THE 3RD ANNUAL GLOBAL PASSWORD SECURITY REPORT

Emerging trends in access and authentication
in businesses worldwide

LastPass •••|
by LogMeIn

WHAT'S INSIDE

INTRODUCTION

In our 3rd annual Global Password Security Report, we strive to share interesting and helpful insights into employee password behavior at businesses around the world. We want to help IT and security professionals understand the greatest obstacles employees face when it comes to passwords, learn how to address challenges of managing and securing data in today's digital workplace and enable them to see how their businesses' password security practices measure up. This year, we're bringing even more data points to the table.

We've expanded our analysis of multifactor authentication usage, providing a closer look at how businesses are using this key security solution.

We've analyzed many more aspects of password security and password management to give you an in-depth look at trends over the years, from user directory integrations to policy usage, password sharing, mobile apps, password reuse and password overload. In addition, the report examines some key international regulations – the profile of which has grown significantly in the past 12 months – driving increased awareness of password security.

THEY SAY KNOWLEDGE IS POWER

Through the knowledge shared in this year's Global Password Security Report, we want to give you the power to make informed decisions about your organization's approach to password security. You can improve your organization's security, one strong password at a time.

KEY TAKEAWAYS

The clear message from this year's Global Password Security Report is businesses still have a lot of work to do in the areas of password and access security.

Businesses are increasing their use of important security measures like multifactor authentication – but unfortunately employees still have poor password hygiene that weakens the overall security posture of their company.

Even as many more businesses make the important investment in solutions to address password security and thus safeguard employee access, more action is needed after deployment to bring password hygiene up to par across the organization.

HIGHLIGHTS FROM THIS YEAR'S REPORT INCLUDE:

- **Worldwide:** More than half of businesses globally have employees using multifactor authentication
- **Progress:** IT admins take advantage of policies and integrations to increase security and streamline management, but more IT admins could be mandating the use of multifactor authentication
- **Leading:** The Netherlands emerges as a leader in security this year, with high usage of multifactor authentication and the top Security Score
- **Mobility:** The ability to access passwords on mobile significantly improves the experience – and employee adoption
- **Risk:** Password reuse is still widespread, and contributes to lower Security Scores
- **Initiatives:** Internationally, increased regulations appear to be a driving factor in password security awareness, especially in EMEA and APAC
- **Accountability:** IT organizations must take responsibility for ongoing training and take proactive measures to eliminate risky password behaviors and improve company-wide Security Scores

METHODOLOGY

Since last year's report, our data set has grown yet again as more organizations began using LastPass as their business password manager. Our approach to analyzing that data, though, has remained largely the same.

We anonymized and aggregated data from more than **47,000** organizations using LastPass. As in previous years, this report represents organizations of varying sizes, industries and regions, providing us with valuable insights into password security at a granular and global level.

Though the data set represents LastPass users, given the breadth and depth of the data set, conclusions are broad enough to be applied to the business community at large.

EXPLORE THE DATA

Review our findings and discover how the password security landscape is shifting.

MULTIFACTOR AUTHENTICATION USAGE IS ON THE RISE

The increase in businesses using multifactor authentication (MFA) is one of the biggest takeaways from this year's report, with significant gains in usage compared to our findings in 2018.

Our data shows that 57% of businesses globally are using MFA, up 12 percentage points from last year's report.

We're thrilled to see more businesses investing in security beyond the password. As multifactor authentication options continue to improve in usability and support for a wide range of use cases, we continue to see usage increase.

A QUICK NOTE

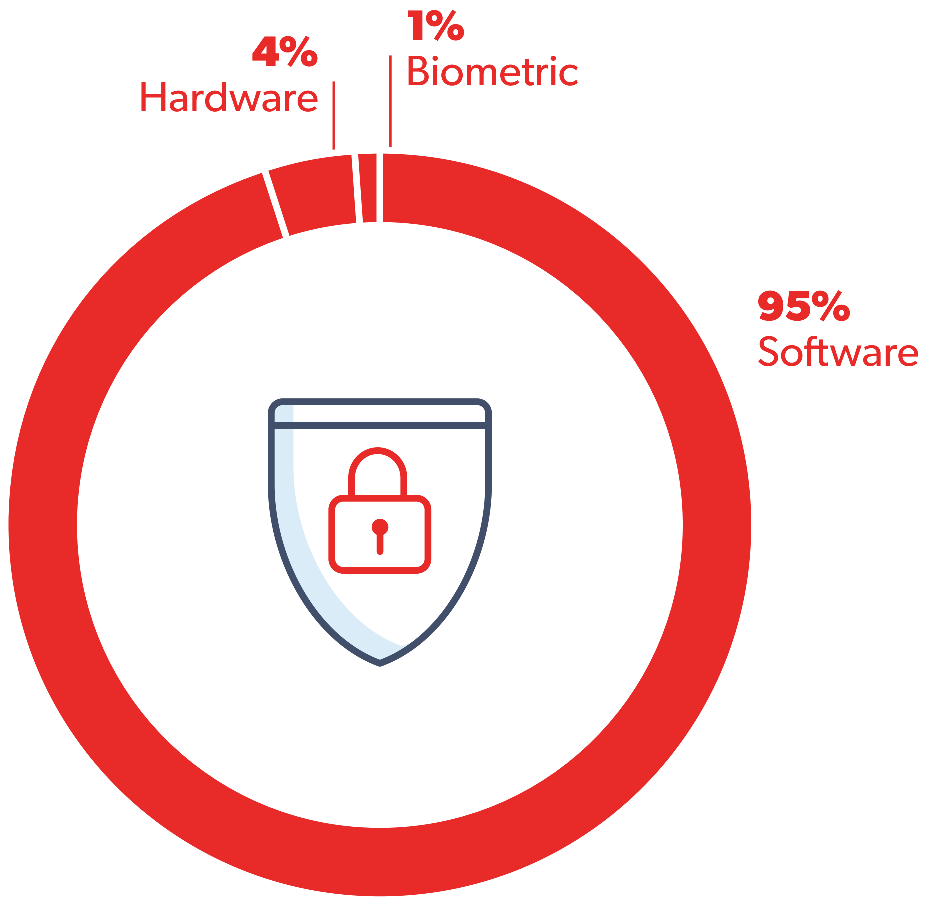
"MFA," as we're using it here, encompasses two-factor authentication (2FA). Two-factor authentication is the requirement of two separate factors to verify a user before granting them access to something. Multifactor authentication, more broadly, refers to the use of two or more separate factors in verifying and authorizing a user. The more factors in use, the stronger the overall security.

SOFTWARE-BASED MULTIFACTOR AUTHENTICATION IS THE MOST POPULAR TYPE OF MFA

Overall, **95%** of employees using MFA are using a software-based multifactor authentication option, such as a mobile app. Only **4%** use a hardware-based solution, and just **1%** use biometrics.

Given the scalability and lower cost of software-based choices, it's unsurprising that they're currently the most popular. Though biometric usage with LastPass is currently 1%, we expect to see this change dramatically in the near future as biometric options become more widely available and accessible, such as with the introduction of our new solution, LastPass MFA.

TYPE OF MFA USED BY BUSINESSES



What's next in MFA?

Other studies show that **62%** of organizations currently use biometric authentication technology and predict that nearly **90%** of businesses will use it by 2020. We expect to see these trends reflected in our own analyses in the future.[1]

[1] www.spiceworks.com/press/releases/spiceworks-study-reveals-nearly-90-percent-businesses-will-use-biometric-authentication-technology-2020/

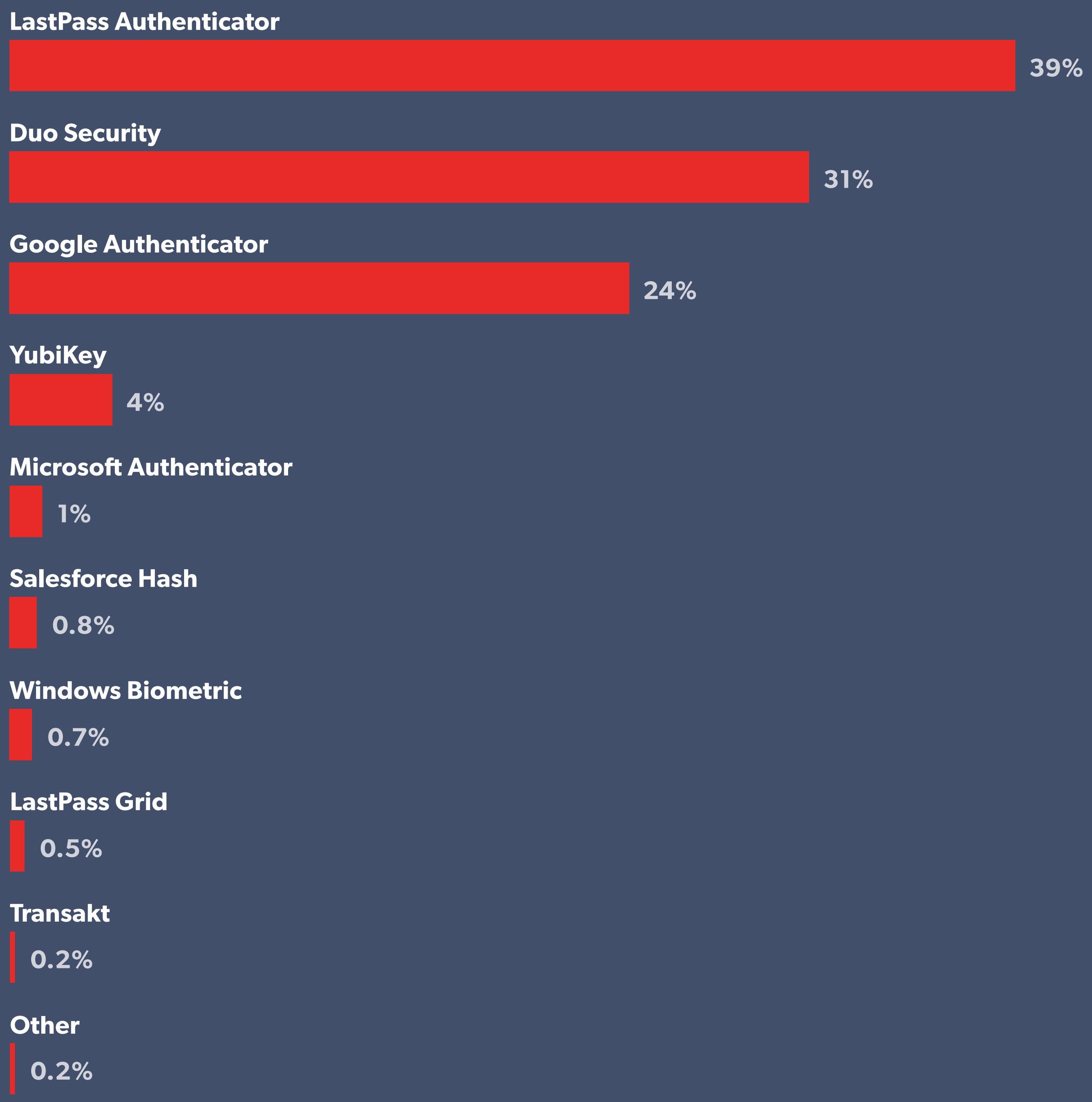
SMARTPHONE-BASED MULTFACTOR AUTHENTICATION APPS ARE THE LEADING CHOICE FOR LASTPASS USERS

Among employees using multifactor authentication with LastPass, LastPass Authenticator is the most popular option at **39%**. Other top choices include Duo Security and Google Authenticator, with **31%** and **24%** of employees using them as their chosen multifactor authentication options, respectively.[2]

These MFA options have a lot in common, so it's not surprising that they're the top three choices. All three are app-based and primarily used from an employee's smartphone. LastPass Authenticator and Duo Security both offer convenient, one-tap authentication from the phone. All three also provide the option to enter a time-based, six-digit code.

MOST POPULAR MFA OPTIONS AMONG

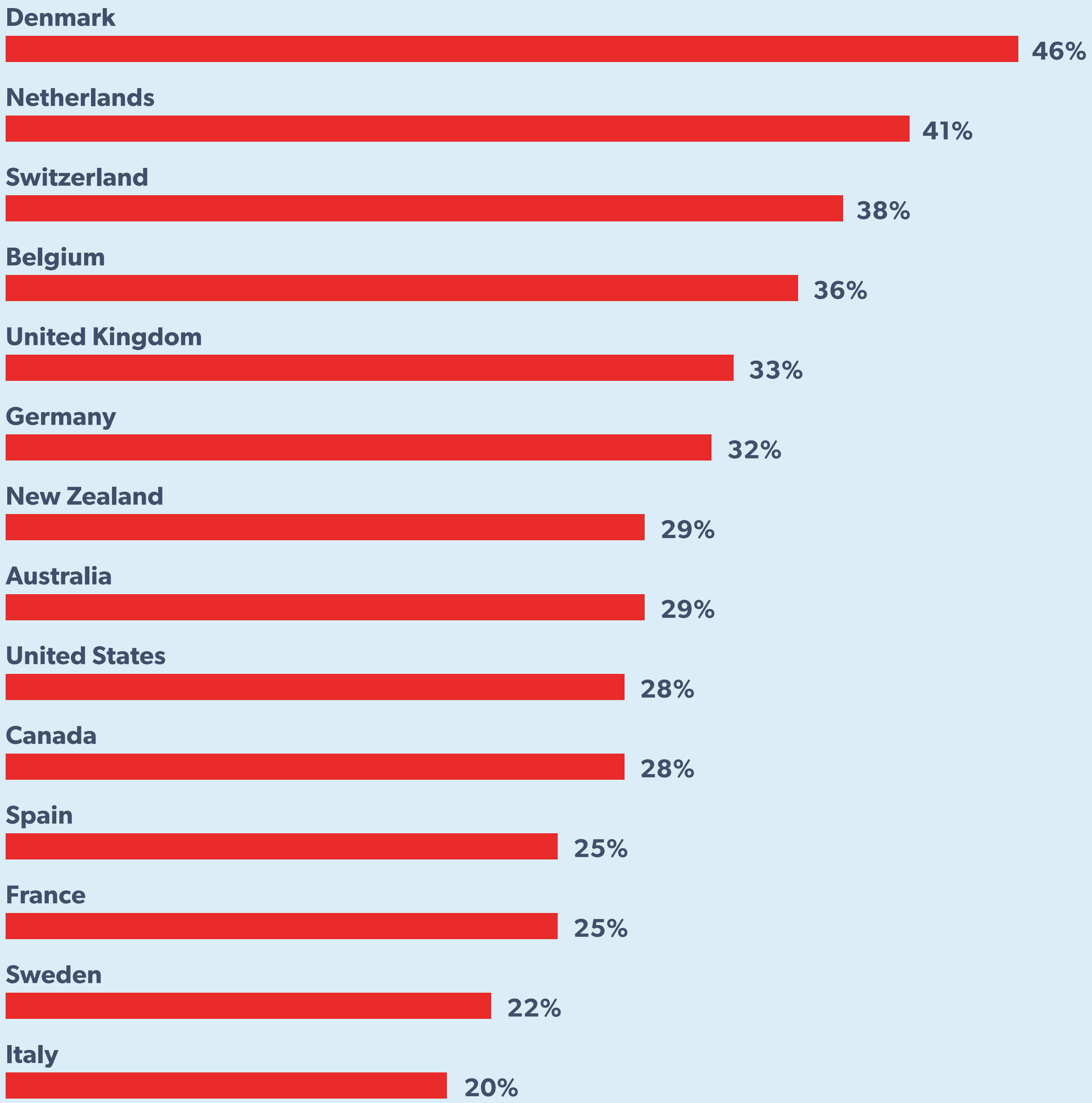
ALL BUSINESSES



**Not to scale*

[2] In 2019, LastPass launched a new solution, LastPass MFA. However, because the report analyzes data from late 2018 to early 2019, data around the new MFA solution is not included.

PERCENTAGE OF BUSINESSES WITH EMPLOYEES USING MFA BY COUNTRY



DENMARK LEADS IN MULTFACTOR AUTHENTICATION USAGE, WHILE ITALY TRAILS

It's encouraging to see overall usage of MFA increasing, but how does usage break down among professionals in different parts of the world?

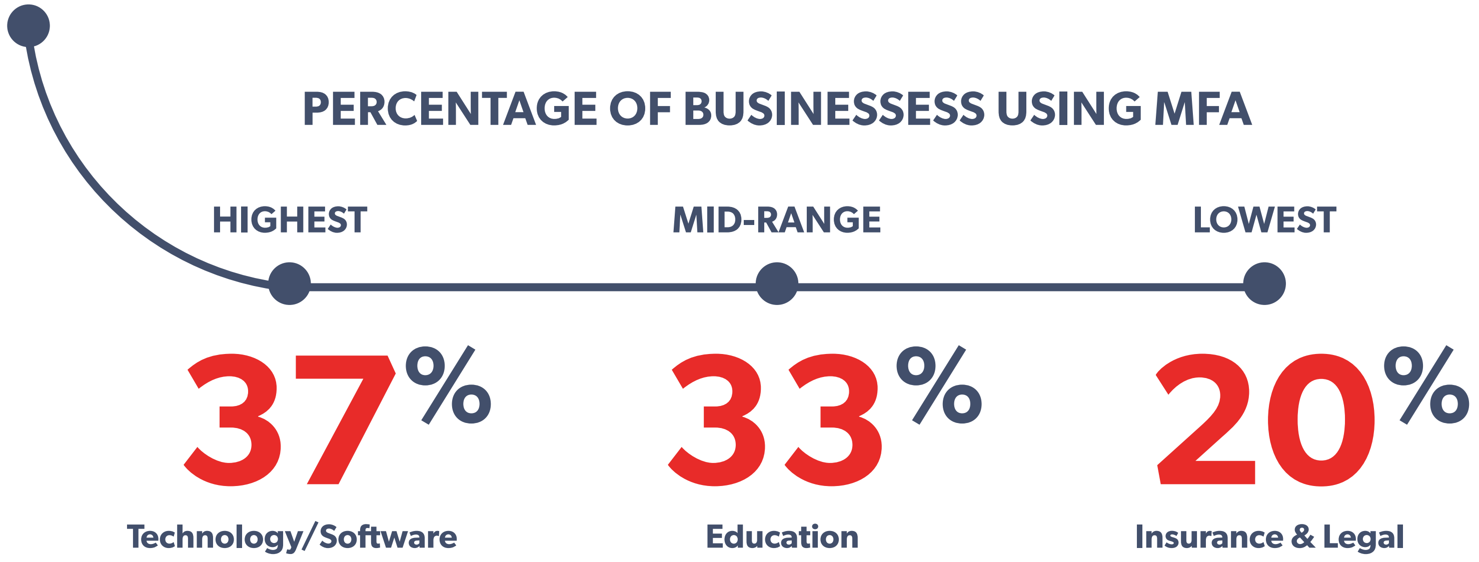
MFA usage is highest in Denmark, with the Netherlands and Switzerland close behind. Unfortunately, in countries like Italy, Sweden, Spain and France, MFA usage is significantly lower. Germany is bridging the gap between leaders and laggards, while the U.S. is slightly lower in MFA usage. As we discuss later in the report in "Global Security Initiatives & Regulations," increased regulations in places like Europe and Australia may be contributing to greater awareness and adoption of MFA.

Overall, businesses in some countries are clearly being more proactive when it comes to increasing their security, while others have more work to do in encouraging usage of MFA.

BUSINESSES IN THE TECHNOLOGY/SOFTWARE SECTOR ARE MORE LIKELY TO USE MULTFACTOR AUTHENTICATION WHILE INSURANCE AND LEGAL HAVE BEEN SLOW TO ADOPT

Compliance regulations can vary greatly from one industry to the next, so it's no surprise that some sectors are more proactive in implementing additional security solutions like MFA. Our analysis found that employees at Technology/Software companies were most often using MFA. Many Education organizations also have employees using MFA. Unfortunately, the industries that would benefit greatly from MFA due to the sensitive customer data they handle – including Insurance and Legal – are least likely to have employees using MFA.

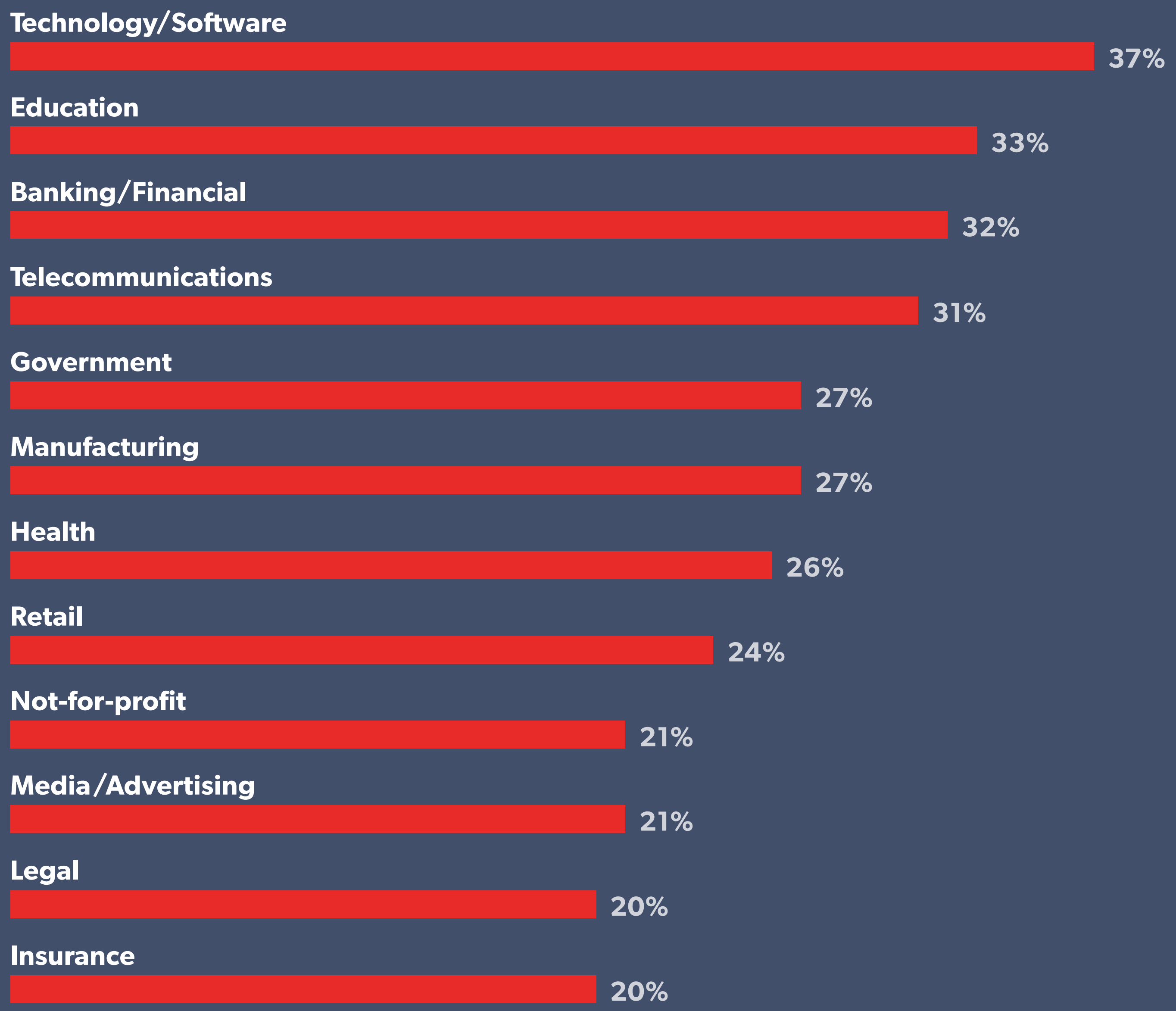
Many businesses who encourage or require employees to use MFA are likely to be significantly ahead of their peers when it comes to mitigating threats. In cybersecurity, doing the basics well often has the biggest impact on preventing the most common attacks, so expect to see more widespread usage of MFA across sectors in the coming years.



PERCENTAGE OF BUSINESSESS USING MFA

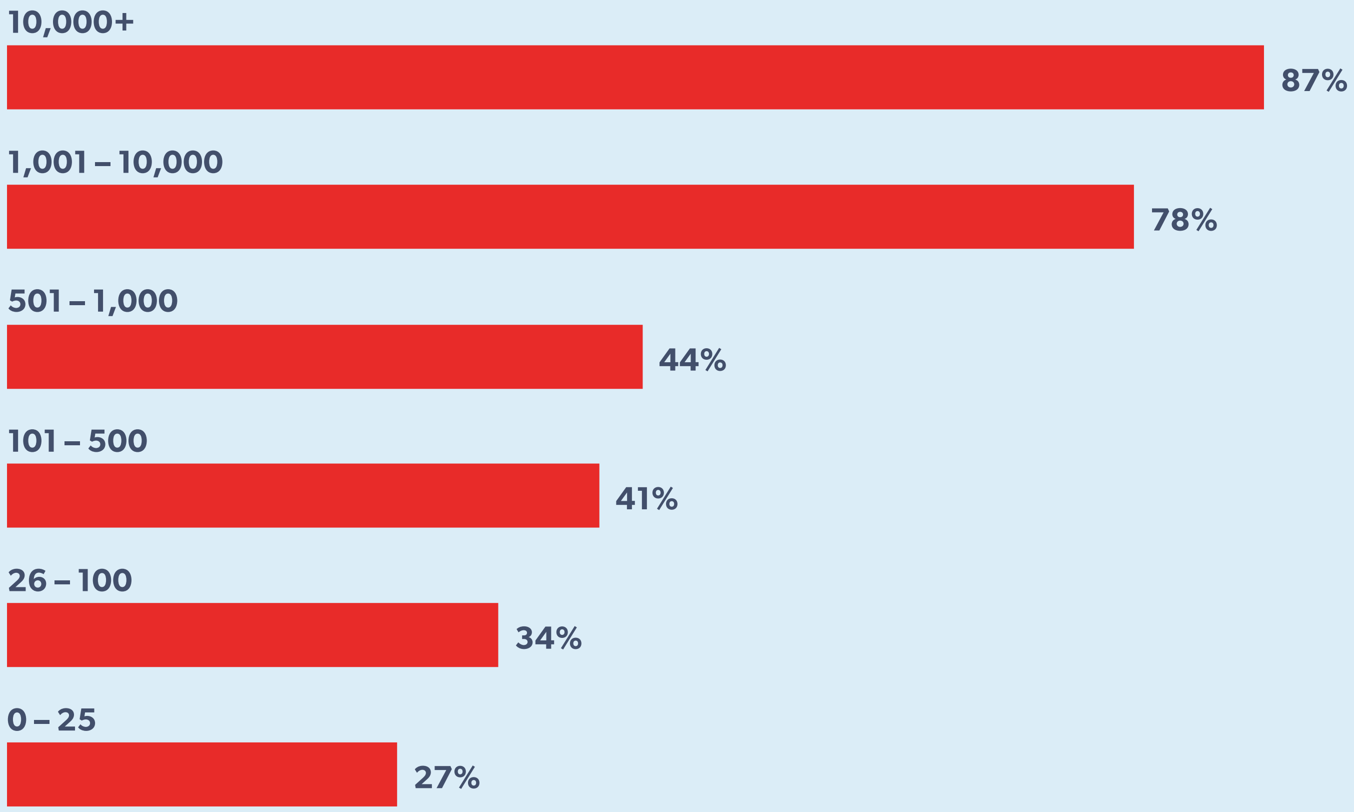
PERCENTAGE OF BUSINESSES WITH EMPLOYEES USING MFA

BY INDUSTRY



PERCENTAGE OF BUSINESSES WITH EMPLOYEES USING MFA

BY COMPANY SIZE



43% of cyberattacks are aimed at small businesses

MULTFACTOR AUTHENTICATION IS MORE COMMON AT LARGE BUSINESSES – AND SMALLER BUSINESSES HAVE SOME CATCHING UP TO DO

Perhaps unsurprisingly, employees at the largest organizations are most likely to use MFA. With thousands of employees, at least a handful are either required or choose to adopt MFA. Also, larger organizations may be subject to more policies and regulations, making it more likely they will turn on MFA (especially IT and security administrators).

Unfortunately, less than a third of the smallest businesses have employees using MFA. We interpret this to mean that either businesses of 1,000 employees or fewer are less familiar with MFA or it's not a priority – which is understandable when you have IT staff who are likely juggling many responsibilities and competing priorities. However, according to the 2019 Verizon Data Breach Investigations Report, **43%** of cyberattacks are aimed at small businesses.[3] Plus, **60%** of small and midsized businesses that are hacked go out of business within six months.[4] Even though businesses with fewer than 1,000 employees may feel like they "fly under the radar," the data says otherwise.

> **In short, no matter the size of the business, multifactor authentication should be part of the "technology stack."** Given the number of affordable, user-friendly options available, every business should be able to find an MFA solution that meets their needs.

[3] https://enterprise.verizon.com/resources/reports/dbir/

[4] National Cyber Security Alliance

WHEN IT COMES TO CUSTOMIZABLE PASSWORD MANAGEMENT POLICIES, IT PROFESSIONALS SEEK ADDED SECURITY AND GREATER CONTROL

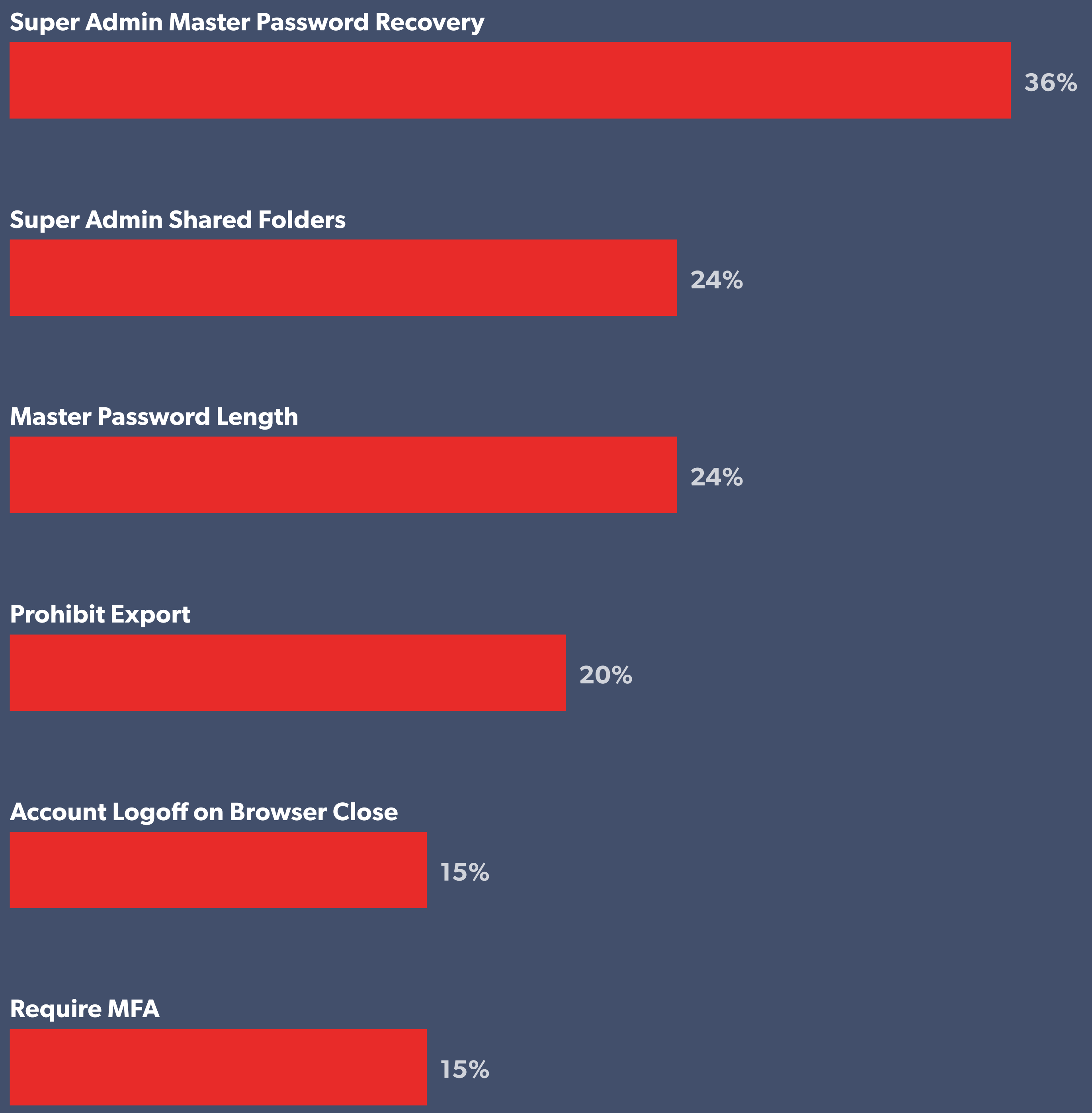
Where are administrators enforcing added protection for user access? Beyond the default policies that provide a standard level of security, many businesses are opting to enable or modify additional policies for extra security and admin control.

For LastPass users, the Super Admin Master Password Recovery policy is the most popular, affording LastPass admins the ability to reset a user's Master Password. Even when users only have one Master Password to remember, admins clearly prioritize a failsafe for forgotten passwords.

The Super Admin Shared Folders policy is also enabled by **24%** of admins, allowing admins the ability to view and edit all Shared Folders in use across the organization. It's clear that expanding admin privileges to provide greater control and flexibility is especially important in the context of password management. Additional popular policies focus on added security. **Many admins want to enforce stronger Master Passwords, and prevent employees from being able to use or export any work passwords if they ever leave the organization.**

Other precautions include logging out of LastPass when a user's browsing session ends and requiring multifactor authentication. As shown in previous sections, quite a few businesses have employees using MFA. However, given the important security benefits it provides, we hope to see an increasing number of businesses enforcing, and not just recommending, multifactor authentication.

MOST POPULAR CUSTOMIZABLE POLICIES IN **LASTPASS**



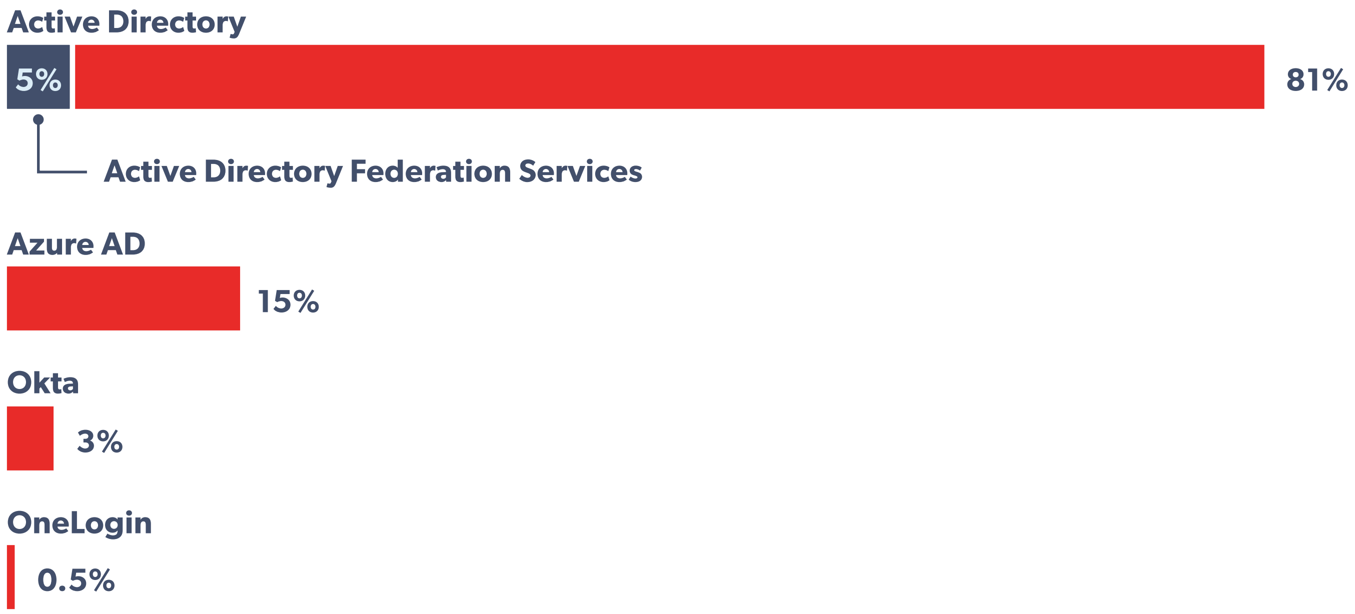
Most businesses maintain a user directory, which allows them to track who works for the organization, as well as what technology and resources those people need access to.

According to our data, **25%** of businesses have taken advantage of the benefits offered by integrating a password manager with their user directory. Doing so helps automate onboarding, offboarding, and other day-to-day management tasks.

Of the businesses that have enabled directory sync, the majority **(81%)** are using the Active Directory client. Another **15%** are using Azure AD. Though less common, some businesses are also using their Single Sign-On provider as a user directory, with **3%** using Okta and 0.5% using OneLogin.

Of businesses using Active Directory, **5%** have also enabled federated login with Active Directory Federation Services (ADFS). This allows employees to access their password manager with their Active Directory password, thereby simplifying the LastPass experience. Given that this is a recently launched feature for LastPass, we expect to see usage rise in the future.

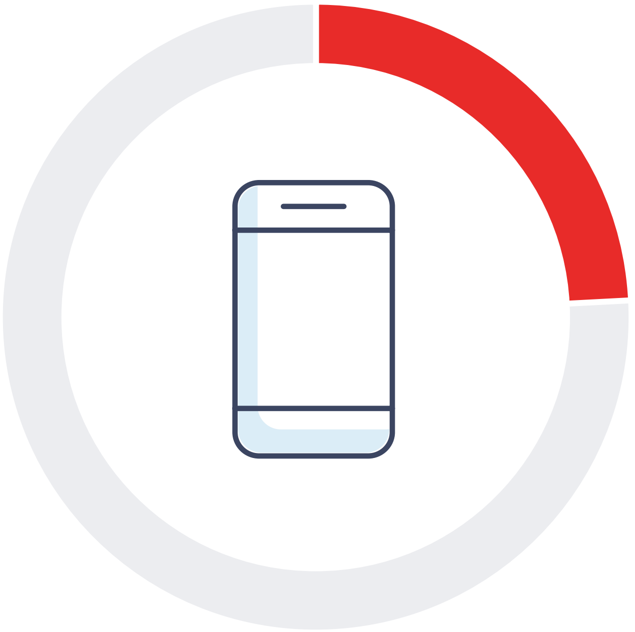
POPULAR IDENTITY PROVIDERS AMONG BUSINESSES USING DIRECTORY INTEGRATION WITH LASTPASS



25% of businesses are automating password management deployments with a user directory integration.

MOBILE USAGE IS ON THE RISE – AND LEADS TO BETTER PASSWORD MANAGER ADOPTION RATES AMONG EMPLOYEES

New to this year's report, we looked at how employees are using their password manager on mobile devices. One thing is clear: when it's convenient for employees to access and use passwords from their smartphone or another device of their choice, they're more likely to use their password manager. The option to save and fill passwords on all devices provides a much better experience overall, according to the data.



Globally,

23%

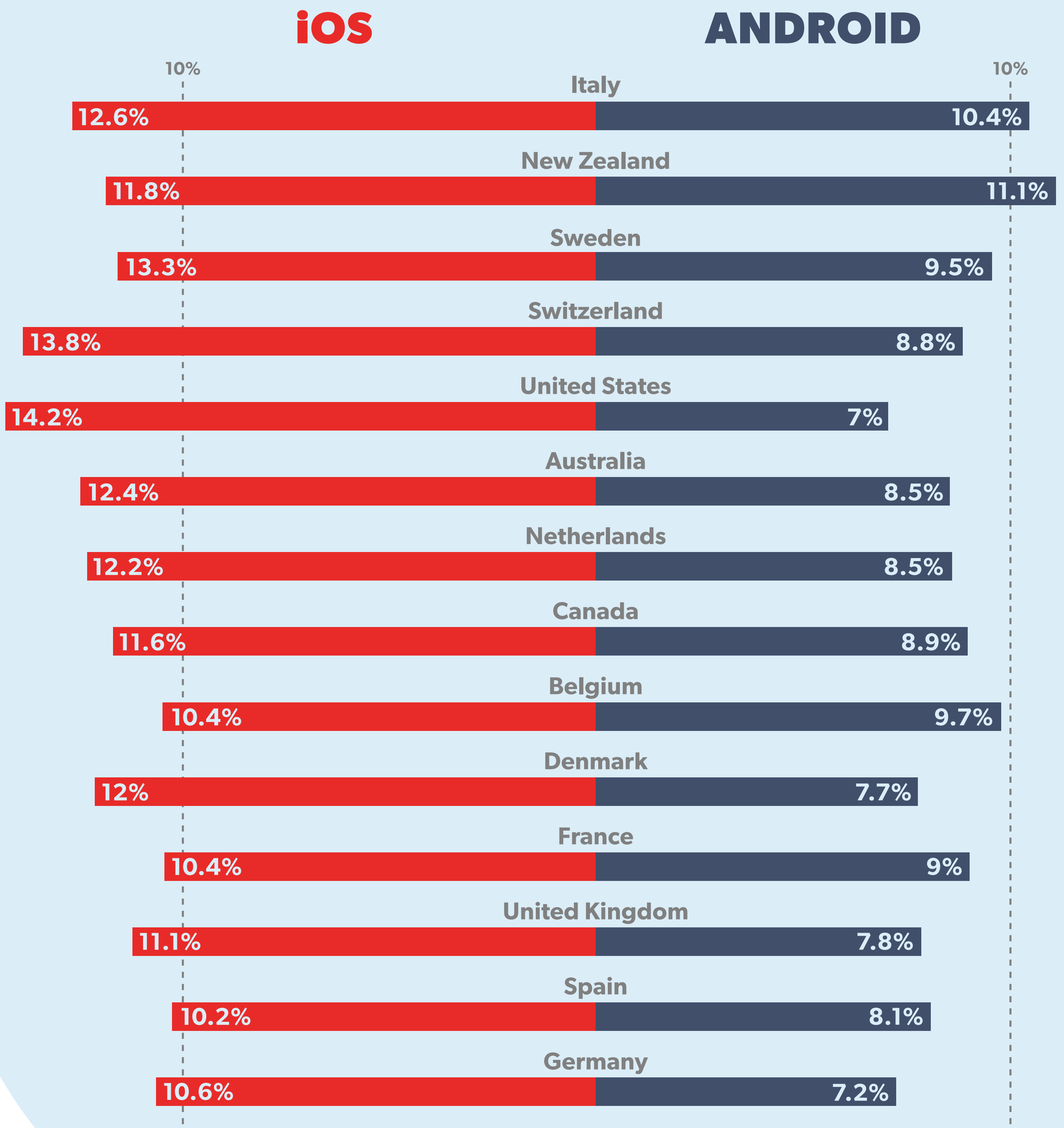
of employees are accessing their password vaults on their smartphone, with 14% using the LastPass iOS app and 9% using the LastPass Android app.

The United States leads in iOS usage: **14%** of businesses have employees using the iOS app to store and fill their passwords. When it comes to Android, though, the U.S. trails – only **7%** of businesses have employees using that platform. Businesses in New Zealand lead when it comes to usage on Android – **11%** have employees accessing their passwords on the Android app. Interestingly, both Italy and Sweden have comparatively high usage on both Android and iOS, showing better adoption across mobile in those countries.

Improvements in mobile platform integrations with password managers have certainly played a role in their increased adoption. After the launch of iOS 12, for example, we saw people interact with the LastPass app more, using LastPass 50% more frequently to log in to apps and sites from their mobile device than previously on their iPhones. iOS 12 changed the landscape for password managers on iPhones, with a positive impact on mobile app usage in the workplace, too.

Overall, it looks like using mobile as part of the onboarding for an Enterprise Password Management solution greatly increases the chances that employees will continue using LastPass. **User retention is about 30% higher on average when mobile usage is incorporated into the onboarding experience.** IT professionals should strongly consider including training about mobile password management features and benefits in their deployment plan when implementing, or continuing to invest in, an Enterprise Password Management solution.

EMPLOYEE USAGE OF THE LASTPASS APP BY OPERATING SYSTEM
PER COUNTRY



PASSWORD SHARING REMAINS A REALITY IN MOST BUSINESSES

As we've discussed in past reports, password sharing is a common practice in most businesses. Many departments or teams may have just one or two licenses for a service that needs to be accessed by several employees, or shared with external contractors or organizations. Once again, our analysis shows that password sharing is alive and well, reinforcing the need for businesses to have a solution in place that facilitates secure, encrypted sharing. **It's not a matter of if employees will share passwords, it's a matter of how securely.**

On average, a business uses 185 shared folders.

This year, we looked at password sharing at the company level to understand the true scale of shared items within a typical business. Without visibility into and oversight of those shared credentials, the average business faces significantly increased security risks.

THE PASSWORD STRUGGLE IS REAL FOR EMPLOYEES, ESPECIALLY AT SMALLER BUSINESSES

Over the years, there's been an alarming increase in the number of passwords the average person must remember. While cloud apps, mobile apps and any number of new technologies have brought many positive changes to the workplace, they've also introduced a plethora of passwords that employees struggle to keep track of. And as we all know, an overwhelming number of passwords leads to poor password hygiene when there's no technology in place to help.

The smallest businesses struggle with the most passwords, while employees at larger companies have notably less passwords to worry about. We can make some guesses as to why. Due to resources and regulations, larger businesses may be more likely to have Single Sign-On solutions in place that enable employees to access more apps with fewer passwords. Employees may also have less flexibility in the types of services they're allowed to use.

> **Regardless, it's clear that employees at businesses of all sizes still have far too many passwords to remember on their own, and each one of those passwords is an access point to the business that needs to be properly secured.**

SMALL BUSINESSES (1 – 25 EMPLOYEES)

85 **average passwords per employee**

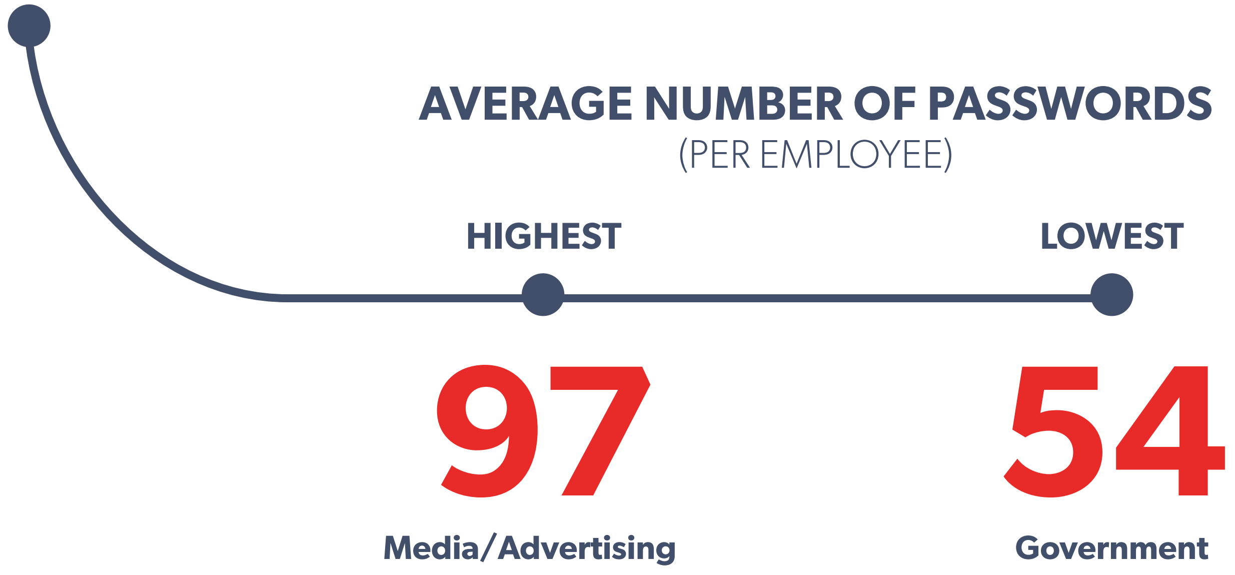
LARGER COMPANIES (1,001 – 10,000 EMPLOYEES)

25 **average passwords per employee**

Less than 50% of businesses have an SSO solution

EMPLOYEES IN THE MEDIA/ADVERTISING INDUSTRY JUGGLE THE MOST PASSWORDS

Who knew there could be such a difference in the number of passwords an employee has to use across different industries? Our data shows that employees in some industries have significantly more passwords to remember.



AVERAGE NUMBER OF PASSWORDS

(PER EMPLOYEE)

HIGHEST

97

Media/Advertising

LOWEST

54

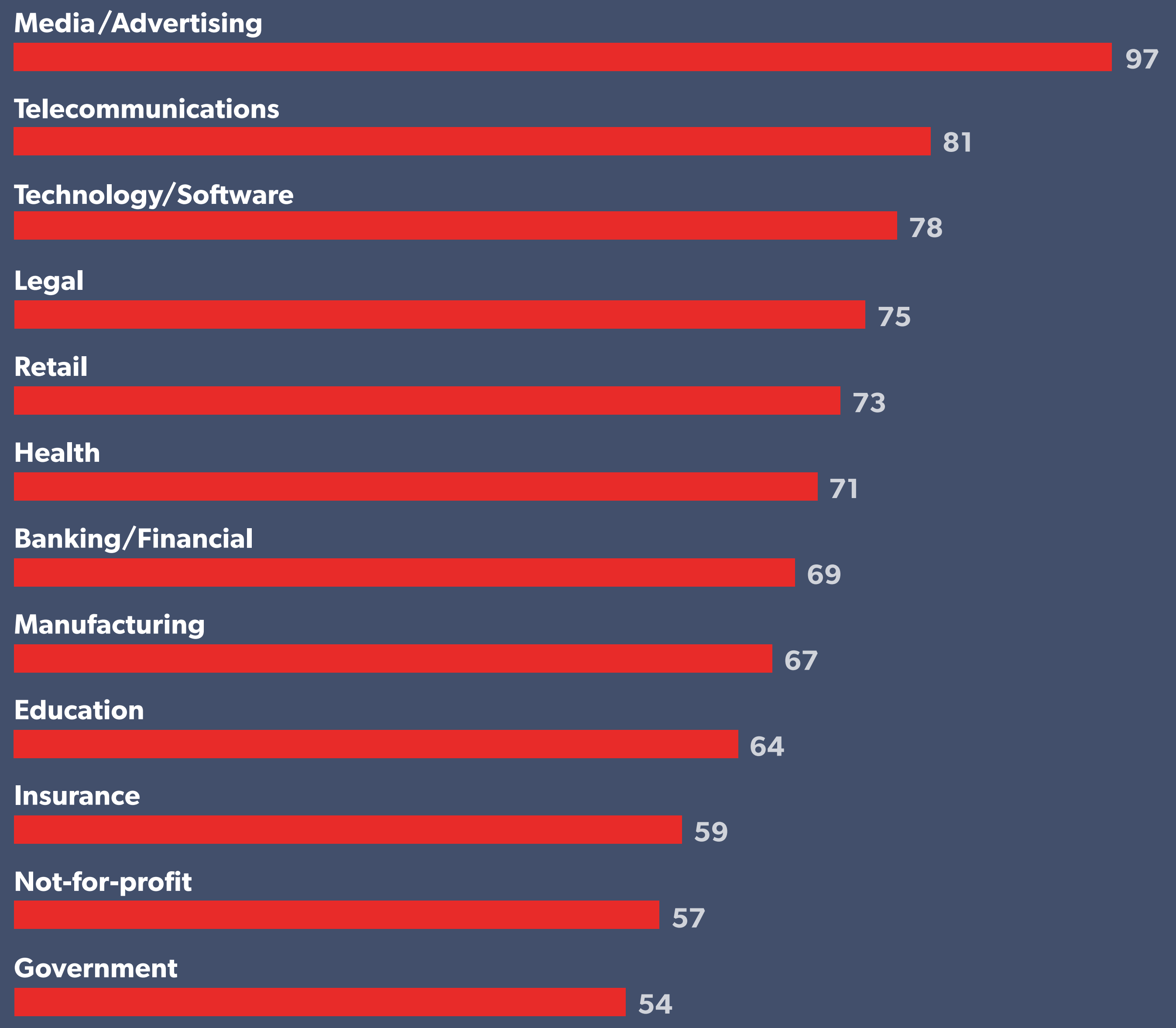
Government

Why the difference?

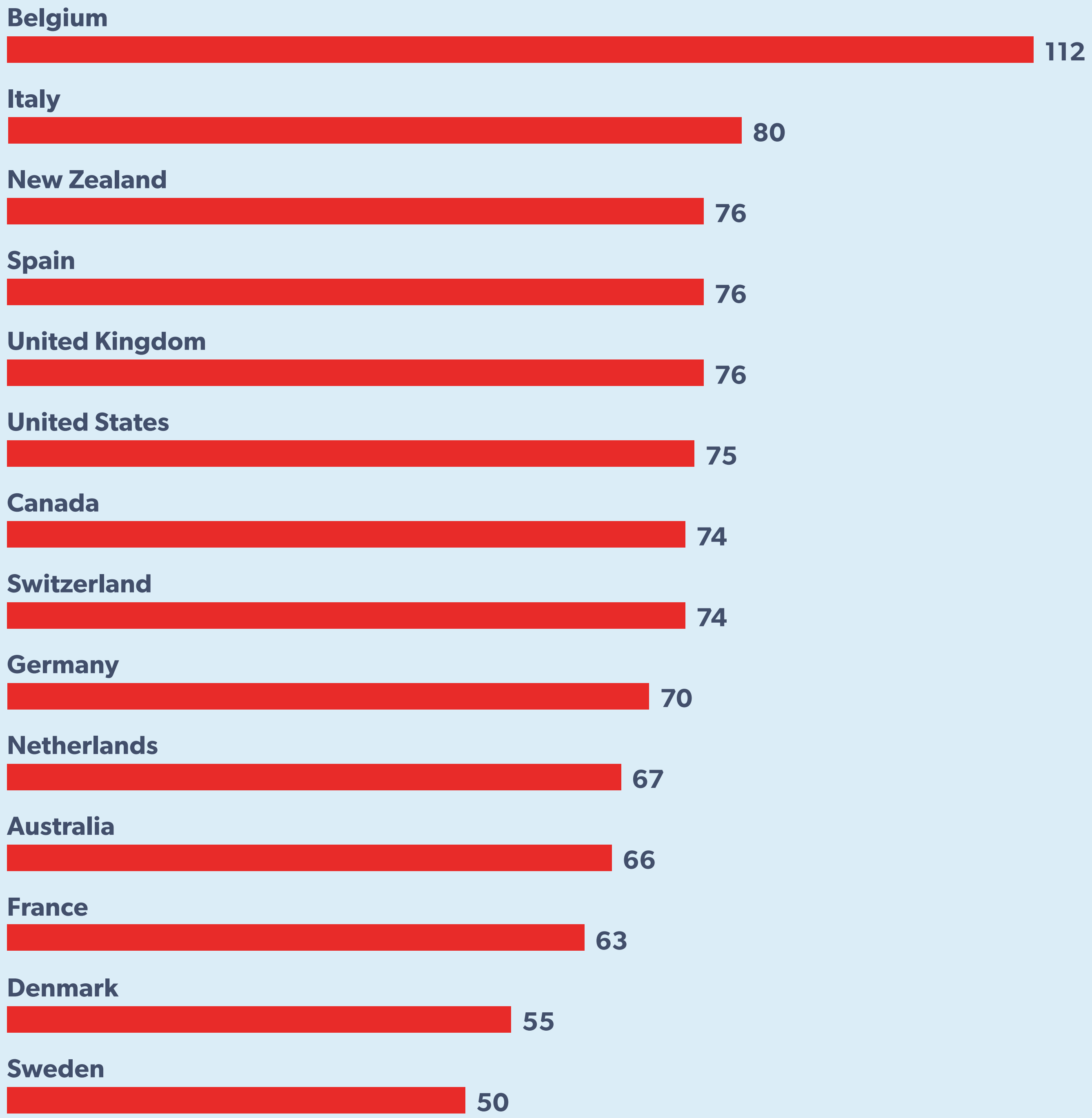
Some industries may be more likely to readily adopt more technology and apps. Some sectors may naturally manage more accounts, especially Media/Advertising firms that may be working with many clients and managing multiple accounts for those clients at any given time. One thing's for sure: if every employee has even 50 passwords to remember, it's in a business's best interest to ensure they're as strong as possible and managed in a way that relieves the password burden for their employees.

AVERAGE NUMBER OF PASSWORDS PER EMPLOYEE,

BY INDUSTRY

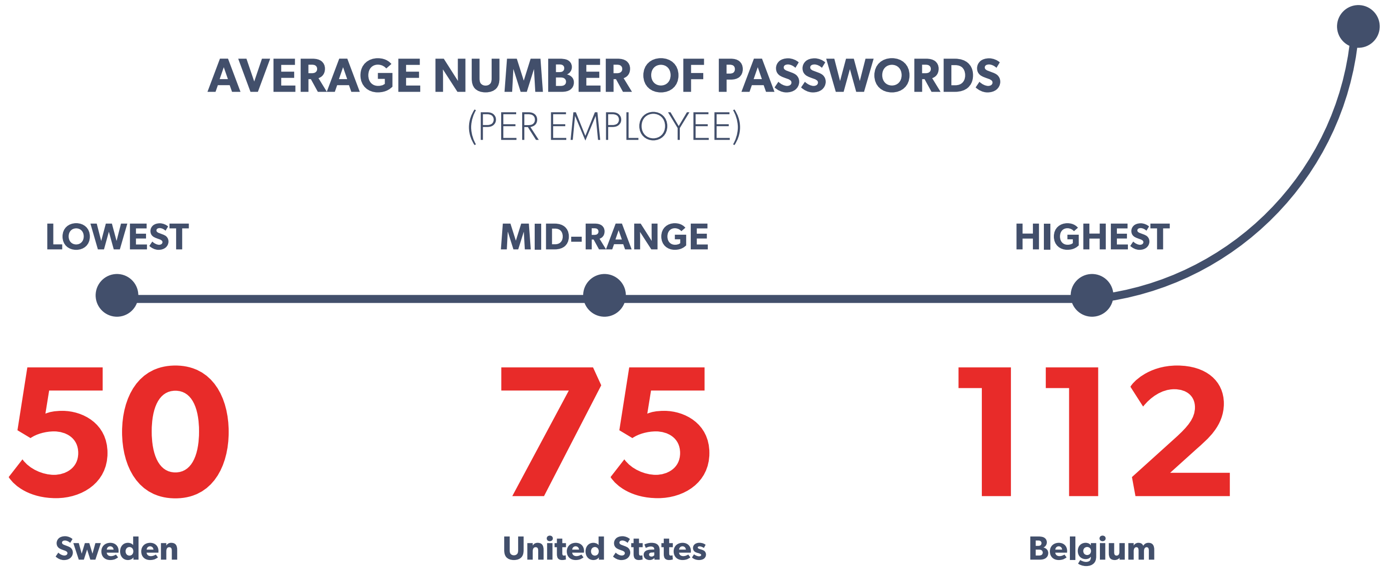


AVERAGE NUMBER OF PASSWORDS PER EMPLOYEE, BY COUNTRY



EMPLOYEES IN BELGIUM ARE ABSOLUTELY SWIMMING IN PASSWORDS – WHILE EMPLOYEES IN FRANCE HAVE IT A LITTLE EASIER

Much like the analysis on password usage by industry, we were equally surprised to find such a range of employee password usage across countries.



AVERAGE NUMBER OF PASSWORDS
(PER EMPLOYEE)

LOWEST	MID-RANGE	HIGHEST
50	75	112
Sweden	United States	Belgium

PASSWORD REUSE IS STILL A WIDESPREAD PROBLEM, BUT SMALLER BUSINESSES STRUGGLE THE MOST

It's now fairly common knowledge that reusing passwords is bad. So why do people still do it? Mainly because employees don't want to have to think of and remember complex passwords. They just want memorable passwords so they can log in to accounts quickly and easily. Of course, once employees start using a password manager, the need to reuse passwords is eliminated, but they do need to remember to change passwords with new, randomly generated ones.

> *Our data shows that employees reuse a password an average of **13 times.***

The risk, of course, is that a stolen or compromised password for one account means an attacker might have the password they need to access several other accounts. The 2019 Verizon Data Breach Investigations Report (DBIR) confirms that stolen and reused credentials are implicated in **80%** of hacking-related breaches.

One of the most effective steps a business can take to reduce the risk of breach is to enable employees to get unique, complex passwords that are the most difficult to steal.

BUSINESSES WITH FEWER THAN 1,000 EMPLOYEES TEND TO HAVE THE HIGHEST RATES OF PASSWORD REUSE

Perhaps smaller businesses have less strict password security policies, or employees aren't as concerned about replacing old, duplicated passwords with newer, generated ones. Smaller businesses need to prioritize replacing passwords with randomized ones and gain visibility of password hygiene across the business by using a password manager.

AVERAGE NUMBER OF REUSED PASSWORDS

HIGHEST

10-14

Less than 1,000 employeees

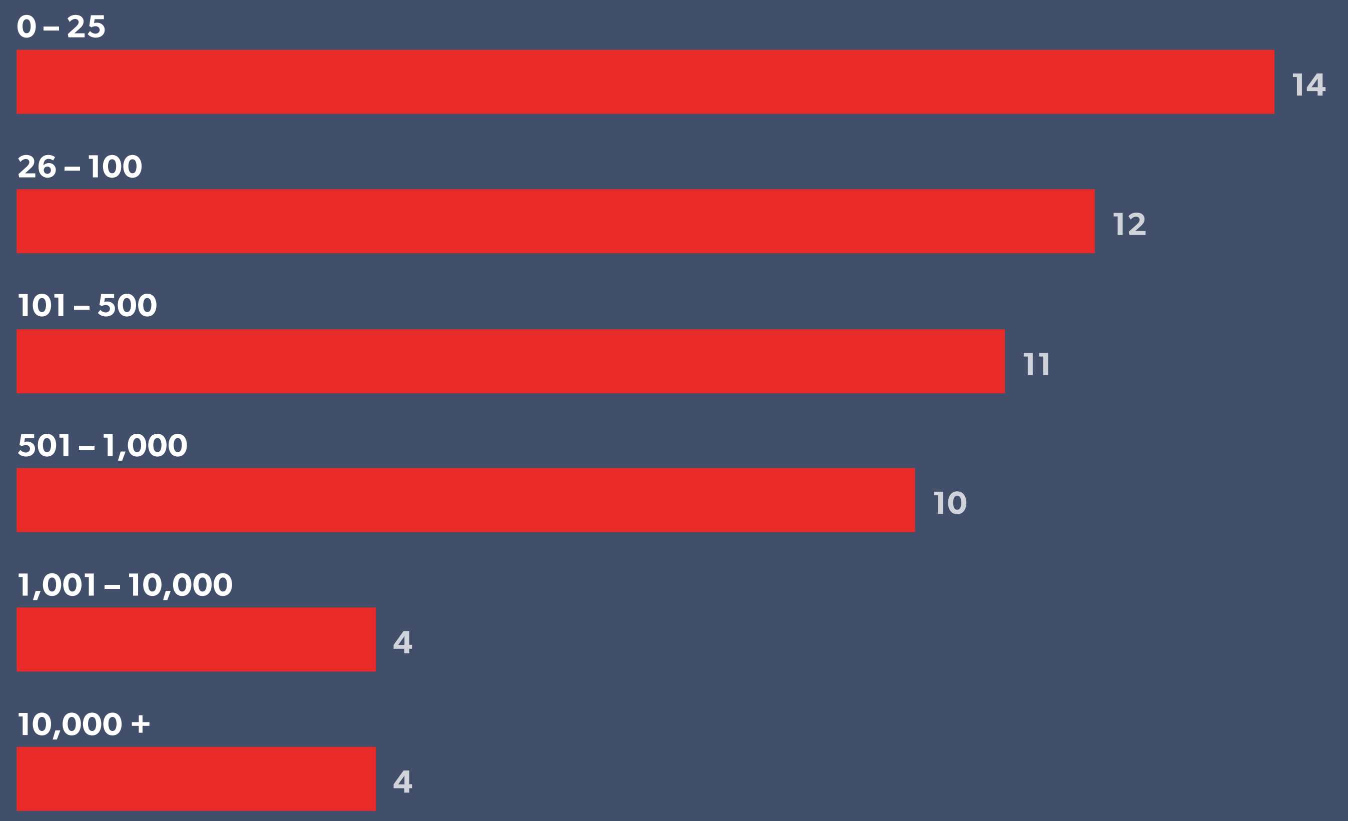
LOWEST

4

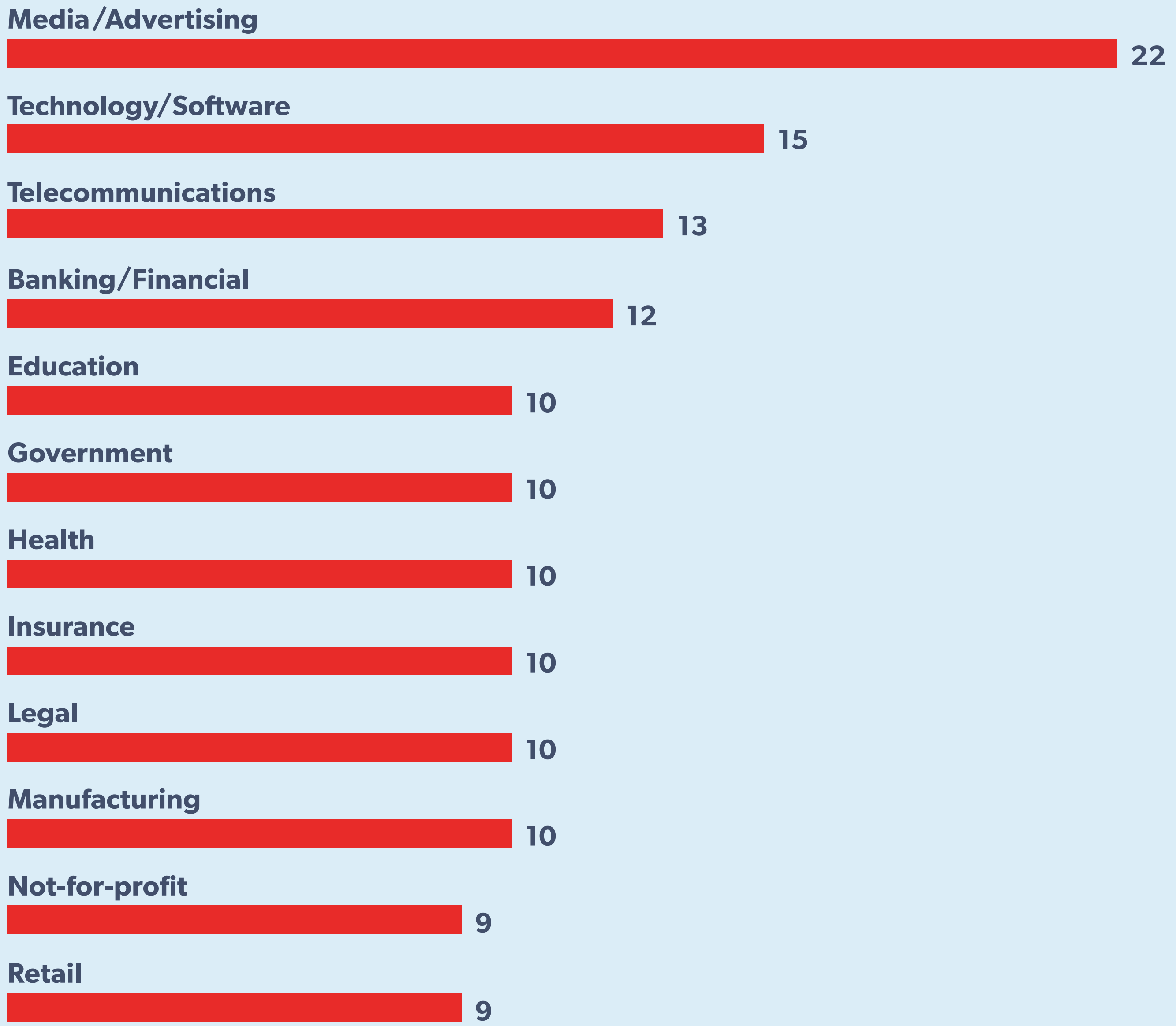
More than 1,000 employeees

AVERAGE NUMBER OF REUSED PASSWORDS

BY COMPANY SIZE



AVERAGE NUMBER OF REUSED PASSWORDS BY INDUSTRY



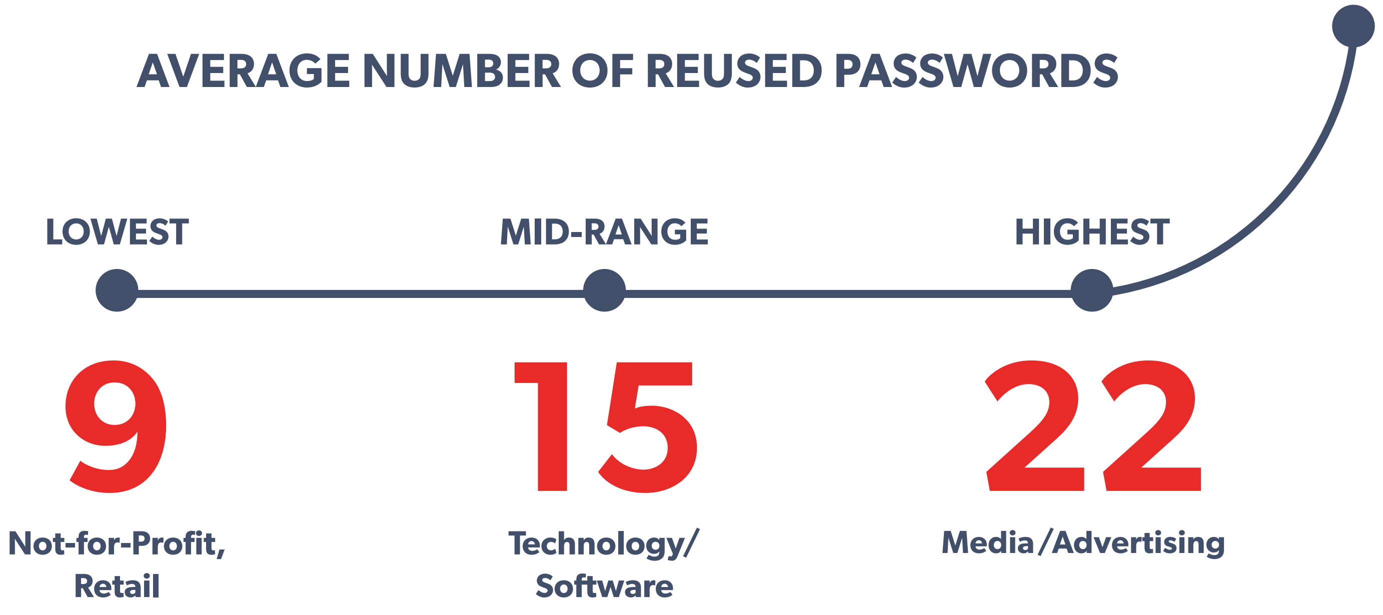
EMPLOYEES AT MEDIA/ADVERTISING ORGANIZATIONS ARE STRUGGLING THE MOST WITH PASSWORD REUSE

When we look at password reuse across different sectors, employees at most businesses are performing about the same. There are, however, a few outliers.

Employees working in Media/Advertising tend to reuse passwords at almost twice the rate of other industries.

No amount of password reuse is safe, but it's clear some sectors have a lot more work to do when it comes to reducing password reuse in the workplace.

AVERAGE NUMBER OF REUSED PASSWORDS



LOWEST
9
Not-for-Profit, Retail

MID-RANGE
15
Technology/Software

HIGHEST
22
Media/Advertising

BUSINESSES IN CANADA NEED TO WATCH OUT FOR PASSWORD REUSE

When looking at password reuse across different locales, the averages are slightly less dramatic. Geography seems to matter much less than company size and sector when it comes to password reuse.

AVERAGE NUMBER OF REUSED PASSWORDS

HIGHEST

15

Canada

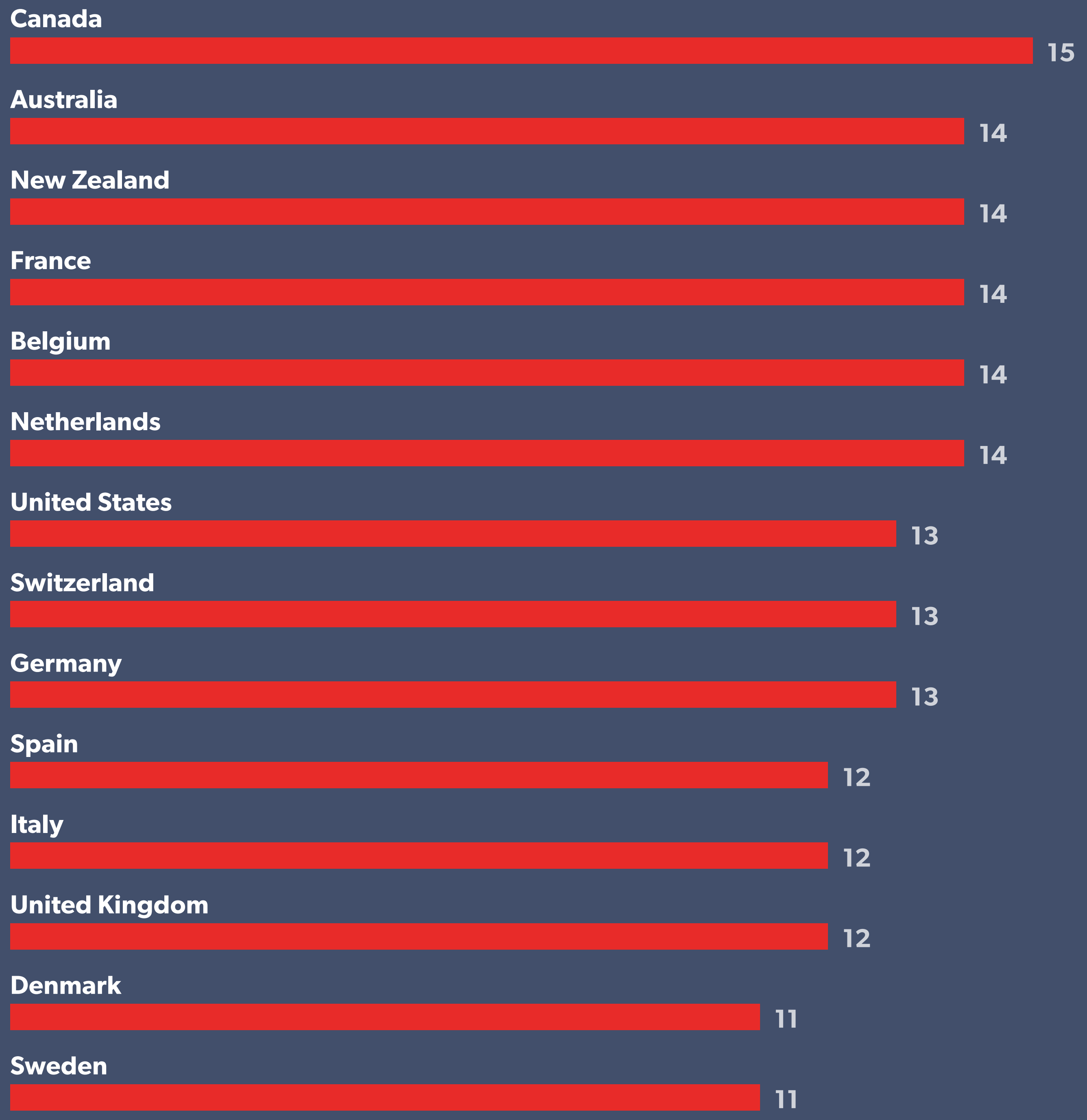
LOWEST

11

Denmark & Sweden

AVERAGE NUMBER OF REUSED PASSWORDS

BY COUNTRY



THOUGHTS ON 2019 SECURITY SCORES, AND WHY DOING PASSWORD SECURITY RIGHT ISN'T JUST A ONE-TIME THING

Last year, we introduced the Benchmark Security Score, a number that offers a way to evaluate the state of password security across businesses of all sizes, in many industries, all over the world. While some of this year's Security Scores were flat – the **2019 Benchmark Score is 49** – we saw some significant gains in specific areas.[5]

There are a few reasons why the 2019 Benchmark Score remains flat. As more users are added, average scores will, of course, be pulled down, though over time we expect those users' scores to increase. In general, we're seeing an increasing number of businesses investing in password security, as well as businesses already using password management that are deciding to deploy the solution to the entire company (rather than just the IT team), which results in a lower score.

As we saw in the preceding sections of the report, the increased use of multifactor authentication will pull security scores up, but ongoing password reuse and poor password hygiene will pull security scores down.

What this report highlights is the ongoing need for businesses to focus on training employees – particularly new users – and continuing to improve password hygiene with the tools offered in a password manager.

[5] As a reminder, the Benchmark Security Score is the average LastPass Security Score for businesses globally. The Security Score is calculated as part of the LastPass Security Challenge, a built-in password-auditing tool available for all LastPass users. For business accounts, this data is also reported to LastPass admins for insight into password hygiene at the employee level. The LastPass Security Score is calculated using the following criteria:

- The number of duplicate passwords
- The number of sites marked "vulnerable" (due to publicly disclosed data breaches)
- The number of weak passwords
- The average strength of each password
- The strength of shared passwords
- The multifactor authentication score

This total score tells businesses not only how strong individual passwords are, but also how well those passwords are protected.

LARGER BUSINESSES MADE BIG GAINS IN SECURITY SCORES

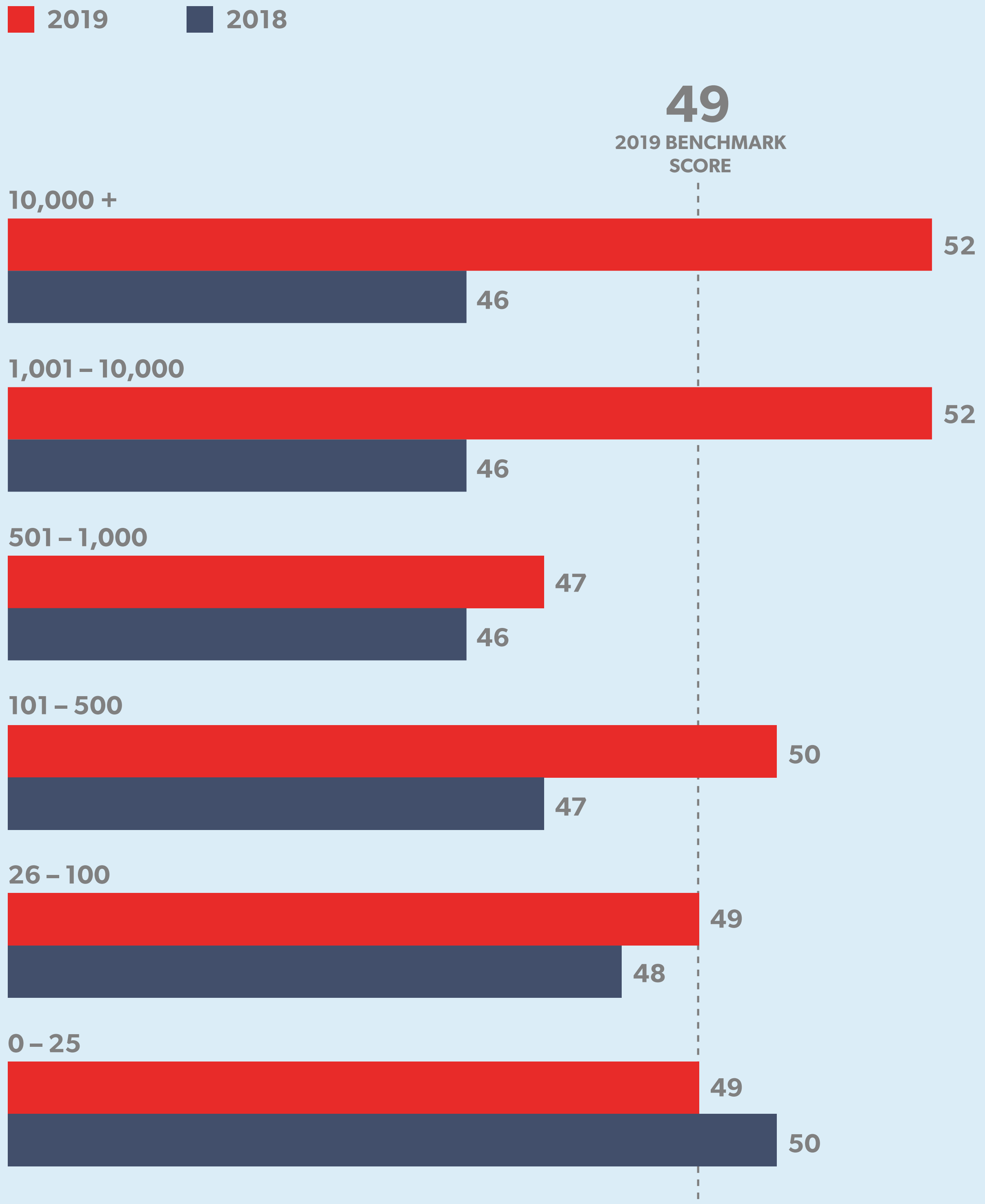
Given that we see larger organizations implementing multifactor authentication at a higher rate, the additional 10 points to the LastPass Security Score could be attributed to that added layer of protection. Another interpretation of those results is that larger businesses have been more successful at building password management into their employee onboarding and ongoing security training, which has shown to not only boost adoption, but also increase the use of key features that raise Security Scores, too.

Businesses with 1,000 or more employees gained several Security Score points.

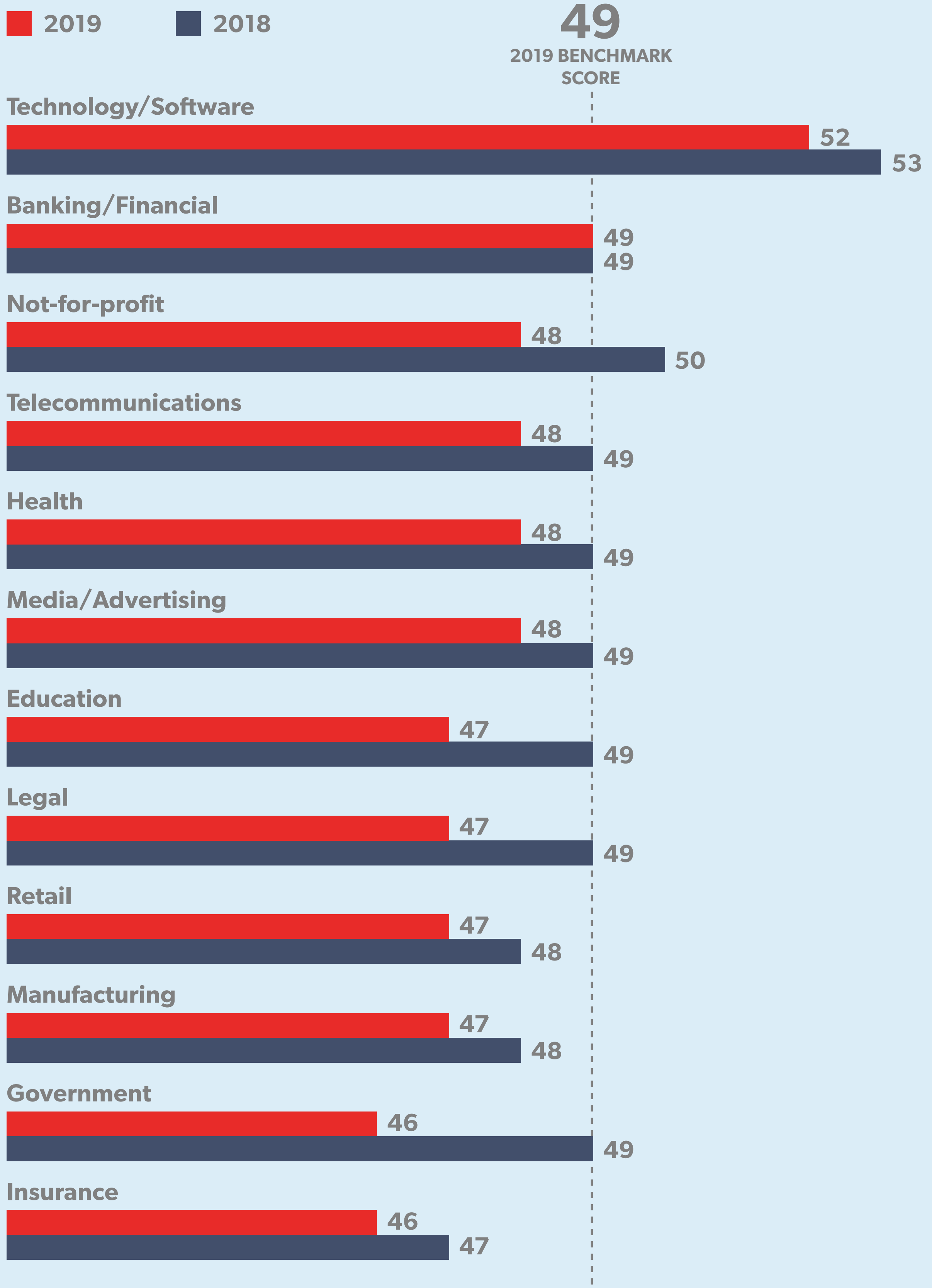
2019 52

2018 46

AVERAGE SECURITY SCORE, BY COMPANY SIZE



AVERAGE SECURITY SCORE, BY INDUSTRY



TECHNOLOGY/SOFTWARE STILL LEADS WITH THE HIGHEST SECURITY SCORE

When looking at Security Scores across different industries, most averages held steady compared to 2018. Technology/Software continues to lead, while the Retail and Insurance industries continue to have lower Security Scores. As we mentioned above, an increased number of users across industries tends to pull Security Scores down, especially when IT is slow to train employees on reducing password reuse.

LOWEST IN 2019

46

Insurance

HIGHEST IN 2019

52

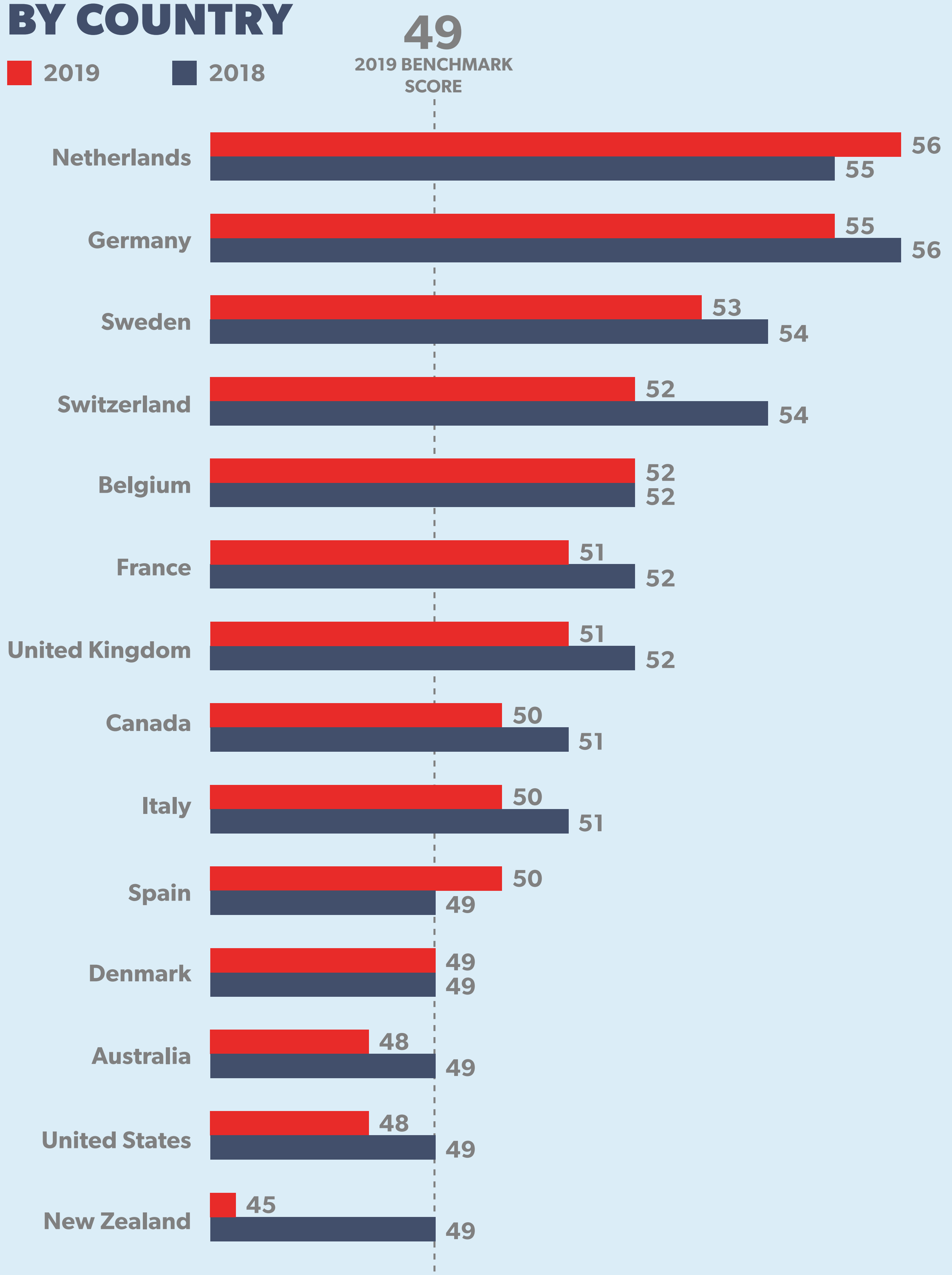
Technology/Software

SPAIN AND THE NETHERLANDS IMPROVE THEIR SECURITY SCORES

Last year, Germany took first place with a Security Score of 56. This year, the Netherlands took the top spot with a score of 56, as Germany slipped back a point to 55. Spain also gained a point this year, with an updated Security Score of 50. Security Scores for most other countries held steady.

AVERAGE SECURITY SCORE,

BY COUNTRY



GLOBAL SECURITY INITIATIVES & REGULATIONS

See how password security is being emphasized the world over.

INCREASED REGULATION AS A KEY DRIVER OF PASSWORD SECURITY EFFORTS IN SOME MARKETS

It's important to remember that security initiatives around passwords and employee access aren't happening in a vacuum. One key driver in some markets is increased regulation. As global threats rise and concerns grow about the privacy of personal information, governments and industries are enacting more regulations, directives and guidelines in order to help protect the digital economy.

As this landscape continues to evolve, organizations that suffer a data breach will feel the implications long after the news headlines have faded away. Equifax and their recent settlement is a prime example of this.

> Two of the better-known regulations and schemes, the EU General Data Protection Regulation (GDPR) and the NDB in Australia, have already had a significant impact on the market, and may start reflecting some of the trends we observe in this report.

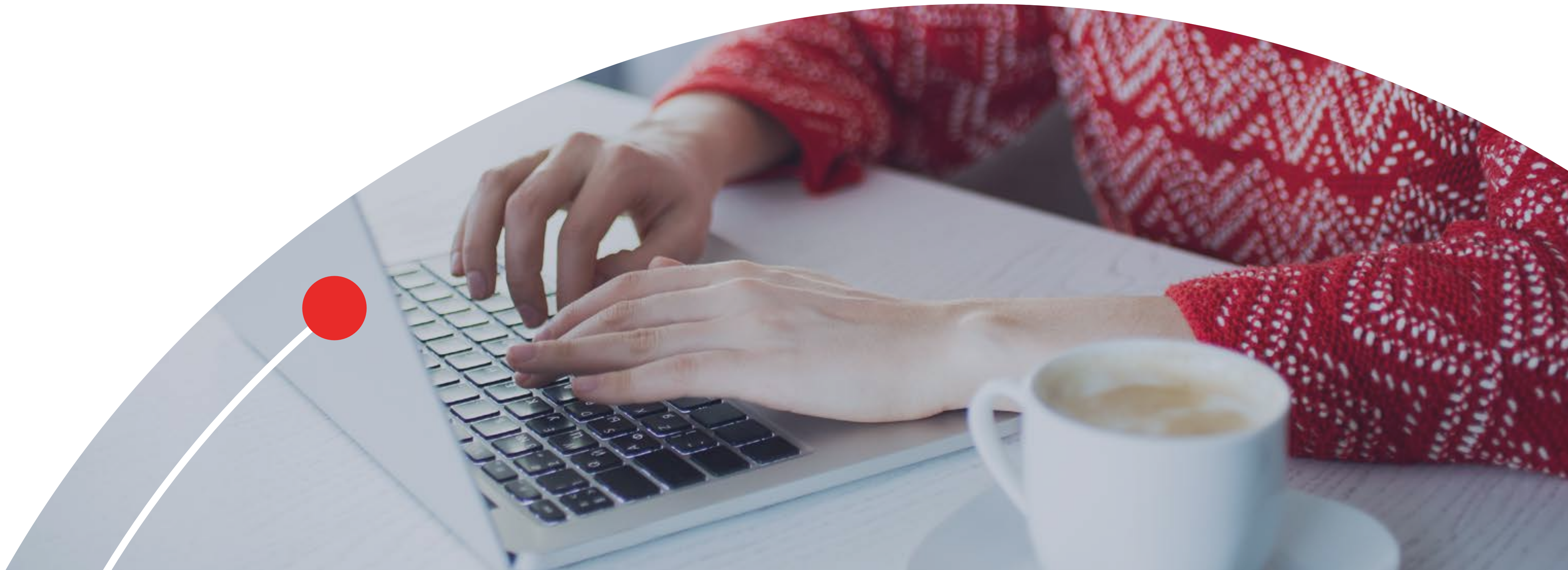
GDPR

The General Data Protection Regulation (GDPR) came into effect in May 2018. Per GDPR, data breach notifications are now mandatory and can lead to fines. After a slow start, the issuing of fines has ramped up, including:

- **€50M ($55.5M)** fine issued by the French data protection office (CNIL) to Google for failing to obtain adequate consent from users when processing their data for the purpose of personalized advertising.
- **£99M ($121M)** fine issued by the UK Information's Commissioners Office (ICO) to Marriott following the exposure of the personal information of approximately 339 million guests.
- **£18M ($22M)** fine issued by the UK Information's Commissioners Office (ICO) to British Airways after visitors to the airline's website were diverted to a fraudulent site where the visitor would enter personal information.

Other fines are shaping the precedent for what may warrant a fine in the future. For example, in Germany, a social network was fined €20,000 ($24,500) because a breach exposed its users' passwords, which were stored unencrypted. Since breaches continue to be so commonplace, organizations need to be more vigilant in how they handle data, how it is stored and how it is protected, including password security.

While it's difficult to directly tie our data to the influence of GDPR, it's hard to ignore the adoption of multifactor authentication by LastPass customers over the past 12 months. Denmark, Switzerland, France and Germany have all seen exponential adoption of MFA, which can only have a positive impact on the security posture of the organizations in these countries.



THE NDB SCHEME IN AUSTRALIA

In February 2018, the Office of the Australian Information Commissioner (OAIC) began producing the Notifiable Data Breach (NDB) Scheme. Since the switch from voluntary to mandatory notification, the number of breaches reported **increased by 712% to 964 in a single year.**

The Australian government said in their 12 Month Insights-Report,[6] "Compromised or stolen credentials underpinned most cyber incidents that led to data breaches in the first year of the NDB scheme."

To help reduce the risk of stolen credentials, the report advocates educating employees about phishing emails and password reuse, implementing anti-spoofing controls and multifactor authentication, and being proactive about security measures through online services and password managers to detect compromise.

While there has been little movement in the Security Score for Australia, the adoption of MFA has increased significantly amongst LastPass users there. In a 12-month period, the MFA score has grown from **6%** to **29%** (see figure on page 10), indicating that measures to reduce the risk of stolen credentials are being implemented.

While MFA adoption is on the rise, according to the 12-Month Insights Report, the Health sector in Australia has the highest volume of breaches, and from our findings, we can tell that the same sector currently has the 2nd lowest MFA score compared to other industries. It's clear that investing in MFA should be a focus for organizations in the Health sector.

An interesting point to note is that **28%** of breaches documented in the Insights Report indicate that credentials were obtained by unknown means, indicating that credential stuffing is now a significant access method for cyber criminals.

Increased activity around government regulations and directives has created a cybersecurity climate in which businesses are more aware of the risks associated with poor password hygiene and unregulated employee access. In some markets, there appears to be a push to invest in solutions like password management and Single Sign-On that will help achieve greater security standards.

[6] The 12 Month Insights-Report (or NDB Report) was produced in 2019 by the Office of the Australian Information Commissioner (the OAIC) which provides interesting and helpful insights into the first year of the Notifiable Data Breaches Scheme (the NDB Scheme).

IMPROVE YOUR SECURITY SCORE

Change the status quo and eliminate password-related risks.

HIGHER SECURITY SCORES REQUIRE THOUGHTFUL PLANNING AND CONSISTENT EFFORT

When it comes to improving password and access security, it's important to invest in an access solution that combines Single Sign-On with Enterprise Password Management and Multifactor Authentication. However, simply purchasing a solution and making it available to employees does not guarantee you'll strengthen your company's password security or achieve a high Security Score. To change the status quo and eliminate password-related risks, companies need to:

1. **Take access security seriously.**
2. **Make a plan.**
3. **Mandate the use of a password manager.**
4. **Train, train and train some more.**
5. **Turn on multifactor authentication.**
6. **Regularly check your Security Score and keep tweaking your approach.**

#1

TAKE ACCESS SECURITY SERIOUSLY

We hope you're reading this report because you understand the importance of securing employee access, and perhaps even the value of an access solution. But too often, we see businesses ignore password security altogether, or only half-heartedly attempt to address it. When 80% of breaches are still linked to passwords, [7] an investment in Single Sign-On and Enterprise Password Management is one of the most effective ways to reduce risks across the organization.

Only once your business is serious about addressing the risks of access security will you be able to make progress.

80% **of breaches are linked to passwords.**

[7] 2019 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/dbir/

#2

MAKE A PLAN

Be thoughtful about problems you're trying to solve, the use cases you need to support, the features you require and the solution(s) you ultimately purchase. Understand what it will take to configure and deploy the solution. Create a detailed schedule for onboarding employees and following up with those who are slow to adopt.

Ensure training for an access solution – including SSO and EPM features – is a part of your company's new employee onboarding and ongoing security education programs.

#3

MANDATE THE USE OF A PASSWORD MANAGER

We've heard many businesses say that they want a password manager, but that they want to make it optional for their employees. We hate to break it to you, but most employees will only implement a new process if it's required and seek out a solution only if the pain gets bad enough.

If you want to proactively secure your company and enforce the use of stronger passwords, you need to strongly consider requiring usage of a password manager for storing, generating and sharing passwords.

If you continue to make password management optional, you cannot expect remarkable improvements in your password security.

#4

TRAIN, TRAIN, AND TRAIN SOME MORE

Not only does training need to be a part of your original onboarding plan, it needs to be an ongoing effort to encourage adoption and usage of security tools. Employees need to understand why they should use the tool, and how best to use it. They need to know how to generate new passwords and replace old ones that are weak or reused.

They need to know how to check their own Security Scores, and understand how their actions contribute to the overall security of the organization. Yes, employee training can require additional time and resources, but it is well spent when you achieve the Security Scores you want to see.

#5

ADD MULTIFACTOR AUTHENTICATION

Adding multifactor authentication to your deployment of an access solution provides an extra layer of protection against bad passwords. Plus, adding MFA instantly raises Security Scores. As we've noted, many employees are already using MFA, and a portion of businesses are even mandating it through policy. We strongly encourage admins to require the use of MFA via policy in an Enterprise Password Manager. If that's not possible, then specifically train employees on the benefits and usage of MFA, and allow them to enable it themselves. However, the best option is to go one step further and invest in an MFA solution that brings the benefits of MFA to all access points in the business, not just the password vault.

#6

REGULARLY CHECK YOUR SECURITY SCORE AND KEEP TWEAKING YOUR APPROACH

When you first deploy an access solution, such as LastPass, take note of your Security Score. Regularly check your scores and notice any trends that emerge. Consider creating a small group of people who are tasked with evaluating the success of implementation and trying to keep improving Security Scores. Identify employees with low scores that need additional training.

As much as we wish an access solution could fix all your security woes without lifting a finger, the reality is that it needs to be a thoughtful part of your ongoing security strategy with regular investments of time and resources. It doesn't have to be extensive, but consistency is key.

LEARN MORE ABOUT LASTPASS IDENTITY

LastPass Identity provides simple control and unified visibility across every entry point to your business, with an intuitive access and multifactor authentication experience that works on everything from cloud and mobile apps to legacy on-premise tools. From single sign- on and password management to multifactor authentication, LastPass Identity gives superior control to IT and frictionless access to users.

- Central admin control
- 1,200+ single sign-on applications
- Industry-leading enterprise password manager
- 100+ access security policies
- Advanced reporting
- Secure password sharing
- User directory integrations
- Adaptive multifactor authentication
- Easy-to-use solution

LastPass ••• |

by LogMeIn

www.lastpass.com/products/identity