



# INSURANCE BUREAU OF CANADA

Cyber Savvy Research



# METHODOLOGY

This report includes selected findings from a survey conducted by Insurance Bureau of Canada from August 17 to 19, 2022, among n=1,525 employed Canadians aged 18+ who work at organizations with 2 to 499 employees and work primarily on a computer or other digital device. The sample was balanced on age, gender and region to the profile of the working Canadian population. All respondents are members of the online Angus Reid Forum. Interviews were conducted in English and French.

For comparison purposes only, a sample of this size would yield a margin of error of +/-2.5 percentage points, 19 times out of 20.

# HIGHLIGHTS



**Only 34%** of surveyed employees at small and medium-sized businesses report that their company provides mandatory cyber security awareness training



**42%** of surveyed employees at small and medium-sized businesses have seen an increase in scam attempts while at work over the last 12 months



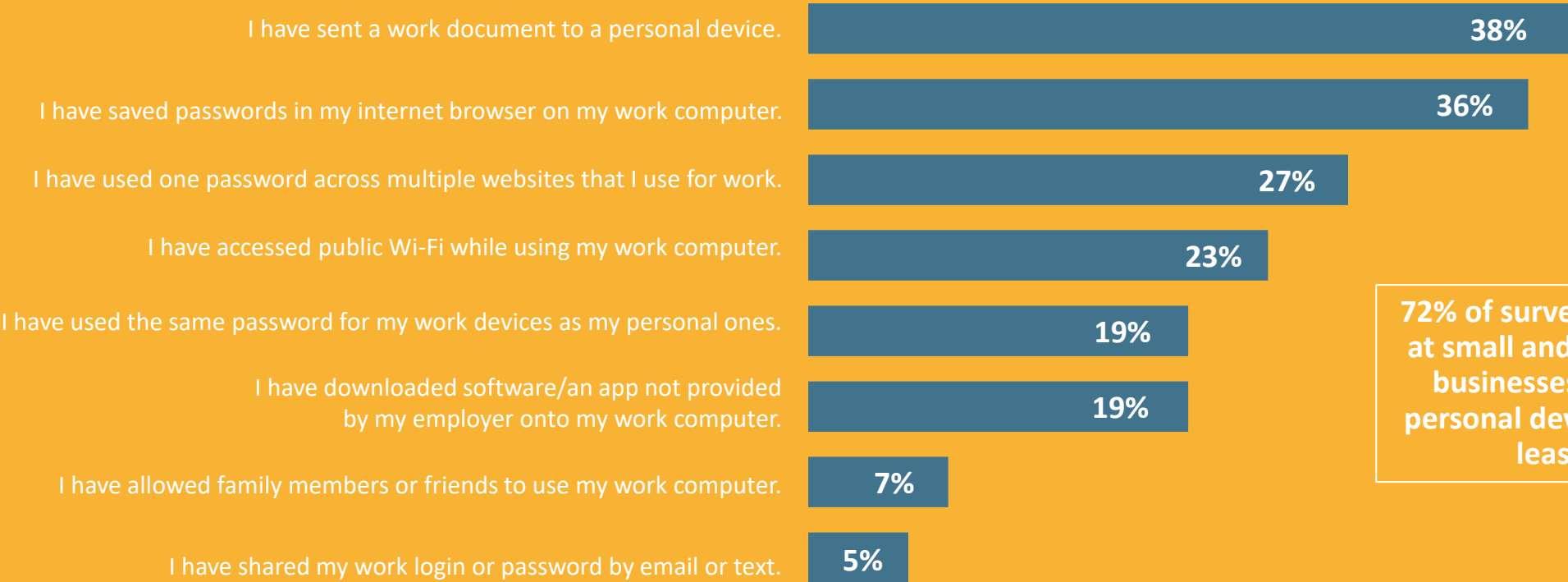
**72%** surveyed employees at small and medium-sized businesses reported at least one behaviour that could potentially compromise their employer's cyber security or data

# EMPLOYEE ACTIONS THAT COULD COMPROMISE EMPLOYER CYBER SECURITY OR DATA SAFETY

Majority (51%) of surveyed employees at small and medium-sized businesses are making it more likely for hackers to get a hold of workplace passwords through actions such as saving passwords in internet browsers and using one password for multiple websites or for work and personal devices.

Which of the following statements, if any, apply to you?

### ACTIONS TAKEN BY EMPLOYEES



72% of surveyed employees at small and medium-sized businesses have used a personal device for work at least once.

# REACTION TO SUSPICIOUS EMAILS & PASSWORD SHARING

Based on responses to cyber security knowledge questions, one-in-five (22%) surveyed employees at small and medium-sized businesses do not know how to properly respond to email phishing attempts, such as requests for personal information or company credit cards.

**Do you agree or disagree with each of the following statements?**

**Emails:**

If you get an email from someone at work asking you to share personal or sensitive information, you should first confirm they are who they say they are.



You should reply right away to an email from your boss asking for information for a company credit card to make an emergency purchase.

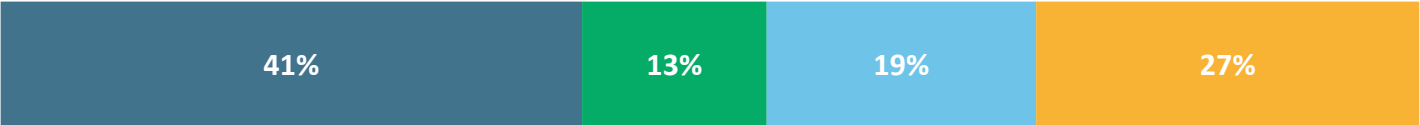


You should immediately click on a link or open an attachment if a vendor sends an overdue payment notice.



**Password sharing:**

You should only share your password or login with a work colleague if it is an emergency.

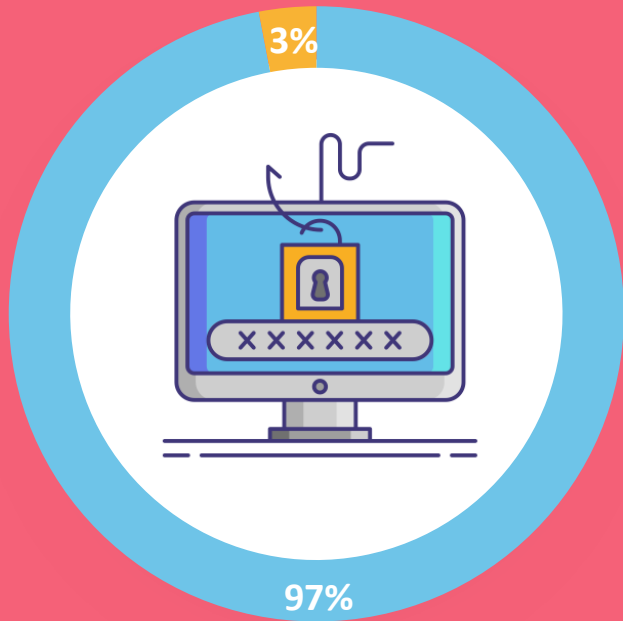


■ Strongly disagree    ■ Somewhat disagree    ■ Somewhat agree    ■ Strongly agree

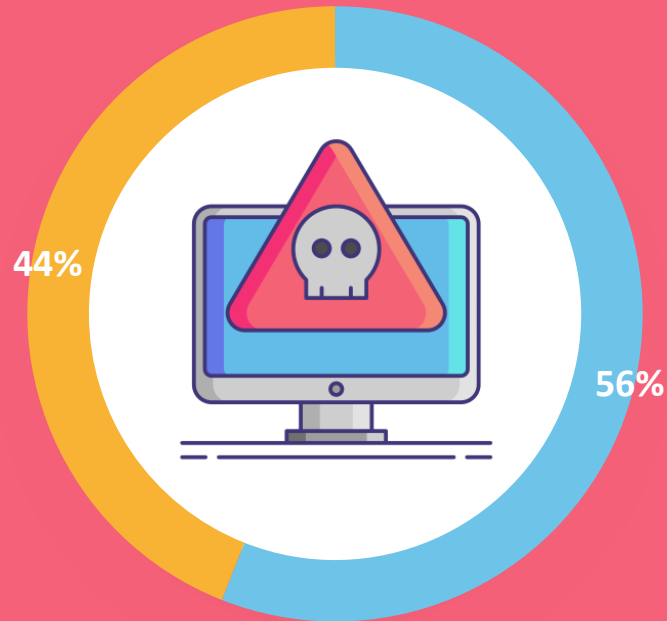
Agree
92%
12%
8%
46%

# UNDERSTANDING OF COMMON CYBER SECURITY TERMS

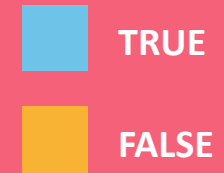
To the best of your knowledge, are each of the following statements true or false?



**PHISHING** Phishing refers to a scam where fraudsters appear to be a reputable source or someone you know in order to solicit confidential information. (True)



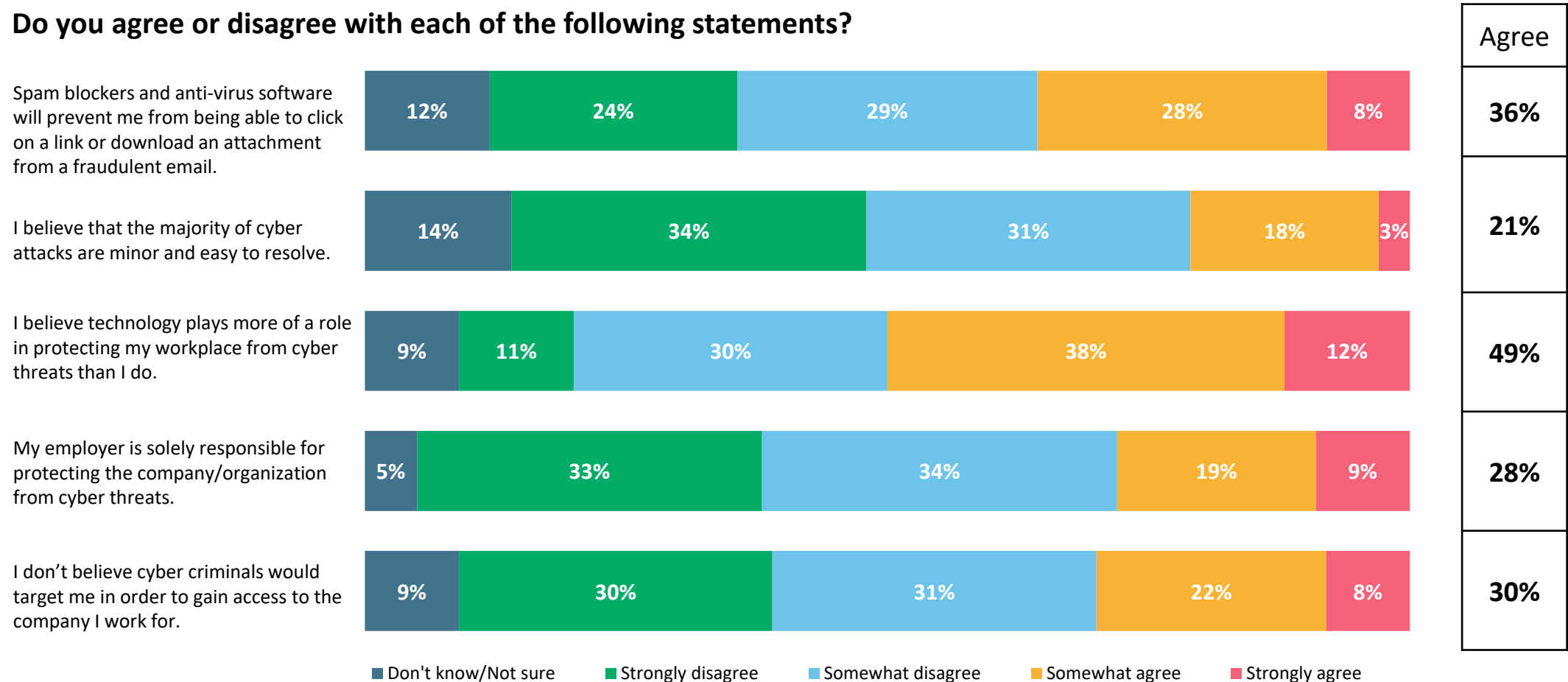
**RANSOMWARE** Ransomware refers to when a criminal steals your work computer and asks you to pay for it to be returned. (False)



# ATTITUDES TOWARDS CYBER SECURITY IN THE WORKPLACE

Many employees may underestimate the role they play in being cyber safe at work and the impact of cyber attacks on their employer.

**Do you agree or disagree with each of the following statements?**



# CORPORATE CYBER SECURITY MEASURES

Which of the following statements, if any, apply to you?

By company size (number of employees)

		2-19	20-49	50-99	100-499
My work computer has anti-virus software enabled	72%	71%	69%	72%	75%
My employer has a system in place to block suspicious email messages	57%	42%	52%	60%	70%
My employer has cybersecurity protocols in place	53%	36%	44%	57%	67%
I use multi-factor authentication to login to work accounts	50%	37%	46%	51%	61%
There has been an increased focus on cybersecurity at my company/organization since we shifted to hybrid/remote work	34%	19%	24%	36%	48%
My employer provides mandatory cybersecurity awareness training	34%	15%	28%	34%	50%
My employer conducts phishing email simulations to assist in promoting employee cyber vigilance and to uncover cyber vulnerabilities	24%	7%	17%	25%	39%
My employer has suffered a cyber attack/data breach	16%	12%	13%	15%	20%
None of the above	8%	12%	9%	8%	4%

■ ■ Significantly higher/lower than other groups at 95% confidence level





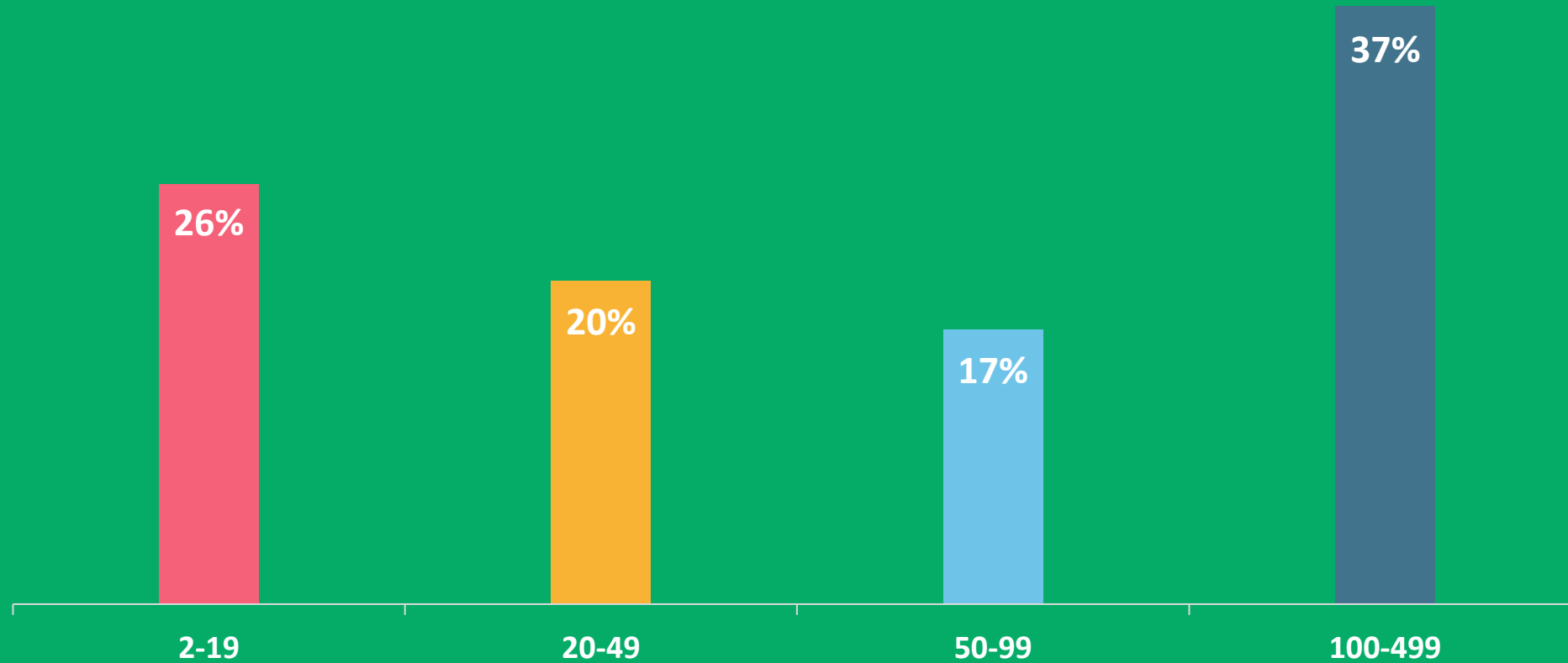
# DEMOGRAPHIC INFORMATION

Cyber Savvy Research

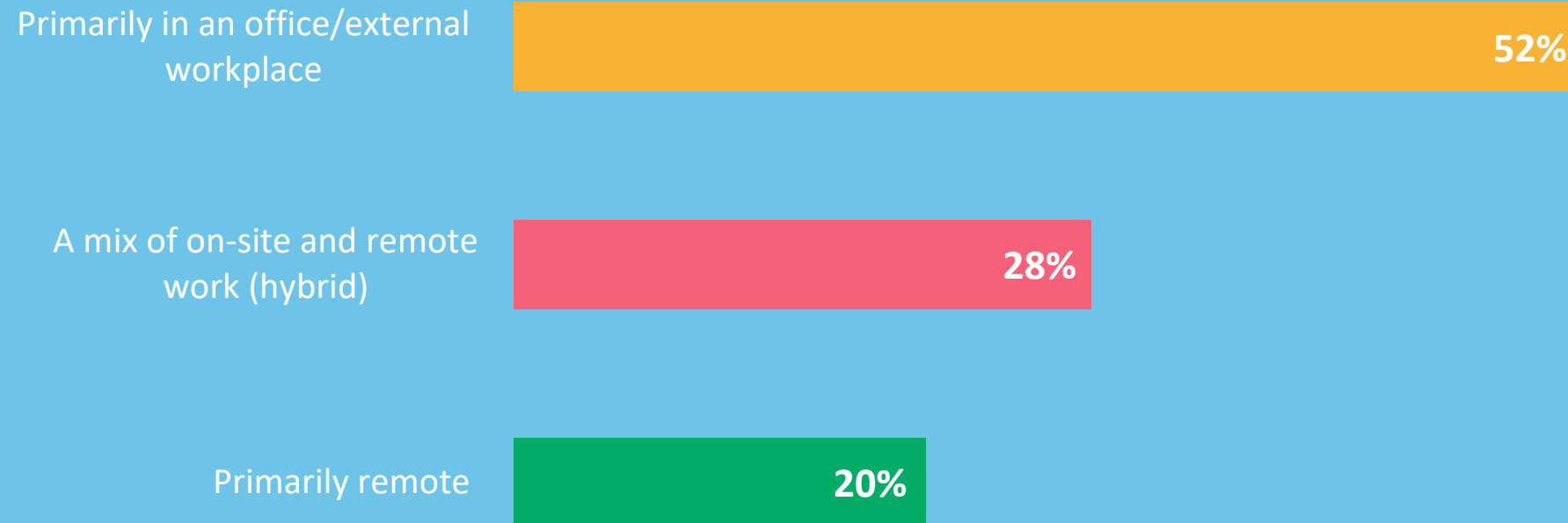


# SIZE OF COMPANY/ORGANIZATION

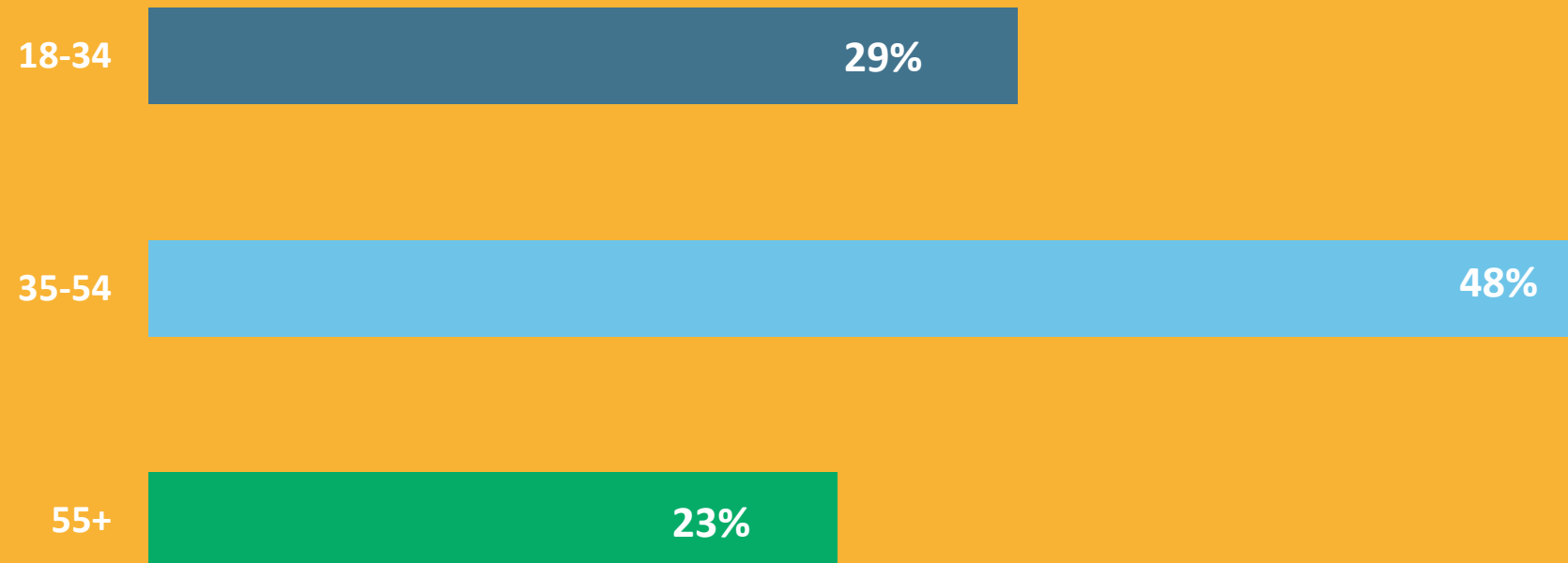
How many employees work at your organization or company?



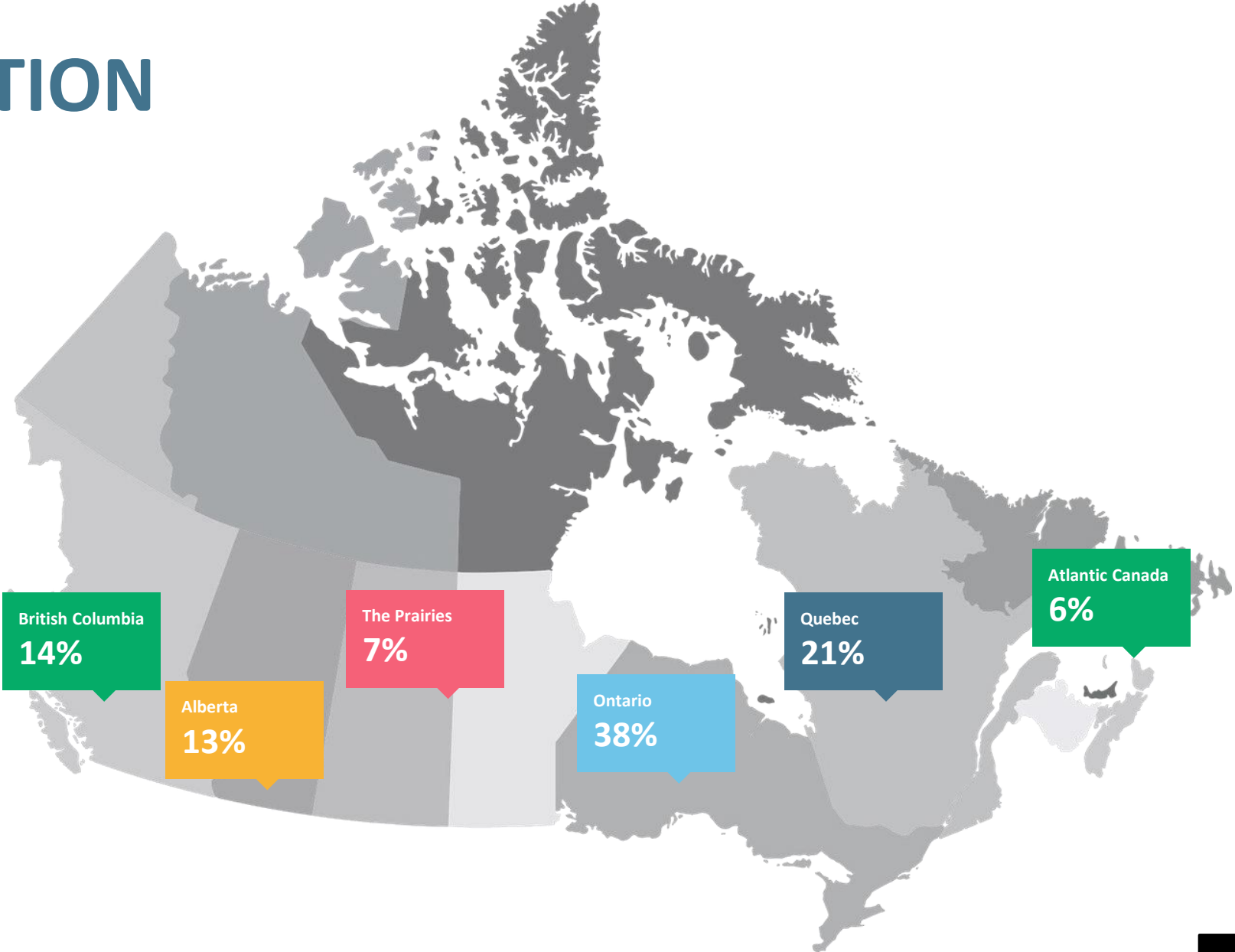
# WORK ENVIRONMENT



# AGE



# LOCATION





**cybersavvy**  
CHALLENGE



©2022 Insurance Bureau of Canada. All rights reserved. This document contains copyrighted material and is not to be modified, copied, reproduced in whole or in part, in any way, without the express written permission of Insurance Bureau of Canada. The content contained in this document is being provided for information purposes only.