

Finance is focused on reducing risk, while integrating their IAM infrastructure



Financial service organizations deal with some of the most sensitive data in the business: money. Finance is dealing with higher stakes than most verticals, which inevitably impacts how they manage employee access and authentication.

Reducing risk is a priority.



Our Take: Due to the high sensitivity of the data and the associated compliance mandates in finance such as the **Financial Action Task Force (TASF), Bank Secrecy Act (BSA) and the EU's Fifth Anti-Money Laundering Directive (5AMLD)**, it's no surprise that reducing risk is a higher IAM priority for finance than most.

Hackers have gained access to my organization.



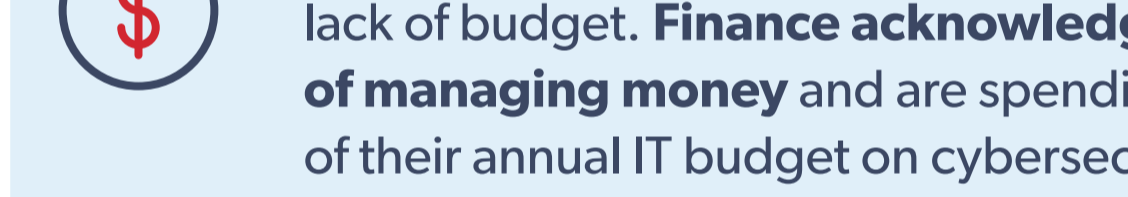
Our Take: However, when it comes to hackers gaining access, finance is struggling. Finance has historically been a target for a breadth of attacks, both the institution and their customers, and **experience the highest cybercrime costs out of all verticals** at an average of \$ US 18.3 million per year.¹

Integrating security infrastructure is my biggest area for improving.



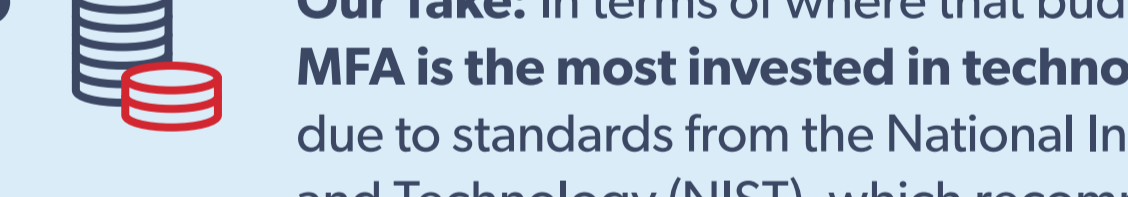
Our Take: In terms of improvements, **finance ranks integrations at the top of the list**, which offer a holistic view of user access and authentication to help reduce the unsettling percentage of hackers gaining access.

Lack of budget for IAM is a challenge.



Our Take: One area where finance is not struggling is lack of budget. **Finance acknowledges the high risks of managing money** and are spending as much as 14% of their annual IT budget on cybersecurity programs.²

I've already invested in MFA.



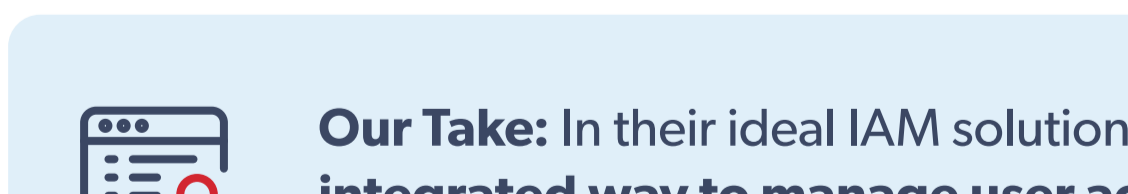
Our Take: In terms of where that budget is going, **MFA is the most invested in technology**. This is likely due to standards from the National Institute of Standards and Technology (NIST), which recommend MFA as a method to increase the security of every login attempt.

I'm planning to invest in password management.



Our Take: **Finance prioritizes password management 10% more than other verticals**, likely because their employees are sharing sensitive credentials. Password management will help finance securely manage and share passwords to meet their objective of reduced risk.

I need an integrated system to manage, monitor and set policies.



Our Take: In their ideal IAM solution, **finance wants an integrated way to manage user access and authentication**, which aligns with their priorities. This will simplify managing IAM across the organization for finance.

OUR RECOMMENDATIONS FOR FINANCE:

- Add MFA everywhere.**
MFA across applications, workstations, and VPN is a simple way to reduce risk and also makes audits and compliance mandates easier to achieve.
- Focus on integrations and flexibility.**
Consider IAM technologies that offer a variety of integrations for complete flexibility to work with your tools of choice.
- Unite IAM wherever possible.**
A unified view of employee access and authentication better enables the business to prevent potential risks.

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