1Password

Data breach prevention checklist

A proactive approach to cybersecurity

Data breaches affect businesses of every size and industry – and they occur more often than you think. The shift to remote and hybrid work, increased **employee burnout**, and faster-paced development cycles can lead to less oversight and poor security habits, exposing new vulnerabilities that can be exploited by criminals.

$4.24 mil

the average cost of an enterprise data breach.

Verizon

10%

increase in the average total cost of a data breach from 2020-2021.

IBM

80%

of IT leaders feel their company is unprepared for an attack.

1Password

50%

increase in global weekly cyberattacks per organization year-over-year.

Techradar

Protecting your organization (and yourself) is an ongoing challenge as threats continue to evolve over time. Investing in the right people, processes, and technologies can reduce your risk and build resilience into your security – and by extension, your business as a whole. Follow our data breach prevention checklist to help create a proactive defense against cybersecurity threats.

Data breach prevention checklist*

Set up a review process for new tool/software requests

Help reduce friction and make it easier for your team to get their work done with the tools they prefer. But, if they are using shadow IT, make sure they know how to use those additional tools safely.

Create a culture of security

Helping establish mindful habits across your company will protect your business and its customers. Download our guide to creating a culture of security.

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.

Use a unique email address for every account

The 1Password and Fastmail Masked Email integration helps protect you from spam and phishing attempts.

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.

Establish a way to securely share information

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

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.

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.

Hire a cybersecurity consultant

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

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.

Regularly review your security plan

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

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.

Use a password manager

By adopting a password manager, you'll have stronger and better-managed company secrets and help your team build safer habits while also working more productively. Read our guide on how 1Password can help prevent a data breach.

82%

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

Verizon

85%

of exposed secrets are found on developers' personal repositories.

GitGuardian

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.

Find out more at 1Password.com.

*This is a general overview of preventative measures you can take to help secure your business – there is no one-size-fits-all security solution, so not everything on this list may be relevant for you or your business.