DASHLANE

The Future of Secure Work for People + Organizations

Key trends on the state of security for growing businesses and predictions on what's to come, plus recommendations on how to jumpstart cybersecurity best practices.

Contents

Introduction

The last two years brought long-lasting effects to the workplace, forever changing how employees work. Employers, too, experienced a shift as they expedited digital tool adoption to boost business resilience. In this evolved workplace, both employees and employers view hybrid models as “the future of work.” For small and growing businesses, the evolution to a hybrid workplace creates new urgencies. With the network perimeter no longer well-defined and employees embracing a “bring your own apps” mentality, companies can't afford to push cybersecurity to the sidelines or keep it disconnected from their business goals. In the hybrid, cloud-first era, security is an opportunity to differentiate because all your stakeholders—from employees to customers and partners—expect you to keep their data safe. Dashlane wanted to understand how small and medium-sized organizations in the private and public sectors view cybersecurity and password management as they embrace the future of work. To learn about cybersecurity sentiments and practices, we surveyed 604 employees and managers and 305 IT decision-makers at small-to-medium organizations across multiple industries. Additionally, we conducted interviews with a select group of IT leaders. (We refer to employees and managers as “employees” and IT decision-makers as “leaders” throughout the report.)

INTRODUCTION

This research builds on last year's Future of Security in the Hybrid Workplace report that focused on employee behaviors and attitudes. For 2022, we broadened our lens to include people and organizations, asking both employees' and leaders' opinions to gain insights into how the continued hybrid work evolution and growth influences security awareness and culture.

One of the things we learned is that remote and hybrid work is going mainstream. Other independent studies have shown that workers now expect flexibility. For example, 73% of 30,000 workers surveyed in 2021 wanted flexible remote work options to continue, according to Microsoft's annual Work Trend Index.[1] We saw this trend reflected in our findings—only 10% of all our surveyed employees and leaders reported no remote workers at their organizations.

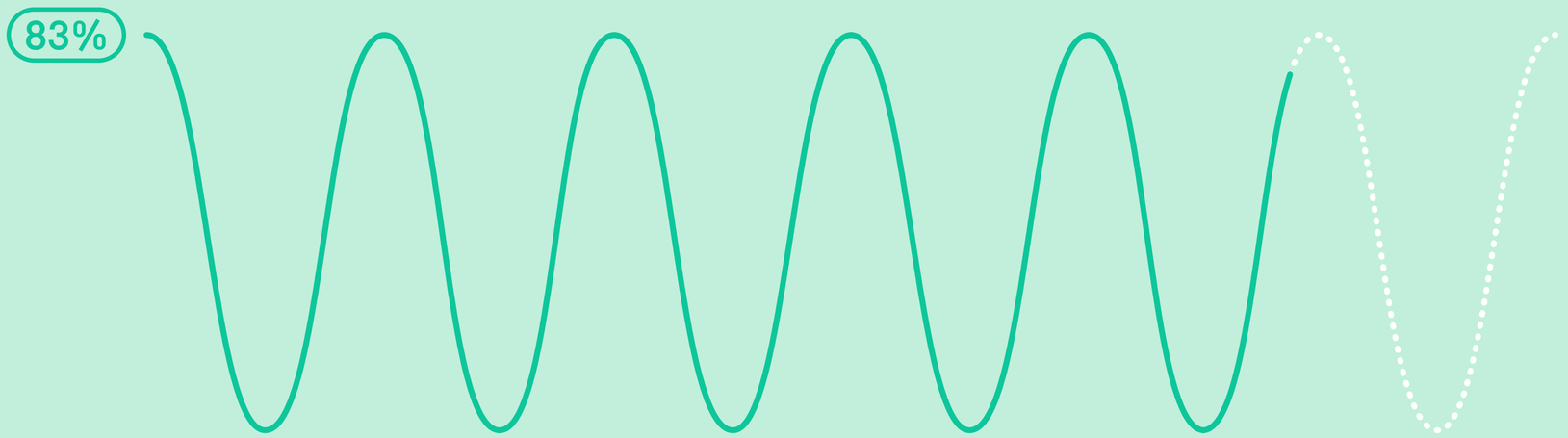
Now that small businesses have embraced remote work, the pace of online tool adoption will only accelerate. Protecting sensitive data in this environment requires behavioral change through a strong, human-centric security culture. In this report, we dig into the trends shaping this behavioral change—and offer our thoughts on what to expect in the next three years.

1. "2021 Work Trend Index: Annual Report," Microsoft, March 2021

FINDING #1

Awareness increased for organizations, but only some took action.

Antennas are up for most organizations. Among all our survey participants, 83% noticed an increased level of security awareness and importance at their organization. This means small and medium-sized organizations realize the stakes are high in the digital era.



This increased awareness translated into action, but only for a small group of organizations. Overall:

38% increased usage of their existing password manager

37% increased cybersecurity training

36% adopted new security policies

23% said their organizations started using a password manager

FINDING #2

Leaders and employees view their organization's cybersecurity posture differently.

Throughout our two separate surveys, we noticed that leaders' perceptions differ from employees' perceptions in many areas. For example:

FEEL THEIR ORGANIZATION PAYS ATTENTION TO SECURITY MORE AFTER RECENT LARGE-SCALE DATA BREACHES

98% leaders

88% employees

REPORTED AN INCREASE IN THE LEVELS OF SECURITY AWARENESS AND IMPORTANCE AT THEIR ORGANIZATION

97% leaders

75% employees

REPORTED INCREASED USAGE IN THEIR EXISTING PASSWORD MANAGER

leaders 65%

25% employees

SAID THEIR ORGANIZATIONS STARTED USING A PASSWORD MANAGER

leaders 32%

20% employees

SAID THEIR ORGANIZATIONS ADOPTED NEW SECURITY POLICIES

43% employees

leaders 31%

NOTED INCREASED CYBERSECURITY TRAINING

40% employees

leaders 23%

These differences are not unexpected because individual roles influence people's view of their organization's inner workings. And since leaders drive many of the security initiatives, they see the changes in awareness and security practices through a different lens than most employees.

However, it's important to ensure that these different perceptions don't create a disconnect between IT priorities and the organization's business objectives and employee needs. To get employee buy-in for security initiatives, organizations need to elevate security so it's not just "an IT problem"—and educate their people about the importance of security to the business and to their job.

FINDING #3

Larger organizations are more enthused about cybersecurity.

Our survey found many differences between larger and smaller organizations. Those with more than 300 employees were more likely to note heightened cybersecurity awareness, changes in security practices, and even higher passion for cybersecurity among employees.

THE SMALLEST ORGANIZATIONS

51–100

WERE THE LEAST LIKELY TO ADOPT NEW SECURITY POLICIES OR INCREASE CYBERSECURITY TRAINING AS A RESULT OF INCREASED REMOTE WORK.

THE INCREASE IN EMPLOYEE AWARENESS GREW WITH THE ORGANIZATION'S SIZE.

82%

401–500

72%

51–100

WITHIN ORGANIZATIONS WITH MORE THAN 300 WORKERS, EMPLOYEES WERE MORE LIKELY TO CHARACTERIZE THEIR CO-WORKERS AS PASSIONATE ABOUT CYBERSECURITY

49% 301–400

52% 401–500

41% OVERALL

- THE RESULTS WERE SIMILAR AMONG LEADERS.

Some of these differences may be attributed to the smaller proportion of remote workers at the smallest organizations. However, the more significant reasons are likely the lack of cybersecurity resources and the illusion that cybercriminals don't target smaller companies. Yet the past few years have demonstrated that size doesn't matter to cybercriminals—smaller companies are just as much at risk of cyberattacks, if not more.

Typically, many smaller businesses don't have a full-time, dedicated IT person, let alone a security team. A robust cybersecurity stack and an employee awareness program are both big asks for these organizations—and consequently, employees overall may also feel less passionate about cybersecurity.

Apart from promoting a passion for cybersecurity, small businesses should also require accountability. Many organizations now include their security, data protection, and confidentiality expectations in their employment contracts. Using these guardrails is another good way to emphasize the importance of cybersecurity. But having those requirements without providing the right resources is unfair to employees. To make security less overwhelming, look for cost-effective, easy-to-use tools that boost not only your defenses but also your security culture.

FINDING #4

Using a password manager is the #1 change organizations implemented to strengthen security.

Increased password manager usage was the top change that organizations made as a result of remote work, with 38% of employees and leaders identifying this shift. Increased cybersecurity training and new policy adoption weren't far behind (37% and 36%, respectively).

This indicates that organizations understand that people and policies are equally important to maintaining a strong security posture. Changing behaviors and improving the security culture also requires human-centric security, and these findings show that many organizations are well on their way to adopting this mindset.

We also found that leaders are much more likely to call out the importance of a password manager—65% noted increased usage of their existing password manager and another 32% said their organization started using one.

OF ORGANIZATIONS INCREASED PASSWORD MANAGER USAGE FOLLOWING A SHIFT TO A REMOTE WORKFORCE

38%

INCREASED CYBERSECURITY TRAINING

37%

ADOPTED NEW POLICIES

36%

OF LEADERS NOTED INCREASED USAGE OF THEIR EXISTING PASSWORD MANAGER

65%

SAID THEIR ORGANIZATION STARTED USING ONE

32%

FINDING #5

Employees now want a password manager—and leaders agree.

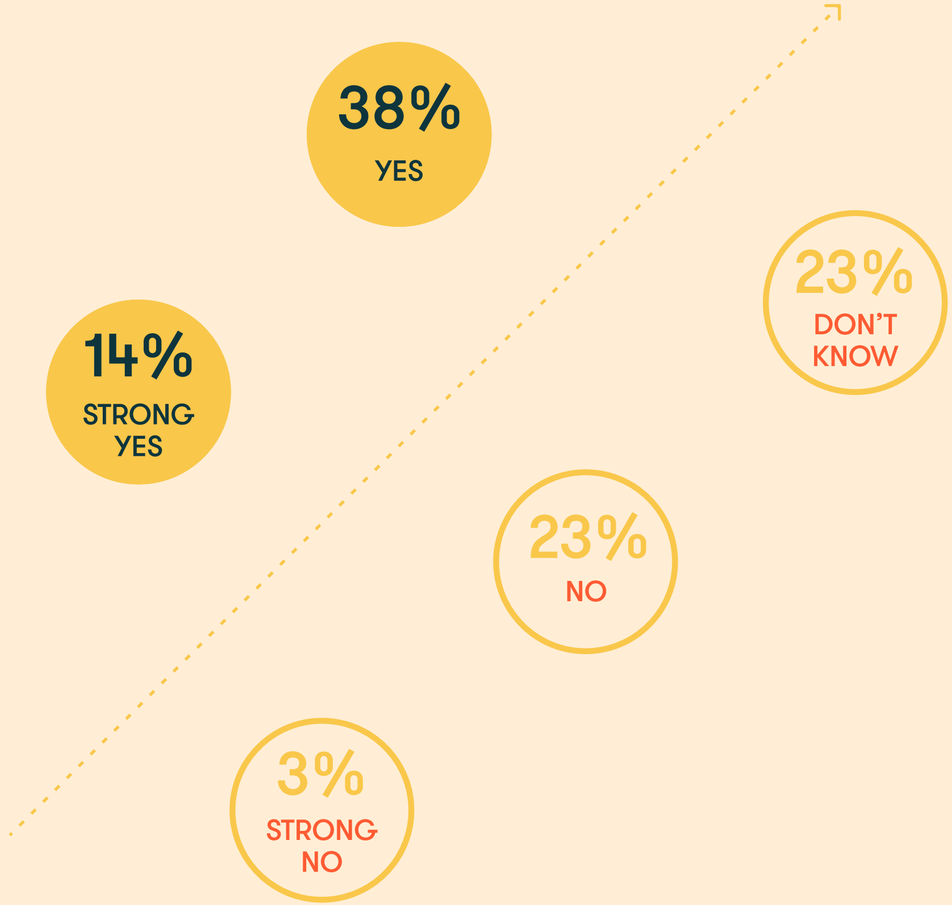
While the employees and the leaders in our two surveys have varying sentiments about different areas of cybersecurity, they're on the same page when it comes to the need for a password management solution. But leaders feel much more strongly about it. About half (52%) of employees believe their organization needs a password manager; among leaders, a resounding 97% feel the same.

This tells us that employees want digital security tools that help them practice better cybersecurity to keep their organization safe—and leaders are fully behind employees' desire to have better tools.

Many employers are already making strides here: 41% of organizations represented in our surveys require a password manager for everyone, with another 18% adopting it for some, and 13% offering it as an option. The cohort requiring this digital security tool the most is employers with 301–400 workers (51%), followed by those with 401–500 workers (42%).

From our supplemental leader interviews, we also learned that employees want a dedicated resource beyond an office manager or IT admin for managing access to a password manager. They feel they can handle it for a while, but once the company grows bigger, too many things can go wrong. Choosing a password manager that's simple and comes with great onboarding features can help achieve this—and the simpler the tool, the more likely employees are to adopt it.

Half of employees overall believe their organizations need a password management solution.



	STRONG YES	YES	NO	STRONG NO	DON'T KNOW
BANKING	22%	50%	22%	0%	6%
CONSTRUCTION	16%	32%	27%	3%	22%
EDUCATION	9%	37%	19%	3%	31%
FINANCE	27%	41%	25%	0%	7%
GOVERNMENT	8%	26%	29%	3%	34%
HEALTHCARE	15%	48%	6%	4%	27%
MANUFACTURING	13%	33%	29%	0%	25%
OTHER	10%	28%	20%	10%	33%
RETAIL	14%	46%	17%	0%	23%

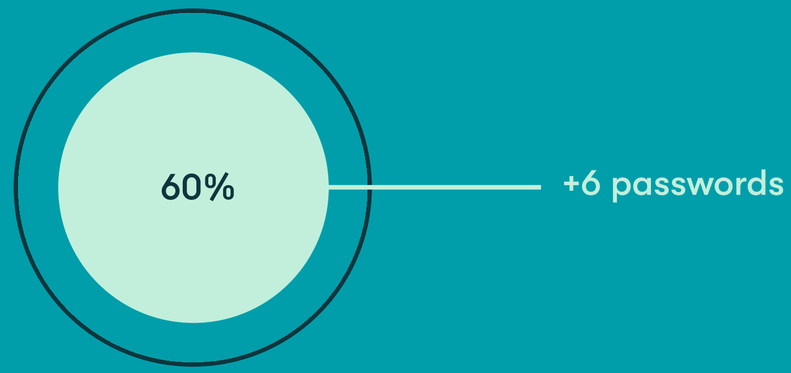
FINDING #6

Most employees wrangle at least five passwords.

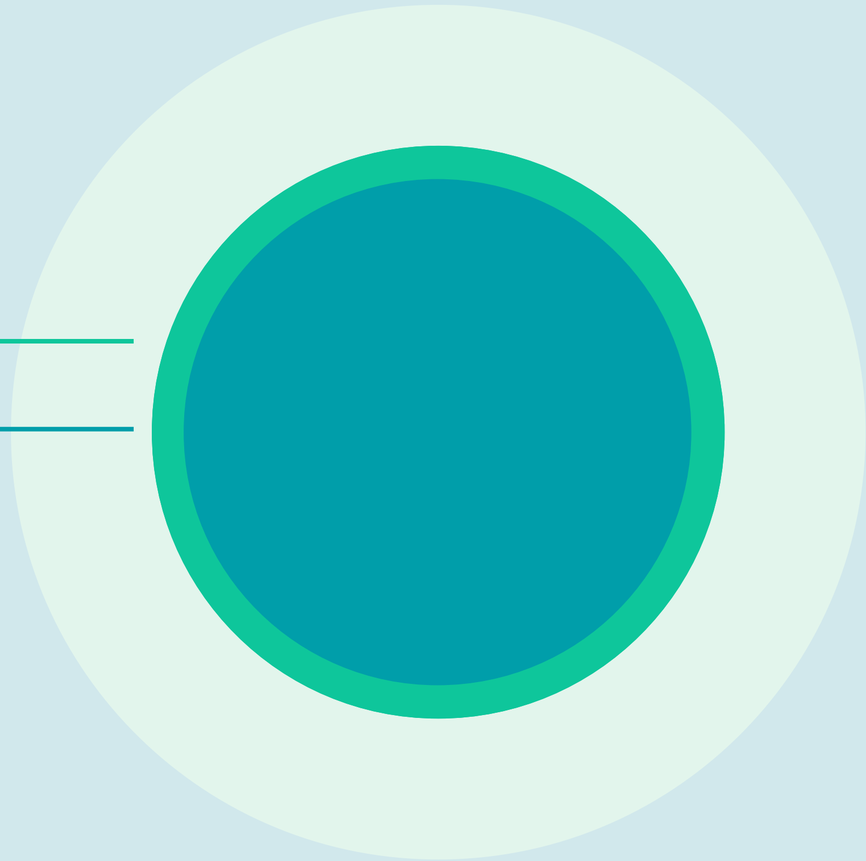
The majority of our participants said they handle more than five passwords for their work accounts regularly, with 6–10 as the most common amount (identified by 41% of respondents). Not surprisingly, given their role, leaders juggle a lot more—72% have more than five passwords, and 53% have 6–10.

Across sectors, employees in banking have the highest access fatigue (with 34% of employees juggling 10 or more passwords), followed by education (25%). Retail and finance tied for the third spot (23%).

Access fatigue could lead employees to look for shortcuts, such as reusing passwords or resorting to simple, easy-to-remember ones. Such shortcuts are highly risky for organizations because malicious actors commonly use compromised and weak passwords to break in.



Nearly half of the employees and leaders have 1–5 password-protected accounts, and one-third have 6–10 accounts; Education, finance, and healthcare workers are particularly likely to be in the 6–10 accounts range.



40%
1–5
PASSWORD-PROTECTED
ACCOUNTS

41%
6–10
PASSWORD-PROTECTED
ACCOUNTS

FINDING #7

Employee usage of password managers remains a challenge.

Despite their jumble of logins, employees are not confident that their co-workers use password managers widely.

Although 41% of surveyed organizations require a password manager, only one-fifth of employees believe the adoption rate among their co-workers is 95–100%. Worse yet, close to one-third (29%) believe the adoption rate is 50% or less. Here, too, leaders have a different view—employees are much more skeptical than IT teams. Nearly 40% of our IT leaders believe the adoption rate at their organization is 95–100%, and only 20% believe the rate is 50% or lower.

Since leaders have a closer view of their companies' security tools than other employees, it's likely that their understanding of the adoption rates better reflects reality. Even so, it's clear that organizations struggle with employee buy-in.

41%

OF SURVEYED ORGANIZATIONS
REQUIRE A PASSWORD MANAGER

ONLY ONE-FIFTH OF EMPLOYEES
BELIEVE THE ADOPTION RATE AMONG
THEIR CO-WORKERS IS 95–100%.

WORSE YET, CLOSE TO ONE-THIRD
(29%) BELIEVE THE ADOPTION
RATE IS 50% OR LESS.

NEARLY

40%

OF OUR IT LEADERS BELIEVE THE
ADOPTION RATE AT THEIR
ORGANIZATION IS 95–100%

AND ONLY

20%

BELIEVE THE RATE IS 50%
OR LOWER.

FINDING #8

Lack of security tool trust and understanding are the top adoption barriers.

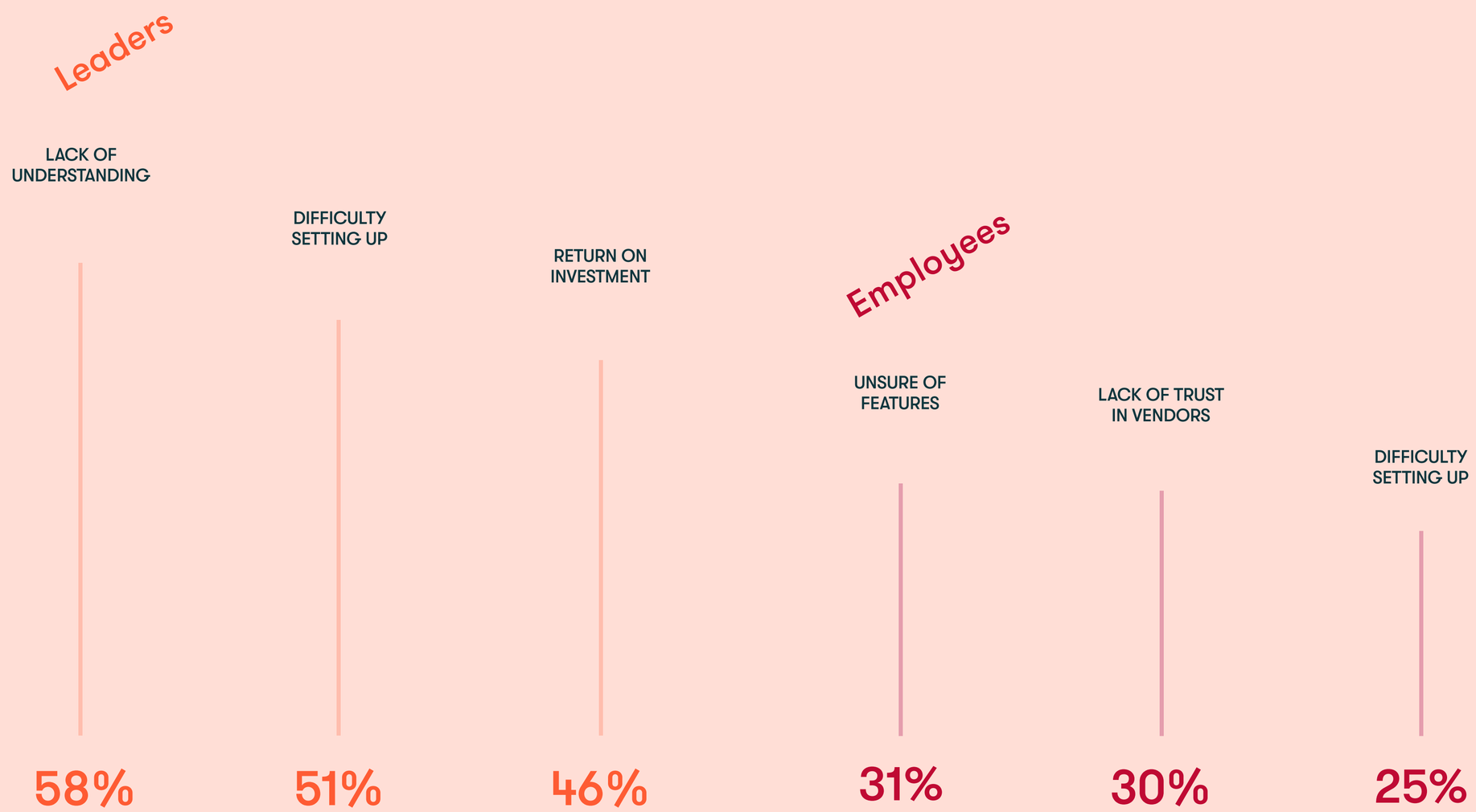
Even when organizations invest in security tools, employees may not use them if they don't trust those tools or learn how to use them. Our survey found that both employees and leaders believe the main barrier to password manager adoption is a lack of knowledge about the features.

Given that so many IT leaders don't understand their password manager's features, find the tool difficult to set up, or don't feel they're getting good ROI, this helps explain the low adoption rates discussed earlier. It would be challenging for leaders to "evangelize" the use of the tool to their organization if they don't understand how the password manager works and don't feel it's easy to use.

For effective onboarding, employees need to know not only why they need a password manager but also what features are relevant to them and how these features improve security. Take advantage of the resources that many vendors offer as part of their onboarding.

Lack of understanding about the features is a much greater barrier for leaders than employees—with 58% of the former citing “unsure of features” as the top barrier, compared to 31% of the latter.

Lack of trust in their vendors is the second biggest reason employees don’t use a password manager (with 30% expressing this view), followed by difficulty setting up (25%). On the other hand, leaders cite difficult setup as the second biggest barrier (51%), followed by return on investment (46%).



FINDING #9

Organizations with a password manager feel less at risk of a cyberattack than those without one.

For organizations that have overcome barriers to adoption, the outcomes are positive. Among our survey participants, both employees and leaders in workplaces that require a password manager believe their organization has a lower risk of being hacked or breached.

Leaders are much more convinced that this is the case—90% expressed that their organization is either “not at risk” or “not at all at risk” for being hacked or breached, compared to 59% of employees.

Leaked passwords are abundant in the criminal underground due to the massive number of data breaches. With automated tools, cybercriminals can check the validity of these passwords quickly and at scale. A password manager lowers the risk of compromised and weak passwords, and our study shows that organizations see the results.

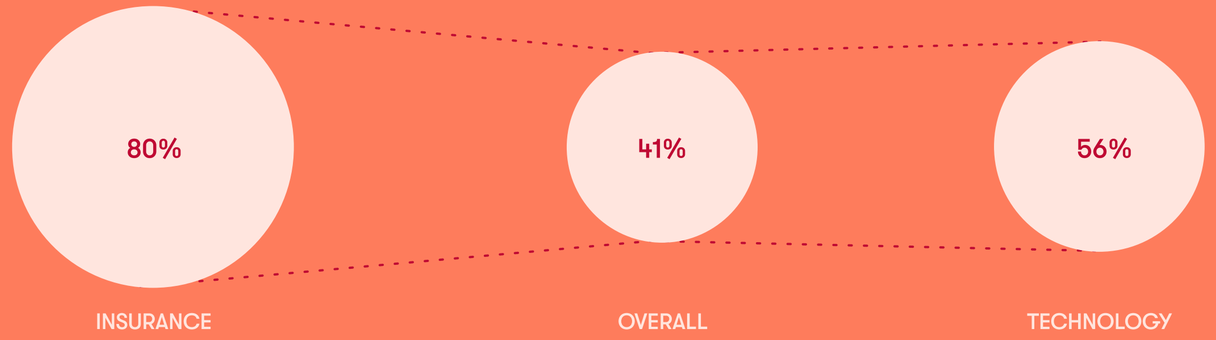

OVERALL
34%
NOT AT ALL AT RISK OF BEING HACKED OR BREACHED
54%
NOT AT RISK OF BEING HACKED OR BREACHED
10%
AT RISK OF BEING HACKED OR BREACHED
2%
AT MAJOR RISK OF BEING HACKED OR BREACHED
90%
OF LEADERS EXPRESSED THAT THEIR ORGANIZATION IS EITHER "NOT AT RISK" OR "NOT AT ALL AT RISK" FOR BEING HACKED OR BREACHED, COMPARED TO 59% OF EMPLOYEES.
PASSWORD MANAGEMENT REQUIRED
39%
51%
9%
1%
NO PASSWORD MANAGEMENT EVER
0%
50%
25%
25%
PASSWORD MANAGEMENT PREVIOUS/ REPLACED
0%
0%
75%
25%
PASSWORD MANAGEMENT OPTIONAL
0%
46%
54%
0%
PASSWORD MANAGEMENT USED BY PART OF THE ORG
29%
66%
3%
3%

FINDING #10

Cybersecurity sentiments and practices differ among sectors.

Insurance, finance, and banking stood out as the sectors embracing security tools the most—perhaps because stricter regulations lead to broader mandates for improving security.

INSURANCE, BY FAR, REQUIRES A PASSWORD MANAGER THE MOST



HEALTHCARE IS ONE OF THE THREE SECTORS WITH THE LARGEST NUMBER OF EMPLOYEES WHO ARE ON THE FENCE ABOUT PASSWORD MANAGERS,

WITH

27%

UNCERTAIN ABOUT THEIR NEED.

THE NEED FOR A PASSWORD MANAGER

EMPLOYEES MOST CONVINCED

FINANCE & BANKING

EDUCATION & GOVERNMENT

EMPLOYEES LEAST CONVINCED

TOP THREE SECTORS SEEING THE HIGHEST INCREASE IN EMPLOYEE AWARENESS (WITH GOVERNMENT IN THE BOTTOM THREE)

MANUFACTURING EMPLOYEES NOTED AN INCREASED CONCERN ABOUT LARGE-SCALE DATA BREACHES THE MOST. AN ASTOUNDING

96%

Cybersecurity best practices may vary slightly from sector to sector, but many are foundational regardless of the industry. Understanding these best practices and adopting the fundamentals will help organizations of all sizes improve their cybersecurity preparedness.

26%

EDUCATION IS THE SECTOR THAT HAS THE HIGHEST NUMBER OF RESPONSES WITH A PASSWORD MANAGER AS OPTIONAL TO USE

WHILE RETAIL HAS THE HIGHEST NUMBER OF EMPLOYEES SAYING THEY NEVER HAD A PASSWORD MANAGER.

ALTHOUGH GOVERNMENT EMPLOYEES ARE AMONG THE LEAST CONVINCED THEY NEED A PASSWORD MANAGER, GOVERNMENT AGENCIES ARE ONE OF THE TOP SECTORS THAT REQUIRE IT THE MOST.

Our predictions for 2022 and beyond

Based on our observations of cybersecurity trends in the past year, along with the findings from our two surveys and the leader interviews, we offer the following predictions for the next three years.

PREDICTION #1

More organizations will prioritize cybersecurity and connect it to their business goals.

As hybrid work continues, organizations of every size will look for ways to secure their business. However, those that prioritize people over policies will improve their cybersecurity the most. People, rather than technology, are the weak link that malicious actors exploit most often—and implementing human-centric security is the best way to win this fight.

PREDICTION #2

Trust will play a greater role in the digital tools organizations select to secure their businesses.

High-profile cyberattacks in recent months have shown the importance of using security tools that are themselves secure. Organizations will pay closer attention to their security partners' and vendors' practices—and demand more transparency.

PREDICTION #3

Organizations will look for security solutions that work across both personal and work spaces to help employees on and off the clock.

Hybrid work erases any remaining lines between professional and personal spaces, and organizations will give preference to solutions that work across both so they can support their people beyond work. When people use cybersecurity tools in their personal lives, they develop good cybersecurity habits and awareness, practicing them both on and off the clock.

PREDICTION #4

Workplace cybersecurity will become a personal concern for more employees.

Security will become personal for a growing number of employees over the next few years, rather than being their employer's sole responsibility. As cybersecurity concerns continue to rise for small organizations, many will succeed at making security an integral part of their corporate culture.

PREDICTION #5

The volume and breadth of hacks and breaches will increase the urgency for better security among small and medium-sized businesses.

Cybersecurity will become a bigger focus for small and midsize businesses, rather than being a concern primarily for larger enterprises. With cyberattacks getting constant attention in the media, smaller organizations are growing more aware of their risks and the implications. The most successful ones will realize they can no longer watch from the sidelines and will take steps toward boosting their defenses—and resilience.

Where do we go from here?

This year's research confirmed that cybersecurity is on the minds of small and medium-sized organizations. Many are boosting their security culture and supporting their employees with the digital tools they need. Yet significant challenges remain for others, keeping security on the back burner.

With hybrid work now commonplace, creating a robust, human-centric security culture is a priority. While behavioral change is not an easy undertaking, a strong culture plays an influential part in this endeavor. Change is not about adding more security tools or policies—it's about ensuring you have the right tools that empower employees to work from anywhere without feeling like security is another burden.

Jumpstarting your cybersecurity best practices: our top five recommendations.

1

Boost security culture with awareness and tools.

Build a strong security culture by encouraging active employee participation. It's not enough for them to understand how their actions affect your organization's security. Awareness is only the first step—ensure they have the right tools to help them change behaviors such as reusing or creating weak passwords.

OUR TOP FIVE RECOMMENDATIONS

2

Put people above policies.

Prioritizing security policies rather than people invites workarounds and creates security gaps. If you implement policies or security tools that get in the way of productivity, employees will find a way around them. They want to get their work done fast, without unnecessary frustration. Human-centric security balances business needs with security rather than meeting one objective at the expense of the other.

3

Embed security practices and awareness into all your processes.

Security awareness and training are not annual or even quarterly events. Work toward a security-first mindset by integrating best practices and training into everything your business does. Make security awareness and training an ongoing effort. Start building a strong security foundation from the moment you onboard new hires and find ways to consistently keep security a part of the conversation.

OUR TOP FIVE RECOMMENDATIONS

4

Start by boosting defenses in the riskiest areas.

Boosting cybersecurity is a multi-faceted process and all those layers can get overwhelming quickly, even for bigger organizations. Start by understanding your highest risks. For example, what areas create the biggest vulnerabilities for your people and processes due to the hybrid environment? What kind of tactics and attack vectors are malicious actors more likely to use against your organization? Work on the most urgent areas first and then continue to evaluate your priorities and add more security layers.

5

Measure progress—and iterate.

To boost your security posture over time, make sure you understand how well your initiatives are working. Determine your key performance indicators and the metrics you can use to measure progress. Monitor the results, share them with your employees, and consistently identify new areas for improvement. For example, if your password manager adoption rate is low, consider looking for a password manager that is easier to use and seamlessly integrates with your identity provider (IdP) and single sign-on (SSO) solution.

What to look for in a password manager

SIMPLICITY AND EASE OF USE

A password manager that's simple to use for employees, as well as admins, will greatly improve adoption rates. You can't afford to invest in a tool that's not being used consistently. Low adoption also means you're still exposed.

CONVENIENCE

Features such as autofill and syncing across devices are not simply convenient—they make your employees more productive and reduce frustration with digital tools. To encourage adoption, ensure you educate employees about these features.

WHAT TO LOOK FOR IN A PASSWORD MANAGER

ROBUST SECURITY

Password managers are designed to help employees securely create, store, and manage passwords—but you should demand a lot more from your password management solution. Features such as password sharing and simplified onboarding and offboarding further boost your security posture by eliminating high-risk practices such as emailing passwords or leaving accounts active long after employees leave the organization.

SSO INTEGRATION

As your business grows, your password manager should grow with it. Many organizations adopt SSO as their processes mature, and ensuring that your password management solution integrates with SSO will reduce rollout issues later.

WHAT TO LOOK FOR IN A PASSWORD MANAGER

PASSWORD HEALTH

To measure progress, you need metrics, and password health is a powerful indicator of how well your security initiatives are working. A password manager that offers a password health feature helps employees understand their habits while helping admins uncover gaps and take corrective measures.

DARK WEB MONITORING

Employees need to act quickly when their credentials are compromised. A password management solution that integrates dark web monitoring will send your employees alerts when their logins appear on the criminal underground and immediately prompt them to change their affected passwords.

About the research

We conducted two separate surveys at organizations ranging in size from 50 to 500 employees, both in the public and private sectors. The first survey included 604 workers and managers, and the second included 305 IT decision-makers.

Participants in the worker/manager survey represented a cross-section of teams, including operations, administration, and finance, to name a few. In total, 23 sectors were represented.

The surveys were distributed in North America and Europe, and responses were classified evenly across organizations with 51–100, 101–200, and 201–500 full-time employees. Additionally, we conducted in-depth interviews with a small, select group of IT decision-makers, including managed security providers.

Inspired by the results?

Start implementing better cybersecurity with a password manager—no matter where your employees or offices are.
Learn more in our latest guide.

Learn More

For more information on Dashlane plans for business,
sign up for a trial or visit our website.

About Dashlane

Dashlane offers businesses a password management solution that is as easy to use as it is secure. Admins can easily onboard, offboard, and manage their employees with the assurance that company data is safe. And employees can enjoy a way to manage their work and personal accounts that's already loved by millions.
Our team in Paris, New York, and Lisbon is united by our passion for improving the digital experience and the belief that with the right tools, we can help everyone realize the promise of the internet. Dashlane has empowered over 15 million users and over 20,000 companies in 180 countries to dash across the internet without compromising their security.

LinkedIn:
https://www.linkedin.com/company/dashlane

Twitter:
https://twitter.com/dashlane

Instagram:
https://www.instagram.com/dashlane

Blog:
https://blog.dashlane.com

DASHLANE