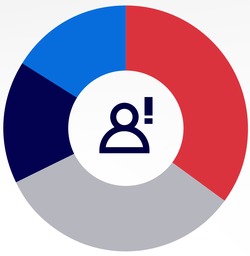
UNDERSTANDING INSIDER THREATS AND DATA LOSS PREVENTION

POLL 1: INSIDER THREAT CONCERNS

WHAT TYPE OF INSIDER THREATS CONCERN YOU THE MOST?

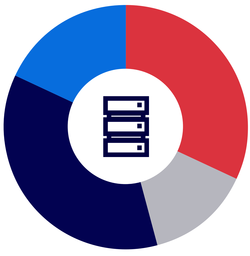


Key Insight

Emerging technologies and human factors drive insider threat concerns. GenAI tools (35%) pose risks like misuse or exposure of sensitive data, while departing employees (33%) create risks of IP theft or unauthorized data transfer. Together, they account for 68% of responses, highlighting the need for careful management of technology and employee transitions. Source code leaks and unsanctioned applications (16% each) show the ongoing challenge of shadow IT and protecting proprietary assets.

POLL 2: CURRENT DLP APPROACHES

HOW DOES YOUR ORGANISATION CURRENTLY APPROACH DATA LOSS PREVENTION (DLP)?

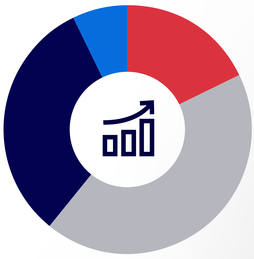


Key Insight

While 36% of organisations are adopting modern behavioural monitoring to proactively identify and prevent data loss, 32% still rely heavily on manual processes and training. These manual approaches focus on educating employees and enforcing policies through awareness programmes and manual checks, which can be effective but may also be limited by human error and inconsistency. Meanwhile, 18% of organisations lack an active DLP strategy, which could expose them to significant data loss risks.

POLL 3: DLP PROGRAMME IMPROVEMENTS

IF YOU COULD IMPROVE ONE ASPECT OF YOUR DLP PROGRAMME, WHAT WOULD IT BE?



Key Insight

Automation and detection tools (43%) top DLP improvement priorities, enabling faster and smarter responses to potential data loss incidents. Employee awareness and training (32%) remain critical, emphasising the importance of human behaviour in protecting data. Real-time visibility into data flows (18%) is increasingly sought to track sensitive information across systems and endpoints, helping detect anomalies early and prevent breaches. Only connected security systems (7%) are a lower priority, suggesting integration is less urgent for most organisations.

CONCLUSION

The results highlight the growing importance of modern tools and strategies to address insider threats and improve DLP programmes. Organisations are prioritising automation, behavioural monitoring, and employee training to stay ahead of risks.

TAKE ACTION

The data is clear: insider threats are evolving—are your defences keeping up?

Mimecast's Incydr delivers real-time visibility, behavioural monitoring, and rapid detection to help close your DLP gaps.

LEARN MORE

Source: LinkedIn polls conducted between May and July among over 100 participants, targeted to Europe and South Africa.
This data is provided for informational purposes only and does not constitute professional advice or a legally binding statement.