

RESOURCE CENTER

Bitwarden 2024 Cybersecurity Pulse Survey

Discover what keeps IT and cyber professionals up at night.

Get the full interactive view at

<https://bitwarden.com/ja-jp/resources/2024-cybersecurity-pulse-survey/>



What will you learn in the 2024 Cybersecurity Pulse Survey?

Bitwarden partnered with Researchscape International to survey over 1,100 IT and cybersecurity leaders across various industries, revealing the latest cybersecurity trends and threats. This year's findings underscore rising concerns about generative AI risks, third-party supply chain vulnerabilities, and sophisticated social engineering tactics.

Despite increasingly advanced threats, consensus remains clear: mastering cybersecurity fundamentals, starting with strong password habits, is the best defense. IT decision makers agree that password managers remain a critical part of their security strategy, both at work and at home.

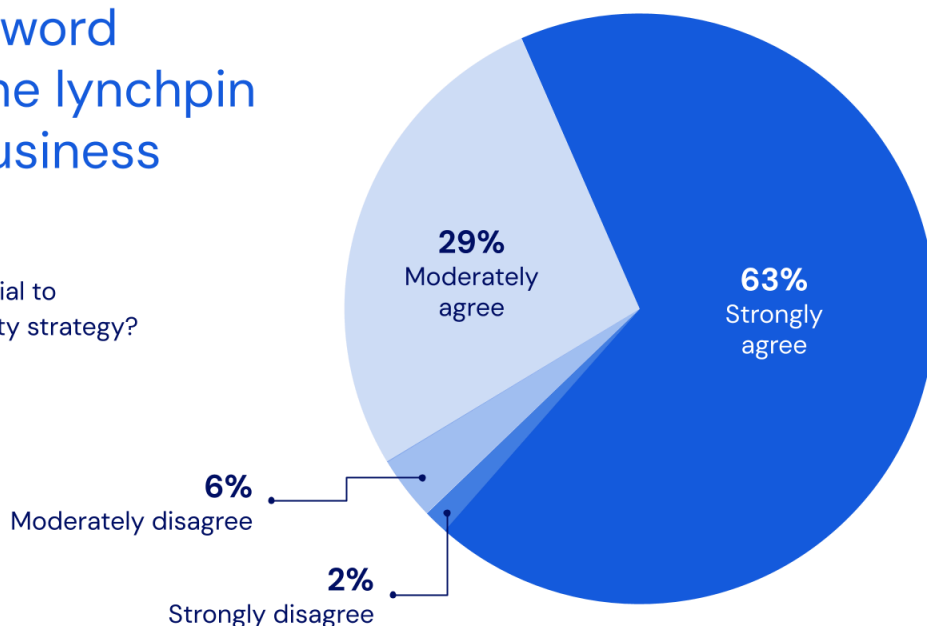
View the [full presentation](#).

Password managers play a critical role in security

- An overwhelming majority (92%) of respondents moderately or strongly agree that password managers are essential to their organization's cybersecurity strategy.
- 63% of respondents agree that, without a password manager, their IT teams would struggle to teach and enforce best practices across their organizations.
- 79% of respondents have recommended using a password manager to family members, underscoring the universal benefits of this tool.

92% agree password managers are the lynchpin to protecting business

Are password managers essential to your organization's cybersecurity strategy?



2024 Cybersecurity Pulse Survey



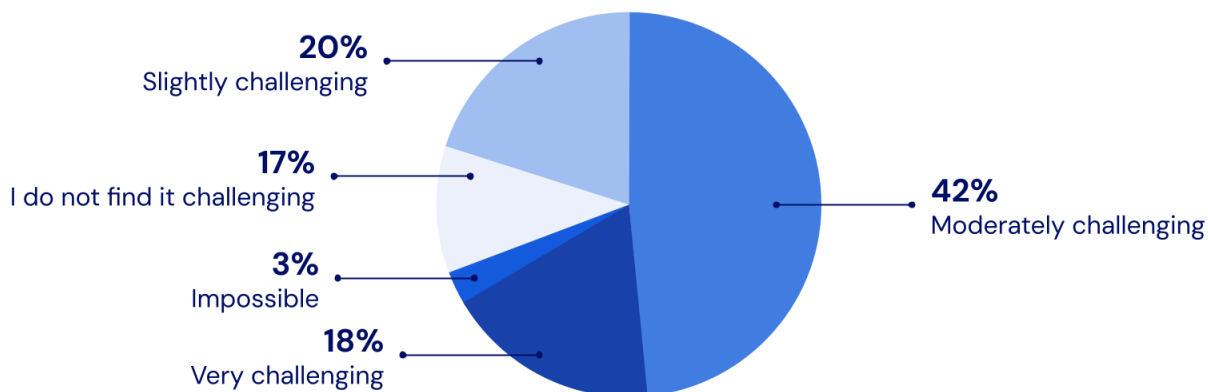
Passwordless authentication is also popular in the workplace – just 3% of respondents reported using no form of passwordless authentication at their company.

Generative AI poses a significant threat

- 89% of respondents expressed concern over the security risks associated with employees incorporating generative AI into their daily workflows.
- 63% find it moderately or very challenging to maintain a strong security posture as more employees use generative AI tools.

Generative AI adds complexity to maintaining strong security in the workplace for 63% in IT

How challenging is it for your organization to maintain proper approvals for devices and applications as more employees seek support from generative AI tools?



2024 Cybersecurity Pulse Survey



Learn more about how organizations can balance innovation and data security in the age of AI in this [free eBook](#).

Cybersecurity threats concern IT decision makers and business leadership alike

- 96% of business leaders discuss cybersecurity at least every month, and nearly half talk about it daily or multiple times a day.
- 55% of respondents expressed high concern about third-party supply chain attacks originating from vendors, partners, or customers.

96% of business leaders discuss cybersecurity monthly and nearly half talk about it daily

How often does your organization bring up cybersecurity, including in emails, meetings, or communications?

Multiple times a day	20%	Quarterly	3%
Daily	28%	Less often	1%
Weekly	30%	Never comes up	<1%
Monthly	18%		

2024 Cybersecurity Pulse Survey



Read more:

[Building a cybersecurity culture in the workplace](#)

Social engineering tactics are getting smarter

- Impersonation-based phishing attempts come in many forms; 46% of respondents reported receiving a phishing scam posing as their bank, 41% as their financial institution, and 36% as a government entity.
- 92% of companies have invested in cybersecurity training for their employees on best practices to identify and defend against social engineering scams.

Variety is the spice of life (and social engineering): 46% report financial institutions are the most commonly impersonated

What types of impersonation-based phishing attempts have you and your organization experienced in the last year?

Financial institution	46%	Job offer	36%	Health care organization	26%
Bank	41%	Boss or a colleague	31%	Family member or friend	22%
Government entity	36%	Shipping industry	28%	Other	5%

2024 Cybersecurity Pulse Survey



Read more:

[What to do if you think one of your online accounts has been hacked](#)