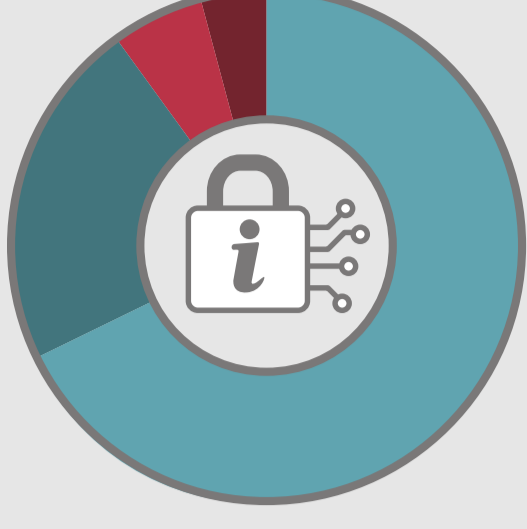


OTRS Spotlight: Corporate Security 2024

Part 2: Information and Device Security at Risk. Additional Resources Needed.

ISMS solutions are meant to keep companies safe. Many teams have already implemented one.



- 68% Actively using
- 22% Not using but planning to
- 6% Not using and not planning to
- 4% Don't know

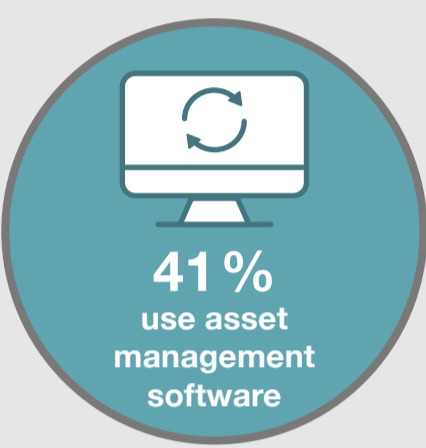
For an ISMS to be as useful as possible, a variety of tools and processes must be integrated. Teams still struggle with this.



Only a third of the tools are integrated.

- 35% Configuration management
- 34% Asset management
- 34% Security awareness and training
- 34% Audit and compliance reporting
- 30% Patch management

When integrating asset management into ISMS processes, teams lean heavily on existing software and integration.



10% use custom scripts and APIs

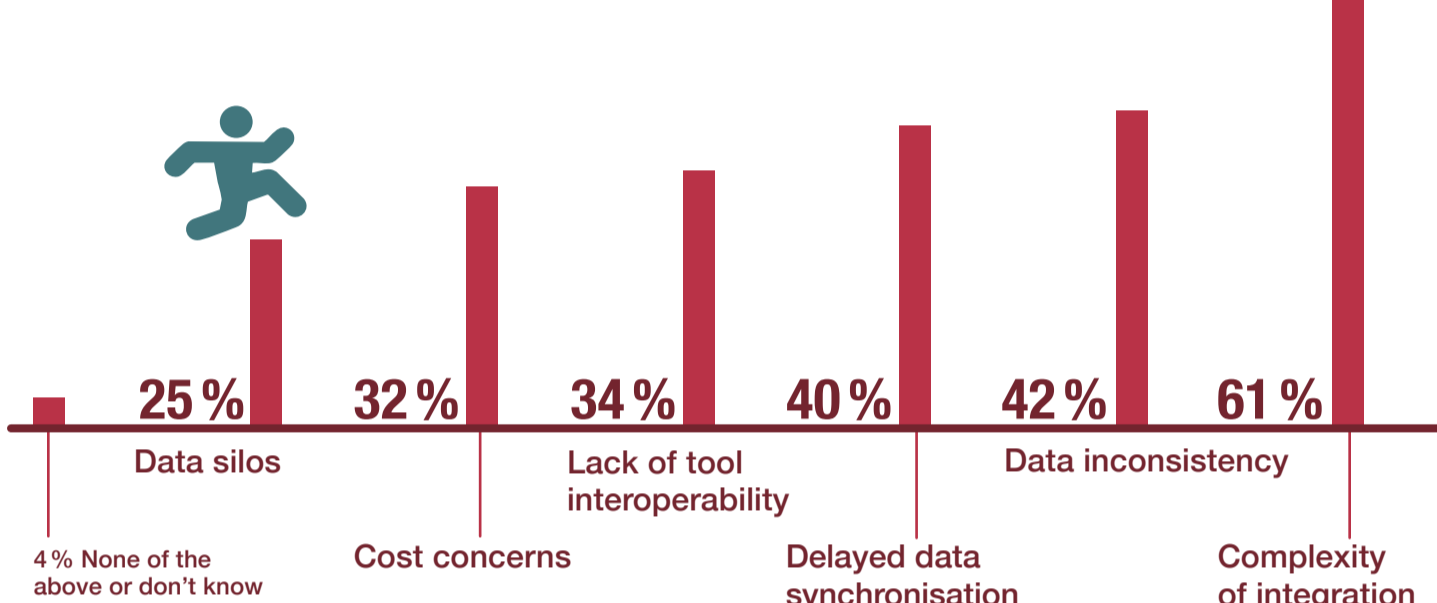


10% use manual data transfer and reconciliation



3% don't know

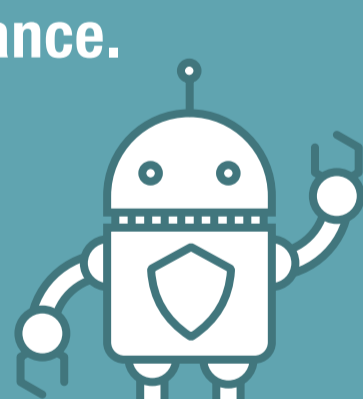
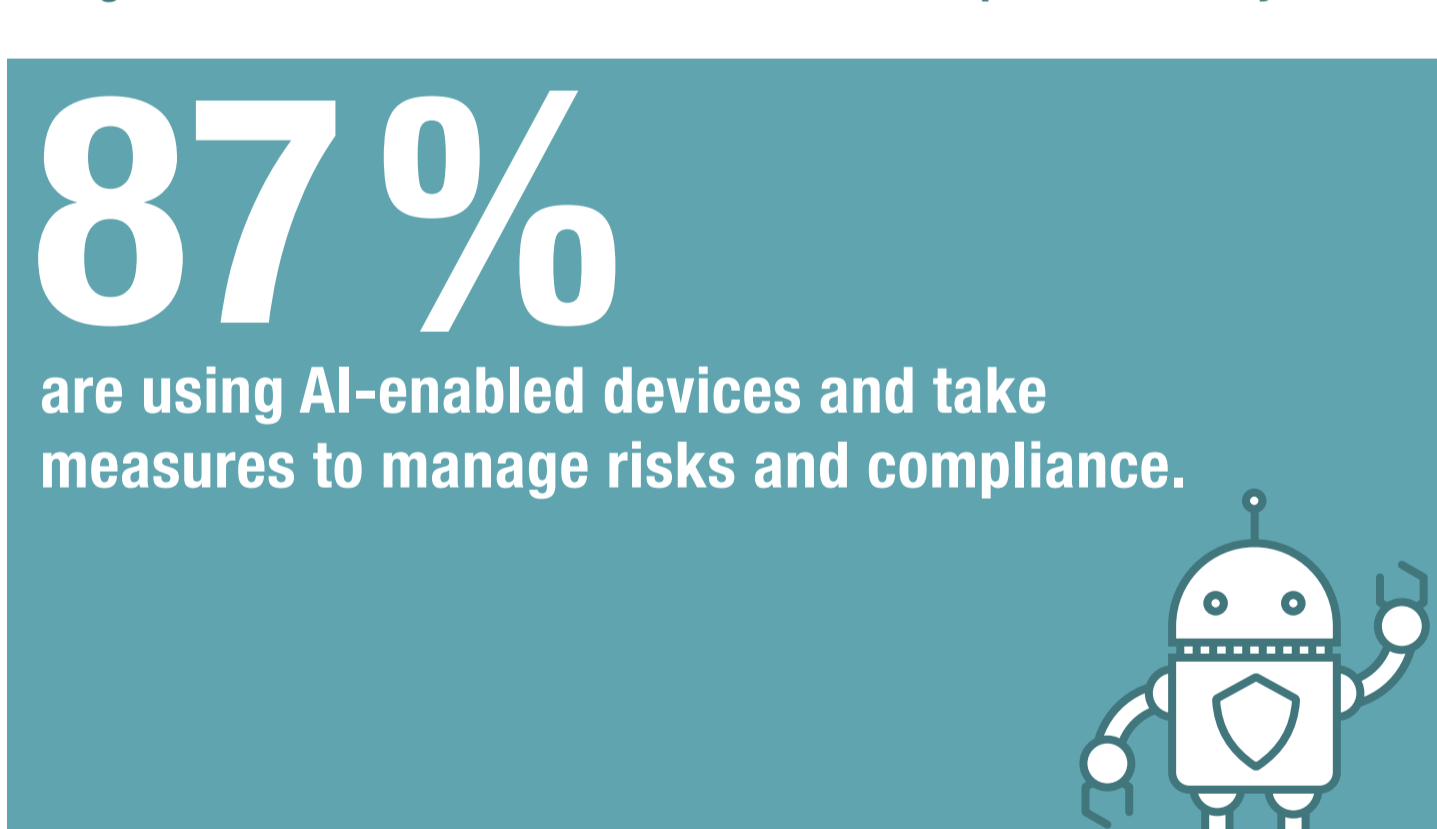
While integrating asset management into the ISMS process is valuable, many teams face obstacles when trying to do so.



ISMS requires teams to implement and monitor configurations. IT and security teams face a number of obstacles when trying to put this into practice.

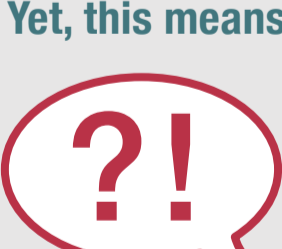


As AI becomes even more mainstream, the challenge of monitoring system configurations increases. Teams must take action to prevent security risks.



- 7% are currently not using AI-enabled devices.
- 5% are using AI-enabled devices and are currently not taking measures to manage risks and compliance.
- 1% don't know.

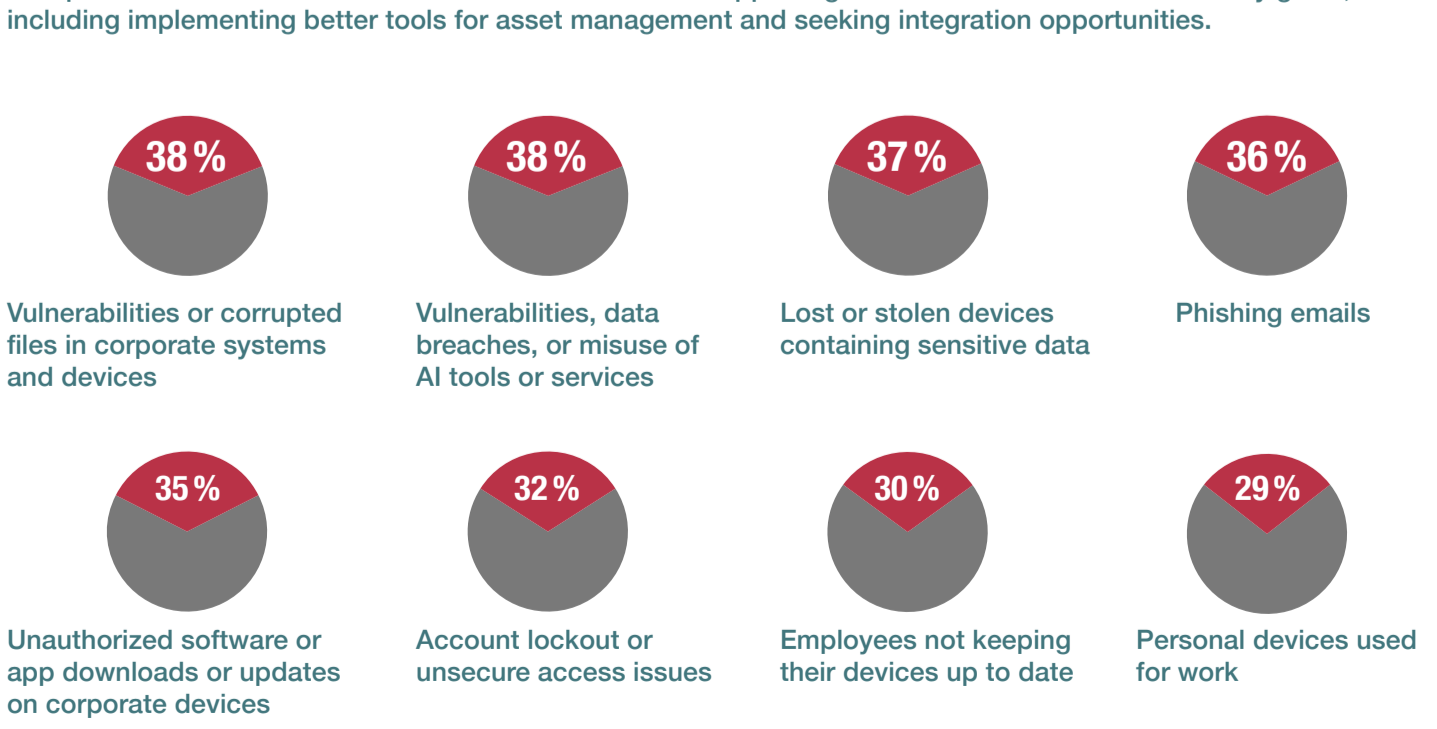
IT teams have made strides in terms of security awareness by end users. Yet, this means more and more questions start to come their way.



- 45% Concerns about suspicious e-mails or potential phishing attempts
- 38% Questions about the legitimacy of software or app downloads or updates
- 36% Concerns about the security of personal devices used for work
- 34% Notifications about the security, privacy, and potential risks for AI tools and services
- 32% Issues with logging in or securely accessing systems
- 26% Reporting lost or stolen devices containing sensitive data

Despite increasing awareness about the security risks, companies must remain vigilant.

Companies must focus their attention and resources on supporting IT teams with information security goals, including implementing better tools for asset management and seeking integration opportunities.



The data used is based on an online survey conducted by Pollfish Inc. on behalf of OTRS AG, in which 476 IT and cyber security professionals in the U.S., Germany, Brazil, Mexico, Australia and Malaysia participated between August 22 and September 17, 2024. Unless otherwise indicated, all figures refer to the average of all countries surveyed.

