LastPass
by LogMeIn

AN INDUSTRY-DRIVEN VIEW OF IDENTITY AND ACCESS MANAGEMENT

Answering the Question: How Do Verticals Shape IAM Requirements?

INTRODUCTION

Identity and access management (IAM) solutions enable organizations to seamlessly and securely connect employees to the work required for their role. IAM technologies work throughout the lifecycle of an employee – from onboarding, to delegating levels of access, managing user authentication during the workday, to offboarding when an employee leaves the organization.

However, every business and industry are unique. Take finance, for example, who are in the business of managing money. How do the finance industry's IAM priorities differ from an IT organization, who is in the business of selling technology? Both verticals need an IAM strategy to manage their employee identities, however their business models, associated risks and organizational priorities are completely different. All of these factors come together to raise the question: how do vertical requirements shape an organization's IAM requirements?

We partnered with research firm Vanson Bourne to evaluate how verticals are managing their IAM programs. We surveyed 700 IT and security professionals at organizations ranging from 250 to 2,999 employees, across a variety of industries including finance, IT and media in North America, Europe and Asia-Pacific.

In this eBook, we evaluate the research to see how IAM trends vary by sector, review how those trends impact IAM requirements and offer actionable recommendations for each vertical to optimize their IAM strategy in the coming year.

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.

70% Finance

66% Overall Average

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.

35% Finance

31% Overall Average

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.

65% Finance

57% Overall Average

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.

17% Finance

24% Overall Average

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.

55% Finance

48% Overall Average

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.

32% Finance

22% Overall Average

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.

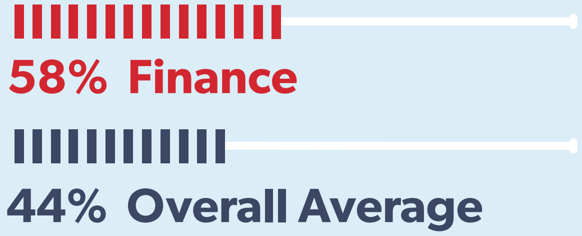
OUR RECOMMENDATIONS FOR FINANCE

Finance needs an integrated IAM solution with unified visibility and control to provide insight into which employees are accessing which resources, and when. This will help finance achieve their objectives around reducing risk as they will be able to proactively monitor and adjust security controls as needed.

To achieve this, finance first must start by integrating their security solutions together. Integrations will not only offer a unified view of end user activity, but will also help finance meet compliance mandates as they will be more simply able to report on their security posture. Reducing risk is also a top priority for finance, which can be achieved through the use of MFA solutions that ensure only the right employees are logging in, while preventing hackers from gaining access.

- **Add MFA everywhere:** applications, employee's workstations and VPN. MFA is a simple way to reduce risk and also makes audits and compliance mandates easier to achieve.
- **Focus on IAM technology** that offers 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.

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 integration priorities. This will simplify managing IAM across the organization for finance.

IT IS FOCUSED ON THE SECURITY BENEFITS OF IAM AND PRIORITIZES MFA

Information technology (IT) is any business who operates in the hardware or software markets. As businesses who are close to technology and managing customer's data, it's clear their relationship with technology impacts their IAM strategy.

Securing data is a top priority.

77% IT

75% Overall Average

Our Take: If anyone knows the potential risks of data loss, it's IT. **IT is likely managing large volumes of data -** their own, and their customer's especially if they are SaaS.

Upgrading IAM is a priority.

61% IT

65% Overall Average

Our Take: It is surprising to see that **improving IAM is less of a focus.** IT may have already upgraded their IAM solutions, or perhaps is not an area they are currently evaluating.

Integrating security infrastructure is my biggest area for improving.

48% IT

57% Overall Average

Our Take: IT is also less focused on integrations, which further suggests that IT's IAM upgrade has already occurred. This is also seen in our 2019 Global Password Security Report, which found that IT is leading the pack with both MFA adoption and security posture.[3]

The security of our IAM solutions is a challenge.

43% IT

40% Overall Average

Our Take: Employee productivity as less of a focus for IT makes sense, given the main challenge they face is security. Data breaches exposed 4.1 billion records in the first half of 2019[4], and as IT manages more amounts of customer data, maintaining control over every access point becomes increasingly complex.

IAM could improve employee efficiency.

47% IT

53% Overall Average

Our Take: Over the next year, **we can expect IT to place their efforts on improving security** with IAM as they are focused less strongly on the productivity benefits. This focus will also help IT address their priority of securing data.

IAM should be a higher priority for my organization.

48% IT

44% Overall Average

Our Take: However, IT is aware that IAM needs to be a higher priority. Every employee has access to 17 million files[5] on average, and when IT is managing customer data as well, this number not only grows but so does the need for tighter controls.

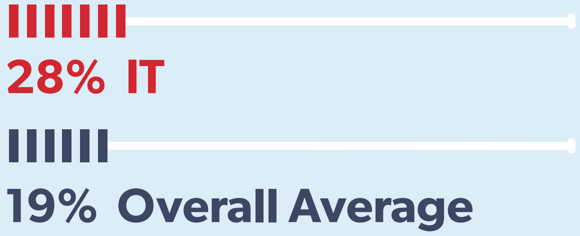
OUR RECOMMENDATIONS FOR IT

IT's main area of focus for its IAM efforts will be around security. For IT to achieve its goal, we recommend finding the right balance between increasing security, but also not impacting productivity. IT should evaluate IAM solutions that not only help increase the overall security of their organization, but also do not add friction for employees.

If a solution is difficult to use, employees will not adopt it which does not help the overarching goal of improved security. An integrated solution, also a priority, will help IT achieve this goal by offering a centralized view for management and a single solution for employees to use. In addition, while IT has many initiatives in place, it's critical for IT to ensure those IAM initiatives are covering every aspect of business – IT should consider whether its strategy covers every aspect of the identity lifecycle from employee onboarding to offboarding.

- **Prioritize ease of use for employees.** With a baseline IAM strategy already in place, now is the time for IT to focus on employee behavior to increase adoption, and ultimately company security.
- **Evaluate whether its approach to IAM is holistic;** IT should evaluate whether its current IAM program covers all aspects of the employee lifecycle and every access point in the business.
- **Upgrade to adaptive MFA.** Adaptive MFA adds increased friction for abnormal login attempts, all while enabling employees to seamlessly authenticate. This will give IT more trust in users' behavior, without getting in the way of their work.

I'm planning to invest in MFA.

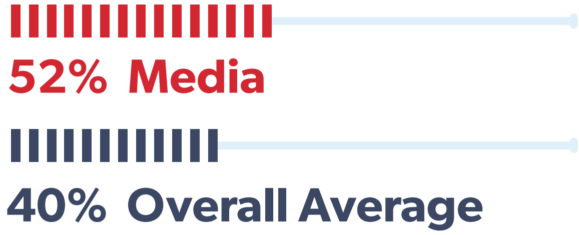


Our Take: We can expect to see IT **focus on MFA over the coming year,** which will help achieve their security challenges because MFA helps ensure only the right employees are able to access sensitive data.

MEDIA NEEDS A SECURE, AUTOMATED WAY TO MANAGE USER ACCESS

Media is the industry of mass communication: digital, social, print, television. Media works with an array of consultants to execute their programs, which leads to a wide array of users, both internally and externally, accessing business resources which complicates IAM.

Quite a lot of improvements are needed in the security behavior of my employees.

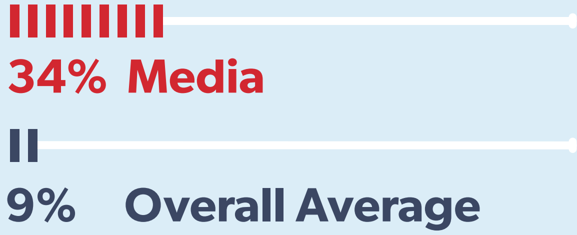


52% Media

40% Overall Average

Our Take: Media feels many security improvements are needed, likely because they work with many consultants and experience insecure sharing practices on a daily basis. Not to mention, 51% of media firms experienced 3 or more cyberattacks in 1 year.[6]

Managing user access is important to my organization.



34% Media

9% Overall Average

Our Take: Managing access is extremely important for media. If they were unable to manage access, external consultants would not be able to access their work and therefore lose productivity.

Implementing a better approach to IAM could improve employee efficiency.

60% Media

53% Overall Average

Our Take: Which is why the **productivity angle of IAM is seen higher in media.** If media is regularly working with consultants, a delay in delegating access does not only decrease productivity - it stops productivity.

Demand for an easy to use solution is a challenge.

44% Media

37% Overall Average

Our Take: Media's end users are demanding an easier to use solution as well - likely a solution that facilitates secure sharing, such as sharing social media credentials, and ways for remote teams to securely collaborate.

Achieving greater visibility over my end users is a priority.

44% Media

41% Overall Average

Our Take: Media also prioritizes greater visibility over their end users, which must be challenging given all the different consultants and solutions in place managing their diverse workforce.

Automating IAM processes is an area for improvement.

49% Media

40% Overall Average

Our Take: Automation is seen as an area of improvement for media. When working with consultants, fast onboarding and offboarding is critical - a delay in onboarding stops productivity and a delay of offboarding opens the risk of exposure.

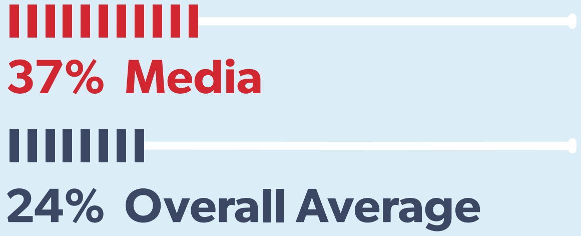
OUR RECOMMENDATIONS FOR MEDIA

Media prioritizes managing user access as its top objective for IAM. Media works with a variety of consultants and therefore needs to manage access for employees and consultants securely and in an automated way.

A delay in managing access not only decreases productivity but can stop productivity. Single sign-on is a secure method of managing user access and can quickly assign and revoke access to consultants as they onboard and offboard, which would be particularly helpful for media. When single sign-on is paired with password management, media will be able secure every app and credential not only to automate the process of delegating access, but to facilitate secure credential sharing amongst teams.

- **Consider single sign-on and password management** to address access challenges. Evaluate IAM solutions that include both, as they are easier for employees to adopt and better on budget.
- **Media should work to automate IAM processes,** so employees and contractors can gain access to get their work quickly and improve productivity.
- **Gain a unified view of end user behavior,** for both employees and contractors so you have clear visibility into end user behavior and credential sharing, and to also help facilitate the security behavior of employees.

Lack of budget is a challenge for IAM.



Our Take: However, **media is struggling to fund all the initiatives** required to address their IAM challenges and 40% are not insured or not covered for cyber incidents under their existing insurance[6], which can explain why media is facing IAM challenges.

CONCLUSION

Finance, IT and media industries each have unique business needs, and as a result have different areas of focus when it comes to their IAM program. Finance is focused on reducing risk and integrations, IT is prioritizing the security components of IAM, whereas media is focused on improving employee productivity.

A one-size-fits-all approach to IAM doesn't work when every industry and business within that industry is unique. Flexibility, breadth of functionality and ease of use are critical, so businesses can customize their IAM strategy in alignment with their business objectives. Organizations need to evaluate what their business needs are in regard to IAM and build their IAM strategy based on those requirements. It's critical to ensure that any IAM strategy is holistic, spans across the business and covers the entire lifecycle of an employee identity.

Learn how LastPass Identity offers unified identity and access management to help every industry tackle unique challenges and achieve their goals through flexible single sign-on, password management and biometric authentication in one solution.

SOURCES:

[1] - https://www.accenture.com/us-en/about/security-index?src=SOMS#block-insights-and-innovation

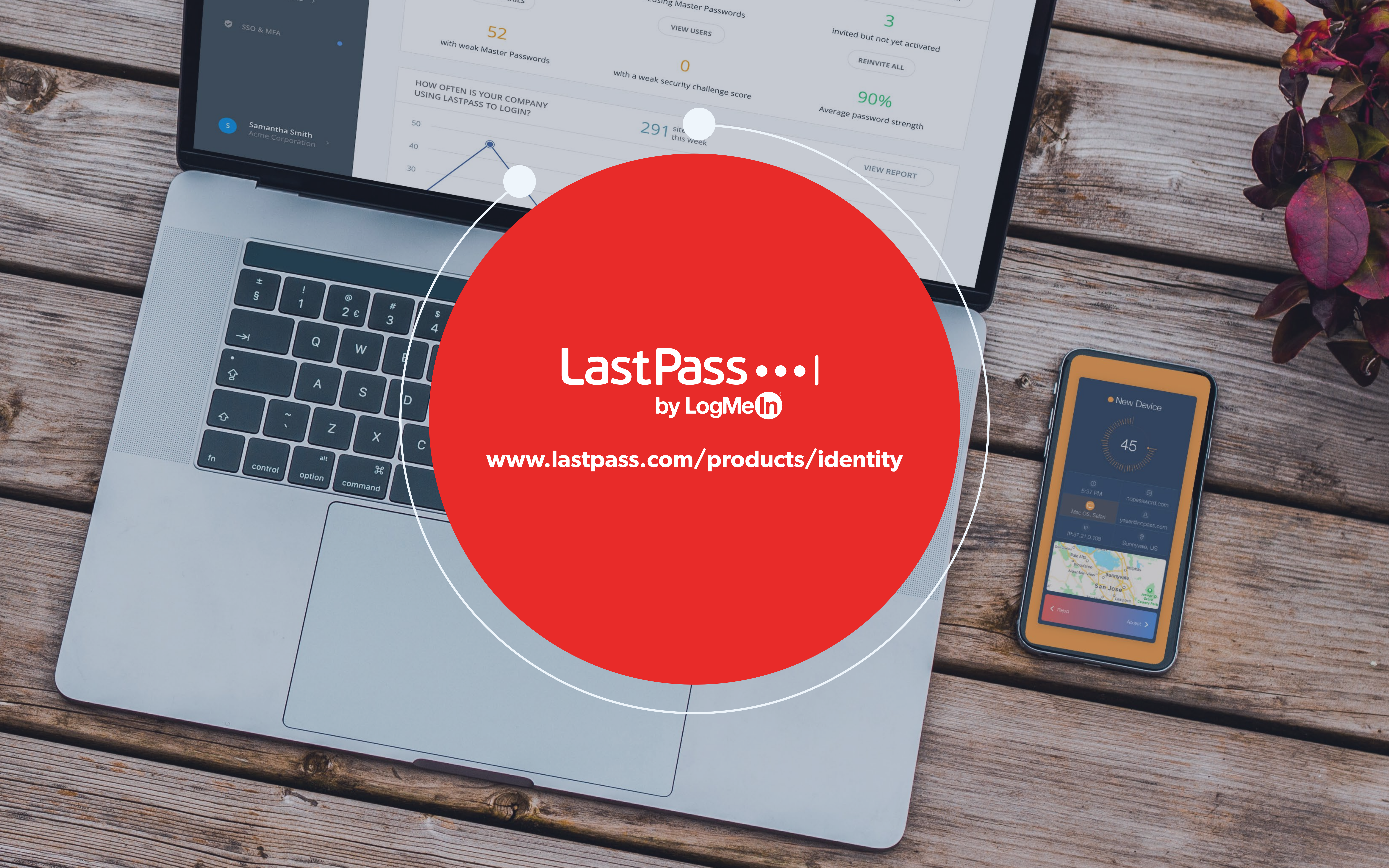
[2] https://www.pionline.com/article/20190501/ONLINE/190509988/financial-services-firms-spend-6-to-14-of-it-budget-on-cybersecurity-survey

[3] https://www.lastpass.com/state-of-the-password/global-password-security-report-2019

[4] https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

[5] https://www.varonis.com/2019-data-risk-report/

[6] https://www.securitymagazine.com/articles/89404-media-and-entertainment-industry-unprepared-for-cyber-risks



LastPass •••|

by LogMeIn

www.lastpass.com/products/identity