1Password

Data breach prevention checklist

A proactive approach to cybersecurity

Data breaches affect businesses of every size and industry, and the risks posed by data breaches are only growing in the modern workplace. The shift to remote and hybrid work and faster-paced development cycles can lead to less oversight and poor security habits, exposing new vulnerabilities that can be exploited by criminals.

$4.4 mil

the average cost of a data breach.
IBM

66%

of employees admit to poor credential hygiene practices.
1Password

46%

increase in global weekly cyberattacks per organization.
Check Point

60%

of data breaches are traced back to a human element like weak or reused passwords.
Verizon

Protecting your organization (and yourself) is an ongoing challenge as threats evolve over time. The problem is overwhelming, and it can be difficult to know where to begin when it comes to protecting a company.

The key is to invest in the right people, processes, and technologies to reduce your risk and build resilience into your business security as a whole. The following data breach prevention checklist is designed to help teams of any size create a proactive defense against cybersecurity threats.

To help keep security focused and achievable, we'll begin with the **top three recommended steps** that teams should take to secure an organization.

Data breach prevention checklist: How to start

According to the 2025 Verizon Data Breach Incident Report (DBIR) the number one attack vector used by bad actors to breach companies are weak and compromised credentials.

As such, to protect your company, you should begin by focusing on managing and securing your credentials. Thankfully, managing credentials is extremely achievable. The first three steps of this checklist are realistic and impactful measures that you can take today to keep your organization secure.

The first three steps to secure credentials

1.

Use a unique sign-in for every account

The vast majority of people reuse passwords across multiple accounts, and hackers love to take advantage of this. One of the most impactful steps you can take to secure your business would be to make sure that every site you log into has a unique sign-in.

Get started:

Use a tool like 1Password, so that even if one user's Facebook password gets stolen, hackers can't use it to log into the user's Salesforce account.

2.

Securely share team accounts

Teams need some way of securely sharing passwords between employees. Ideally, those passwords should be encrypted or otherwise protected as they're stored or shared, as storing credentials in plaintext can all too easily expose them to compromise.

Get started:

With 1Password, you can securely manage and share access to teams' information.

3.

Secure developer secrets

In a 2023 survey, 73% of developers agreed that their work's security tools interfere with their productivity. When that happens, developers often look for faster workarounds - like hard-coding credentials: GitHub found 39 million secret leaks in 2024, and Verizon found that the average time to remediate leaked GitHub secrets is 94 days. If they're not secured properly, these secrets pose an outsized risk to a company's most critical infrastructure and data.

Get started:

Enable developers to access secrets in a way that's both streamlined and highly secure with 1Password.

These three measures are the first things that small teams should prioritize when building up their security. Ensuring that credentials and access are secure will have a major impact on a company's ability to guard against breaches.

We won't pretend that these measures are always easy to implement. Particularly as a company grows, it can be easy to become overwhelmed by the growing number of unique credentials they need to be able to store and share. However, with the correct tools – like a business password manager – all of these methods are achievable for teams of any size.

When looking to improve security, these are the initial steps to prioritize. Once these are achieved, you can begin thinking of the next steps to take for your company's security.

Data breach prevention checklist: Maturing security over time

Once you've built up systems to securely manage credentials, your team can begin to prioritize the next steps you want to take to mature your overall security program. There's no particular order in which these steps must be followed, as one team may need to prioritize certain measures over others. Rather, think of the following checklist as a tool to better understand your company's broader needs in securing your **people, processes,** and **technology.**

People

- **Provide ongoing security training**

  By educating your team on common types of social engineering attacks, like phishing, you set them up for success in avoiding security pitfalls that put your company at risk.

- **Create an anonymous reporting option**

  Some team members may not be comfortable coming forward with potential security risks like insider threats. Create a way for anyone in the company to report issues, missteps, and suspicious activity.

- **Create a culture of security**

  Helping establish and enforce mindful habits across your company will protect your business and its customers. Learn how one company built an ingrained security culture.

- **Hire a cybersecurity consultant**

  Having a professional assess your company's overall security and test for vulnerabilities could reveal blind spots and weaknesses, while also advising on opportunities for improvement.

- **Employ the principle of least privilege**

  Only give employees access to what they need to complete their jobs. With 1Password you can enforce access control for the use and secure sharing of passwords and other sensitive information.

Processes

- **Make an incident response plan**

  Part of being proactive is having a playbook in place if you do experience an incident. Check out our Incident Response Guide to learn how to create an incident response plan.

- **Monitor your security health**

  Review security reports regularly to identify potential exposure risks before they're exploited. With 1Password you can use our Insights dashboard, which gives a company-wide view of security risks to your organization and also integrates with Watchtower and our SIEM partners.

- **Establish a way to securely share information**

  Data breaches can occur while information is in transit. By providing safe ways to share passwords, secrets, and other data you can help prevent your information from ever being at risk.

- **Encrypt your data**

  By encrypting your data, you ensure that even if someone manages to acquire it they won't be able to read or use it.

- **Regularly review your security plan**

  Security risks are always evolving. You need to adjust your strategy as well to keep pace with the changing security landscape. Create a process that allows you to consistently review your security measures as your company scales and transforms, so you're not caught with outdated practices.

Technology

- **Use a password manager**

  If you haven't already, adopting a password manager gives you stronger, better-managed company secrets and helps your team build safer habits while also working more productively.

- **Use a unique email address for every account**

  The 1Password and Microsoft 365 Email integration helps you set security policies regarding employee email accounts.

- **Enable two factor authentication (2FA)**

  1Password can act as a 2FA authenticator, helping you manage and enforce 2FA as a security measure for your team. manage and enforce 2FA.

- **Monitor SaaS tools for risk**

  It's important to enable teams to get their work done with the tools they prefer. However, SaaS sprawl is a growing problem, and 80% of employees use non-sanctioned shadow IT. IT and security teams need to monitor and secure all SaaS being used at their company, whether managed or unmanaged.

There’s no such thing as a perfect security program, and there’s no perfect security checklist either. The goal of this document is to help you understand the first steps you should take as you map out your journey to better security. That work is well worth the effort; not only does it guard your company against costly breaches, it can even be a competitive advantage, as OneMethod learned when they strengthened their cybersecurity posture.

1Password is the world's most-trusted enterprise password manager. Industry-leading security and usability help businesses securely manage passwords, secrets, and private documents to protect their most sensitive data from online threats.

Ready to learn more? Read our guide on how to convince your leadership team that a password manager is a necessary investment or get in touch with our team for a personalized demo.

Conclusion

1Password

We've seen that employees will find ways to work around security systems that interrupt their workflows, unintentionally exposing their company to risk. It's up to IT teams to adapt to how and where their team is getting work done. Productivity and security don't have to be a "one or the other" option.

That's why over 175,000 businesses rely on 1Password's Enterprise Password Manager to secure their business. With 1Password, companies are able to secure every sign-in, regardless of where your workforce is. 1Password is built with your team in mind, ensuring they're secure without slowing them down.

Learn more about 1Password for small and mid-size businesses.