IT is focused on the security benefits of IAM, and prioritizes MFA.

- **Securing data is a top priority.** 77% IT, 75% Overall Average
  - IAM is necessary for ensuring that only authorized users can access sensitive information.
  - Multiple authentication factors (MFA) are essential for providing an extra layer of security.

- **Upgrading IAM is a priority.** 61% IT, 65% Overall Average
  - Enhancing IAM systems helps improve security posture and reduce the risk of data breaches.
  - MFA adoption is crucial for achieving this outcome.

- **IAM could improve employee efficiency.** 48% IT, 53% Overall Average
  - Implementing better IAM solutions can streamline access management and reduce friction for users.
  - This can lead to improved productivity and a better overall user experience.

- **The security of IAM solutions is a challenge.** 43% IT, 40% Overall Average
  - Addressing security vulnerabilities is critical to maintaining user trust.
  - Implementing adaptive MFA can help mitigate these risks.

- **IAM should be a higher priority for my organization.** 48% IT, 44% Overall Average
  - This is important for ensuring the protection of sensitive data.
  - A strong IAM strategy is essential for safeguarding against cyber threats.

OUR RECOMMENDATIONS FOR IT:

- **Prioritize ease of use for employees.** Evaluate how users interact with IAM solutions and make sure they are user-friendly.
- **Evaluate whether their IAM approach is holistic.** Ensure that the program covers all aspects of the employee lifecycle and all access points.
- **Upgrade to adaptive MFA.** This will help in identifying and mitigating abnormal login attempts, enhancing overall security.

Learn more: https://www.lastpass.com/products/identity

Sources:
4. LastPass survey data