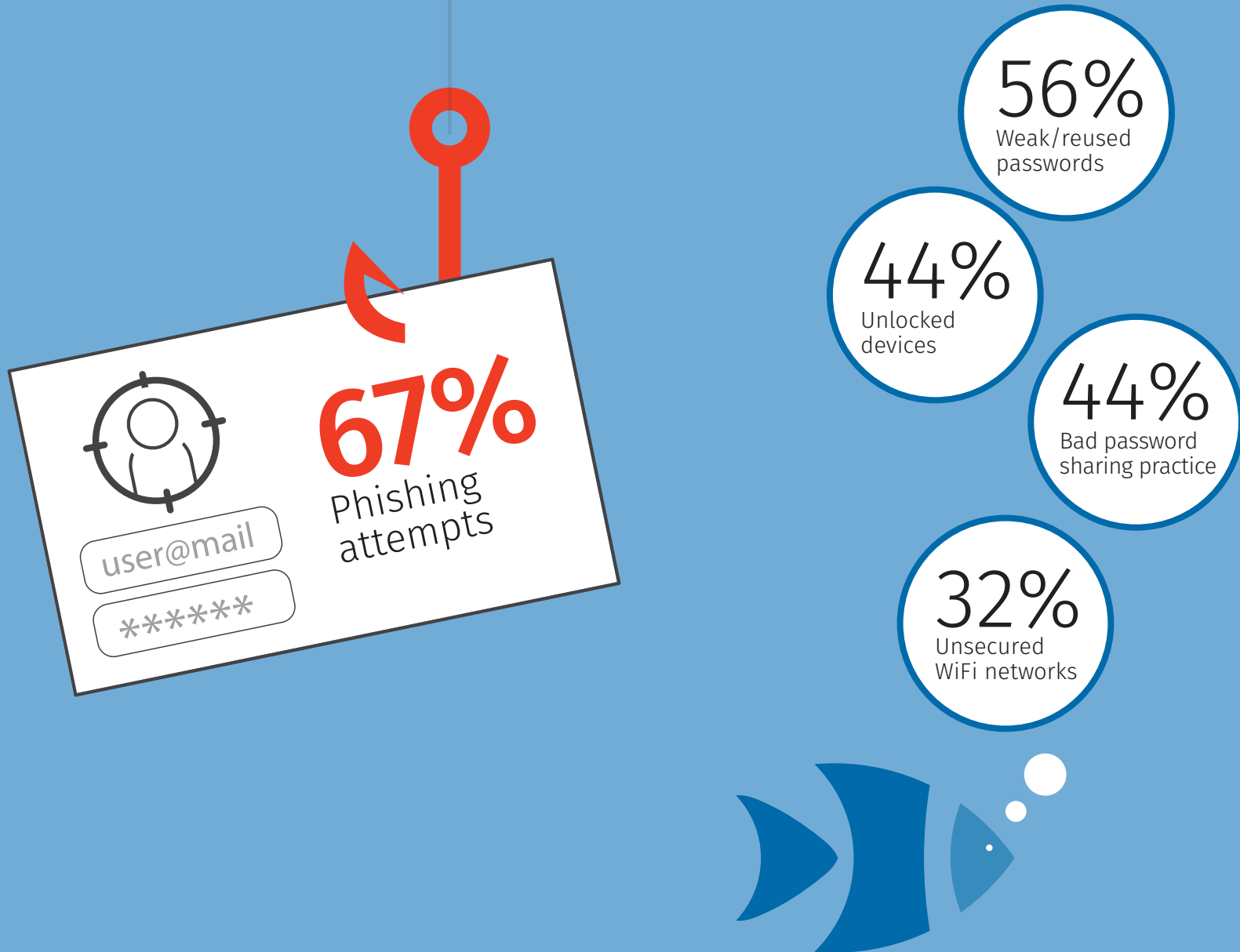
Most Vulnerable Data

Which data types are most vulnerable to insider attacks?



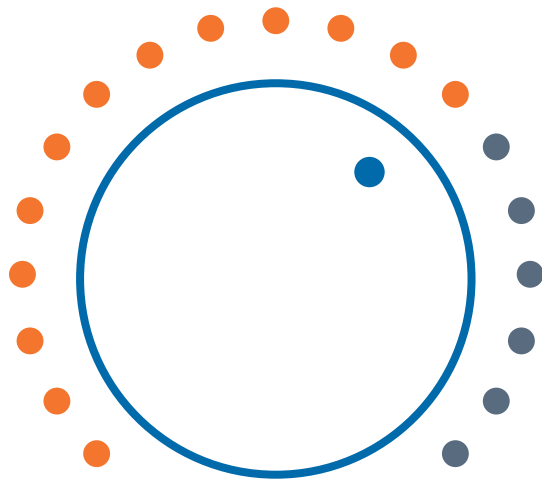
Infiltration Methods

What are the biggest enablers of accidental insider threats?



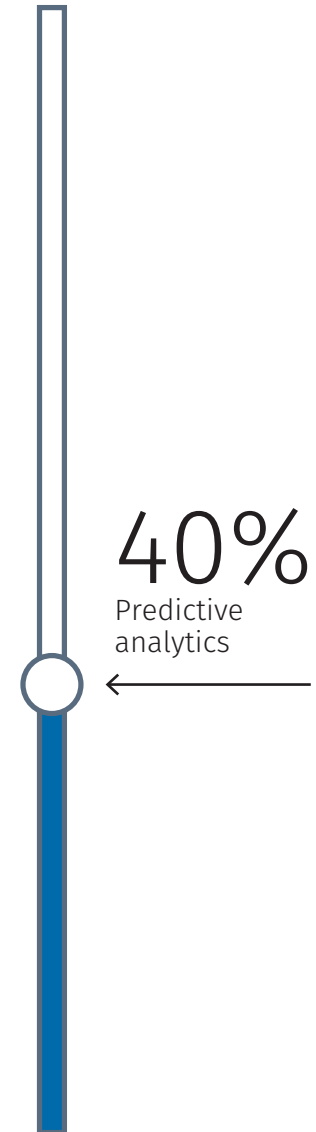
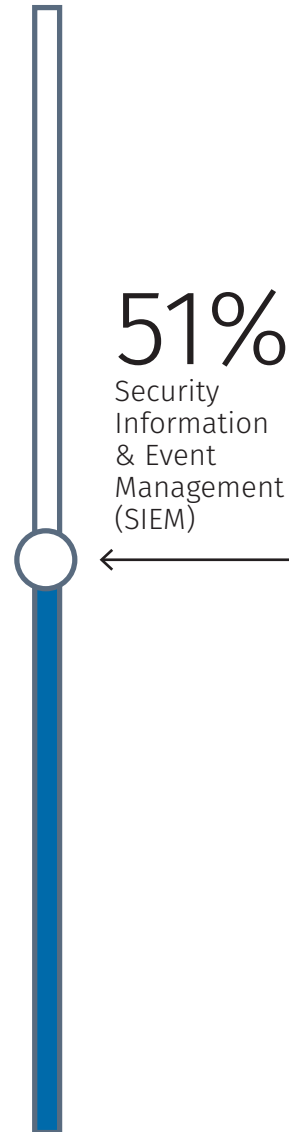
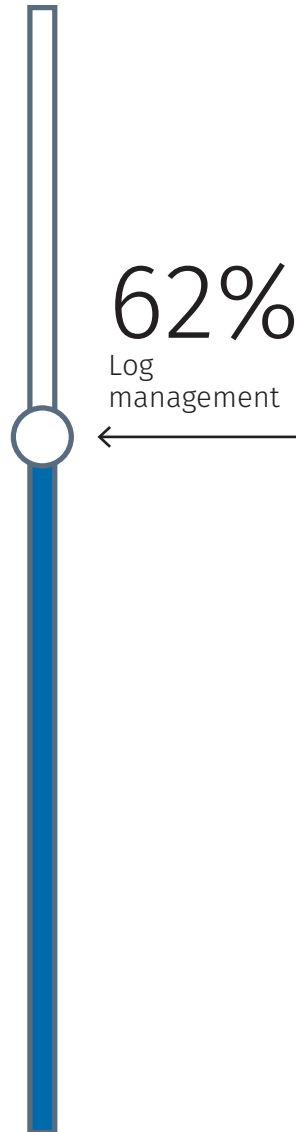
Current Cybersecurity Tools

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



63%

Intrusion detection & prevention system



Threat Management Obstacles

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

#1

52%
Lack of training
& expertise

#2

43%
Lack of
suitable
technology

#3

34%
Lack of
collaboration
among separate
departments

#4

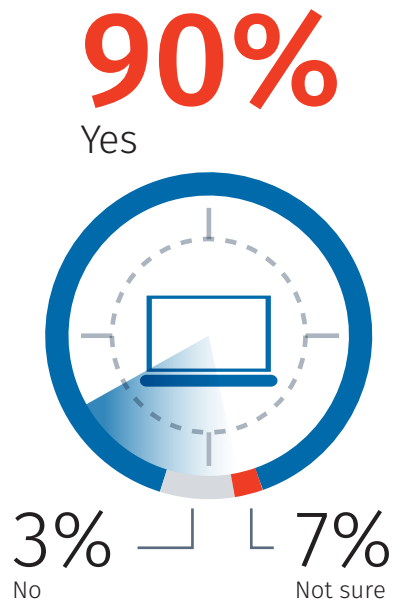
34%
Lack of budget

#5

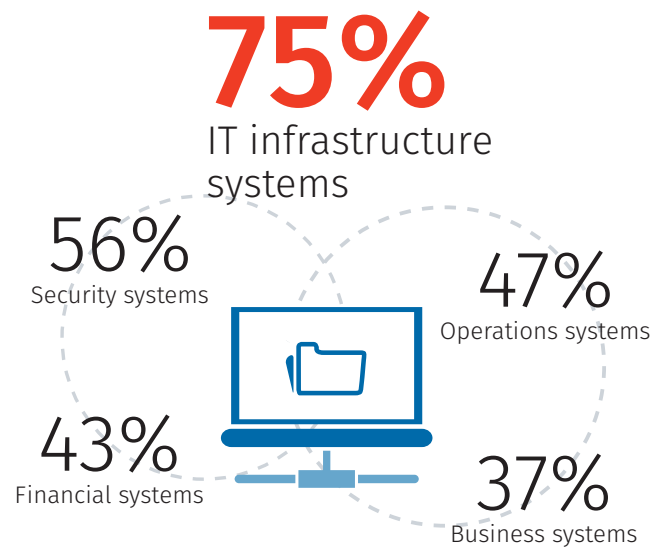
25%
Lack of staff

How to Fill the Security Gap

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



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



Does your organization leverage analytics to determine insider threats?

