



September 2023

# Nationwide Cybersecurity Survey Report

# SURVEY METHODOLOGY



## Audiences

### **General Consumers**

*Age 18+ - nationally representative by age, gender, race, region*



## Sample Size

**N=1,000**



## Methodology

**20-Minute  
Online Survey**



## Timing

**Survey Fielded  
August 8<sup>th</sup> – 19<sup>th</sup>, 2023**

---

# Cyber Security

# KEY FINDINGS

## 1 Cyber threats still are top of mind for consumers today

Over half (59%) of consumers are concerned about falling victim to a cyberattack. This concern is driven primarily by perceptions that cyberattacks have increased (55%), the use of AI technology (54%), and the proficiency of today's hackers (51%). When it comes to the various types of cybersecurity threats, consumers are most familiar with phishing (46%), malware (45%), and cyber bullying (44%), while roughly half are not at all knowledgeable about digital tax fraud (48%), deepfakes (51%), DoS attacks (53%), or digital unemployment fraud (54%).

## 2 However, consumers are not prepared to manage cyberattacks

Only a third (34%) of consumers feel prepared to prevent a cyberattack, and only 41% are confident in their ability to recover from an attack. As a result, nearly half (45%) would hire or outsource someone to lead the recovery process if they were to personally fall victim to an attack.

## 3 1 in 10 consumers have been victims of an attack, primarily related to stolen passwords, malware, and data breaches

Those who have personally been a victim of a cyberattack (10%) most commonly report experiencing password attacks (40%), malware (34%), and data breaches (30%). Only about half (53%) say they knew what to do when they identified the attack and 51% report an impact on their personal finances. As a result, many of these consumers have changed passwords (58%), updated cybersecurity software (40%), or purchased ID theft protection (31%).

## 4 A lack of knowledge is holding consumers back from purchasing both cyber insurance – but interest is increasing

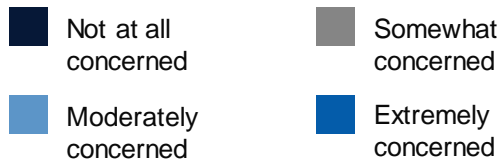
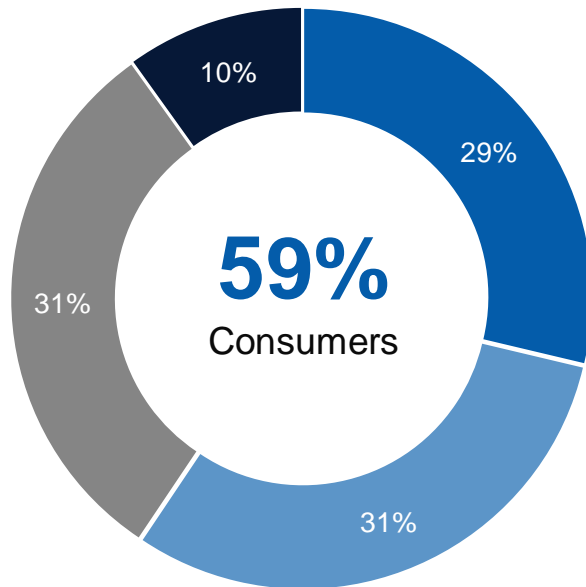
Very few consumers report currently owning cyber insurance (15%), with the top factors discouraging consumers from purchasing a policy surrounding a lack of knowledge (40%), a lack of awareness of their availability (36%) and the perceived costs (29%). However, nearly half agree recent events like the increased reliance on technology (47%), development of AI (47%), and cyberattack news (47%) have made them more likely to purchase cyber insurance, specifically resources like identity recovery (75%), financial account monitoring (74%), and computer attack protection (72%).

# 6 in 10 consumers are concerned about potential cyberattacks

Top reasons for concern include the recent increase in cyberattacks (55%), use of AI technology (54%), and the proficiency of today's hackers (51%).

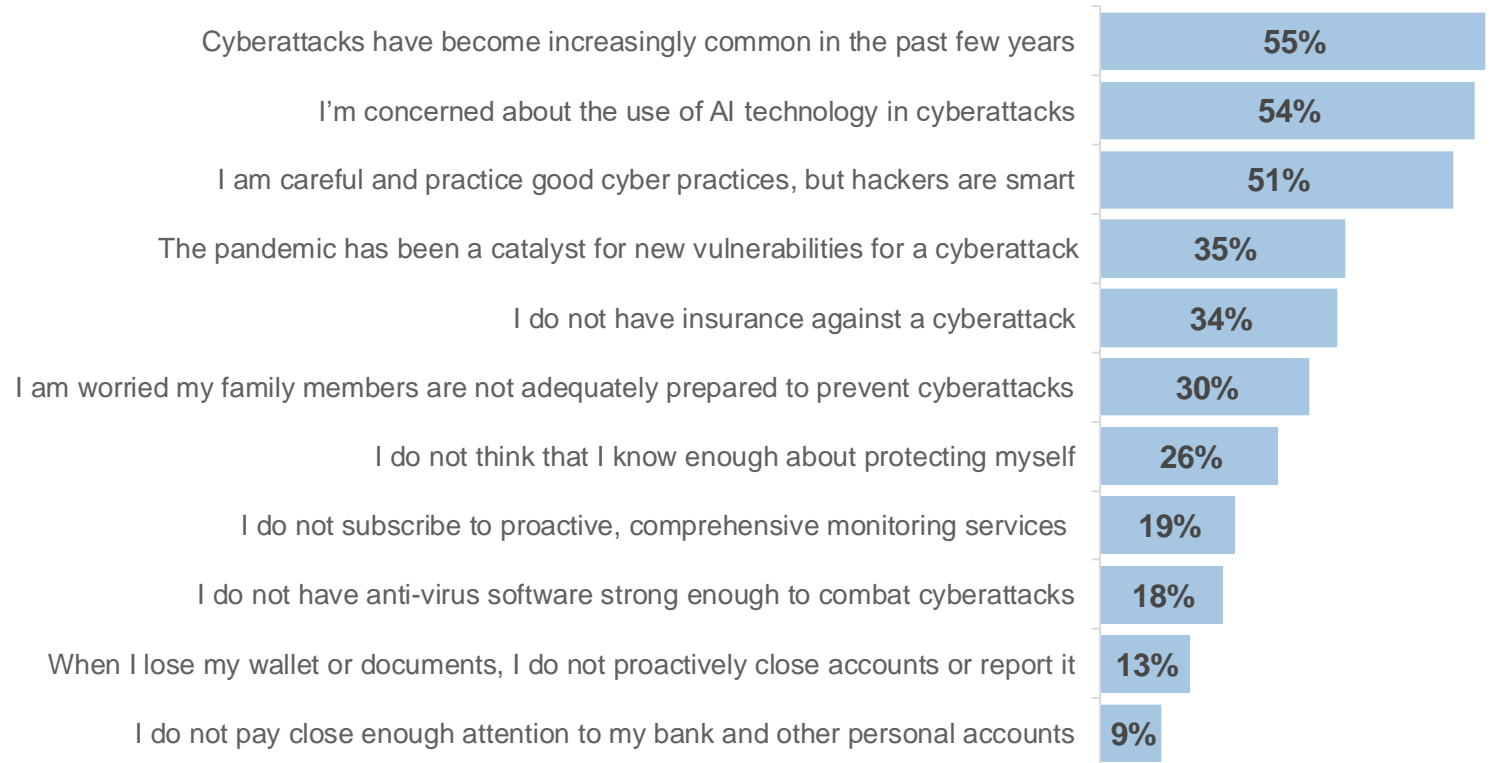
## Concern Around Cyberattacks

(Shown % Selected T2B Extremely/Moderately Concerned)



## Reasons for Concern

(Shown % Selected, among those concerned about cyberattacks)

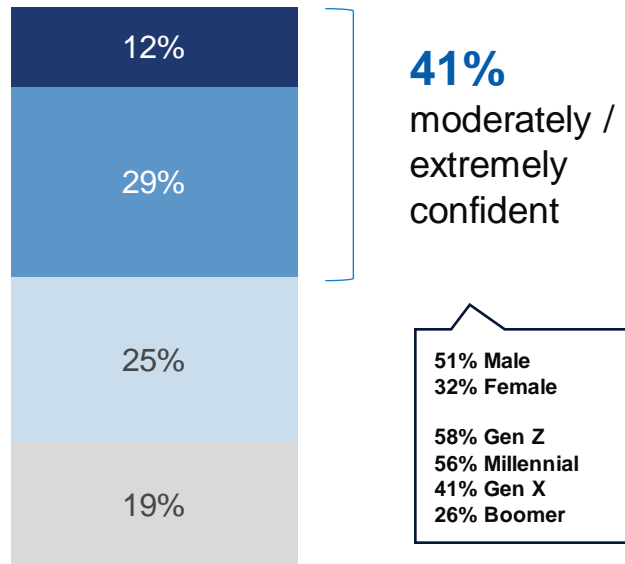


# Consumer confidence in their ability to recover from a cyber attack is low

Boomers are the least confident when compared to other generations. Common first steps consumers would take if they were the victim of a cyberattack include freezing financial accounts, contacting authorities / lawyers, and changing passwords.

## Confidence in Ability to Recover

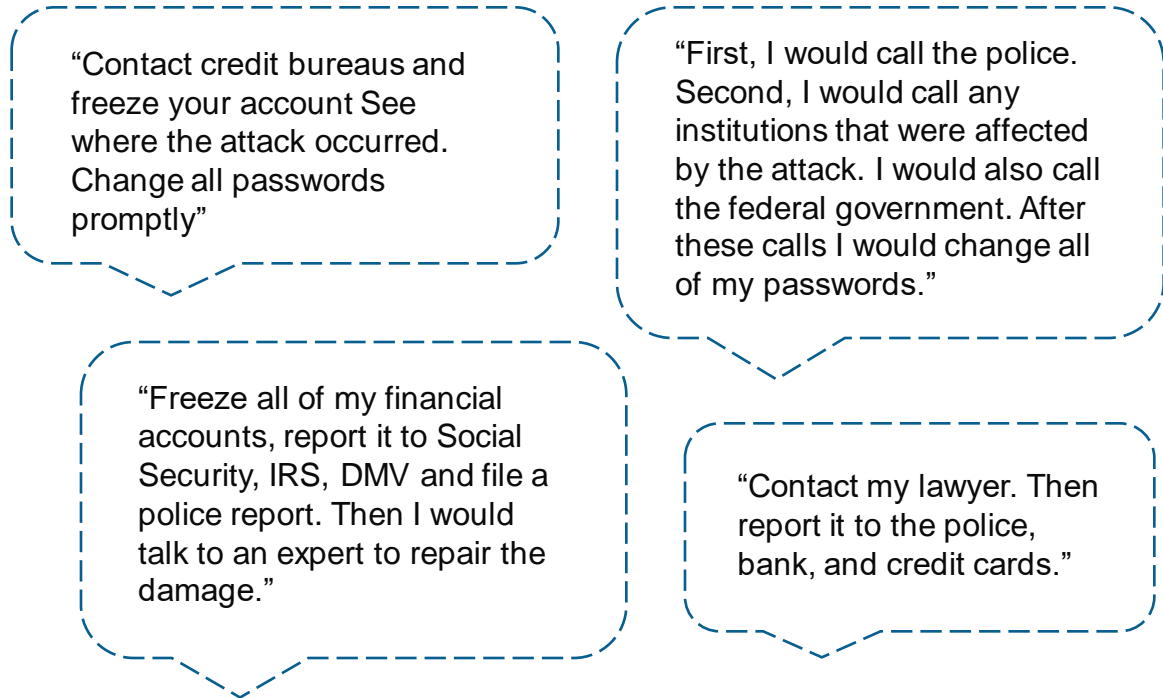
(Shown % Selected)



- Not at all confident
- Somewhat confident
- Moderately confident
- Extremely confident

## Steps to Start the Recover Process

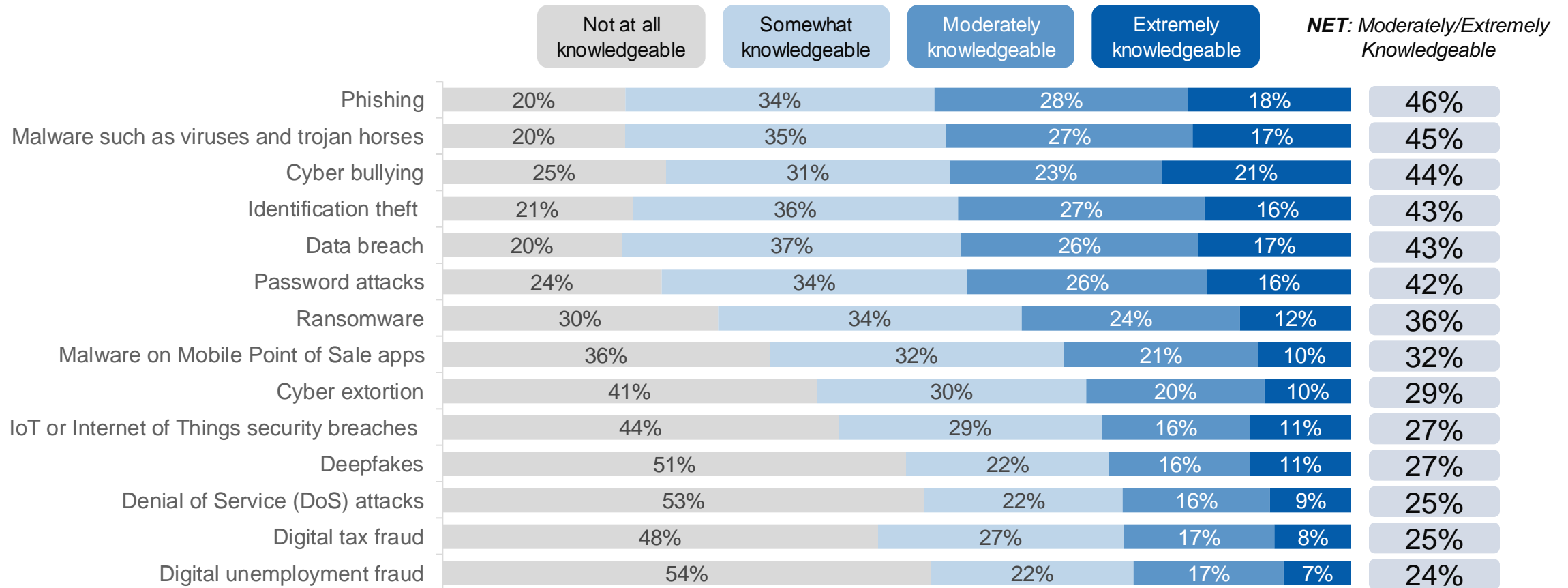
(Shown Open-ended response)



# Consumers are most familiar with phishing, malware, and cyberbullying

However, roughly half are not at all knowledgeable about deepfakes (51%), DoS attacks (53%), digital tax fraud (48%), or digital unemployment fraud (54%).

**Knowledge of Cybersecurity Threats**  
(Shown % Selected)



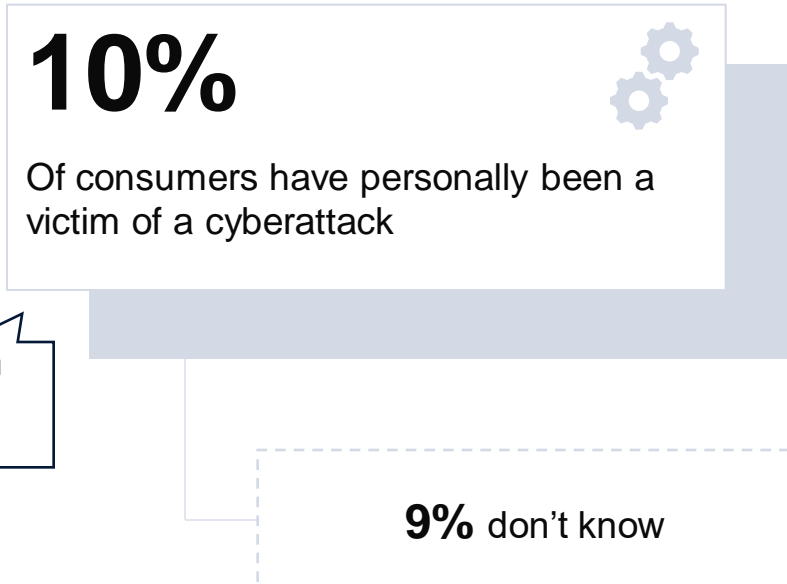
Q6. How knowledgeable are you on the following types of cybersecurity threats? Base: Consumers (n=1000)

# 1 in 10 consumers have experienced a cyberattack– with password attacks, malware, and data breaches being the most common

The least common cybersecurity threats include digital tax fraud (14%), digital unemployment fraud (13%), and deepfakes (10%).

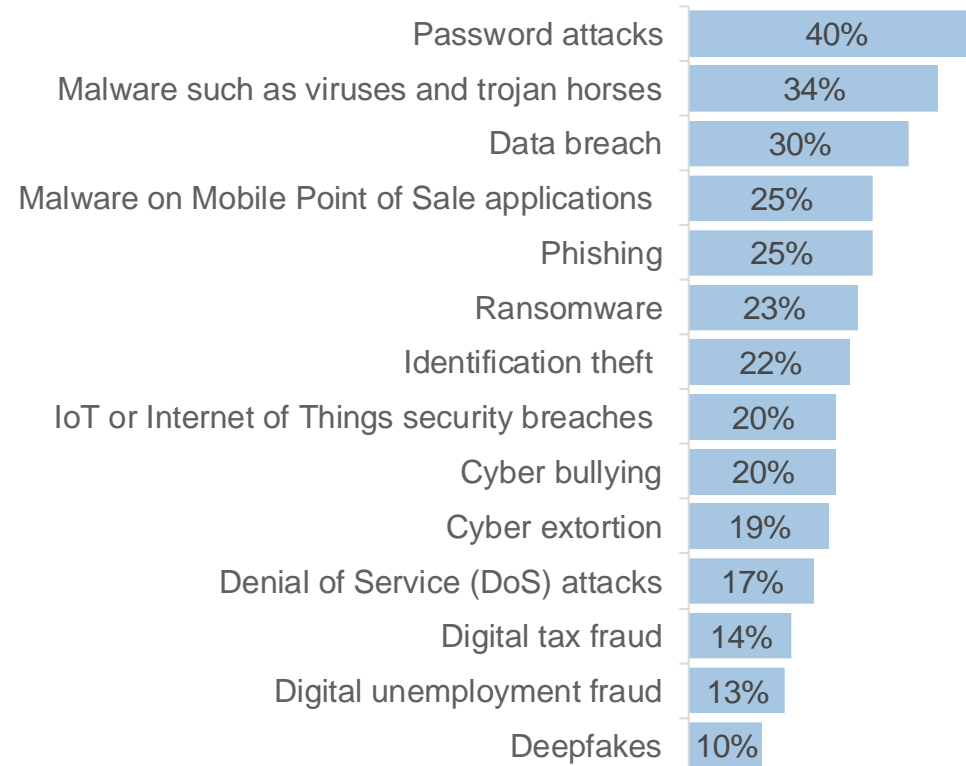
## Victims of a Cyberattack

(Shown % Selected 'Yes')



## Cybersecurity Threats Experienced

(Shown % Selected, among those who have experienced a cyberattack\*)



\*Small base size, findings should only be used directionally

Q7. Have you personally ever been a victim of a cyberattack? // Q8. Which, if any, of the following cybersecurity threats have you experienced? Please select all that apply.

Base: Consumers (n=1000), Consumers who have experienced a cyberattack (n=99\*)

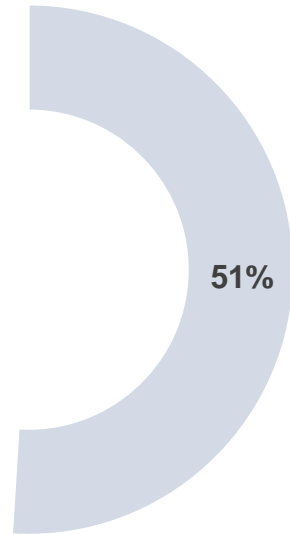


# Among those who have personally been a victim of a cyberattack, 1 in 2 claim that it impacted their personal finances

6 in 10 (59%) report having cyber insurance coverage at the time of the attack.

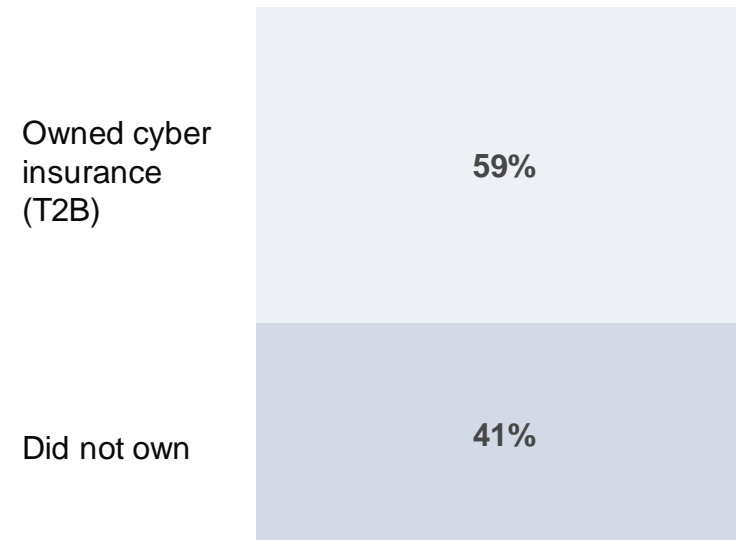
## Cyberattack Impacted or Jeopardized Personal Finances

(Shown % Selected 'Yes', among those who have experienced a cyberattack\*)



## Cyber Insurance Status at Time of Cyberattack

(Shown % Selected, among those who have experienced a cyberattack\*)



\*Small base size, findings should only be used directionally

Q9a. Did the cyberattack impact or jeopardize your personal finances? // Q10. Which of the following best describes your situation when the cyberattack occurred?

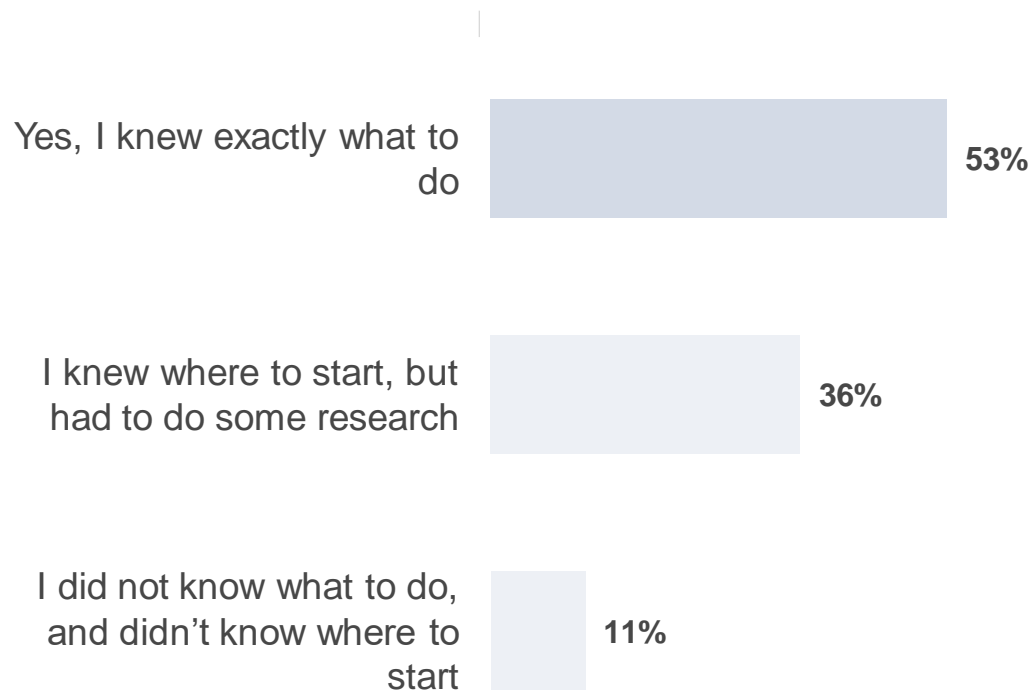
Base: Consumers who have experienced a cyberattack (n=99\*)

# Only about half of consumers knew exactly what to do after they experienced a cyberattack

The most common steps taken to prevent future attacks include changing passwords (58%), updating cybersecurity software (34%), and adding multi-factor authentication (35%). Less than 2 in 10 (17%) report buying cyber insurance after an attack.

## Response to Cyberattack

(Shown % Selected, among those who have experienced a cyberattack\*)



## Steps Taken Since Experiencing Cyberattack

(Shown % Selected, among those who have experienced a cyberattack\*)

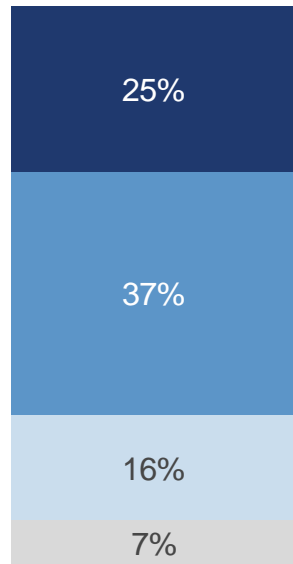
Changed my passwords	58%
Updated my cybersecurity software	40%
Added multi-factor authentication to accounts	35%
Purchased identification theft protection	31%
Asked my friends and family for advice	29%
Added comprehensive monitoring of all my accounts	28%
Began using a password manager	28%
Installed a new cybersecurity software	25%
Talked to my family members about the risk of cyberattacks and how to mitigate them	22%
Asked my insurance agent for advice and information about insurance	19%
Bought cyber insurance	17%
Set-up parental controls	9%

\*Small base size, findings should only be used directionally

Q11. Did you personally know what to do once you identified the attack? // Q11b. Which, if any, of the following steps have you taken since experiencing a cyberattack to prevent future attacks? Please select all that apply. Base: Consumers who have experienced a cyberattack (n=99\*)

# While most agree it would be difficult to cover the costs of a cyberattack, there is no consensus around how expensive it is to recover from the average attack

**Ease of Covering Recovery Costs**  
(Shown % Selected)

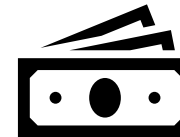


**61%**  
somewhat /  
very difficult

65% Male  
57% Female  
  
67% Boomer  
62% Gen X  
61% Gen Z  
53% Millennials

- Very easy
- Somewhat easy
- Somewhat difficult
- Very difficult

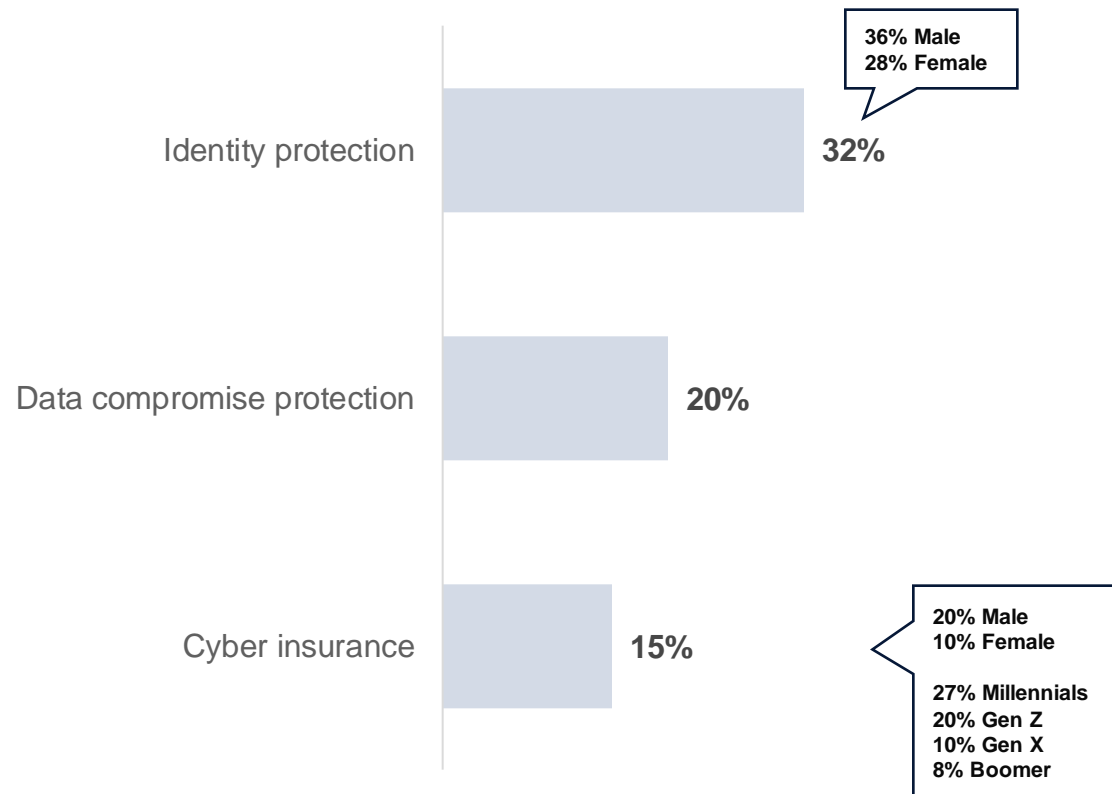
**Anticipated Cost of Recovery from Average Cyberattack**  
(Shown % Selected)



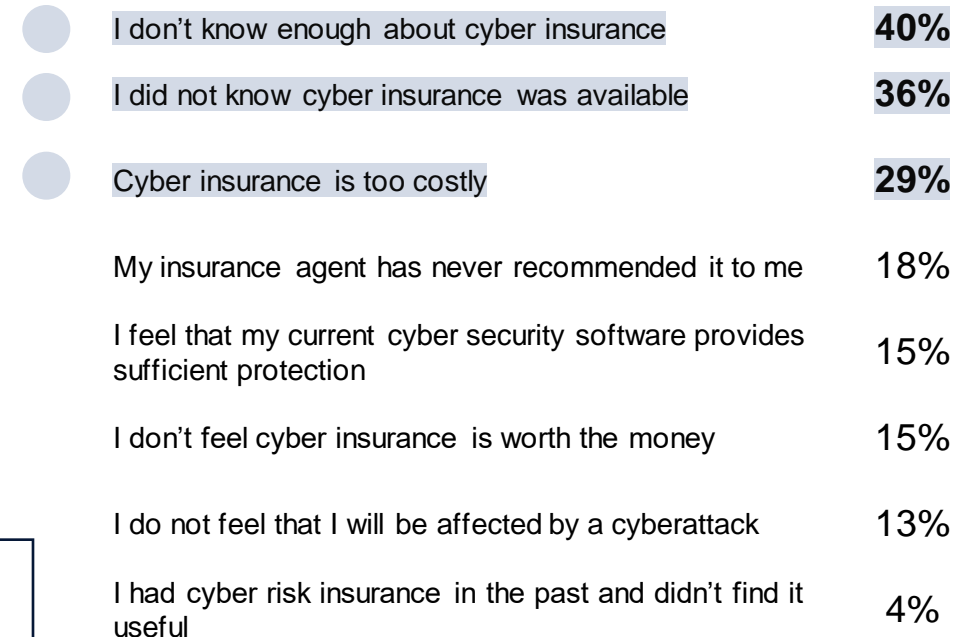
Under \$100	9%
\$100-\$499	15%
\$500-\$749	12%
\$750-\$999	9%
\$1,000-\$1,999	18%
\$2,000-\$2,999	11%
\$3,000-\$3,999	4%
\$4,000-\$4,999	3%
\$5,000+	21%

# Lack of awareness is still the top barrier to consumers purchasing cyber insurance – with less than 1 in 5 currently covered

## Security Protection Ownership (Shown % Selected “Yes”)



## Why Consumers Don't Buy Cyber Insurance (Shown % Selected)



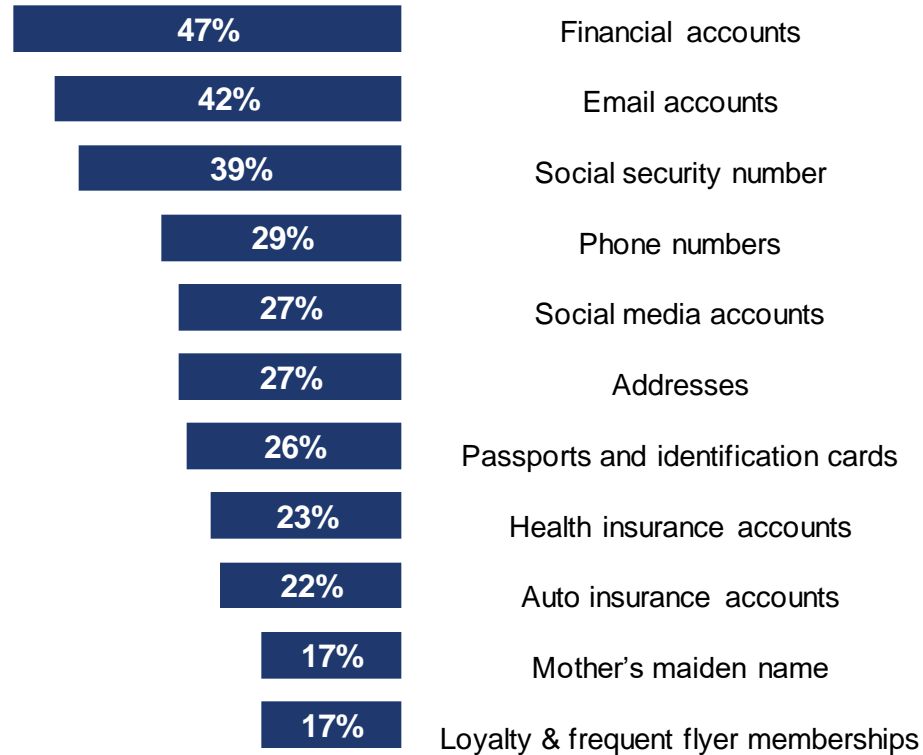
# Most consumers who monitor their personal information or accounts do so themselves rather than using an external service

Financial accounts (47%), email (42%), and social security numbers (39%) are most likely to be monitored.

## Personally Monitored Information or Accounts

(Shown % Selected)

55% Boomer  
46% Millennials  
42% Gen X  
33% Gen Z



## Designated Person to Monitor

(Shown % Selected)

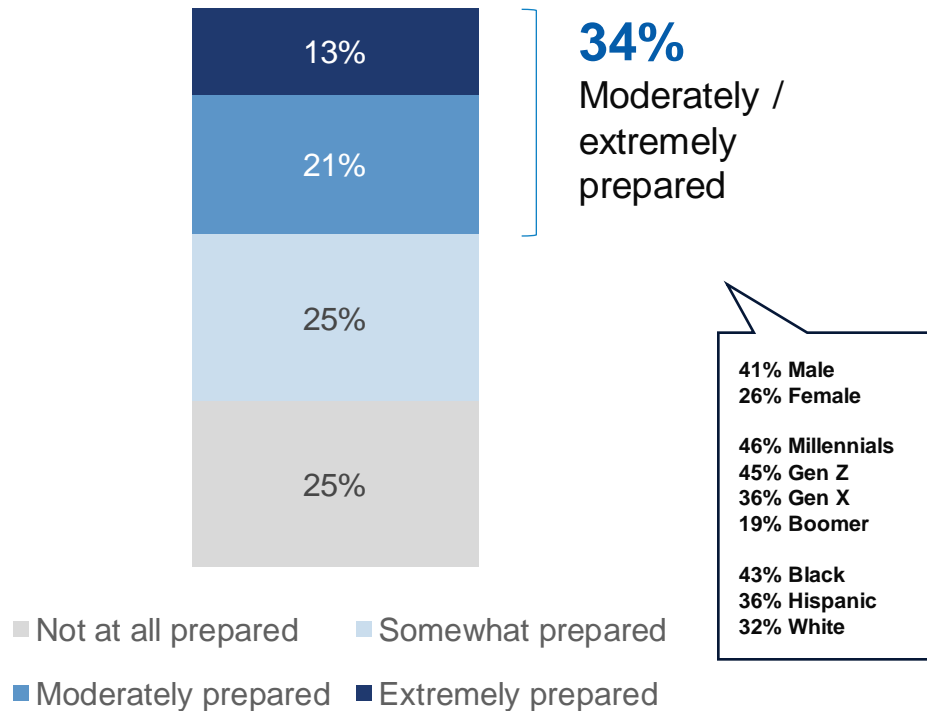
	Self	External Service
Financial accounts	67%	33%
Email accounts	75%	25%
Social security number	63%	37%
Phone numbers	67%	33%
Social media accounts	79%	21%
Addresses	64%	36%
Passports and identification cards	65%	35%
Health insurance accounts	78%	22%
Auto insurance accounts	74%	26%
Mother's maiden name	66%	34%
Loyalty & frequent flyer memberships	75%	25%

# Only a third of consumers feel prepared to prevent a cyberattack

Less than half (45%) would hire someone to lead the recovery process for them.

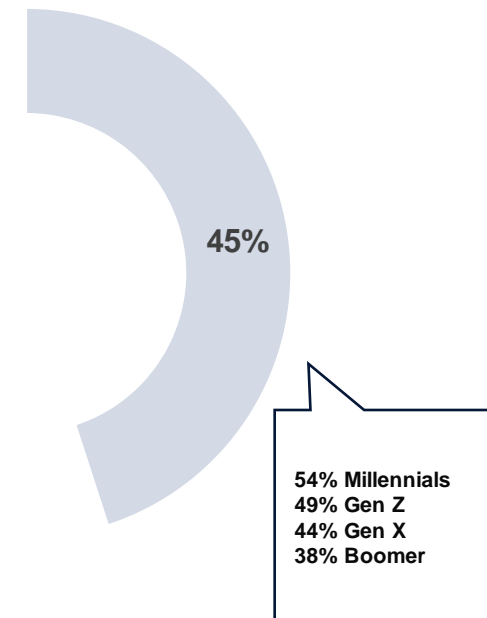
## Sense of Preparedness for Preventing a Cyberattack

(Shown % Selected)



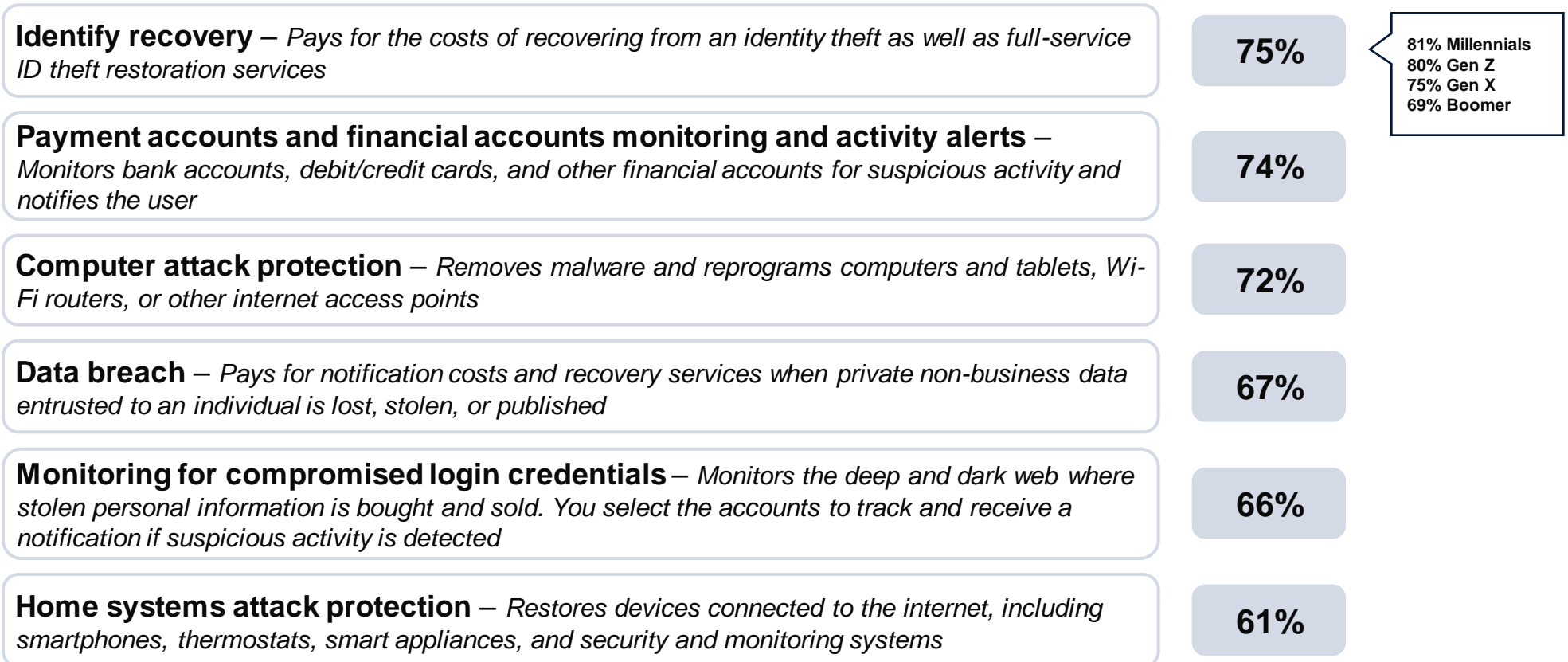
## Response to Hire Someone To Lead The Recovery Process

(Shown % Selected "Yes")



# 3 in 4 consumers are interested in investing in resources or products affiliated with identity recovery and financial account monitoring

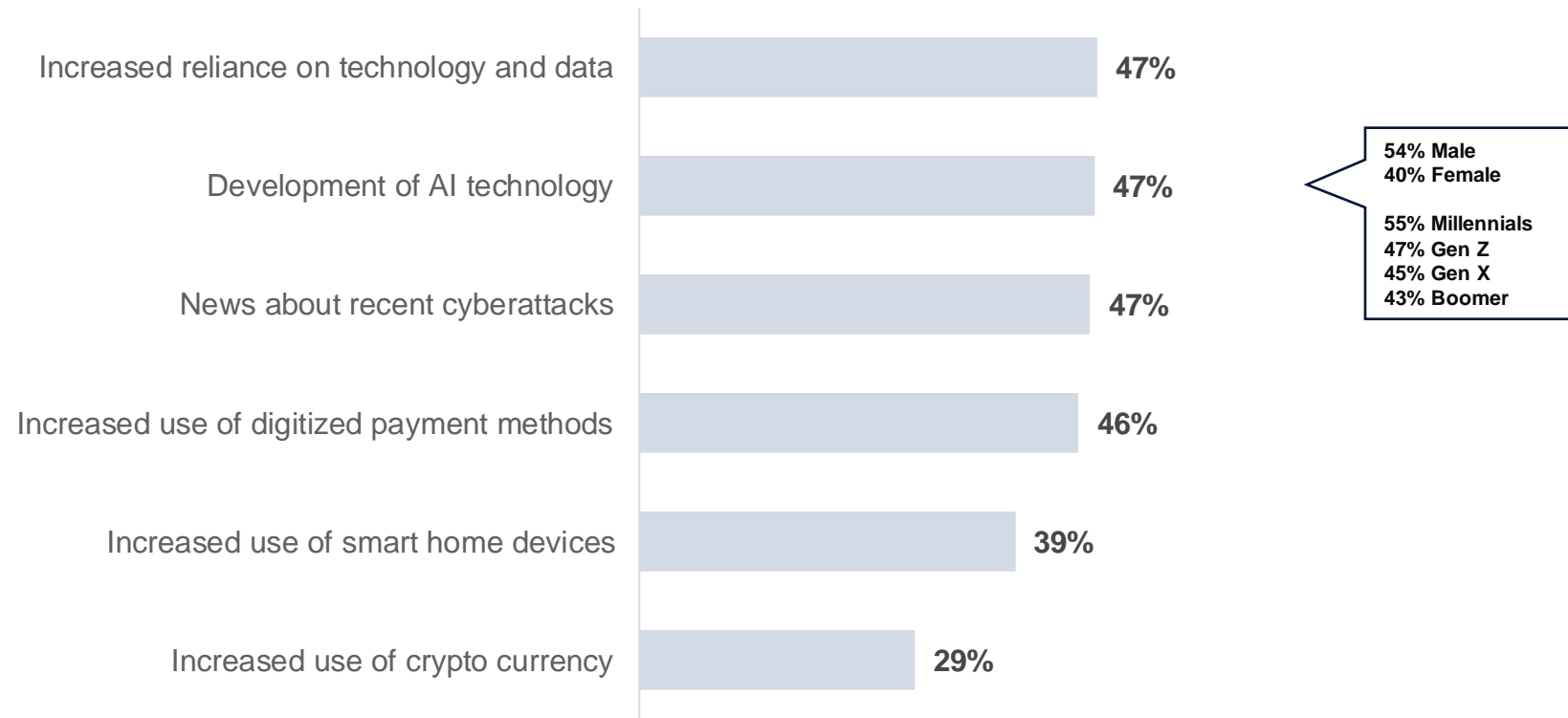
## Interest in Purchasing Cyberattack Protection Resources or Products (Shown % Selected T2B Somewhat/Very Interested)



# Increased reliance on technology, development of AI technology, news about recent cyberattacks, and the use of digital payment methods have made consumers more likely to consider purchasing cyber insurance

## Impact on Likelihood to Purchase Cyber Insurance Coverage

(Shown % Selected T2B More Likely)





---

# Appendix: Demographics

# Demographics: Consumers

Gender	
Man	49%
Woman	51%
Non-binary	1%
Age	
18-24	8%
25-34	11%
35-44	23%
45-54	18%
55-64	14%
65+	27%
Region	
Northeast	24%
Midwest	19%
South	36%
West	21%
Community Type	
Urban, or a downtown area	30%
Suburban, on the outskirts of an urban area	50%
Rural	20%

Ethnicity	
Asian or Asian American	4%
Black or African American	13%
Hispanic	13%
White	68%
Other	2%
Prefer not to answer	<1%
Education	
Some grade school	<1%
Some high school	2%
High school graduate	19%
Technical or vocational school	5%
Some college	20%
College graduate	33%
Graduate or professional school	21%
Prefer not to answer	<1%
Income	
Under \$25,000	13%
\$25,000 - \$49,999	19%
\$50,000 - \$74,999	18%
\$75,000 - \$99,999	15%
\$100,000 - \$149,999	18%
\$150,000 - \$199,999	8%
\$200,000+	5%
Prefer not to answer	3%

Employment Status	
Full-time	46%
Retired	27%
Part-time	11%
Unemployed	8%
Homemaker/Stay-at-home parent	5%
Student	3%
Prefer not to answer	1%