1Password

The 1 for Business

The guide to creating a culture of security

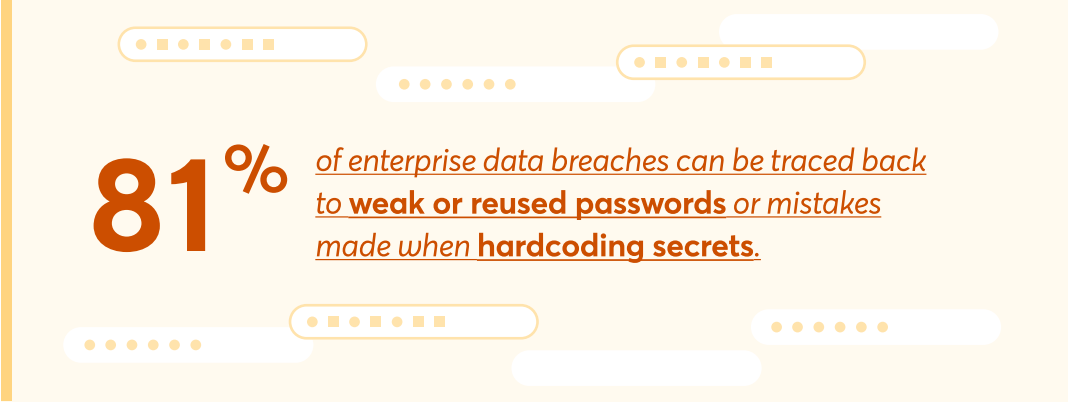
Contents

The guide to creating a culture of security

Your business data has never been more valuable or more vulnerable. Faster development, countless apps, smart devices – new security gaps are being created each day, putting your critical data at risk. The recent shift to remote work has accelerated this transformation, with distributed end points and less oversight into security protocols and employee behaviors. And costly investments like single sign-on and multi-factor authentication, while useful, don't offer the full coverage that you might think.

At the same time, cyber threats are both evolving and multiplying. Losses from cybercrime such as data breaches **rose six-fold in 2020**, with more than 37 billion records compromised. An average data breach can cost a business upwards of $4 million, damage consumer trust irreparably – and worse, put customers at personal risk.

All it takes is a slight human error – that is, weak or reused employee passwords, or mistakes when hardcoding secrets into applications. A single entry point can give a cyber criminal access to your most sensitive data.



Password or secret management habits are rooted in your company's security culture. Or, for too many businesses, the lack of one. How management and IT think about security risk management is at the crux, and holistic security involves everyone at the organization. In short, **security is not an isolated task**. Decisions like the tools you use and the policies you implement all play a part, so employees do their jobs the secure way – and keep the business safe as a result.

Company security: the perception and the reality

Around 80% of IT security leaders currently feel their organization lacks sufficient protection against cyberattacks, according to a recent IDG survey. There's a central theme: Everyone outside of IT thinks security is just an IT problem, and IT thinks it's an "everyone else" problem. The truth is, both are right.

Perception	Reality
Employees are creating strong passwords.	**45% of U.S. adults** use weak passwords (8 characters or fewer.)
Company security guidelines are being followed.	**70% of U.S. workers** think it falls on the company to protect work accounts.
Employees aren't using software not installed by IT.	**63.5% of U.S. workers** have created at least one account that IT doesn't know about (aka shadow IT).
Access management tools (SSO, MFA) cover all the bases.	**33% of those who created shadow IT accounts** reused memorable passwords.
Logins are only shared securely, on a need-to-know basis.	**36% of IT/DevOps workers** share credentials over insecure channels to save time.
DevOps would never be lax with secrets or credentials.	**81% of IT/DevOps leaders** have reused secrets between projects.
Engineers know not to hardcode passwords or secrets.	**85% of exposed company secrets** were found on developers' personal repositories.

91% of workers understand the risk of password reuse...

but **66%** admit to doing it anyway.

This shows the core problem, in a vacuum:
Proper security risk management requires everyone at a company to do their small part, but they likely aren't – because they don't have the tools or guidance.

Today's dev-centric enterprise has complicated the issue further. DevOps is managing more vulnerable secrets than ever before. Often choosing the fastest route in production, they'll skip over steps to protect this data (ex. tokens, certificates). Case in point:

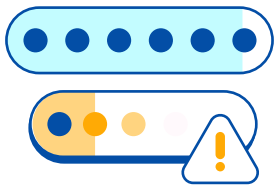
80% *of IT/DevOps organizations admit to not managing their secrets well.*

60% *have experienced secrets leakage.*

With this in mind, it's time to rethink our approach toward security, to stay truly protected in these tides of change, and keep your customers safe as well.

Bad habits, good intentions: the (many) roots of the problem

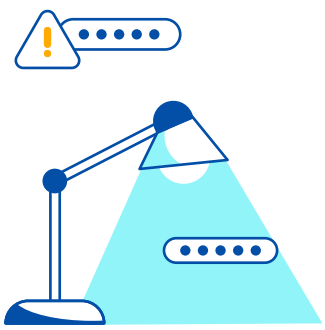
Let's shoot straight: **Weak passwords and secrets are your single greatest vulnerability.** And your workforce, including executives and managers, is partially responsible. But that's often because they aren't given the tools or guidance to help.



A third of workers repurpose **only 2-3 passwords** for all their accounts – when likely registered for 100 or more at any given time. And even this small handful of unique logins may not qualify as "strong." In the U.S., for example, **45% of adults use weak passwords** of only 8 characters or fewer.

DevOps has their own set of challenges. Speed has become the rule in today's development, sometimes to a fault; in-house dev teams might be taking daily shortcuts to meet the lofty deadlines set by the organization. This can include hardcoding access information into programming, which then gets shared far and wide.

This need for productivity is coursing through the work environment as a whole. Employees across the organization are continually looking for ways to work faster and get stuff done. They'll download apps and tools not covered in the company's approved – and protected – stack. This shadow IT without enforced password behaviors makes it nearly impossible for IT to maintain oversight, until it's too late.



Remote work has been another security pain point, despite the positive (and overdue) paradigm shift. Almost overnight, a majority of office-based businesses transitioned either fully or partially to remote and hybrid work. In the process, security protocols were often relaxed or simply went unchanged despite this seismic transformation, while shadow IT usage skyrocketed. Many will return to the office in 2021, but remote work is here to stay for millions, with its added risks in tow.

Another feature of today's enterprise is outside contractors and agencies, who collaborate on files with the in-house team and often have loosely monitored access to sensitive data. In many cases, these workers aren't being trained in or held to security protocols like your internal employees.

Lastly, what happens with employee accounts when they change departments or leave the company? Permissions and secrets will leave with them. When this happens, the team will be locked out, unable to access what these secrets were created for. In some situations, it can also leave dormant accounts that don't get updated properly when compromised. And beyond the usual threats, disgruntled former employees may pose a threat as well – **77% of IT and dev workers still have access to a past employer's infrastructure secrets.**

Productivity and modernization don't have to come at the expense of security. But that's unfortunately the case for many organizations. What your team may be doing to save time is putting your company at risk. When you put security first – across your entire business, and not just with IT – you will naturally speed up workflows, while keeping you and your customers safe.

Creating a culture of security

What does a culture of security look like?

Security should be a team effort – with every single employee involved. That's the essence of a "culture of security." By nurturing this mindset, you'll discover benefits across your organization. Not only will you protect the business and its customers, but also increase overall productivity by letting employees work the way they need to work – while staying secure in the process.

It will take time, training, and ongoing reinforcement. But the effort is far outweighed by the results. And your team, business partners, and customers will thank you for putting security first.

What a culture of security can do for your business

- **Enable your team to be both productive and secure**

  Free your employees to work in ways that make them productive without losing peace of mind. Provide the right tools and guidelines from their first day, and let them use the personal tools they need with the aid of a password manager.

- **Lighten the load on IT**

  By sharing responsibility for security risk management across your whole organization, IT will deal with less support tickets, password resets, data breach attempts, and stress overall.

- **Secure DevOps processes and streamline development workflows**

  Protect your company's machine secrets and help direct them to the right people, services, and apps at the right time. Empower your DevOps team to work securely without slowing or stalling production.

Read more about 1Password Secrets Automation

- **Gain better oversight of all the tools your team is using**

  You can also keep track of employee password hygiene across their tools, and stay notified of any accounts that are compromised. This way, even when security issues (inevitably) arise, you can prevent them from becoming a problem by quickly updating these accounts.

- **Help employees stay secure at work and at home**

  The line is blurring between work and personal life, and better protection of personal accounts and home devices means tightened security for the company.

How you can build it

With a thoughtful, methodical approach, you can design a lasting culture of security and close your biggest security gaps. In doing so, security risk management will be a built-in feature of your business, rather than a moving target you're always chasing.

A fully realized culture of security won't happen overnight. It's a labor of love, and thoroughness is crucial. Do it right the first time, so you don't discover holes or run into confusion later on.

Prepare

- Write new security policies
- Create training content
- Update onboarding resources
- Build compliance into reviews

Determine the policies and protocols with buy-in from leadership, IT, and the Security team. Then, nail down your education materials (e.g. security guidelines, password policies) and the tools that will be cornerstones of your security risk management strategy, such as an enterprise password manager.

Launch

- Upload and share policies
- Deploy software and schedule training
- All-hands kickoff event

Upload your policies and deploy the software that will define your culture of security, rounded out by a formal kick-off event. This is not a blip on your company's radar – it's a complete shift in your way of thinking. Treat it seriously so your employees (and contractors) will do the same.

Roll out

- Existing employees
- Contractors
- New employees

Even with the best intentions, employee training will make or break this culture shift in your organization. Hold engaging, comprehensive (and mandatory) training sessions for both new and existing employees on these policies and tools they'll use to achieve them, with ongoing education you can plan at regular intervals.

Reinforce

- Gamification – reward safe habits
- Provide ongoing support
- Monitor, tweak, repeat
- Periodic training to ensure compliance

Security risk management training should be an ongoing event on your calendar. Tweak your approach where needed, award employees for their involvement, and reinforce best practices with periodic training. Don't just remind your team of their role, but help them feel empowered and supported.

Revisit

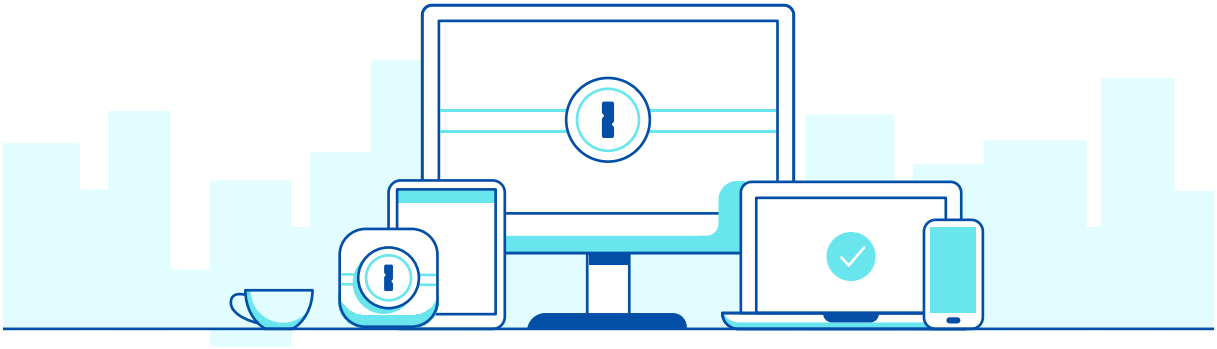
The threat landscape changes quickly and often – even with the tools and guidelines in place, you can never get too comfortable. Your security tool providers should help ensure you have the latest technologies and insights to stay current, and IT should update company policies and provide new training when the time calls.

See our infographic on how to build a culture of security

Learn more

Choosing the right enterprise password manager is a huge leap in the right direction. Approximately 59% of people manage their passwords by memory, and are often using weak or reused passwords even if they are safely organized.

A password manager should tackle both problems, with password creation, storage, and sharing all in one place. 1Password offers all this, plus cross-platform compatibility (including Mac, iOS, Windows, Android, Linux, and Chrome OS), syncing across devices, Secrets Automation, and more.



What's next? Like anything worth doing, a culture of security takes some effort. To start, identify the people on your team who will be steering the initiative. There are several roleplayers who will work together toward the end goal.

Leadership

The executive team sets the tone and direction for a culture of security. With leadership on board, the HR, IT, and Security teams can invest time and resources into defining protocols, employee training, software rollouts, and so on.

Security and Privacy teams

These teams are integral in creating a transparent, judgement-free culture of security so employees can speak up with questions or when issues arise. They can also help empower employees to secure their own tools and devices, when handled properly.

IT and DevOps

A culture of security, and the org-wide behavior changes that are involved, should not fall squarely on these teams. But they can implement the tools that make it achievable, such as 1Password.

HR

Security risk management, including training on password management policies and software, is a must-have in today's employee onboarding. Your HR team needs to build out initial process training and ongoing education into new hire roadmaps.

> 1Password customers Sigrid.AI and Intercom explain how onboarding that includes 1Password has transformed their training experience, and helped instill safe habits while boosting collaboration and productivity:
>
> *"[1Password] is part of the culture for many teams, and the company in general to an extent."*
>
> INTERCOM
>
> *"Every team member at Sigrid.AI uses 1Password, and all of our clients are integrated into the 1Password ecosystem as part of our standard client onboarding process."*
>
> Sigrid[AI]

Team managers

Department heads and team managers are key role players in the top-down effort, encouraging and empowering employees to follow best practices. They should be readily available as a first line of communication, to help resolve issues and nurture good security habits.

Individual employees

Whether your staff is 10 or 10,000, they each need the right tools and education when it comes to security risk management. Following policies and building safe habits is a consistent task for each and every person at your organization.

Making the shift to a more secure culture

Department	Mindset shift	Behavior shift
Leadership	We are a security-first company. Employees need the right tools and guidance to work securely.	Show employees and customers that you believe it. Work with department leaders to shape strategy and roll out tools and policies.
HR (onboarding)	Everyone needs to do their part. Security is integral to the company's success.	Update employee handbook and onboarding process. Incentivize involvement and add to performance reviews.
IT Leaders	Our company can do better at managing passwords and secrets. We're not alone in building this culture.	Send reminders and offer help in shifting habits. Download 1Password resources and share with employees.
Security	Poor password habits make the company vulnerable.	Work across the company to build and strengthen policies.
DevOps	We don't have to slow down to be safe. Some breaches are our team's responsibility.	Use Secrets Automation tools to help prevent hardcoding. Get on board with tighter security policies.
Team managers	My team is crucial to overall company security.	Reinforce best practices and offer help wherever possible.
Employees	I am an active contributor to company and customer safety.	Develop secure passwords with 1Password, and follow security guidelines.

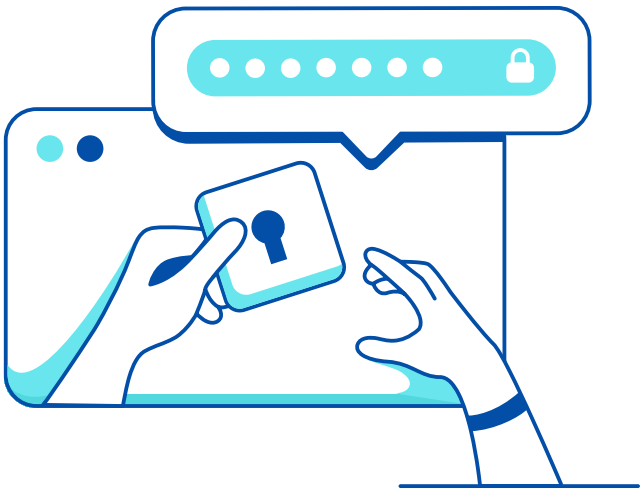
Where to begin

Like all great endeavors, a culture of security begins with a single step. Gather your executive and IT leadership teams for a kickoff meeting. Explain the problem and the solution. Build awareness and excitement. Determine goals and make a timeline to reach them.

Company-wide education should follow. Every employee, including contractors, should understand the risks of using technology and the internet, and how their individual accounts are entry points to the company's data as a whole. The solution is quite simple, and effective security risk management is achieved when everyone does a few small things consistently.

A password manager like 1Password should then be deployed, if it's not part of your stack already. Not only will it be an essential security tool, but improve productivity and collaboration across your business.

> *"We've seen employees adopt 1Password and its sharing capabilities into their daily workflows. And even turn it into a verb: '1Password it to me.'"*
>
> ada



Why 1Password?

Experience is everything. Creating unique, complex passwords for every account is tedious without the right platform – which can lead to a lack of motivation and, in turn, employees creating weak passwords or reusing old ones. You'll need a password manager that integrates easily with existing tools, doesn't impede productivity, is easy to manage, and creates strong passwords with just a click.

A password manager only works if everyone uses it. High usability = more adoption = greater security. 1Password offers the best possible security through the most user-friendly platform on the market. This has helped **more than 80,000 businesses transform their information security** and get everyone involved.

> *"Any tool that, like 1Password, we deploy to every person and every user endpoint at Intercom has to be something we are confident people will be able to use easily. It's something that weighs in on many of the decisions we make when considering its infrastructure."*
>
> INTERCOM
>
> *"1Password makes complex processes easier and integrates them seamlessly into practice. And, as a result, helps us stay true to Flo's security and privacy principles."*
>
> Flo
>
> *"If a password manager fails to deliver a good user experience, people might opt-out of using it at all, or use it in the wrong way. 1Password has a simple user interface, all the features we need, and is very healthy security-wise – exactly the combination we were looking for."*
>
> detectify

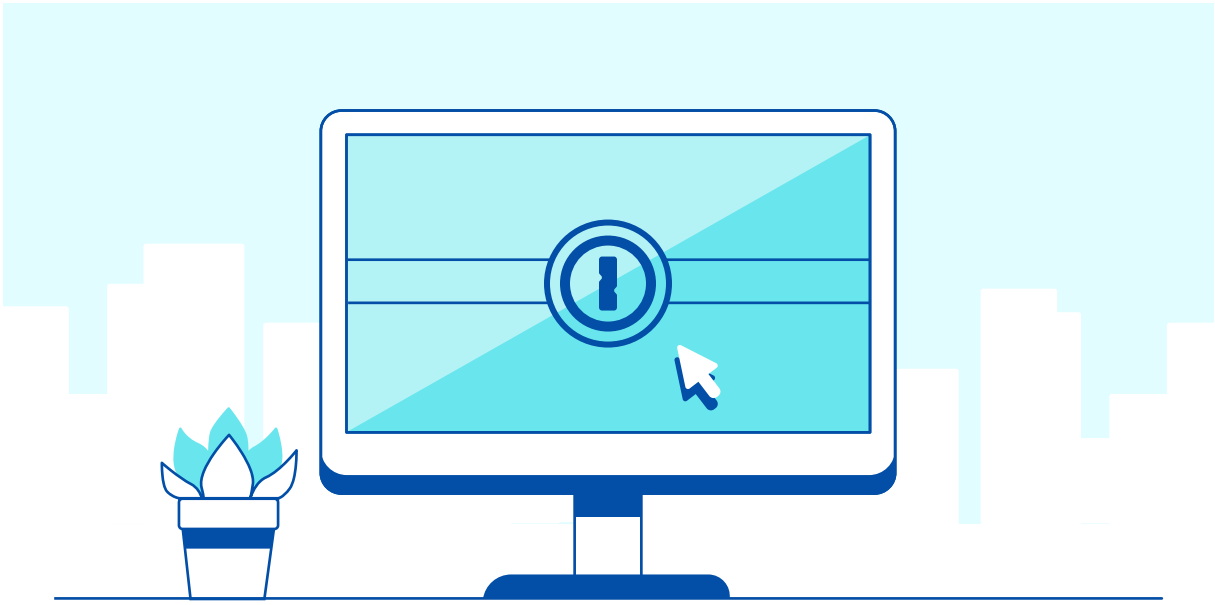
We understand the ever-changing needs of our customers; feedback is what drives our product roadmap. 1Password is **built for today's enterprise**, with seamless integrations into the security and collaboration tools you already use. Along with your company passwords, 1Password can help manage your infrastructure secrets, legal documents, corporate credit cards, and other sensitive data. All with the highest standards in data privacy.

Administration is effortless. IT can deploy 1Password in minutes to the entire organization, and solve your number-one security problem by enabling employees to create and manage strong, unique passwords for all their accounts. And with data breach reports and notifications, you can take fast action if any accounts are compromised.

Already trusted by some of the biggest names in tech

IBM slack PagerDuty GitLab

We're dedicated to your business making the most of 1Password, with no bumps along the way. Our Support team is available to help with any aspect of your experience, both in using 1Password and building a culture of security on top of it. Webinars, blogs, and a responsive social community set you and your team up for continued success, long after you get started.



Start building a culture of security today

Head to 1Password.com/business to sign up for a 14-day free trial, or contact the 1Password Sales team to chat and learn more. Follow us on Twitter and LinkedIn, and visit the 1Password blog for product tips, company updates, and more.

1Password is the world's most-trusted enterprise password manager, used by more than 80,000 businesses of all sizes. Industry-leading security and usability help teams create strong passwords for the apps and services they use, and protect this sensitive data – as well as legal documents, machine secrets, credit cards, and more – from online threats.