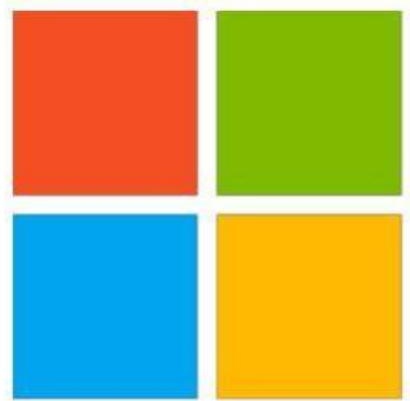


IT Security Stance of Public Sector Units

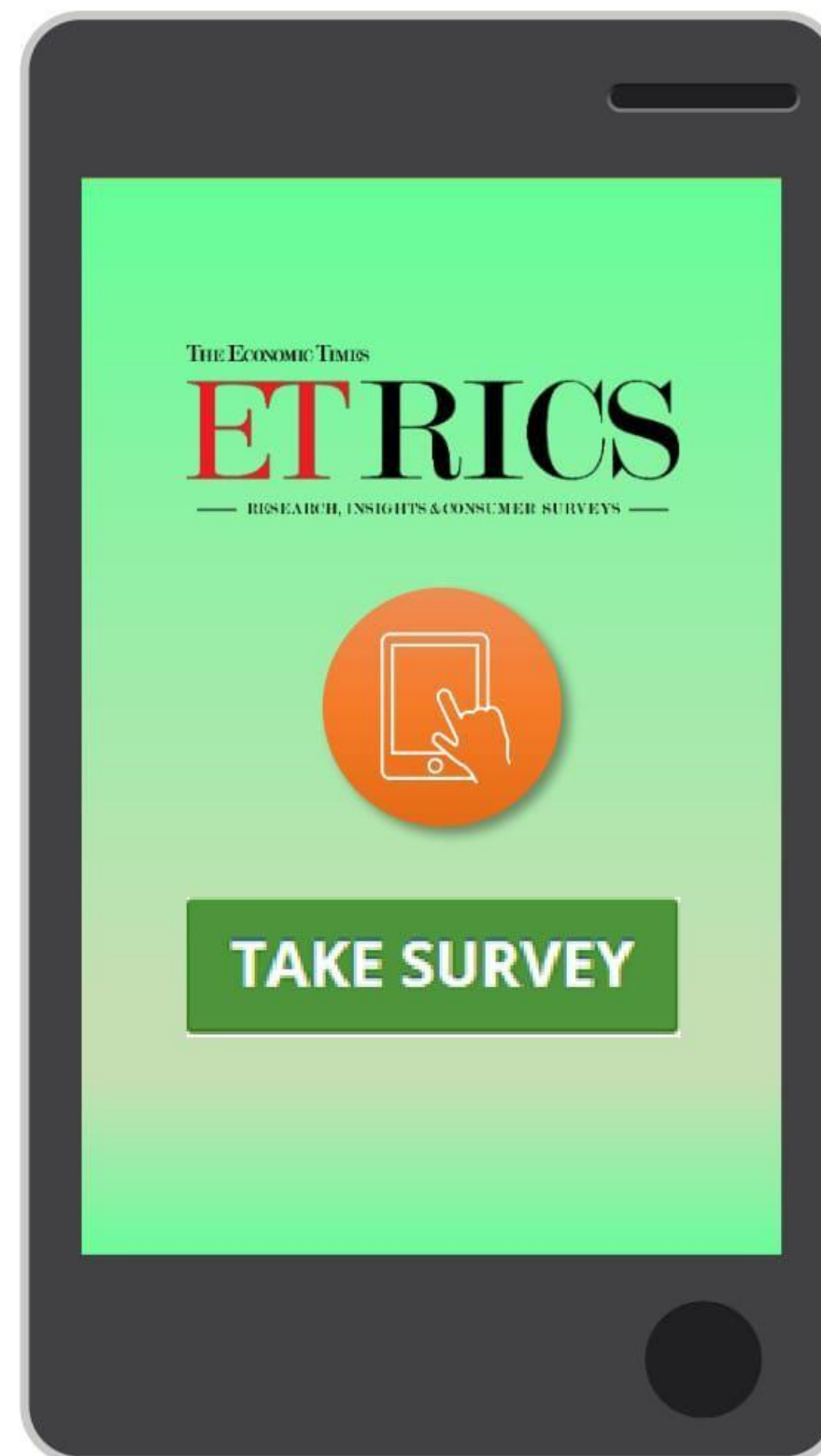


Microsoft



Analysis and Report compilation done by

- 1** The **Economic Times**' initiative on consumer research, which over time has grown into a full service consumer research entity.
- 2** **ET-RICS** now provides **customized research solutions** across almost all key sectors
- 3** **ET-RICS** is committed towards arming its clients with **superior insights** while ensuring **quick turnaround** and **high ROI**



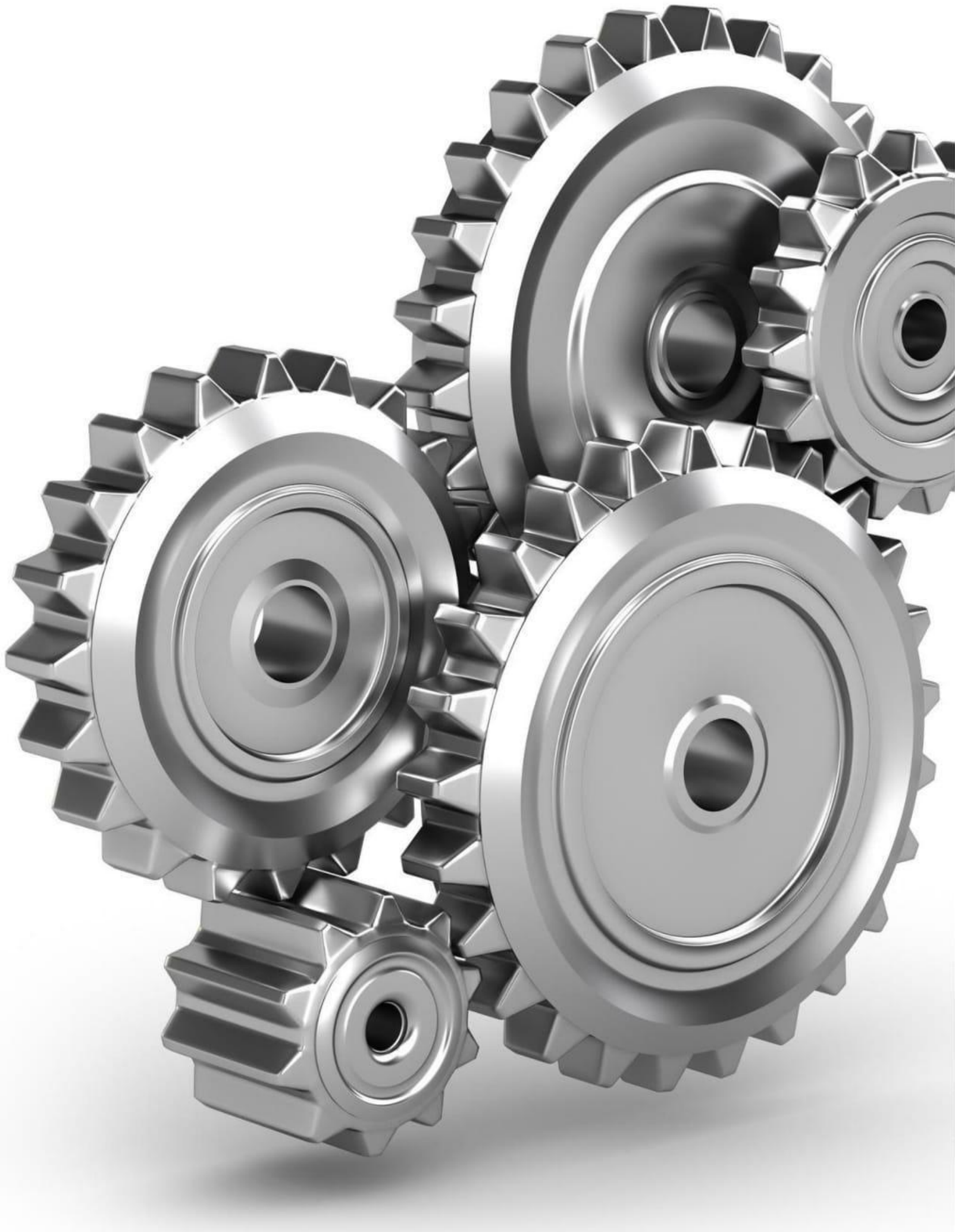
Exploratory studies / Consumer Purchase analysis

Campaign Evaluations / Brand tracks / Awareness studies

Hypothesis testing / Dipsticks / Event specific surveys

Concept / Product tests*





Objective & Methodology

- The objective behind this study was to understand the status and perception of Indian PSUs regarding IT security in their respective organizations.
- The interview questionnaire was prepared with information security experts from Microsoft.
- Responses were collected through Face-to-Face interviews with 12 PSU IT leaders.
- Survey participants: BHEL, BPCL, BSNL, HPCL, IFFCO Tokio, IFFCO, IOCL, NSE, NTPC Petronet LNG, RCF and SCI

Overview

The PSU sector has played a critical role in India's growth. The state-owned enterprises have enabled capital formation, employment generation, balanced regional development, and promotion of research and development.

However, to continue their stellar work, PSUs would have to take into account the fast-changing business environment. One of the biggest threats for businesses today is that of information security.

As technology is changing at scorching speed, hackers are becoming more persistent, turning the response to cyber security incidents an increasingly complex challenge.

Against such a scenario, **Economic Times CIO and Economic Times RICS**, in association with Microsoft, decided that it would be pertinent to explore and understand the thoughts and opinions of IT decision makers from India's top PSU on the crucial subject of information security.

The Economic Times CIO, therefore, caught up with India's top 12 PSU IT decision makers, and interviewed them one-on-one on diverse information security areas.

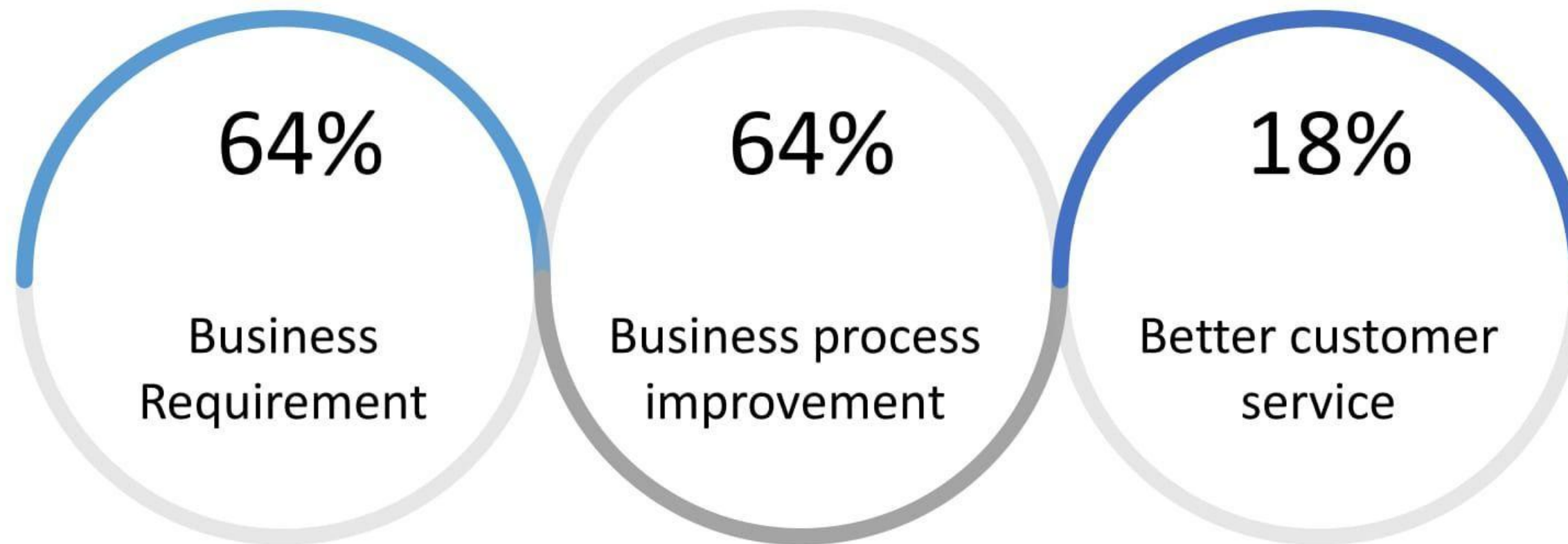
The outcome of the comprehensive discussions has been captured in this insightful report, which provides an accurate and deep understanding of the information security stance of some of India's top PSUs.



Digital Transformation Imperatives

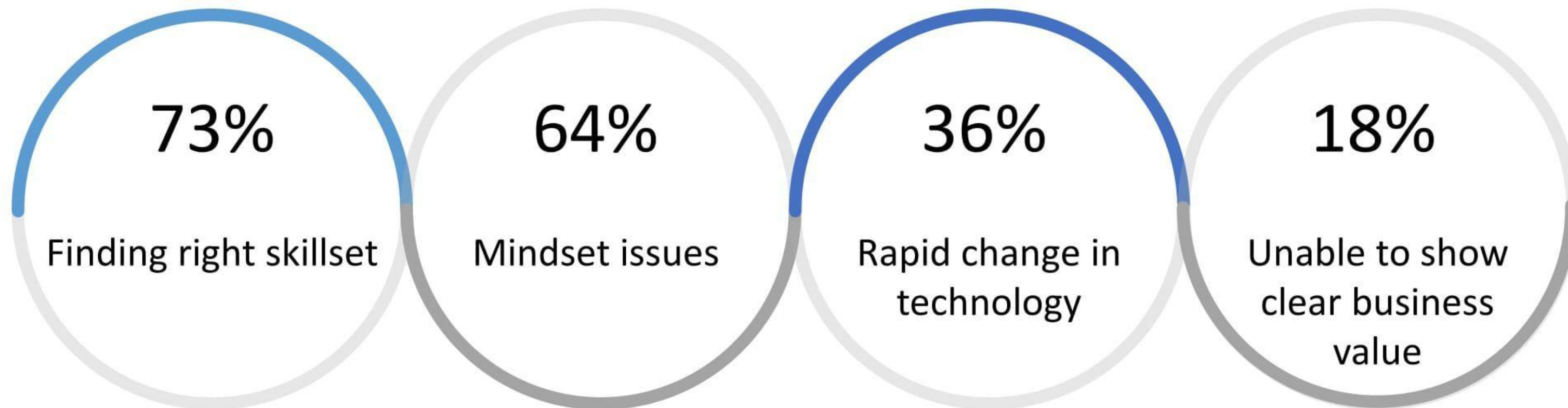
Business need, and drive to increase efficiency are key forces driving PSUs towards digitization

Key reasons for going Digital



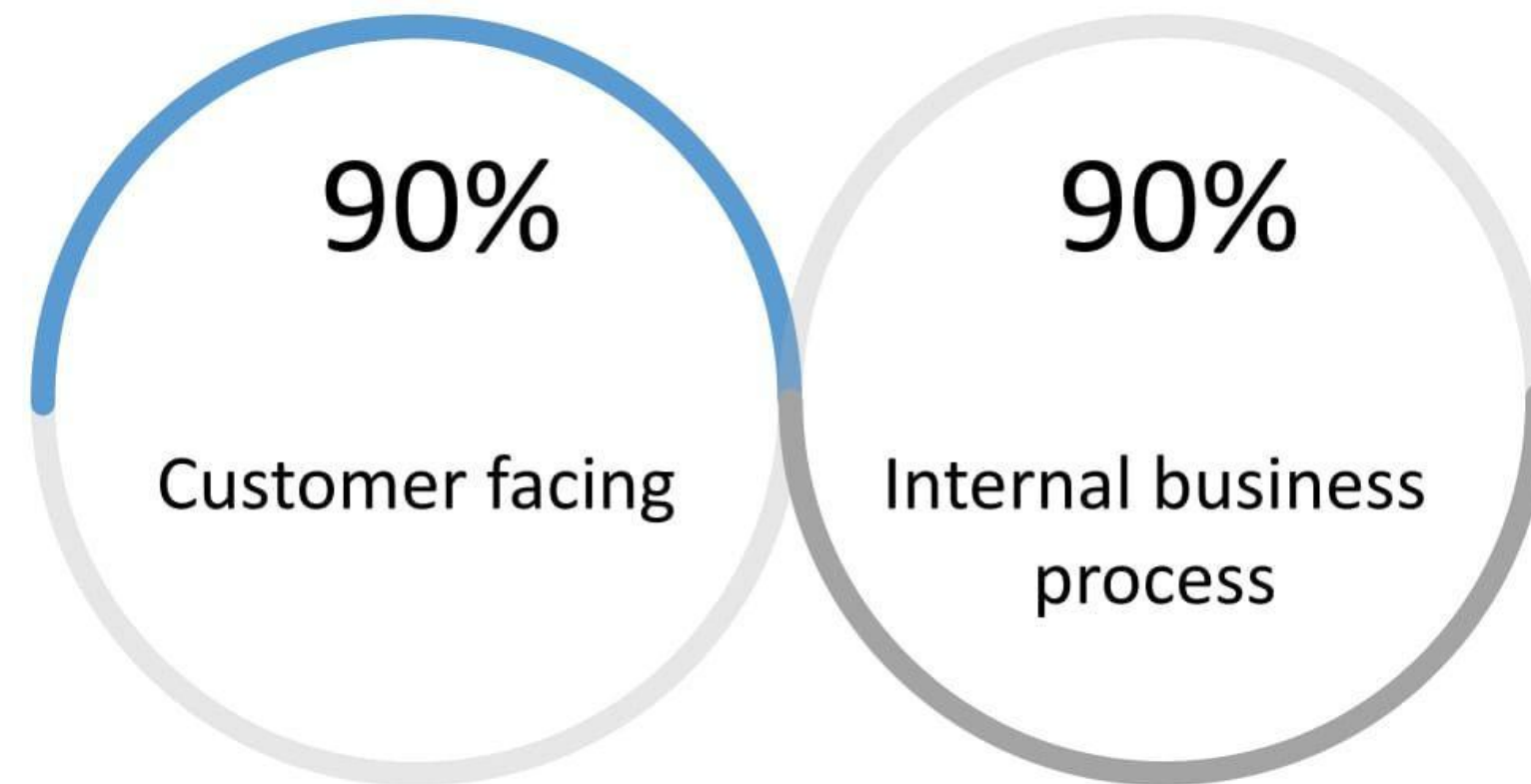
Shortage of right skill set and mindset of internal stakeholders seem to be the biggest hurdles faced by PSUs while going digital

Key challenges in going Digital



Most PSUs are planning to go for complete digitization, which would change their internal processes as well as customer interface

Areas being prioritized for digital transformation



Majority of PSUs dealing in sensitive customer transaction & customer interaction data which makes it imperative for them to focus on data security

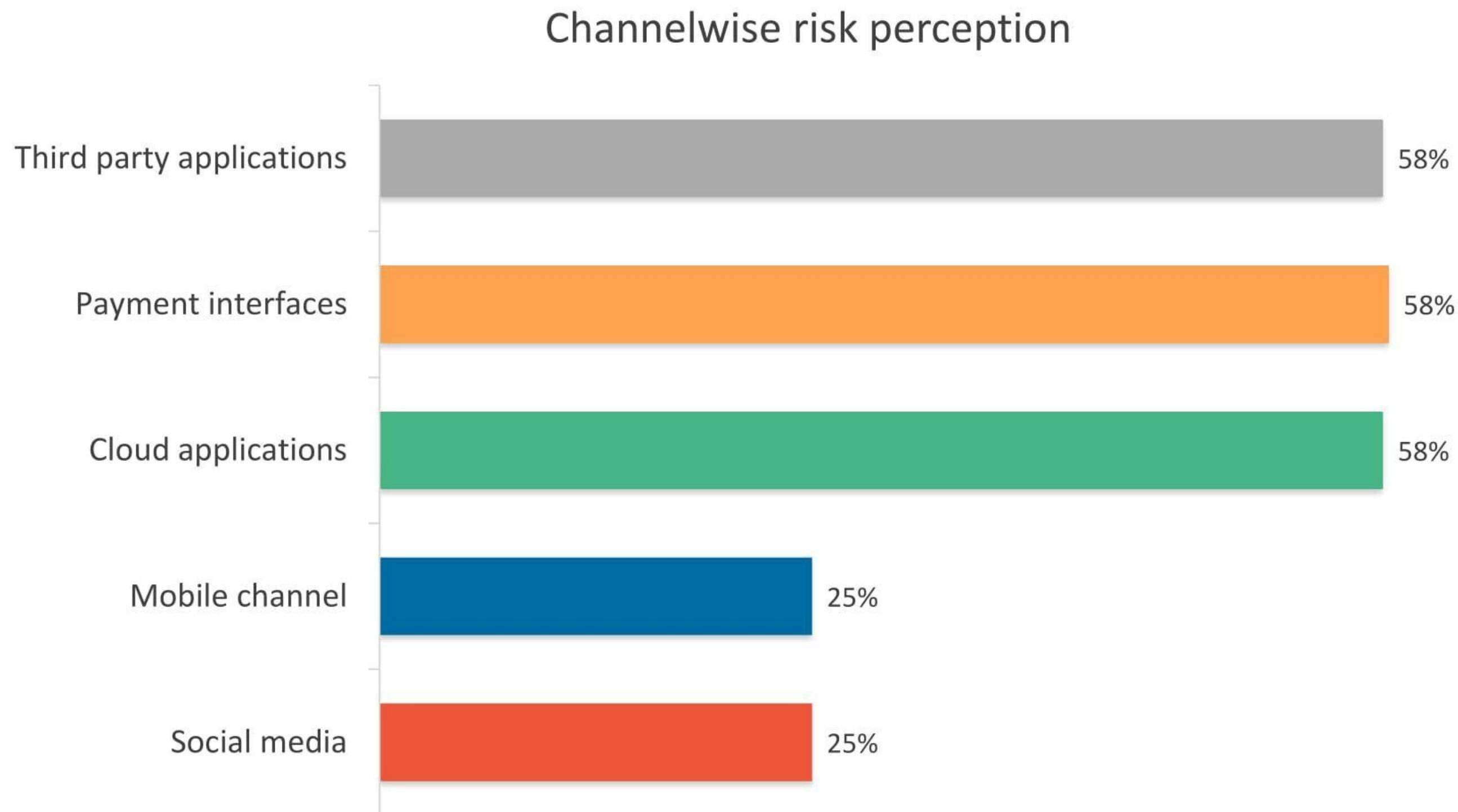
Customer data being collected



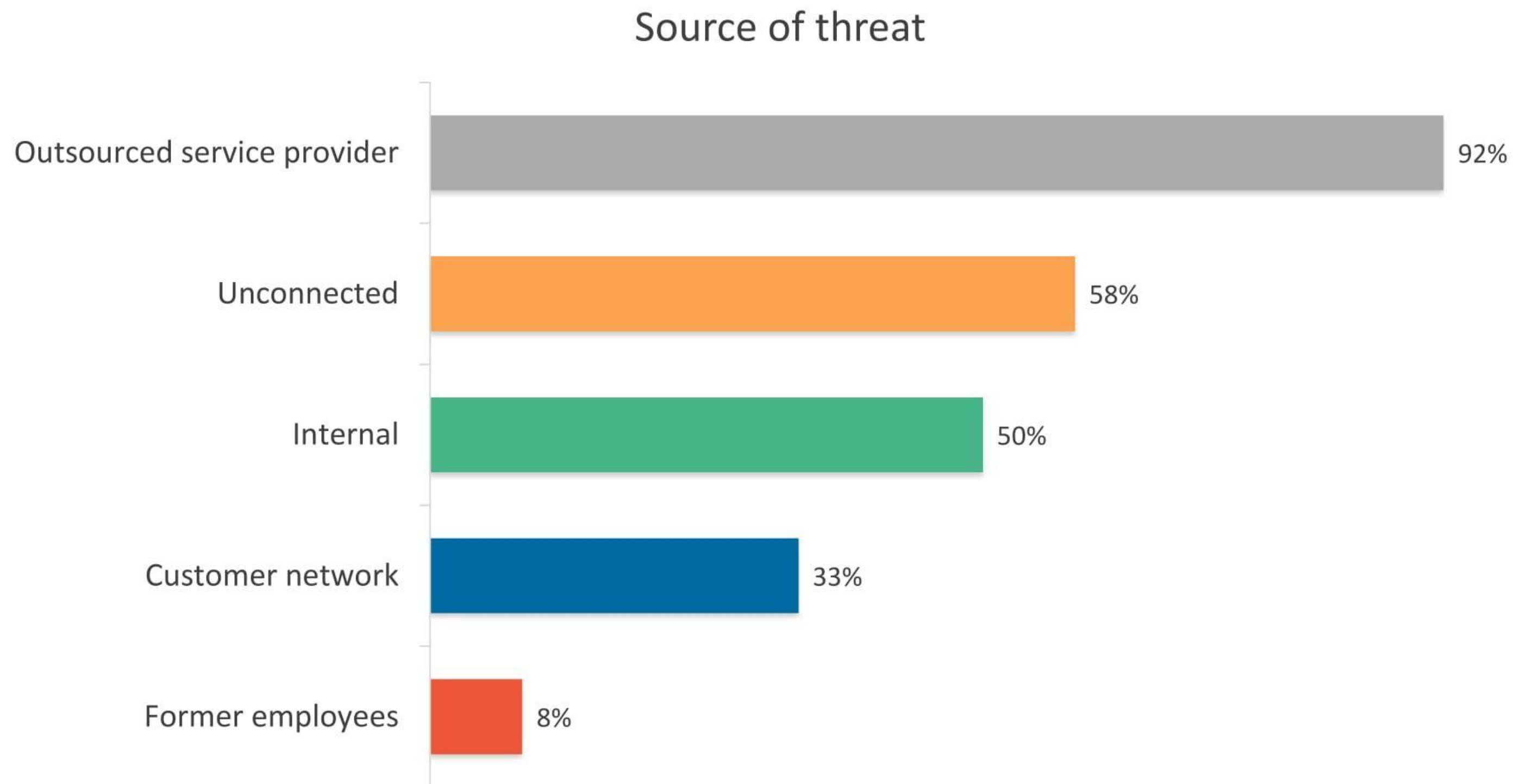


Risk Perception

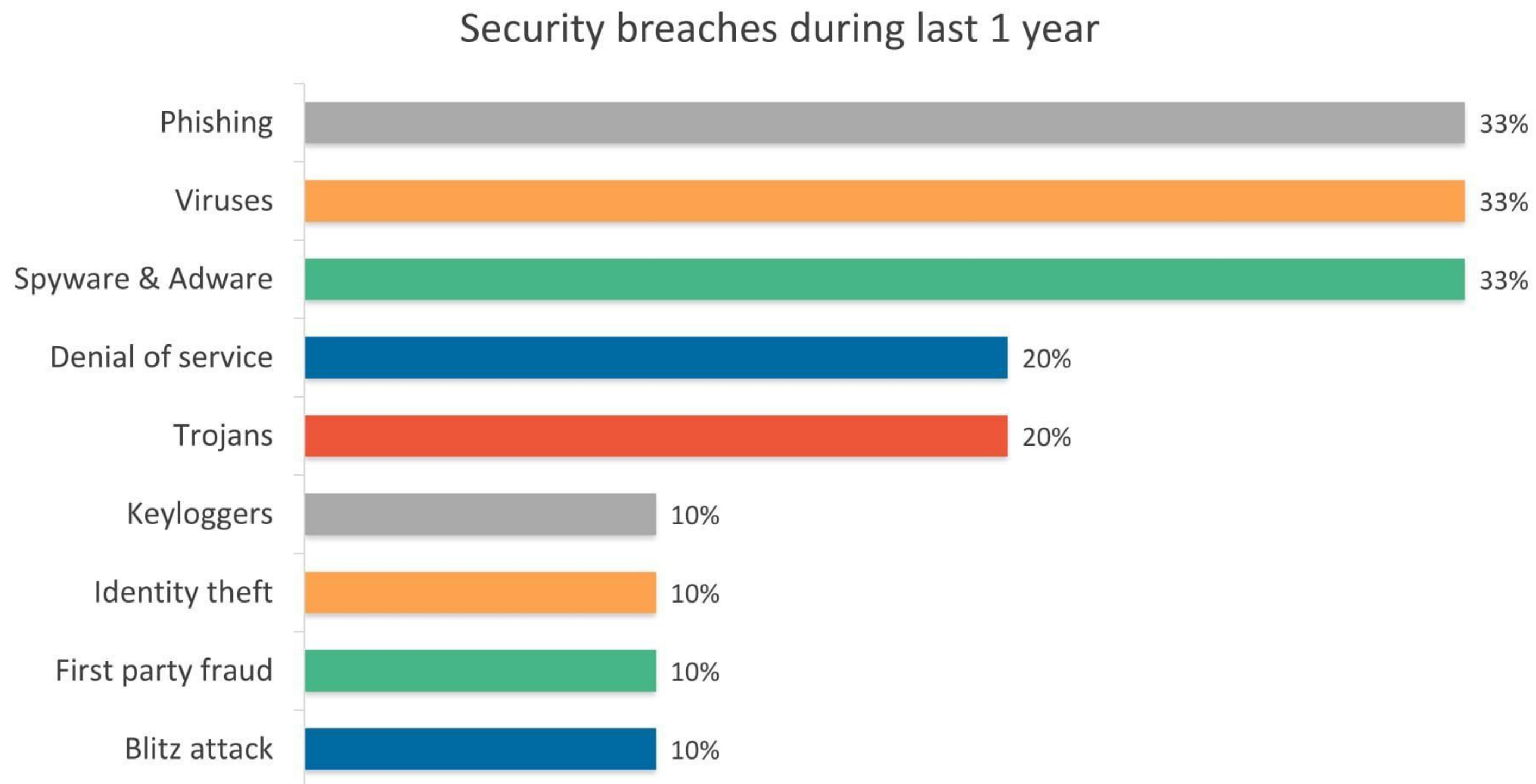
Applications & payment interfaces emerge as biggest concern for PSUs regarding data security



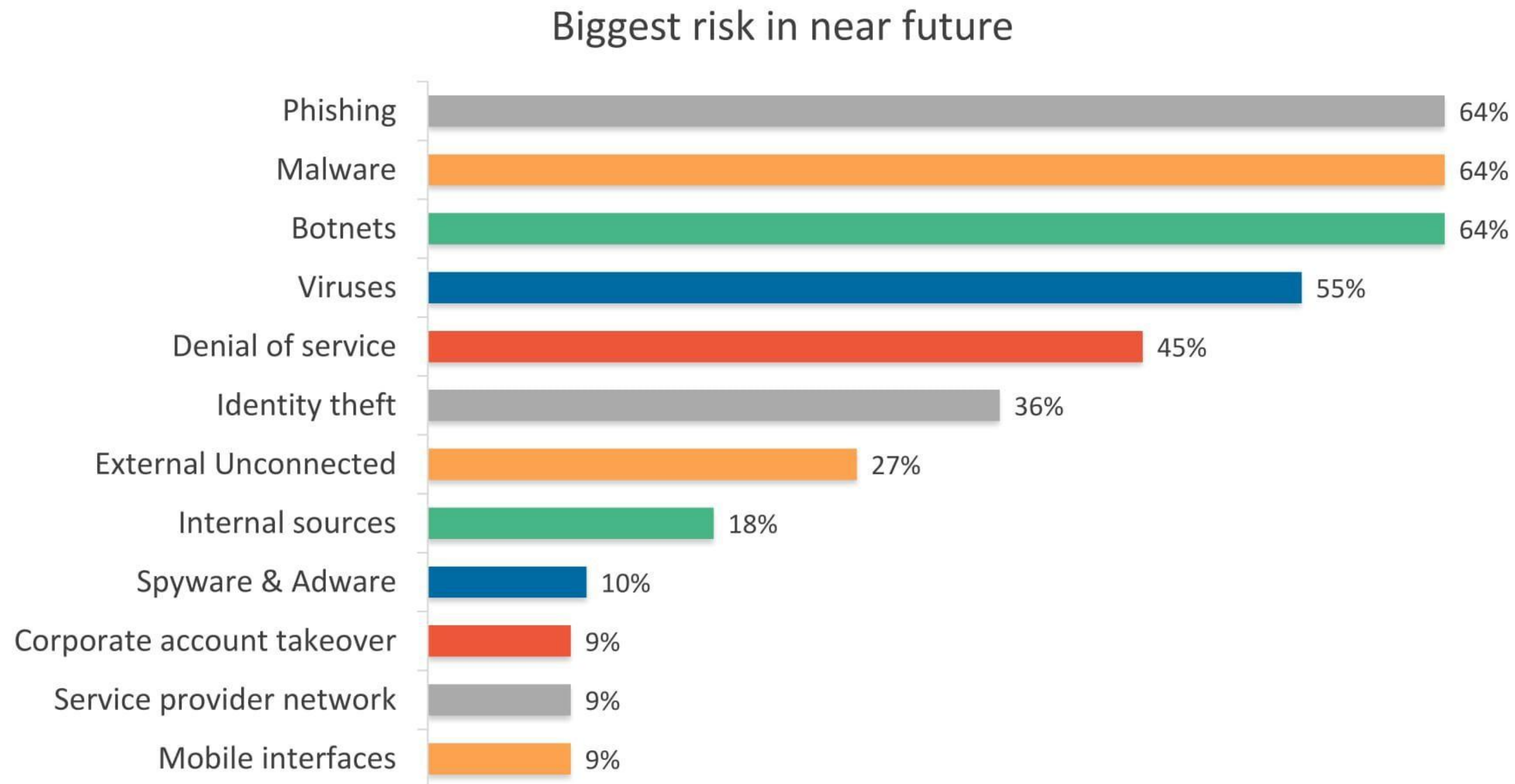
11 out of 12 PSUs pointed outsourced service providers as a potential risk source



Phishing, Virus & Spyware/adware attacks lead the threat pack

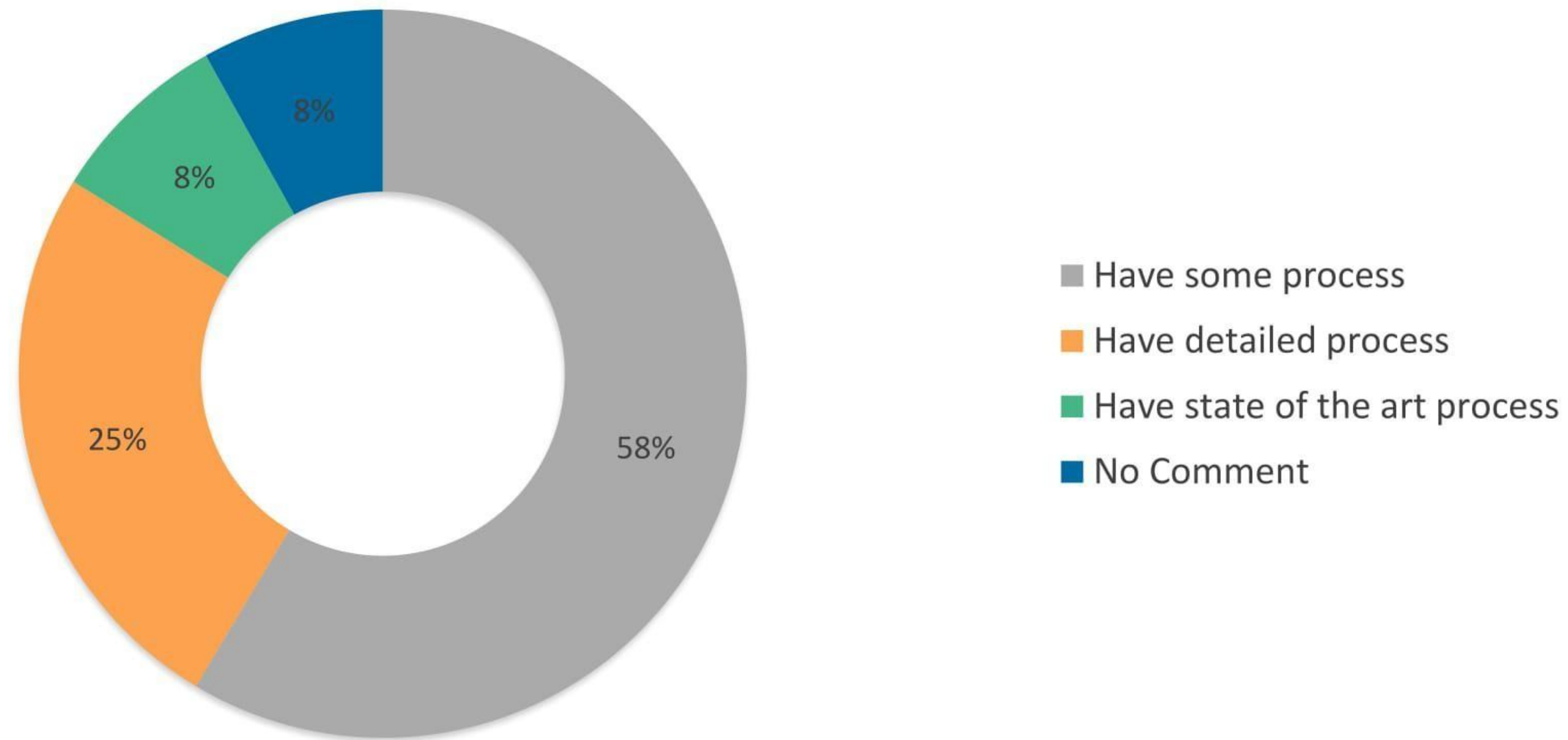


PSUs anticipate biggest risk emerging from Botnets, Phishing and Malware attacks



Majority of PSUs lack a detailed process to recognize and prioritize new threat sources

Presence of process to identify & prioritize new threat sources

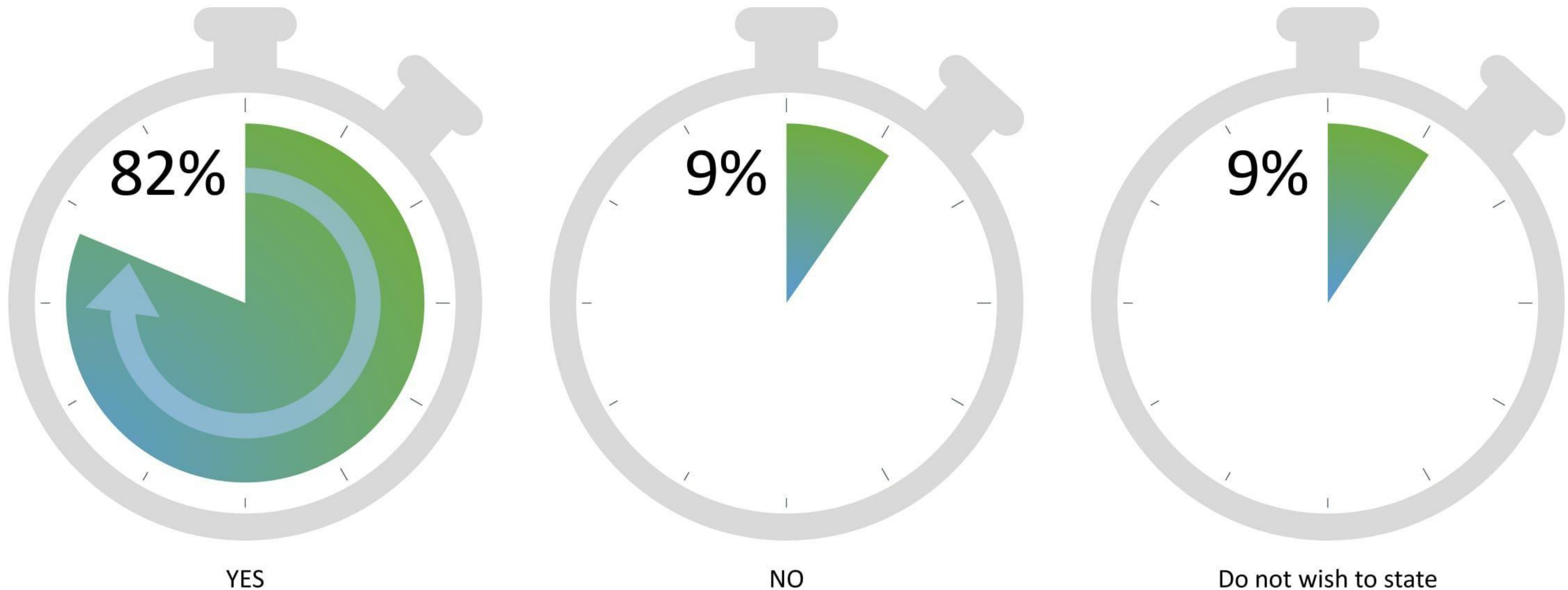




Organizational security & Risk Awareness

9 out of 11 PSUs reported having a board approved policy to manage cyber security

Presence of board approved Cyber Security Policy



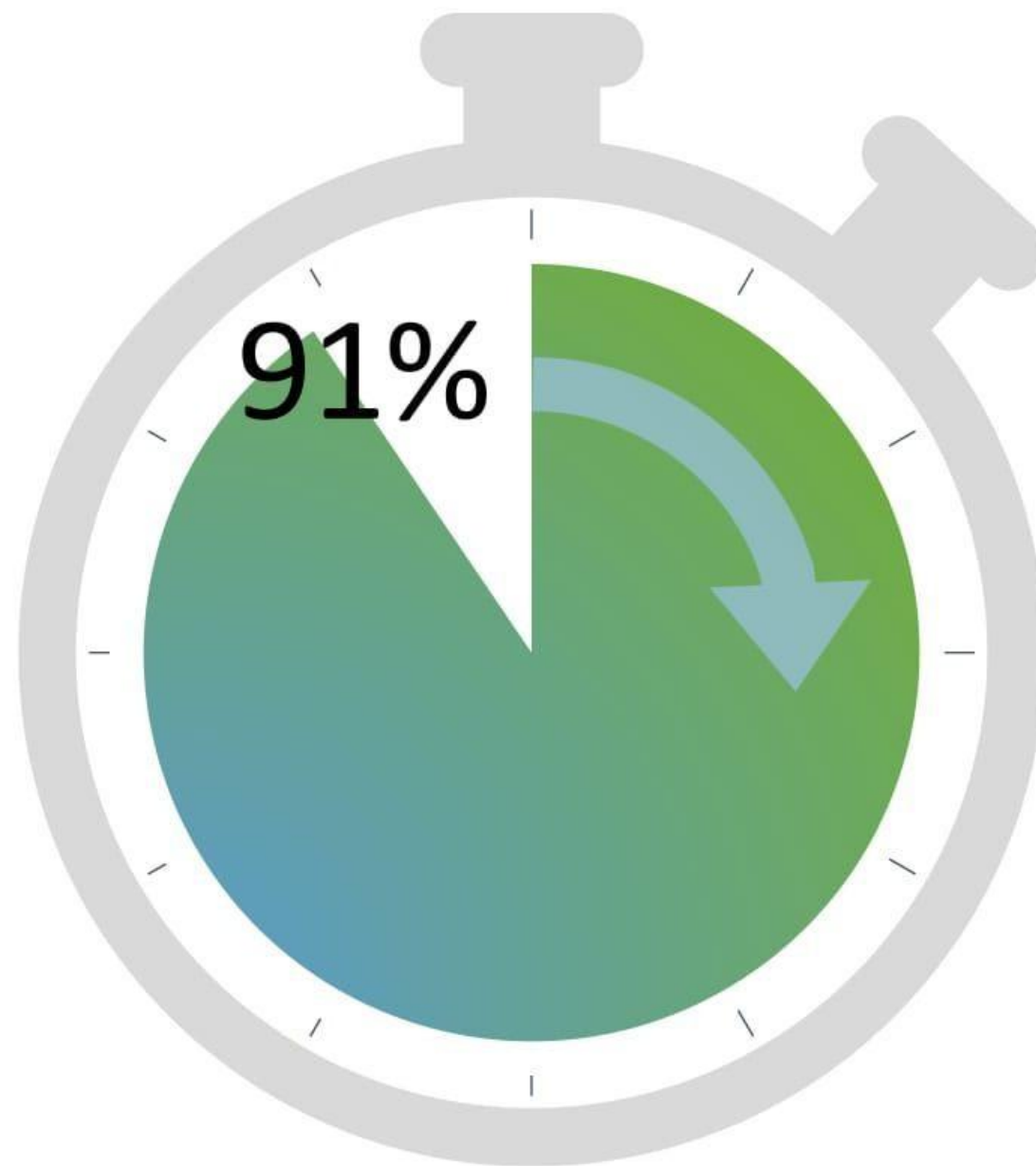
YES

NO

Do not wish to state

10 out of 11 PSUs conveyed having adequate funding towards their IT security setup

Current funding status for IT security setup



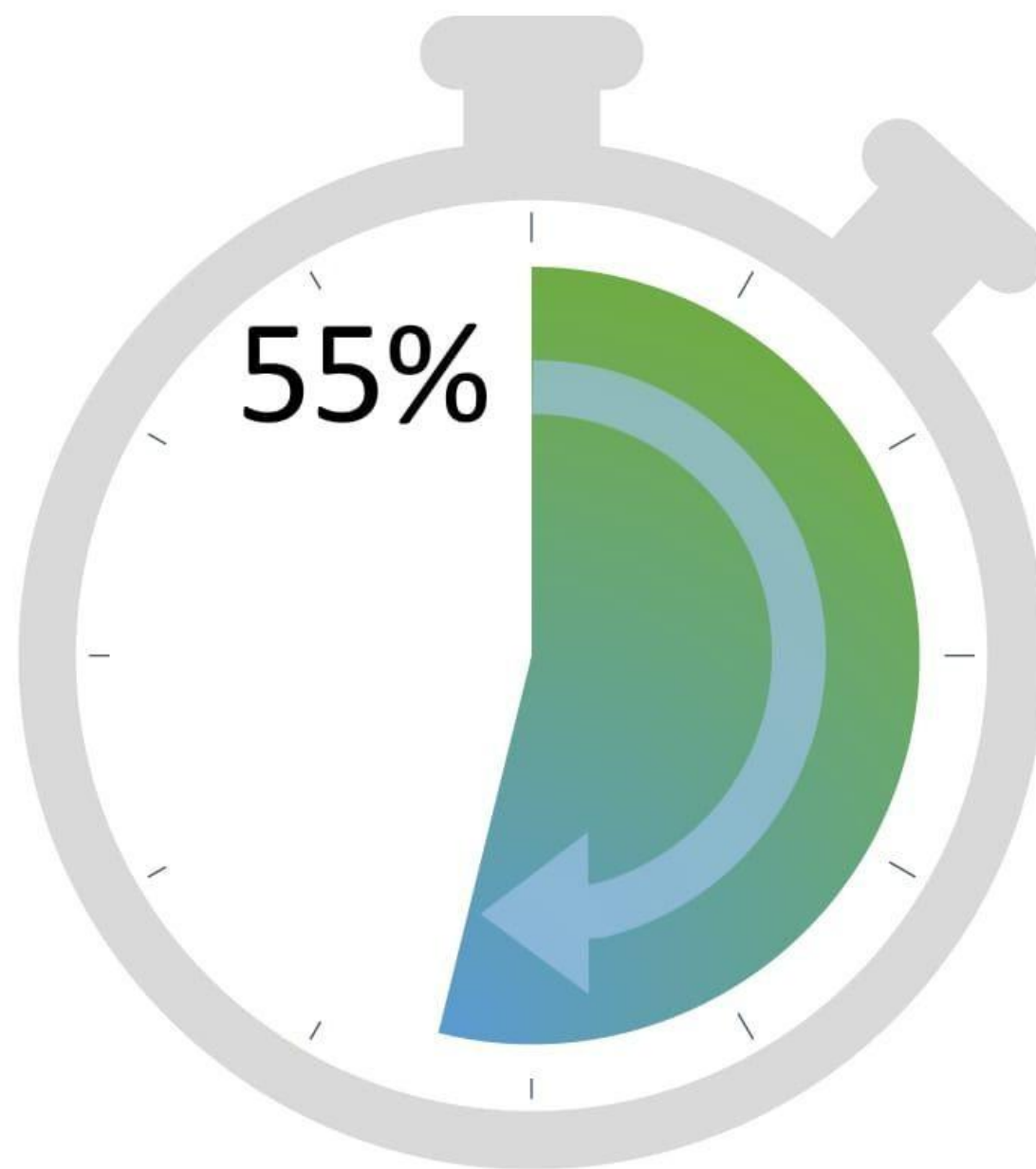
Sufficient funding



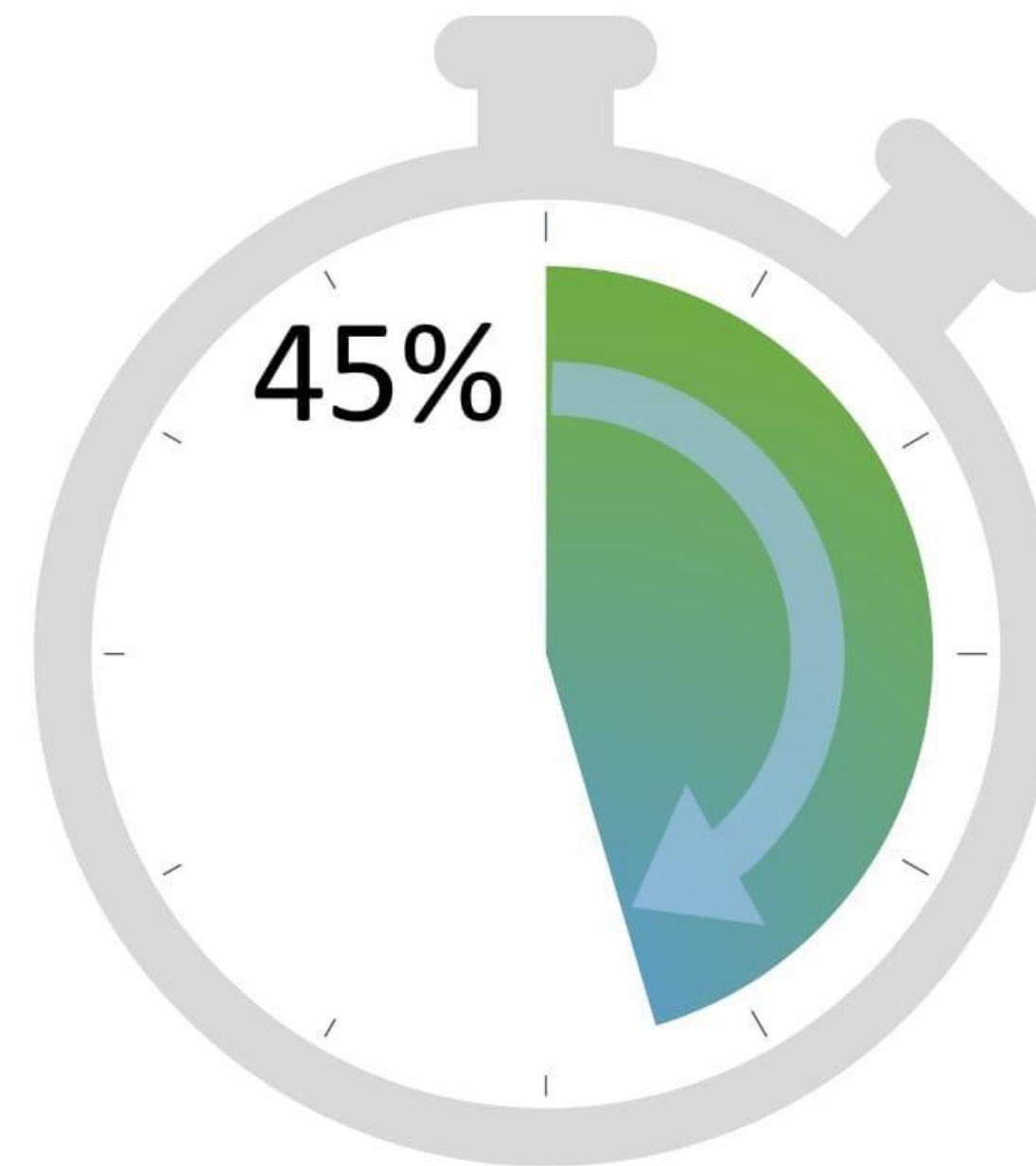
Funds are constrained

A large number of PSUs seem to rely on random updates for making internal stakeholders cognizant of security threats

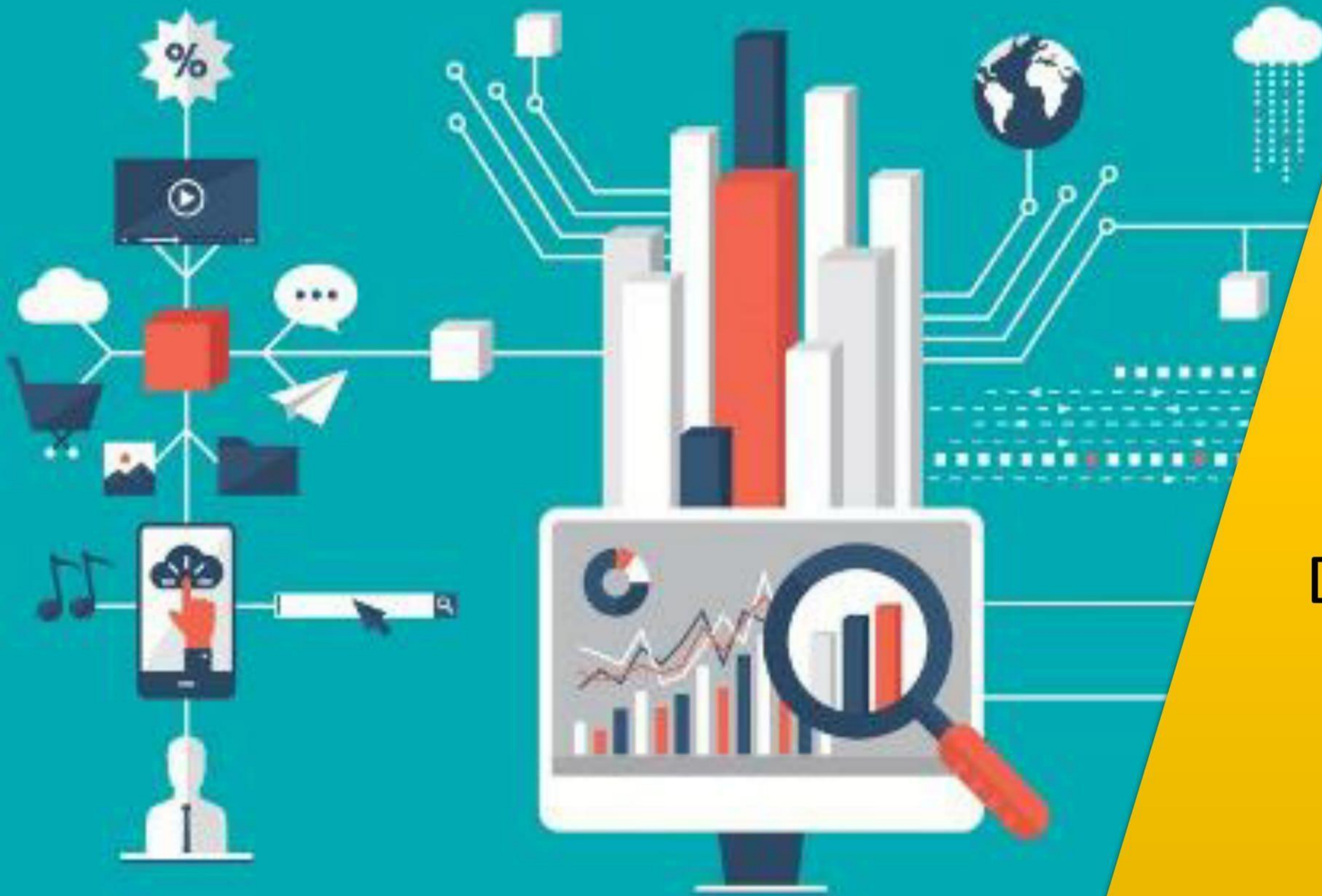
Process to spread awareness of security threats among employees/associates



Regular updates



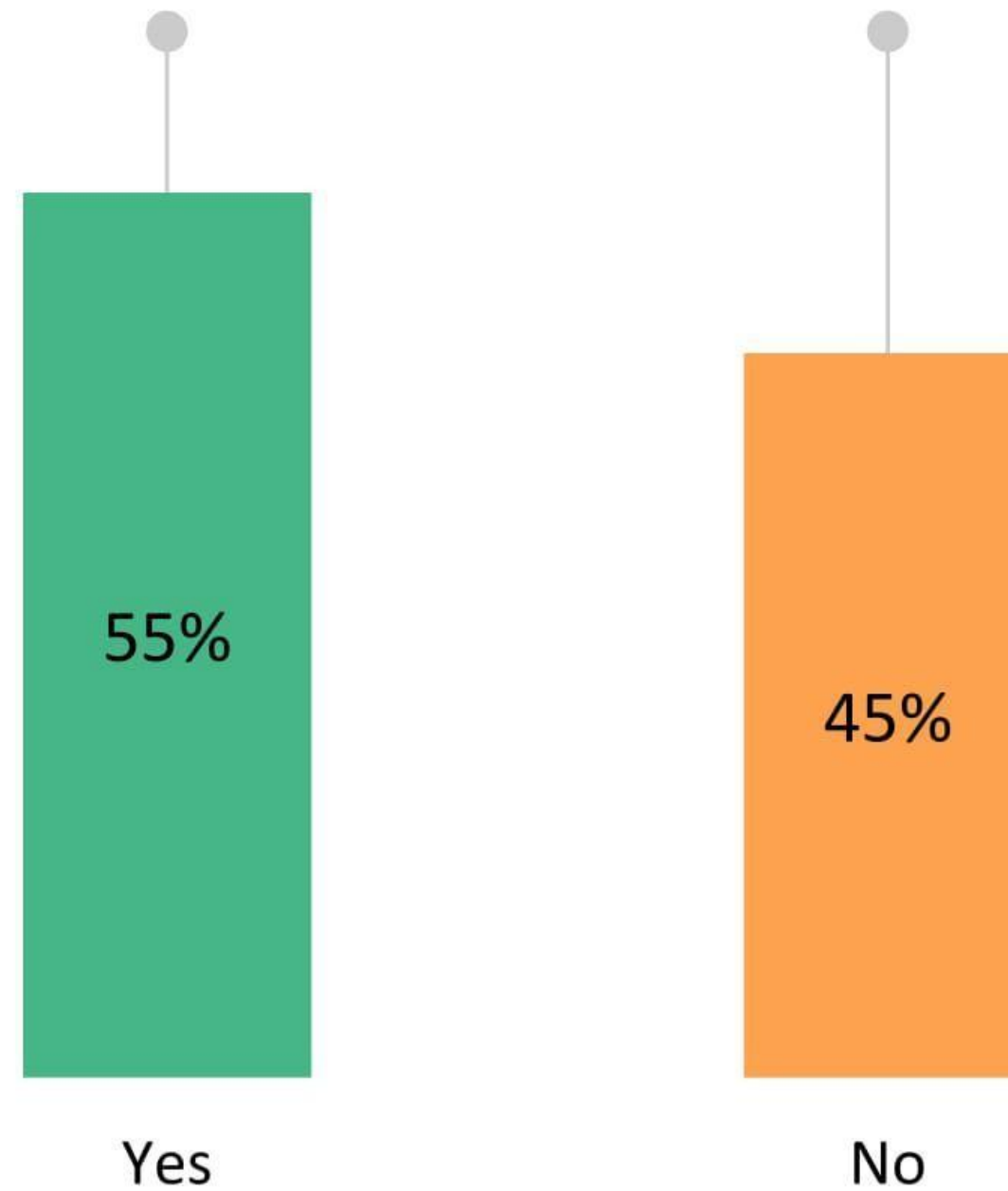
Occasional updates



Data classification & Governance

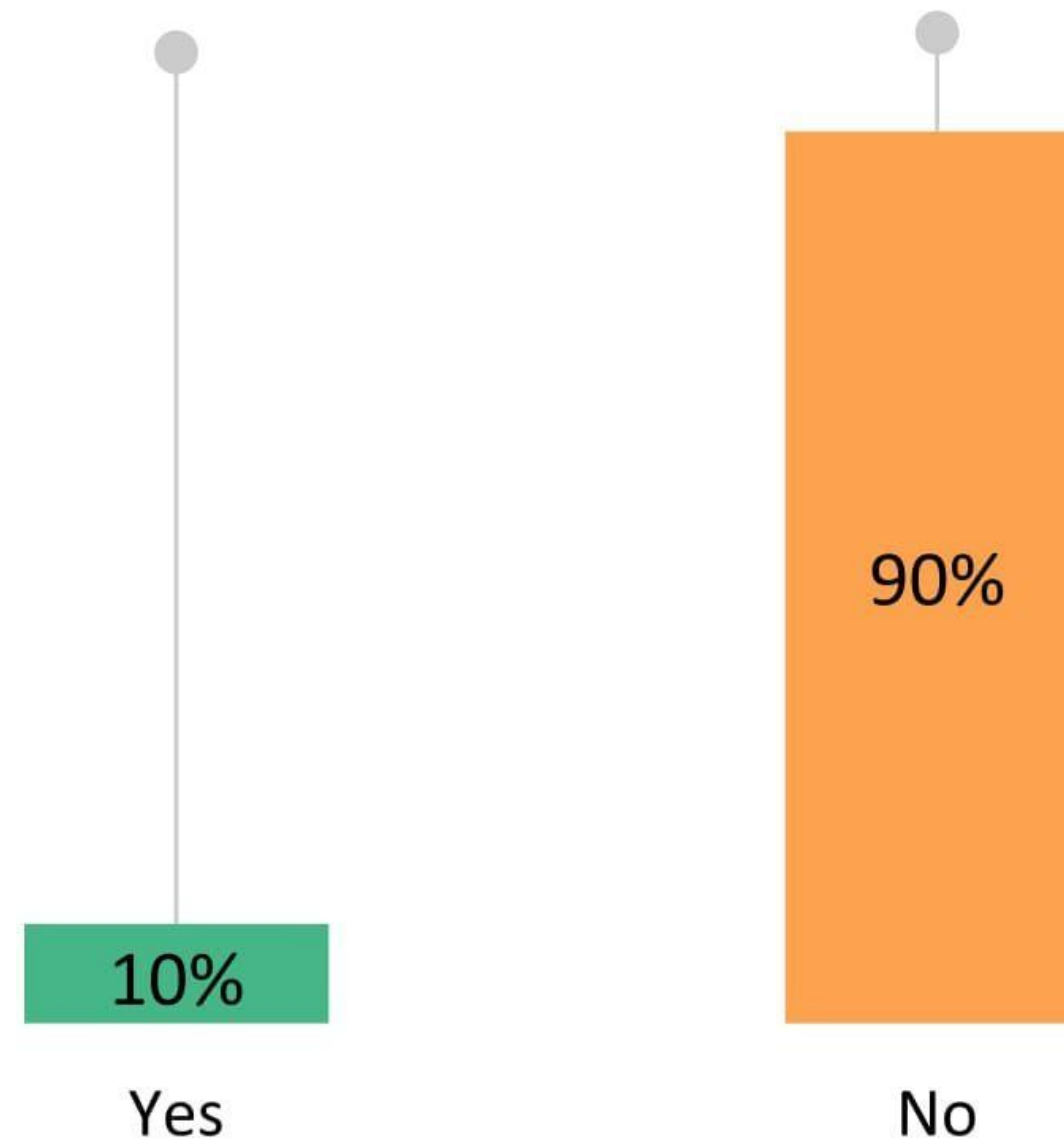
5 out of 11 PSUs do not have any data governance tool to manage data handling

Presence of data governance tools for data handling



9 out of 10 PSUs lack advanced e-discovery tools that leverage machine learning and help reduce the cost/time for compliance audits

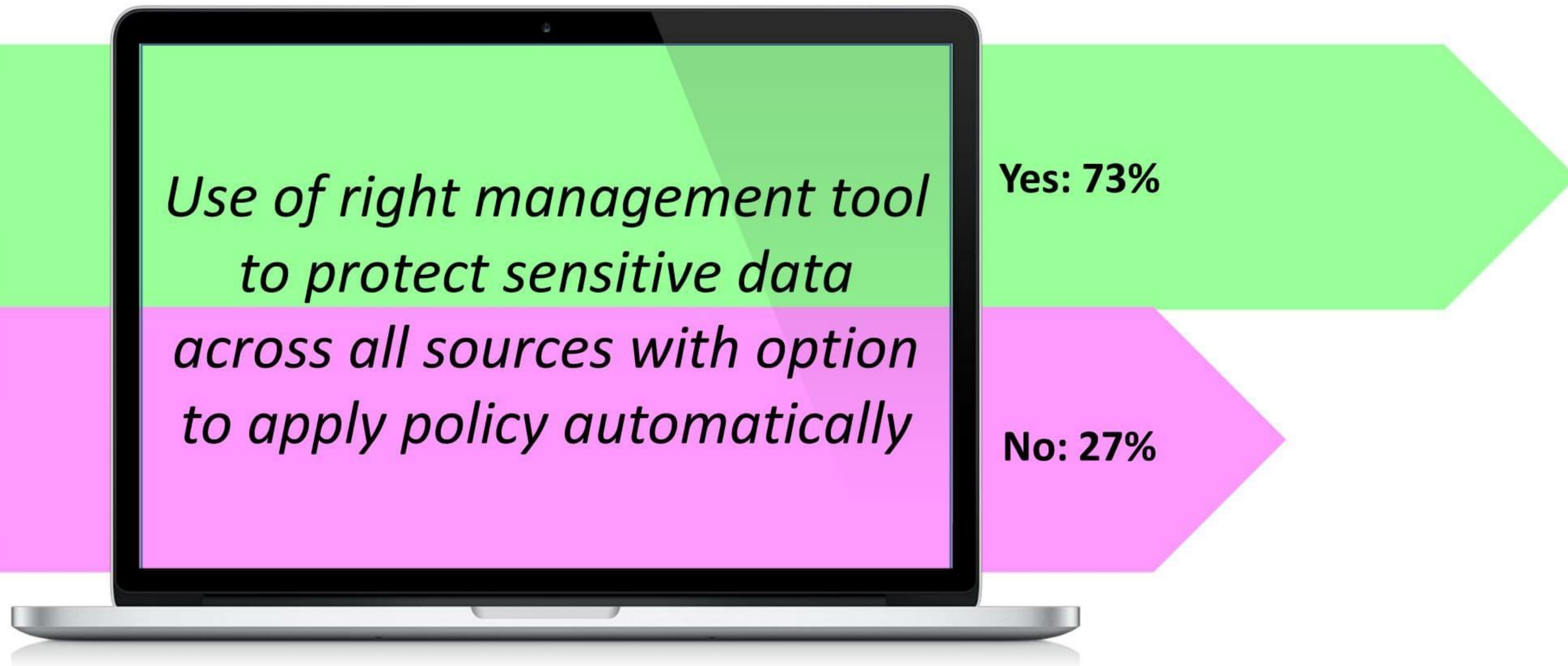
Presence of advanced e-discovery tools





Information protection

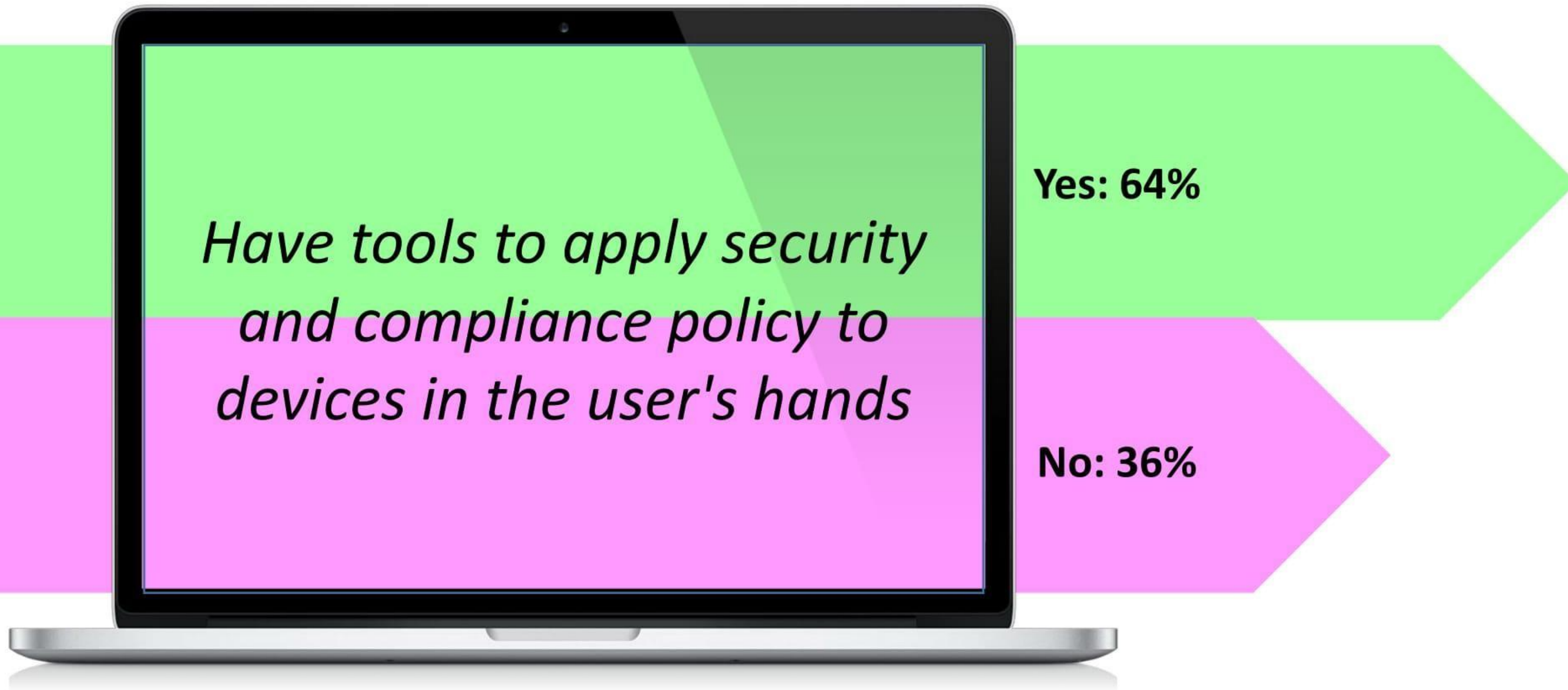
Majority of PSUs are confident of using the correct tool for protection of sensitive data



Majority of PSUs still not using data loss prevention tools



4 out of 11 PSUs still do not apply compliance policies to laptops and handheld devices



Of the total PSUs analysed, more than half admitted of having no knowledge of the file storage & sharing apps used by their employees

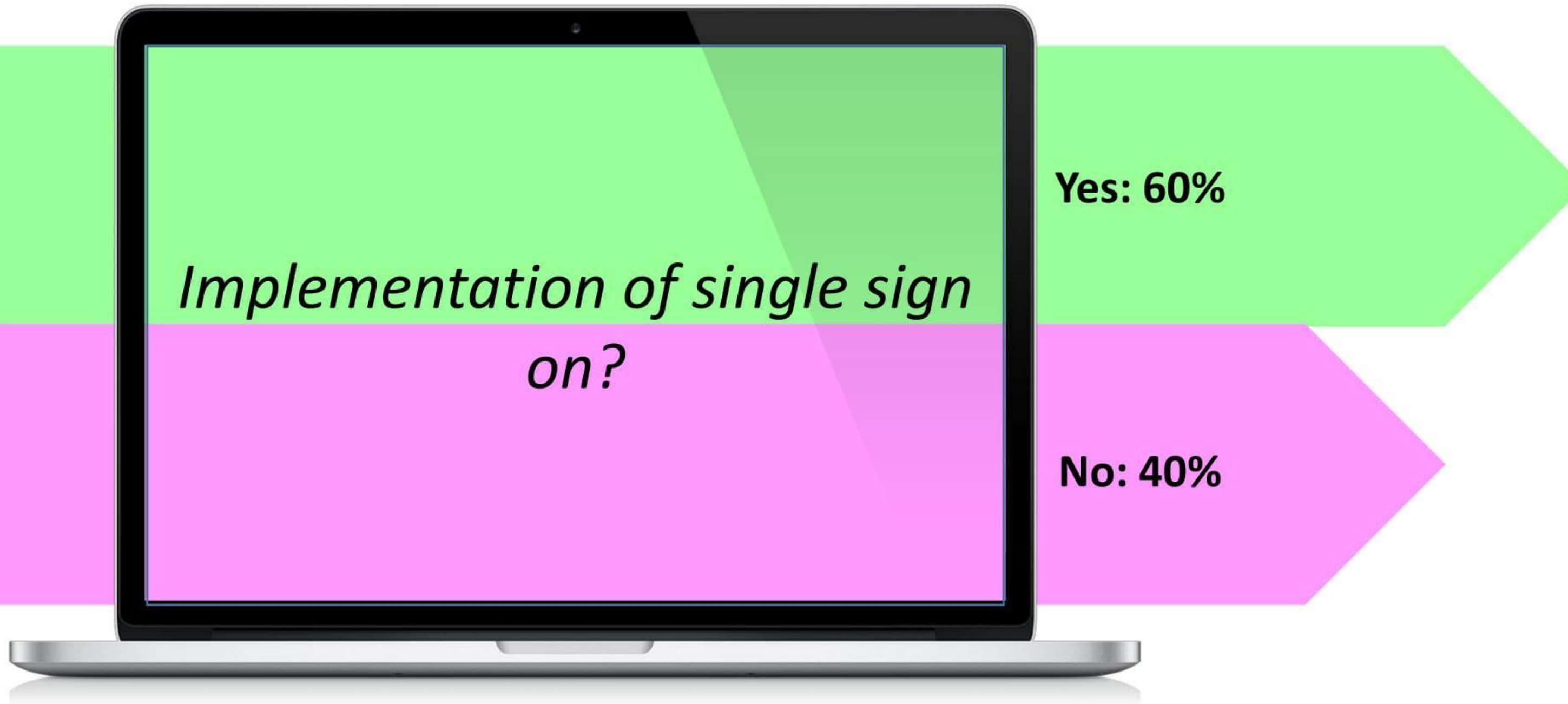


*Do you know which SaaS apps
your employees are using for
file storage & sharing?*

Yes: 45%

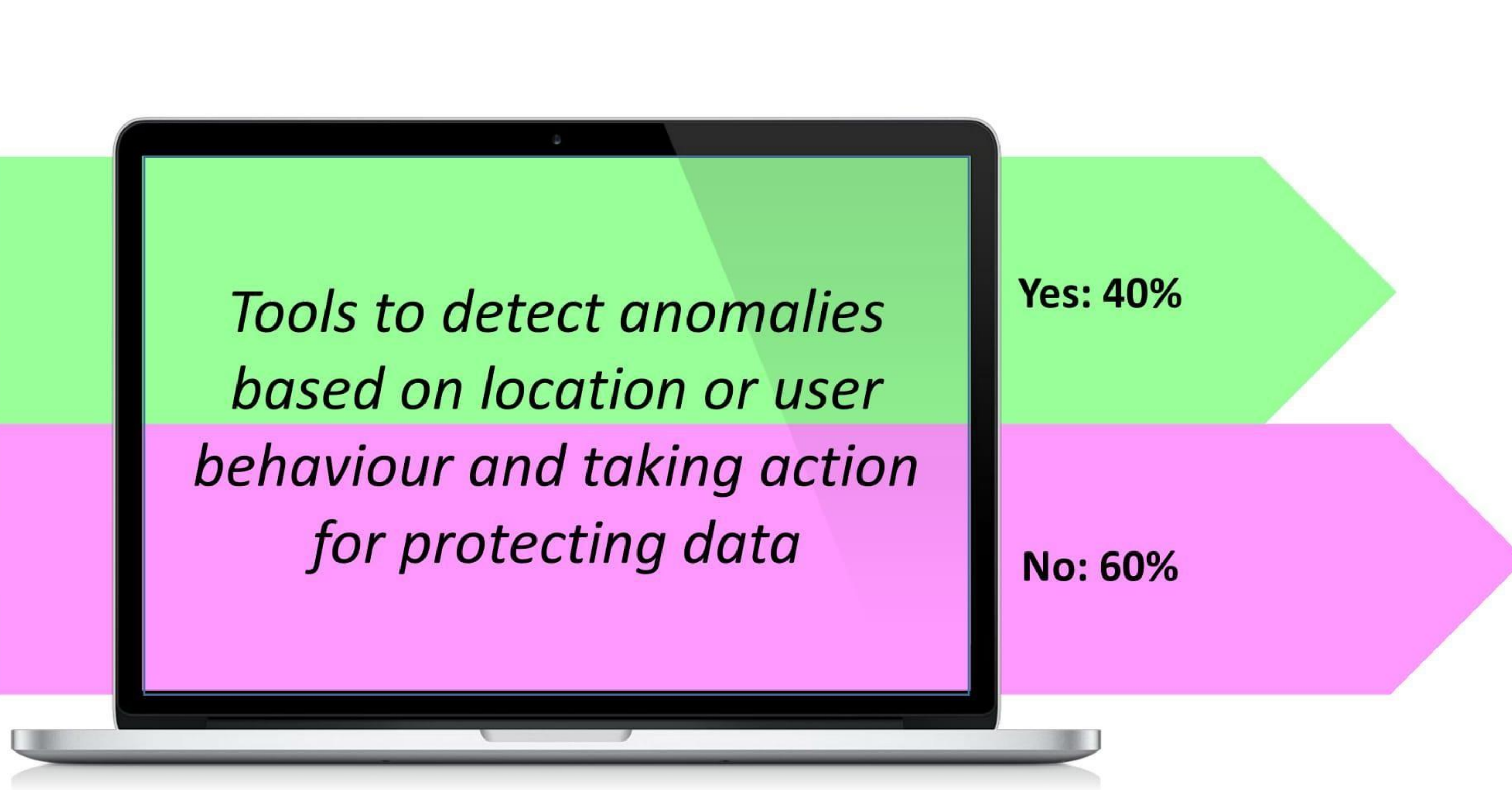
No: 55%

Use of single sign on seems to be gaining traction as 6 out of 10 PSUs reported using it



Total respondents = 10

Real-time anomaly detection still has a long way to go among PSUs as currently 6 out of 10 have not deployed it

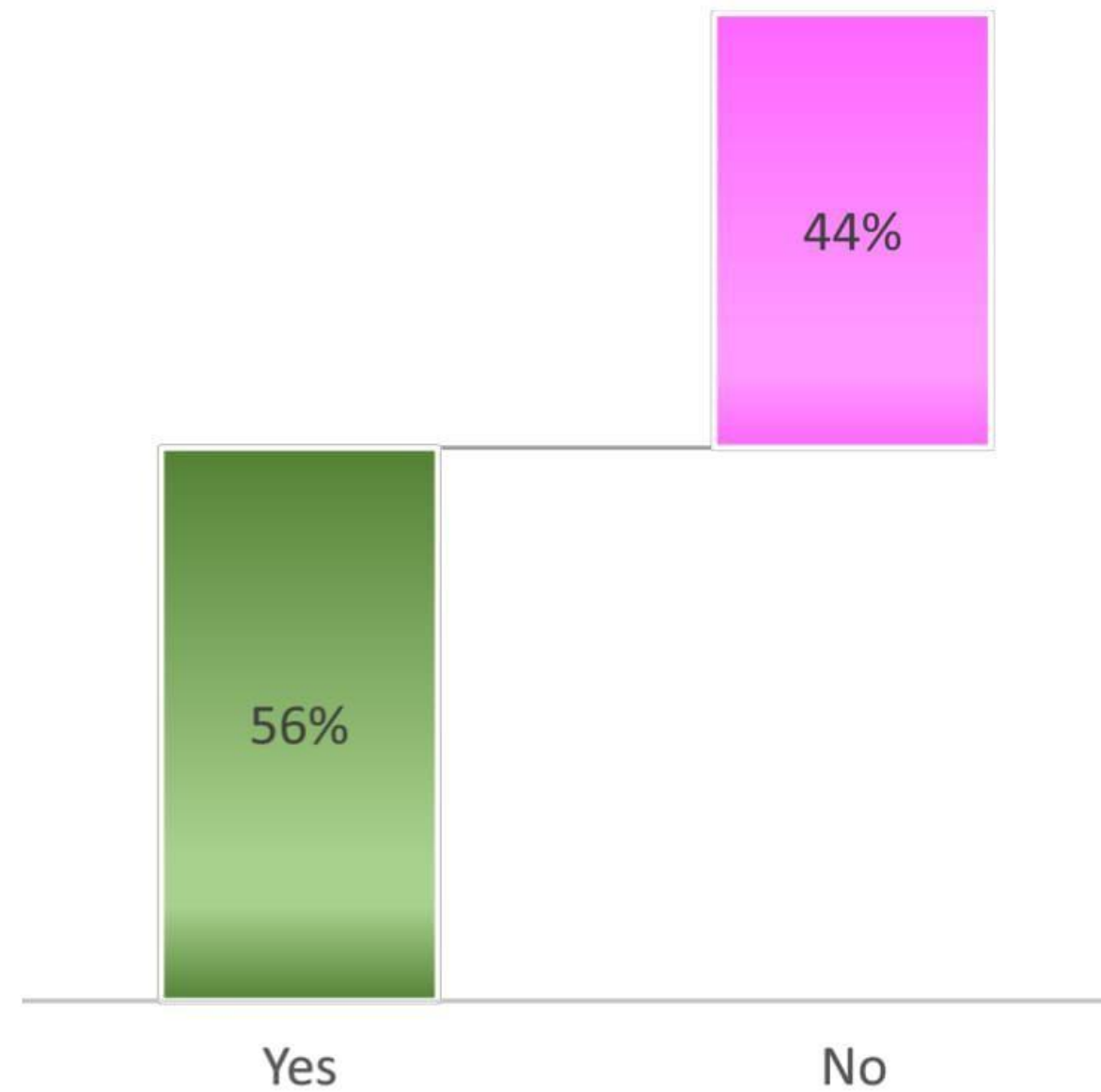




Threat Intelligence

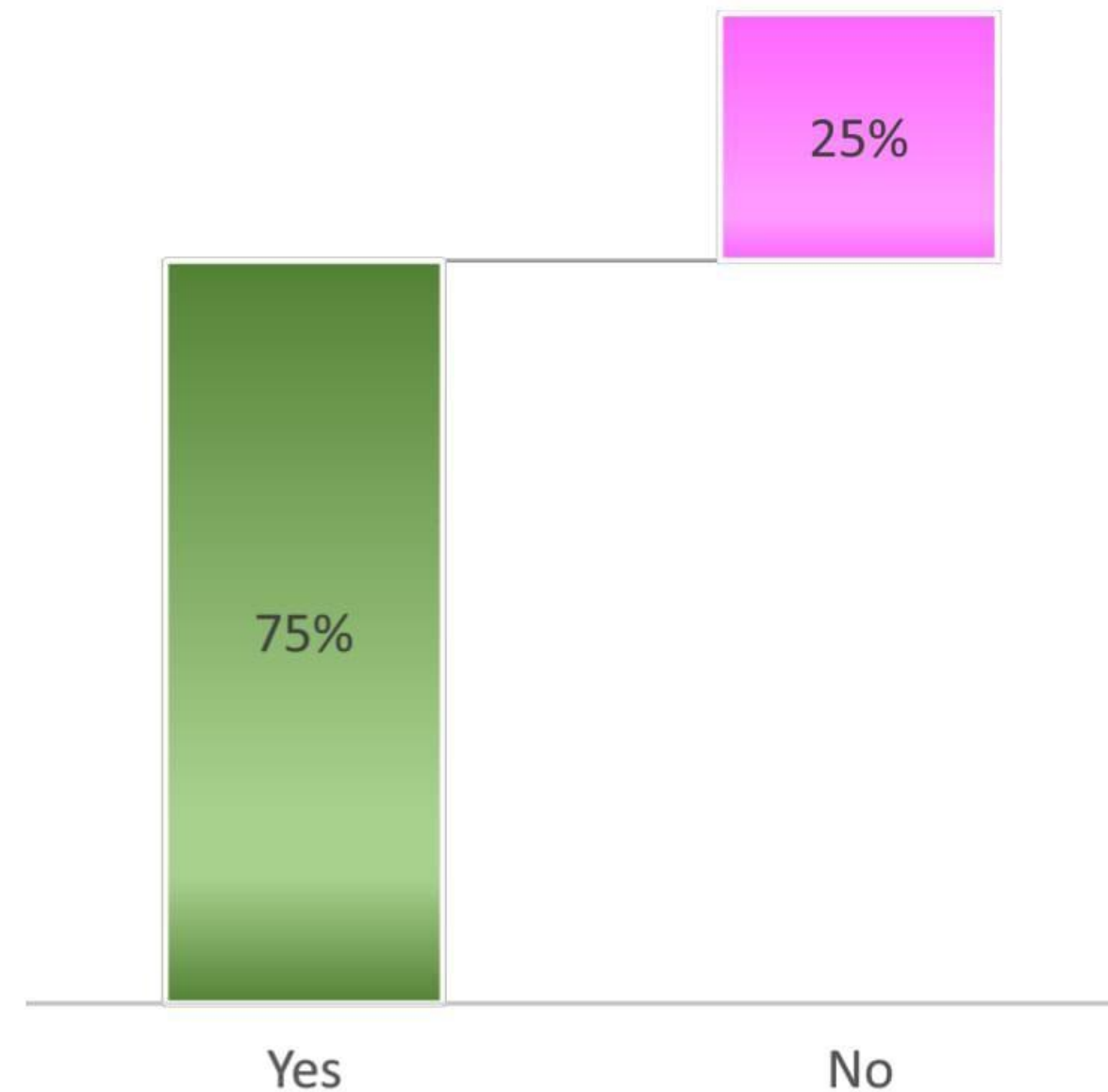
5 out of 9 units reported presence of a strong threat intelligence framework

Robust framework for threat intelligence



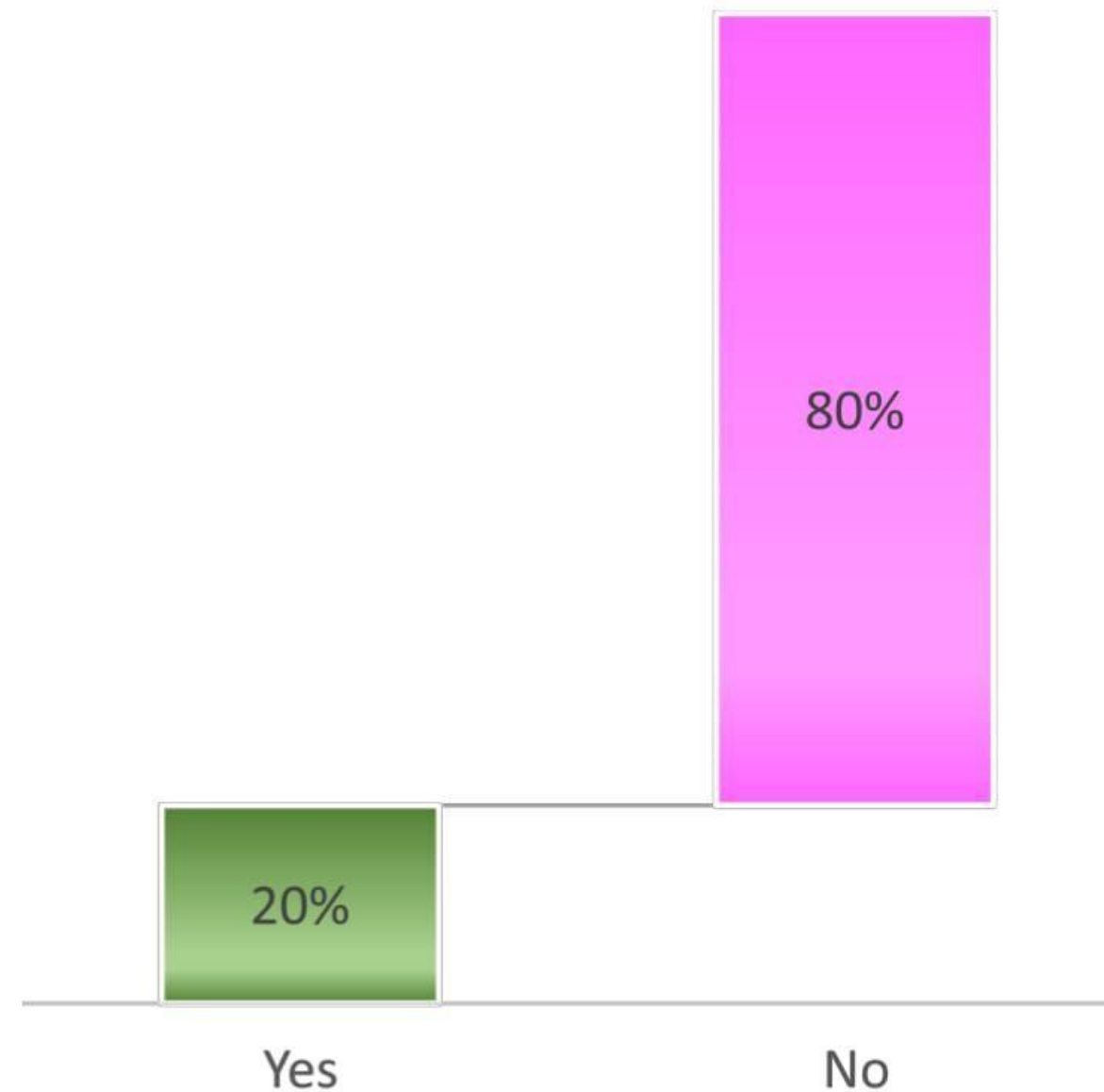
Most PSUs gearing up to handle and protect from zero day virus/spam attacks

Behavioural detection in Antivirus/Antispam engine



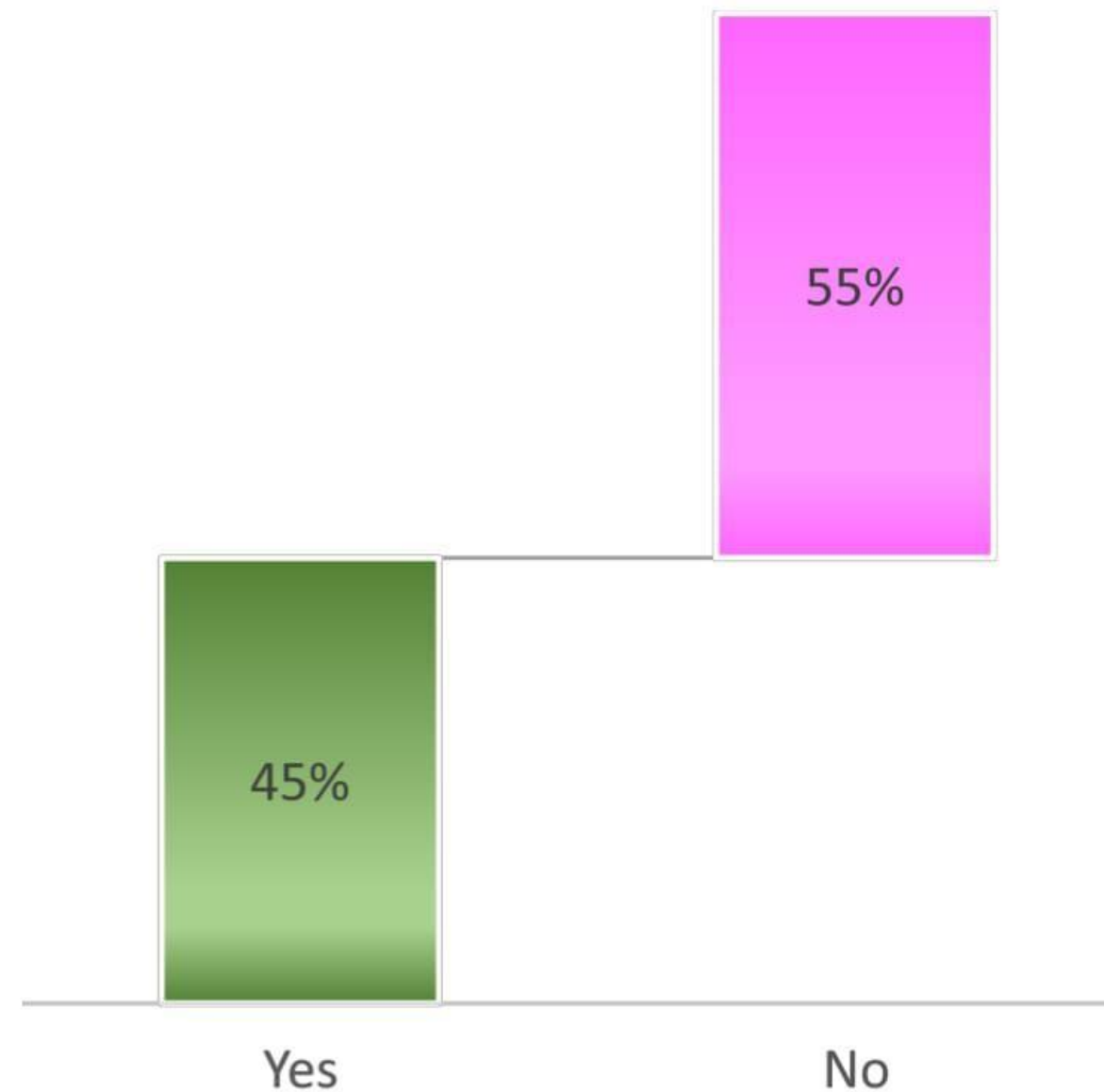
IT security at most PSUs has not evolved to the level of deploying machine learning to monitor and analyze past events & triggers to predict future security events

Use of machine learning to predict future security events



6 out of 11 PSUs currently do not use Big Data and Predictive Modelling for real time fraud analysis & risk analysis

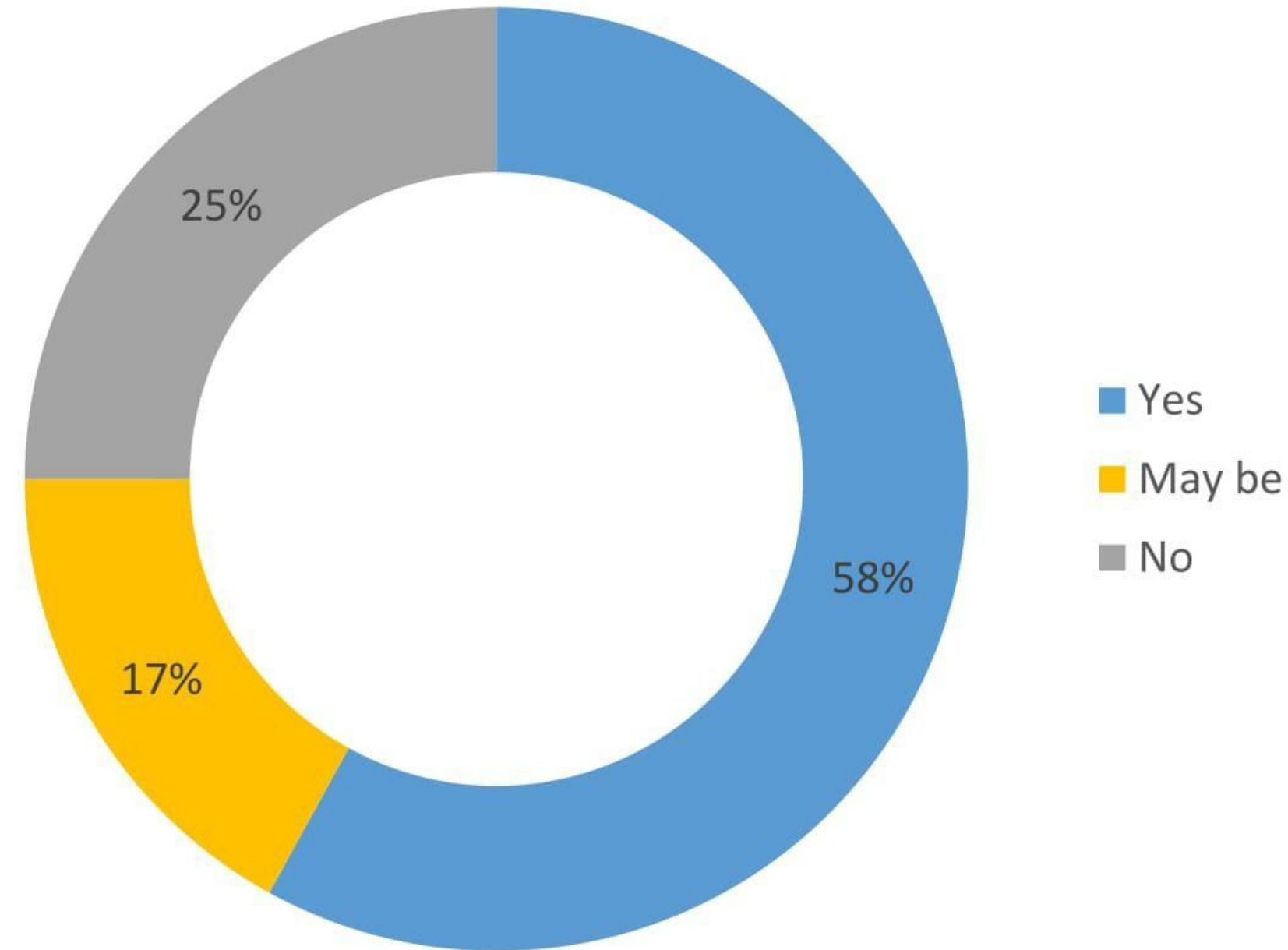
Real-time fraud analysis & risk analysis





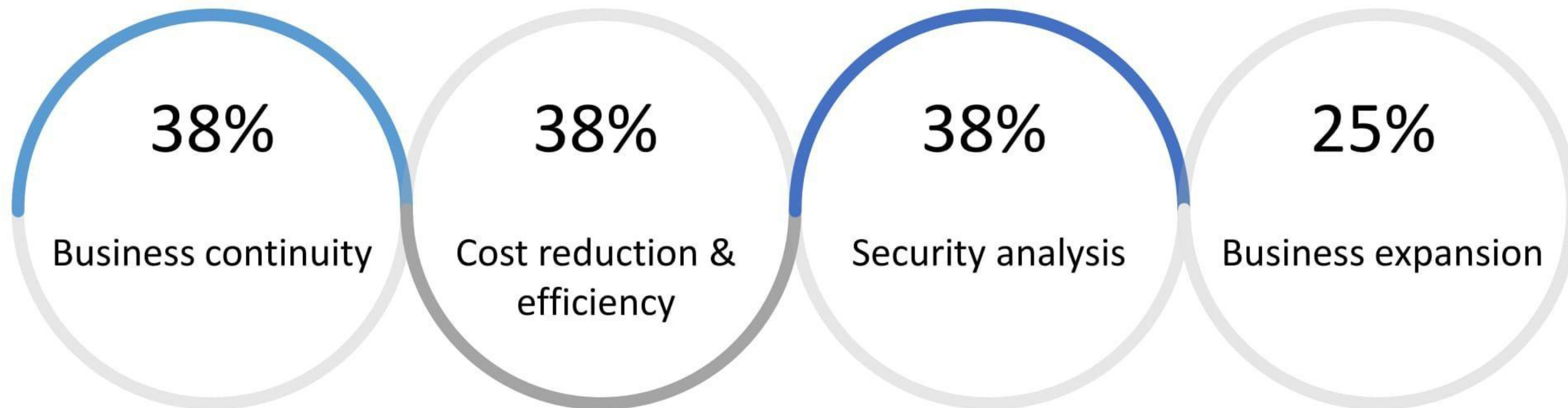
Leveraging Cloud

9 out of 12 PSUs have either planned to transition to cloud computing or have begun evaluating the same



Reason behind the transition towards cloud computing seems multi faceted

Key reasons behind going for cloud computing



PSU Security Stance Survey Findings

Digital Transformation

Indian Public Sector Units (PSUs) are undoubtedly going digital. They realize that digital transformation is a critical business need and is imperative to drive efficiency and productivity. Hence, they are aggressively digitizing their customer-facing as well as internal processes. However, there are impediments in this journey. Shortage skilled manpower and legacy mind-set issues come across as key challenges in the PSUs quest to digitization.

Organization security & Risk Awareness

Most PSUs have a board-approved cybersecurity policy in place backed with adequate budgets.

Threat Intelligence

While a majority of PSUs have a strong threat intelligence framework and are gearing up to counter zero day attacks, they are far from implementing next-gen technologies such as machine learning and predictive solutions for pre-empting threats.

Risk Perception

Digitization and information security go hand-in-hand as the former opens up PSUs to external threats. PSUs feel third party applications and payment interfaces are the biggest areas of concern, while outsourced service providers are overwhelmingly believed to be the biggest potential risk source. Amongst future threats, Botnets, phishing and malware are feared the most.

Data Classification & Governance; Information Protection

PSUs fall woefully short when it comes to Data Classification & Governance; Information Protection. Few use e-discovery tools and almost half of them still don't leverage data governance tools and data loss prevention tools. Most PSUs also lack visibility into file storage and sharing apps being used by employees.