Nationwide®

August 2026

Nationwide Cybersecurity

Survey Report

SURVEY METHODOLOGY

Audiences	Sample Size	Methodology	Timing
General Consumers *Age 18+ - nationally representative by age, gender, race, region*	**N=1,000**	**20-Minute Online Survey**	**Survey Fielded July 10th – July 29th, 2026**
Small Business Owners *Owners of small businesses, defined as 1-50 employees and less than $10M in annual revenue*	**N=300**		
Mid-Market Business Owners *Owners of middle-market businesses, defined as 50-500 employees or $10M-$500M in annual revenue*	**N=300**		
Independent Insurance Agents *Mix of Principals, Producers, and CSRs*	**N=300**		

Consumers

KEY FINDINGS

1 Consumers know the AI threat is here, but few feel equipped to spot it

More than 8 in 10 Consumers (84%) are concerned about criminals using AI to steal someone's identity, and awareness of common AI-powered scams is widespread. Yet just 19% are very or extremely confident they could identify an AI-powered scam, and only 17% have created a family code phrase to verify a loved one's identity during an urgent call or message. The findings point to a significant gap between awareness of emerging AI threats and preparedness to respond to them.

2 Cybersecurity concerns aren't always translating into safer digital behavior

Most Consumers are taking basic precautions, including installing software updates when prompted (78%) and using multi-factor authentication (74%). Yet half (50%) still use the same password across multiple sites or apps, and 40% share personal information over the phone. When it comes to AI-powered threats, most rely on monitoring and vigilance, while only about a third use tools such as robocall filtering (35%), email security protection (34%) or identity theft/credit monitoring services (33%).

3 Boomers are especially concerned about emerging cyber threats—and are taking some of the strongest precautions

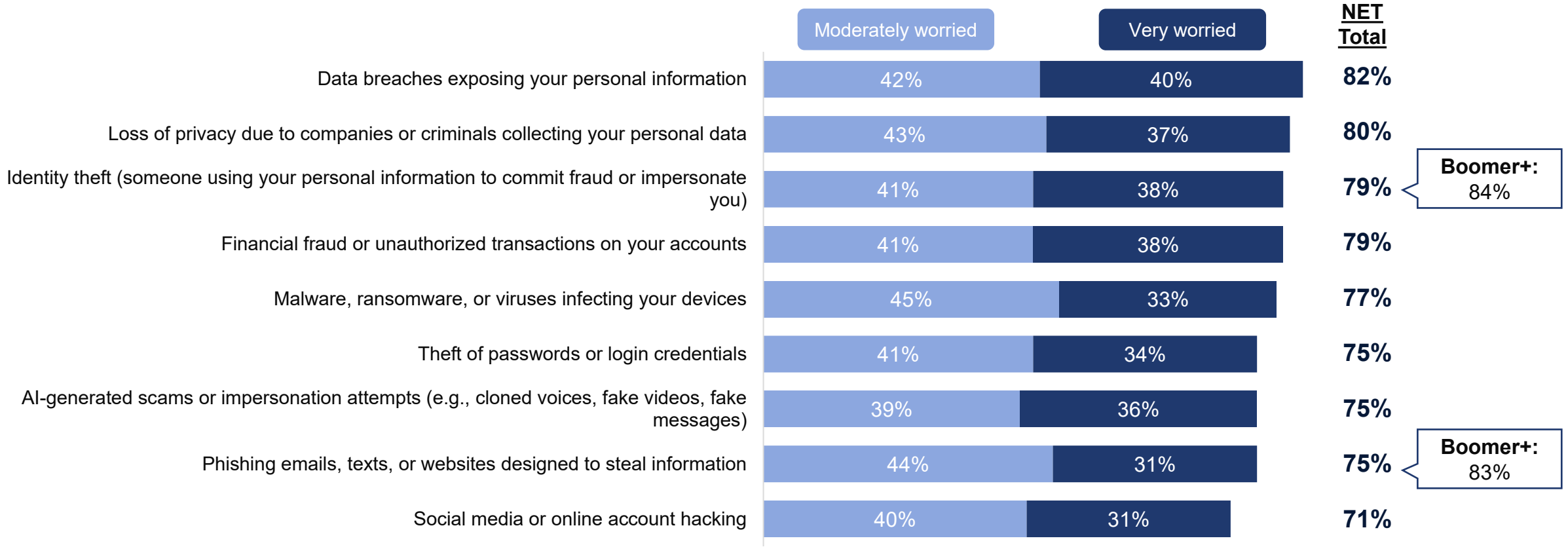
Boomers show particularly high concern about emerging digital risks, with 91% concerned about criminals using AI to steal someone's identity. They also stand out for taking several protective actions: 75% monitor their financial accounts for suspicious activity, 71% limit the personal information they share online and 52% use fraud alerts or account-monitoring services – all at higher rates than the average Consumer. At the same time, a third (33%) are not at all confident they could identify an AI-powered scam, underscoring the challenge even for a generation taking the threat seriously.

Consumers are most concerned about threats to the security of their personal information and the risk of identity theft

Women are more likely to be worried about all cybersecurity threats than men.

Concern Around Cybersecurity Threats

(Shown: % Selected)



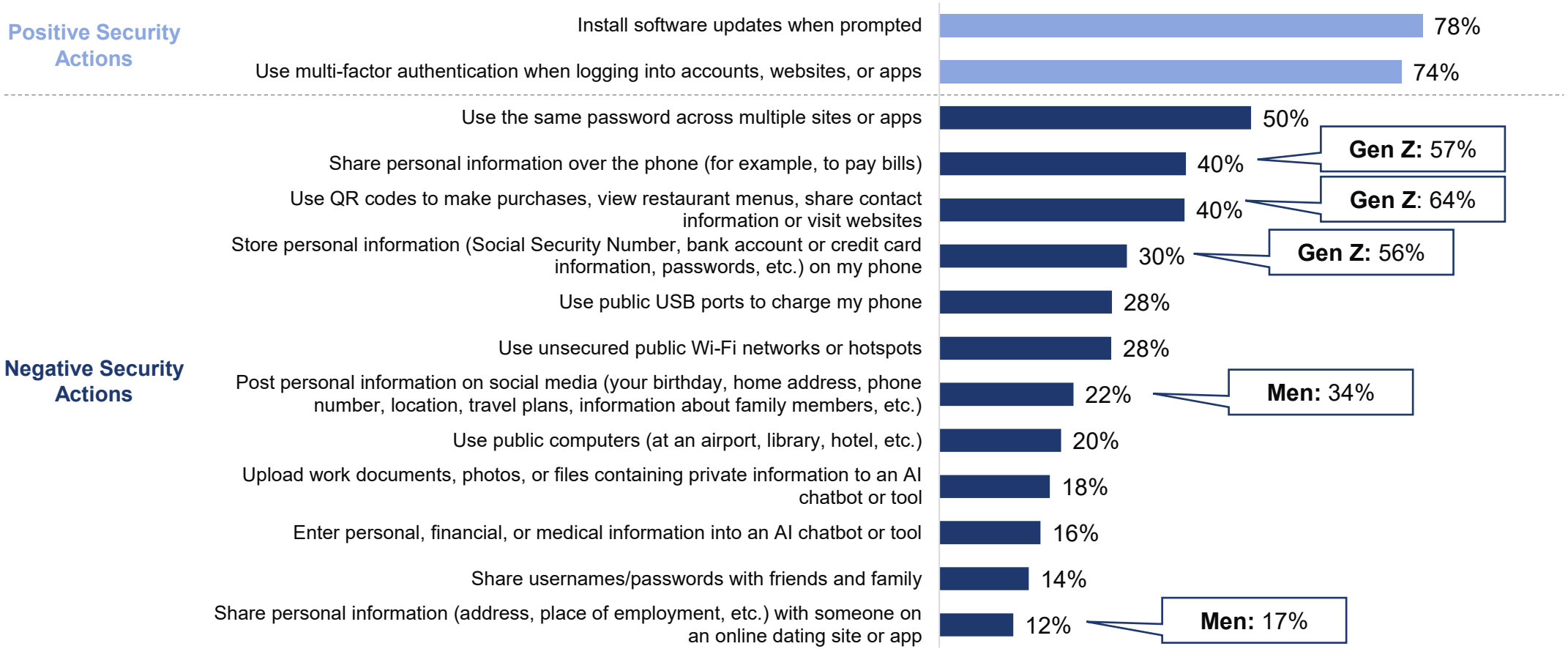
Q2. How concerned are you about each of the following cybersecurity threats happening to you?
Base: Consumers (n=1,000)

While most Consumers promptly install software updates and use MFA, many are still engaging in risky behaviors

Half of respondents report using the same password across multiple sites or apps, while 4 in 10 are sharing personal information over the phone. Gen Z is more likely to be engaging in risky behaviors such as using QR codes, share personal information over the phone, and store important personal information such as their social security number on their phone.

Online Activities

(Shown: % Selected, T2B Do Action Sometimes/Often)



Q1. How often do you do each of the following actions? Base: Consumers (n=1,000)

Most Consumers have experienced a threat in the past year, with phishing being the most common

A third have experienced identity theft and found the greatest impact to be the time spent resolving the issue and emotional stress.

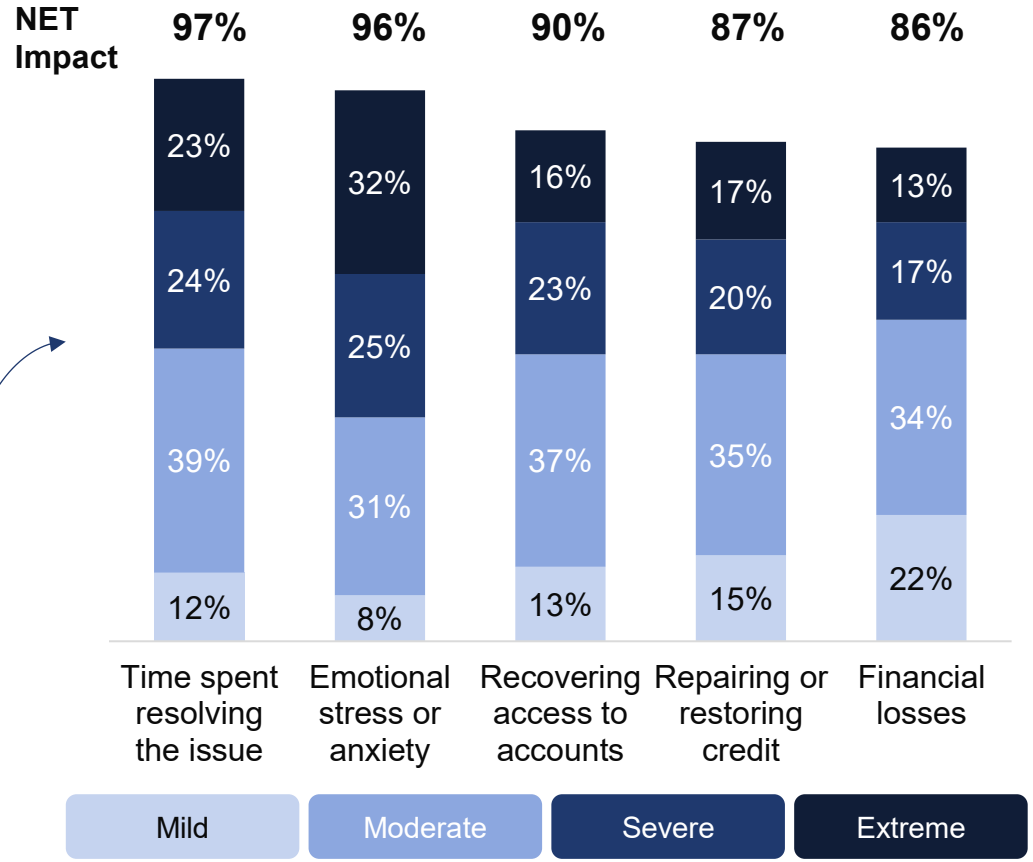
Cybersecurity Threats Experienced in the Past 12 Months

(Shown: % Selected "Yes", to myself or a family/friend)

80% *Report they or someone they know has **experienced at least one of the above threats** in the past year*

Impacts of Recently Experienced Identity Theft

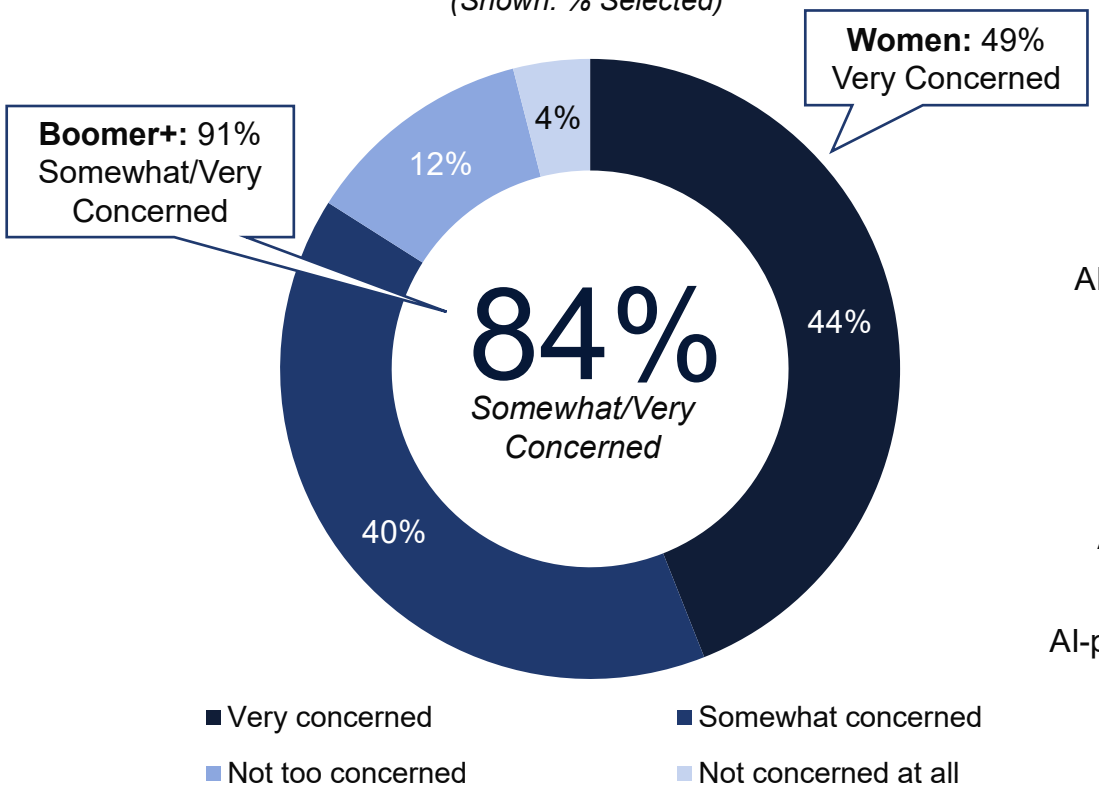
(Shown: % Selected)



Consumers are highly concerned about AI-enabled cybersecurity threats – with the majority aware of various types of these scams

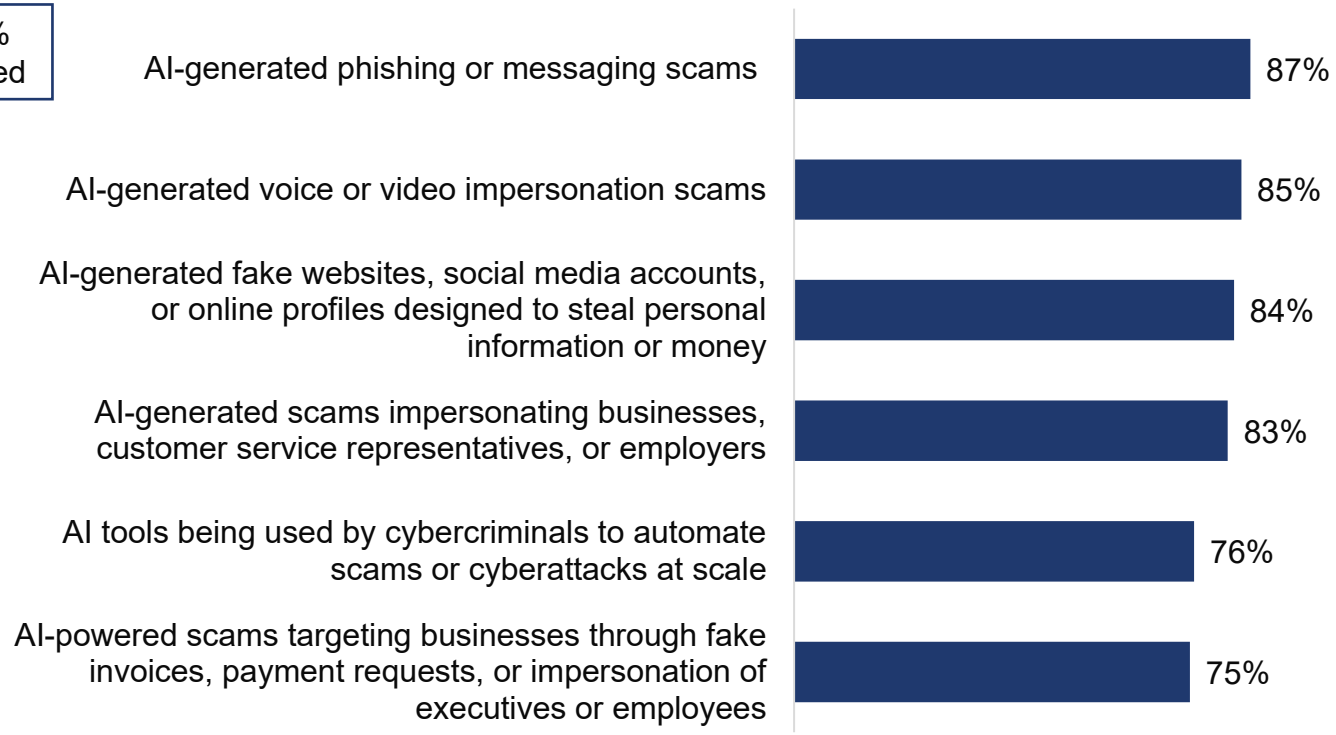
Concern About AI Use for Identity Theft

(Shown: % Selected)



Awareness of AI Scams and Cyber Threats

(Shown: % Selected T2B "Aware")

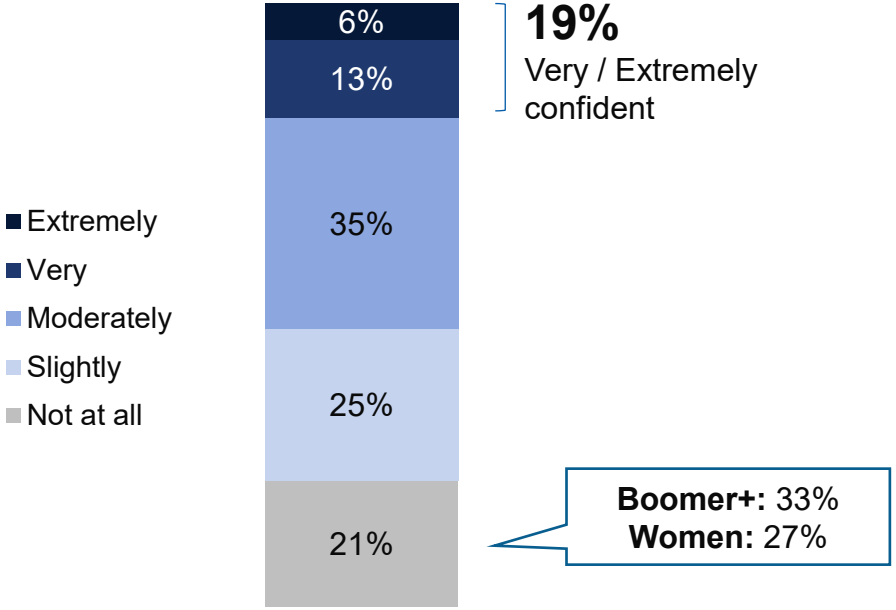


Q5. How concerned are you about the use of AI (artificial intelligence) by criminals to steal someone's identity? Base: Consumers (n=1,000)
Q6. Are you aware of the following types of AI-powered scams or cyber threats? Base: Consumers (n=1,000)

While Consumers know the AI threat is here, only 1 in 5 are highly confident they can spot an AI-powered scam and just 17% have a family verification code

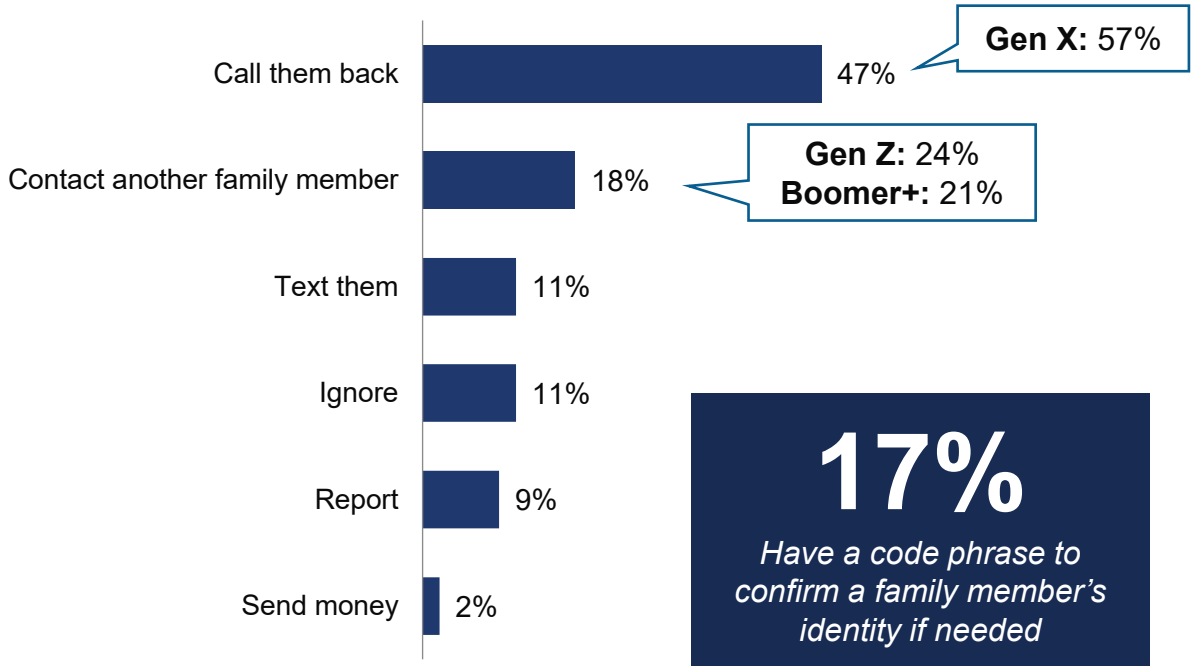
Confidence in Identifying an AI-powered Scam or Cyberthreat

(Shown: % Selected "Confident")



Likely First Actions Upon Receiving a Voice Message that Sounded like a Family Member Urgently Asking for Money

(Shown: % Selected)



17%

Have a code phrase to confirm a family member's identity if needed

Q7. How confident are you that you could identify an AI-powered scam or cyber threats?
Q8. If you received a voice message that sounded like a family member urgently asking for money, what would you most likely do first?
Q9. Has your family / household created a code phrase or verification term to confirm a family member's identity during an urgent call or message? Base: Consumers (n=1,000)

While around 6 in 10 are monitoring their financial accounts and limiting online information to protect from AI-powered threats, fewer are utilizing specific tools and services

Actions Taken to Protect from AI-powered Fraud / Cyber Threats

(Shown: % Selected "Yes")

Monitor my bank, credit card, or financial accounts for suspicious activity	62%	**Boomer+:** 75%
Limit the personal information I share online	60%	**Women:** 65%
Carefully review calls, emails, texts, or messages before responding or taking action	60%	**Women:** 65%
Keep my devices, apps, and software up to date	58%	
Use strong, unique passwords for my accounts	57%	**Boomer+:** 67%
Limit what I post on social media	55%	
Enable multi-factor authentication (MFA)	47%	
Use fraud alerts or account monitoring services provided by a bank or financial institution	43%	**Boomer+:** 52%
Avoid posting voice recordings, videos, or other content that could be used to impersonate me	40%	
Use spam, scam, or robocall filtering tools	35%	
Use email spam, phishing, or security protection tools	34%	
Use identity theft protection or credit monitoring services	33%	**Boomer+:** 39%
Freeze or lock my credit reports	28%	

Q10. Which of the following steps, if any, do you currently take to help protect yourself from AI-powered scams, fraud, or other cyber threats? Base: Consumers (n=1,000)

Consumers turn most to banks for information on cyber threats and as the first point of contact after an AI scam, very few turn to their insurer

About a third (31%) would contact their bank first after an AI-powered scam; just 1% would turn first to their insurer

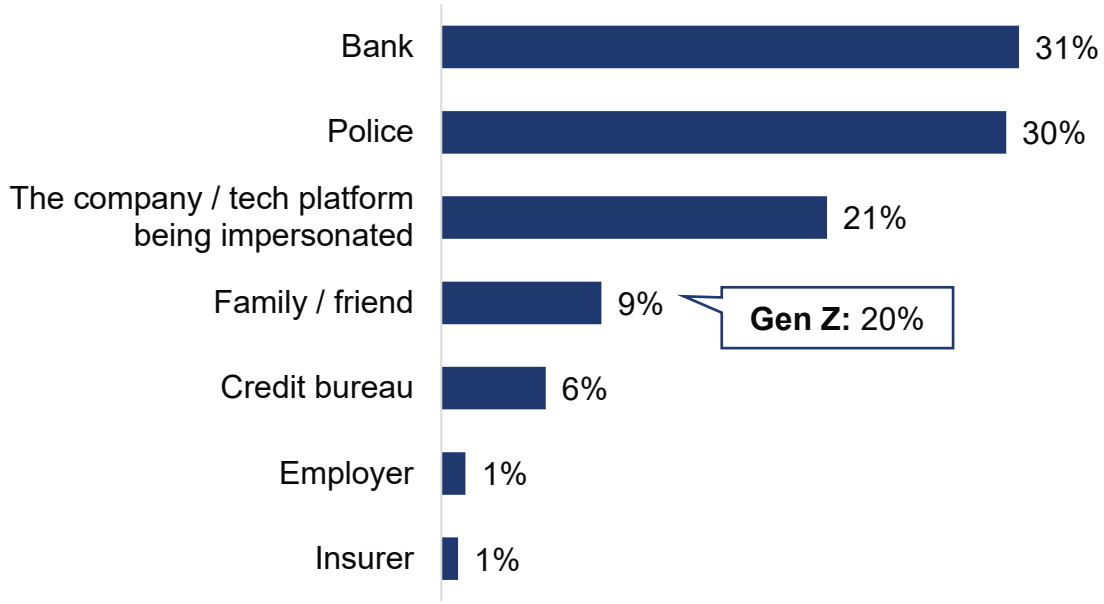
Most Visited Sources of Information about Protection from Identity Theft and Cyber Scams

(Shown: % Selected)

	Consumers
Bank, credit union, or other financial institution	40% ↑+12
Websites, blogs, or forums	28% ↑+5
Friends and family	27%
Government resources	21%
Technology companies / manufacturers	20%
Social media	13%
My insurance agent	8%
My employer	5%
I never look for this information	19%

First Point of Contact After Falling for AI-powered Scam / Cyber Threat

(Shown: % Selected)



57% are confident they know who would help them if…	one of their online accounts was hacked
	if their identity was stolen

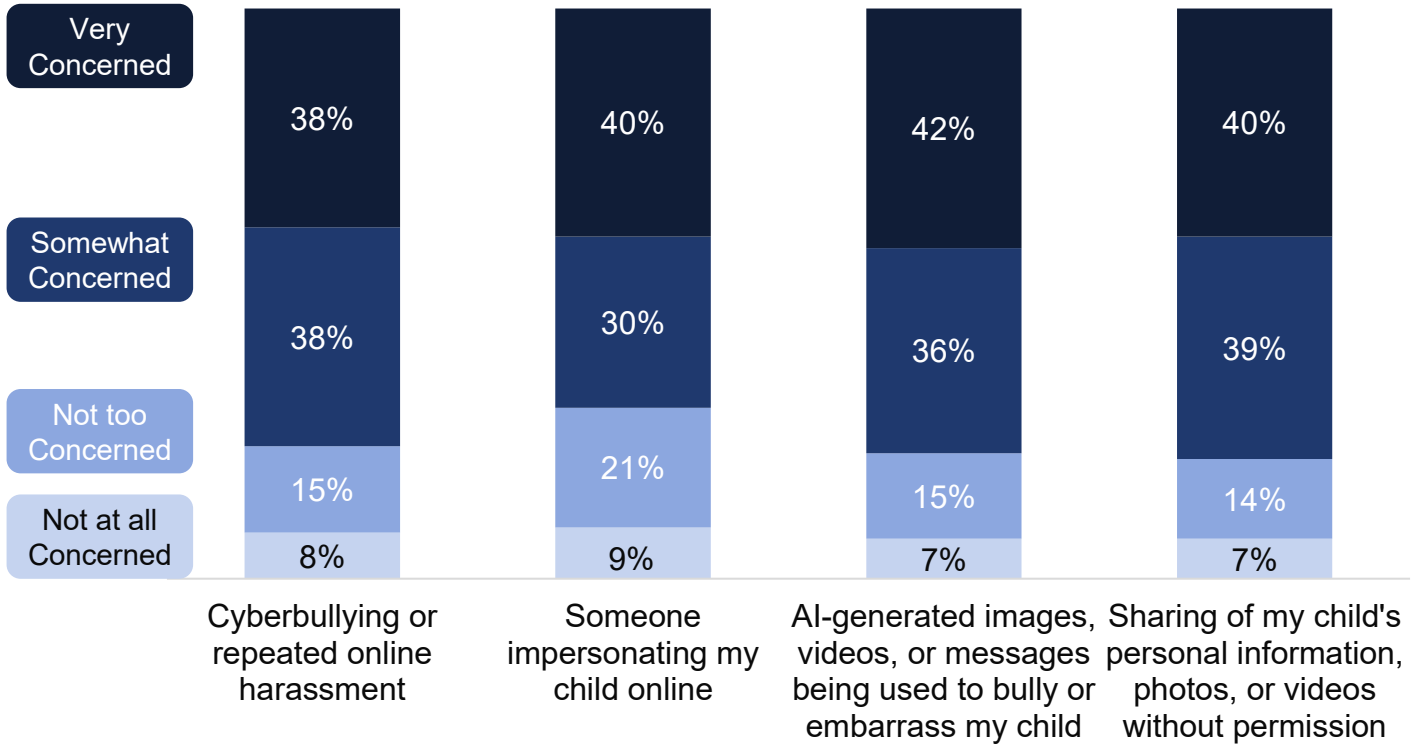
↑↓ = 2024 comparisons

Q11. If you fell victim to an AI-powered scam or cyber threat, who would you contact first?
Q16. Where do you most often go for information about protecting yourself from identity theft and cyber scams?
Q30. How much do you agree or disagree with the following statements? Base: Consumers (n=1,000)

Over two thirds of parents are concerned about cyber threats are affecting their children, but most are confident they could identify AI threats

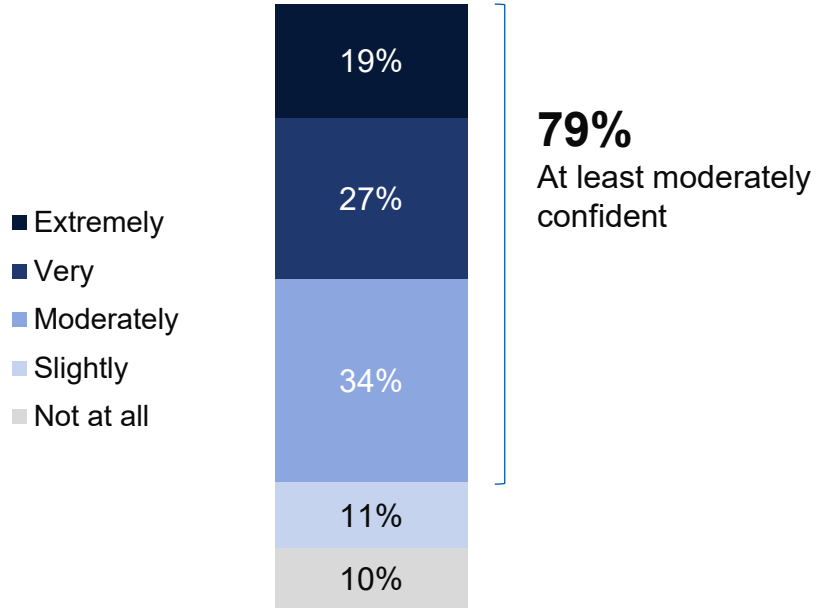
Parents' Concerns About Online Threats to Their Children

(Shown: % Selected)



Parents' Confidence in Recognizing AI-Enabled Online Threats

(Shown: % Selected "Confident")

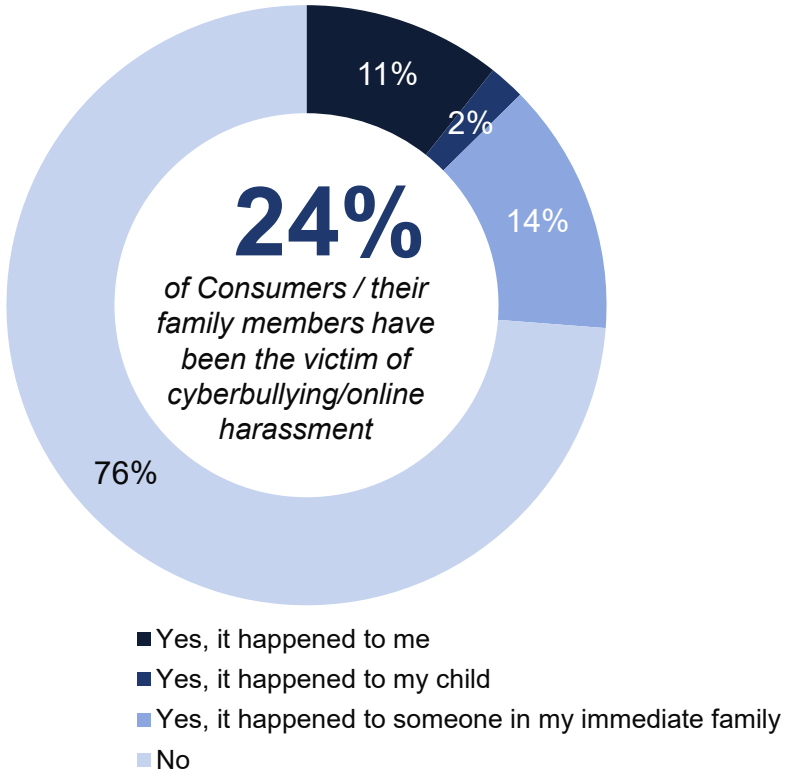


Q25. How concerned are you that your child could experience each of the following online?
Q26. How confident are you that you would recognize if your child were being targeted by AI-generated bullying, impersonation, or other malicious online activity? Base: Consumers with children (n=260)

1 in 4 Consumers or their loved ones have been victims of cyberbullying/harassment; most just blocked/reported the individual, but over half are interested in a service to help respond

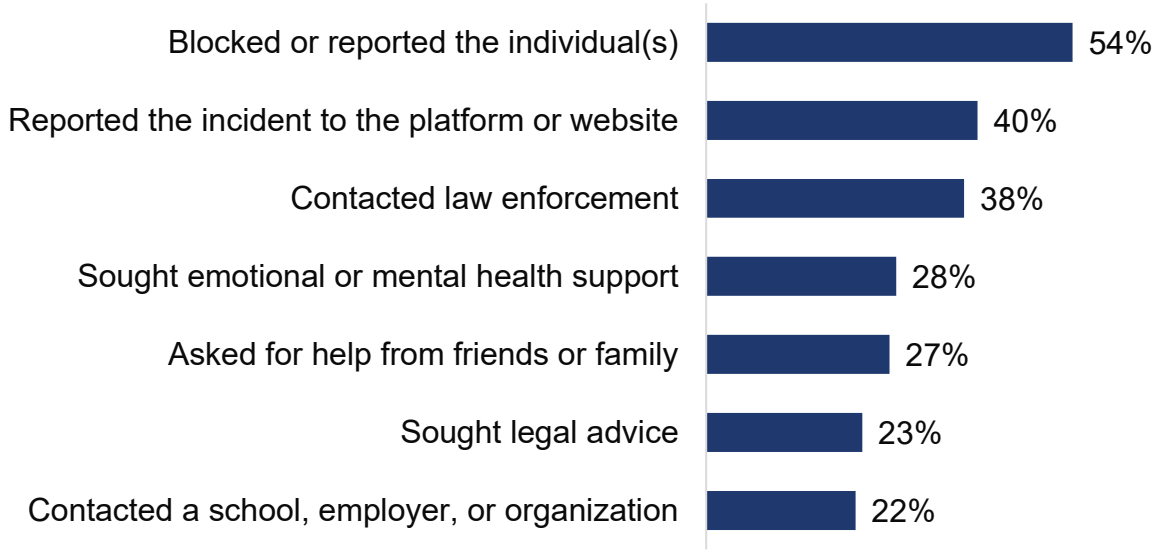
Experience with Cyberbullying or Online Harassment

(Shown: % Selected)



Responses to Cyberbullying or Online Harassment

(Shown: % Selected)



55% *Are interested (T3B) in a service to help respond to cyberbullying or online harassment*

Q27. Have you or anyone in your immediate family ever been the victim of cyberbullying or online harassment? For example, repeated malicious comments, threats, impersonation, sharing private information without permission, or other targeted abuse through social media, messaging apps, gaming platforms, or other online services. Q28. How did you or your family respond? Q29. How interested would you be in a service that helps individuals or families respond to cyberbullying or online harassment? Base: Consumers (n=1,000)

Business Owners & Agents

KEY FINDINGS – BUSINESS OWNERS

1 Cyberattacks are becoming a fact of business for the mid-market, while concern remains high across businesses of all sizes

More than two-thirds of Small Business Owners (68%) and 4 in 5 Mid-Market Business Owners (81%) are concerned about a potential cyberattack. For MMBOs, the threat is especially tangible: 62% say their business has experienced a cyberattack, compared with 16% of SBOs. Since 2024, reported attacks have increased 6 percentage points among MMBOs while declining 7 points among SBOs.

2 Small businesses face a meaningful preparedness gap despite widespread concern about cyber risk

While 81% of MMBOs feel prepared to prevent a cyberattack, just 63% of SBOs say the same. The gap extends to employee preparedness: 95% of MMBOs provide formal cybersecurity training at least annually compared with 72% of SBOs, and MMBOs are more than twice as likely to conduct phishing tests at least every few months (65% vs. 30%). Notably, two-thirds of SBOs (66%) admit they haven't given much thought to what they would do if they fell victim to a cyberattack.

3 Cyber insurance adoption is surging among mid-market businesses, while small-business adoption remains stagnant

Nearly three-quarters of MMBOs (73%) now purchase cyber insurance, a 34-percentage-point increase since 2024, while SBO ownership remains at 42%. Among uninsured SBOs, education and awareness remain important barriers: 29% say they don't know enough about cyber insurance and 24% didn't know it was available. Uninsured MMBOs are more likely to cite cost (41%) and confidence in existing cybersecurity software (33%).

4 AI is expanding the cyber threat—and businesses say they need help keeping pace

More than a quarter of SBOs (26%) and more than a third of MMBOs (36%) say their company was targeted by a generative-AI scam or fraud attempt in the past year. Nine in 10 or more believe AI is making it easier for cybercriminals to launch attacks at scale, while 88% of SBOs and 75% of MMBOs say they need more information and resources to protect their businesses from AI-enabled cyberattacks.

KEY FINDINGS - AGENTS

1 Agents see themselves as trusted cyber advisers—but say their clients have significant knowledge gaps

Nine in 10 Agents (90%) say clients view them as a credible source of cybersecurity information, and 87% feel confident discussing clients' cyber vulnerabilities and relevant coverages. Yet 80% are concerned about clients' lack of cybersecurity knowledge, 76% say many clients are unaware of their exposure to cyberattacks and 74% say many clients are unsure what cyber insurance covers.

2 Cyber risk is firmly part of the commercial client conversation, with Agents actively recommending coverage

Nearly 8 in 10 Agents (79%) say their commercial lines clients are moderately or extremely concerned about potential cyberattacks, compared with 62% of personal lines clients. In response to the evolving threat landscape, 89% of Agents say they regularly recommend cyber insurance to their customers, reinforcing the increasingly important role Agents play in helping clients understand and manage cyber risk.

3 Agents see a major preparedness gap among commercial clients—particularly before an attack occurs

Agents estimate that just 24% of their commercial clients have an incident response plan in place and only 30% keep their cyber coverage level current with the evolving threat landscape. The findings point to an opportunity for Agents to expand the cyber conversation beyond purchasing coverage to include incident preparedness and regular reassessment of clients' changing exposures.

4 AI is raising the urgency of cyber protection, but Agents say clients aren't fully prepared for the threat

More than half of Agents (52%) have observed an increase in claims related to generative-AI scams or fraud attempts in the past 12 months, yet only about half (51%) believe clients are prepared to identify and respond to AI-powered cyber threats. At the same time, 62% say they need more information and resources to help protect clients from AI-enabled cyberattacks.

SBOs

MMBOs

More than two thirds of Business Owners are concerned about cyberattacks, largely due to potential financial loss

Concern about Cyberattacks

(Shown: % Selected Extremely/Moderately Concerned)

Concerned about a potential cyberattack on their business

68% -1 pts since 2024

of Small Business Owners

81% +4 pts since 2024

of Mid-Market Business Owners

Top 5 Reasons Why Businesses are Concerned about Cyberattacks

(Shown: % Selected, among those concerned about attacks)

	Small Business Owners		Mid-Market Business Owners
#1	A cyberattack could result in financial loss, fraud or theft	#1	A cyberattack could result in financial loss, fraud or theft
#2	A cyberattack could expose sensitive customer employee or business information	#2	A cyberattack could disrupt our business operation
#3	Cyberattacks have been increasingly common in the last few years	#3	A cyberattack could expose sensitive customer employee or business information
#4	A cyberattack could disrupt our business operation	#4	Recovering from a cyberattack could be costly and time-consuming
#5	Recovering from a cyberattack could be costly and time-consuming	#5	Cyberattacks have been increasingly common in the last few years

Q31. A cyberattack is an unwelcome attempt to steal, expose, alter, disable or destroy information through unauthorized access to computer systems (computer, smart phone, smart device, etc.) How concerned are you about a potential cyberattack on your business? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300) Q34. You indicated that you are moderately or extremely concerned about a potential cyberattack. Why are you concerned? Please select all that apply. Base: Small Business Owners concerned about a potential cyberattack on their business (n=278), Mid-Market Business Owners concerned about a potential cyberattack on their business (n=299)

SBOs

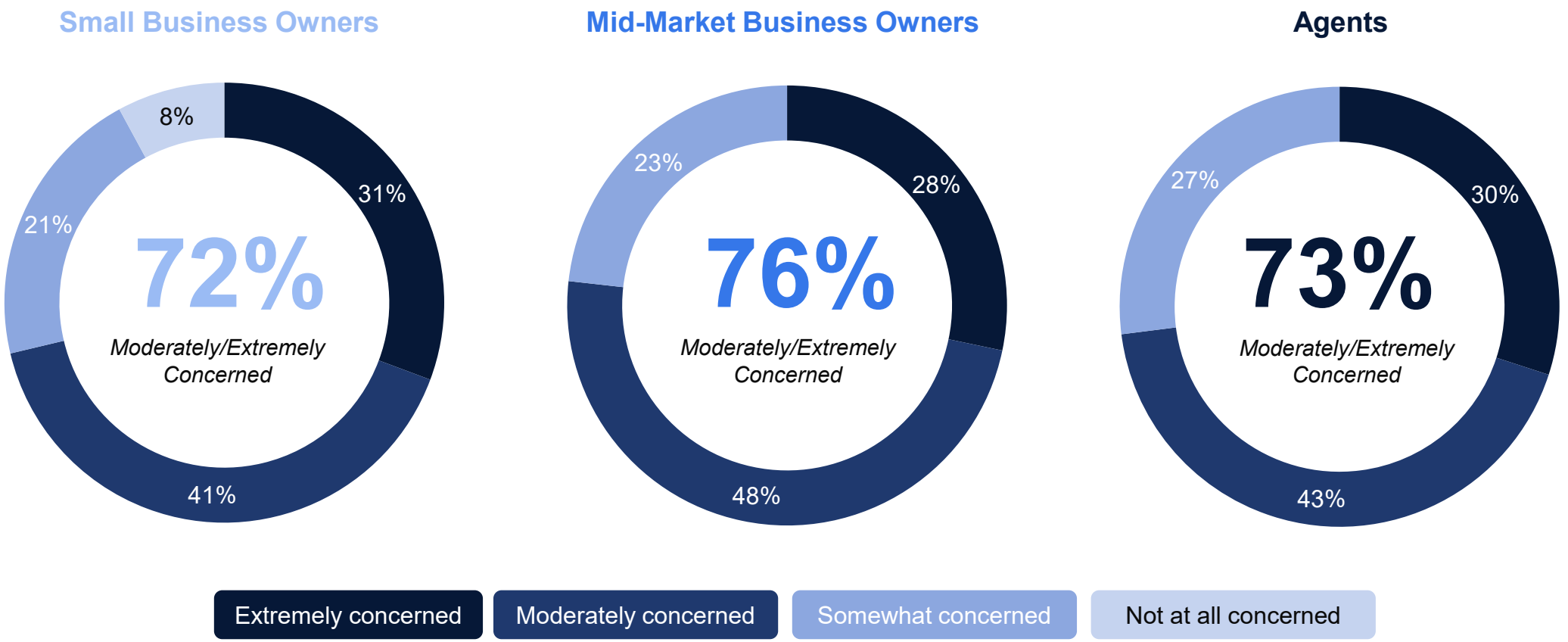
MMBOs

Agents

Business Owners and Agents are highly concerned about AI advancing the speed, scale and sophistication of cyberattacks

Concern About AI Technology Increasing the Speed, Scale, and Sophistication of Cyberattacks

(Shown: % Selected)



Q33. How concerned are you about advancements in AI technology increasing the speed, scale, and sophistication of cyberattacks against businesses today? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300), Independent Insurance Agents (n=300)

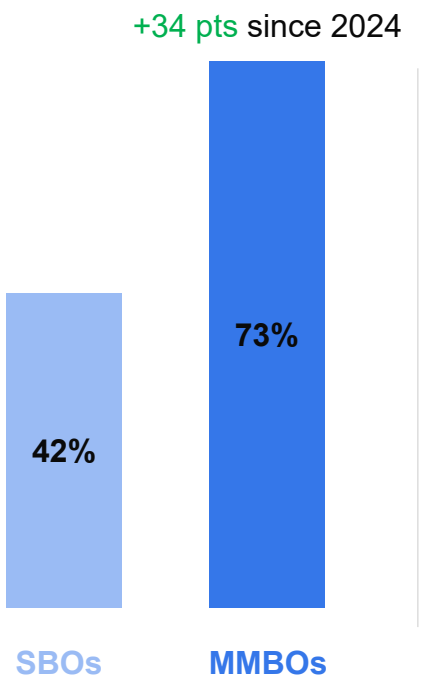
SBOs

MMBOs

Mid-market businesses are much more likely to have cyber insurance – at a significantly higher rate than 2024; despite high levels of interest, lack of knowledge holds SBOs back from purchasing coverage

Cyber Insurance Ownership

(Shown: % Selected "Yes")



Why Business Owners Don't Buy Cyber Insurance

(Shown: % Selected)

	Small Business Owners		Mid-Market Business Owners
#1	I don't know enough about cyber insurance	#1	Cyber insurance is too costly
#2	I did not know cyber insurance was available	#2	I feel that my current cybersecurity software provides sufficient protection
#3	My business is too small to need cyber overage	#3	I believe my business' cyber risks are already covered with other insurance policies
#4	My insurance agent has never recommended it to me	#4	I have trained by employees sufficiently to protect my business from a cyberattack
#5	Cyber insurance is too costly	#5	I don't know enough about cyber insurance

Interest in Cyber Insurance Offerings

(Shown: % Selected, T2B 'Interested')

	SBOs	MMBOs
Cyber defense preparation programs and resources	85%	70%
Discount offers based on a track record of better cyber defense preparation	84%	74%
A system where the insurer directly works with a security service provider to manage a claim	83%	74%
Cyberattack defense simulation exercises	78%	60%

Q56. Does your business purchase cyber insurance? Q36. As a business owner, how interested would you be in an insurer offering the following to better defend your enterprise against cyberattacks? Q57. Why don't you currently have cyber insurance? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

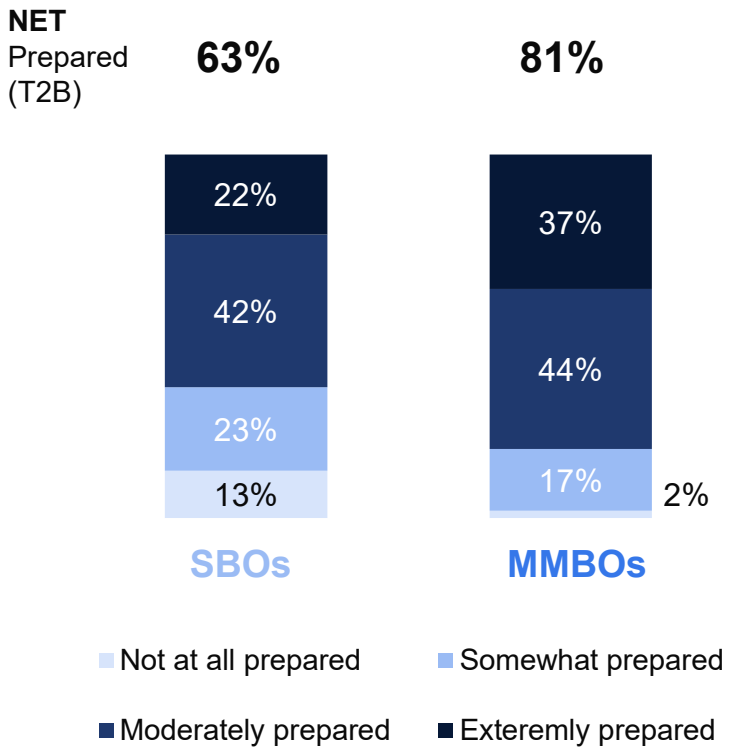
SBOs

MMBOs

Small BOs are less likely to feel prepared to prevent a cyber attack, likely due to lower rates of cybersecurity training and internal comms

Preparedness for Preventing a Cyberattack

(Shown: % Selected)



Cybersecurity Training Actions

(Shown: % Selected)

	Sending Phishing Test Emails to Employees	*Providing Formal Cybersecurity Training*	*Send communications / have conversations on the importance of cybersecurity measures*
SBOs	**30%** sent at least every few months	**72%** offered training at least annually	**82%** sent comms at least annually
MMBOs	**65%** sent at least every few months	**95%** offered training at least annually	**96%** sent comms at least annually

Q37. How often does your business do each of the following regarding employees' cybersecurity roles and responsibilities?
Q46. How prepared is your business in preventing a cyberattack? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

SBOs

MMBOs

Agents

Mid-market businesses are significantly more likely to have experienced a cyberattack; phishing is among the most common threats across audiences

Additionally, of those who have fallen victim to a cyberattack, 87% of MMBOs and 55% of SBOs report that they have experienced threats powered by or generated using AI.

Experienced a Cyberattack

(Shown: % Selected 'Yes')

16% **Small Business Owners**

-7 pts since 2024

62% **Mid-Market Business Owners**

+6 pts since 2024

59% **Independent Agents**

+10 pts since 2024

Cybersecurity Threats Experienced

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

		SBOs*	MMBOS	Agents
1	Password attacks	40%	33%	33%
2	Malware	32%	28%	36%
3	Phishing	32%	45%	39%
4	Ransomware	28%	32%	22%
5	AI-generated impersonation or fraud attempt	26%	34%	29%
6	Deepfakes	23%	17%	17%
7	AI-assisted phishing or social engineering attack	23%	38%	31%
8	Business email compromise	21%	29%	29%
9	Social engineering	21%	22%	26%
10	Business identification theft	19%	26%	28%
11	Data breach / security event	17%	32%	36%
12	Invoice fraud	17%	25%	21%
13	Utility fraud	15%	14%	12%
14	IoT or Internet of Things security breaches	13%	16%	21%
15	Digital tax fraud / unemployment fraud	11%	12%	17%
16	Attacks on the supply chain	9%	15%	22%
17	Denial of Service (DoS) attacks	6%	16%	23%
18	Skimming devices	6%	10%	11%
19	Sim card swap	4%	14%	14%

Highlighted text indicates significant difference between groups at the 95% confidence level

SBOs

87%

experienced an AI-powered cybersecurity threat

MMBOs

55%

experienced an AI-powered cybersecurity threat

Agents

39%

of clients experienced an AI-powered cybersecurity threat

Q38. Has your business ever been a victim of a cyberattack? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300), Independent Insurance Agents (n=300)
Q39. Which, if any, of the following cybersecurity threats has your business experienced? Q40. To the best of your knowledge, were any of the cybersecurity threats your business experienced powered by or generated using AI?
Base: Small Business Owners who have experienced a cyberattack (n=47), Mid-Market Business Owners who have experienced a cyberattack (n=184), and Independent Agents who have experienced a cyberattack (n=178)*

SBOs

MMBOs

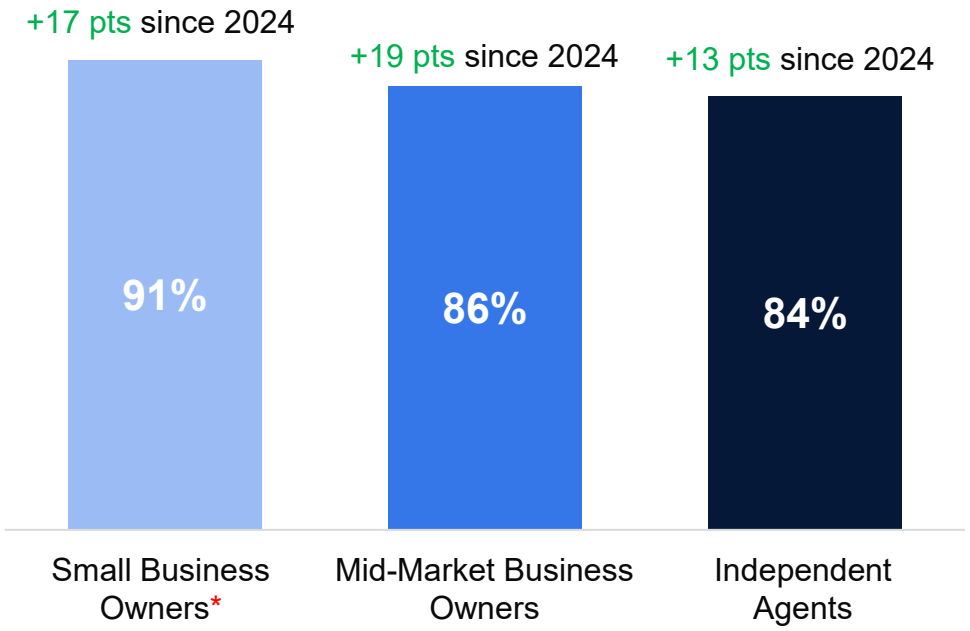
Agents

Cyberattacks don't just hit the balance sheet — nearly every victim reports damage to customer trust

The financial impact of cyberattacks has risen since 2024, and impact on customer trust remains high among those who have experienced attacks.

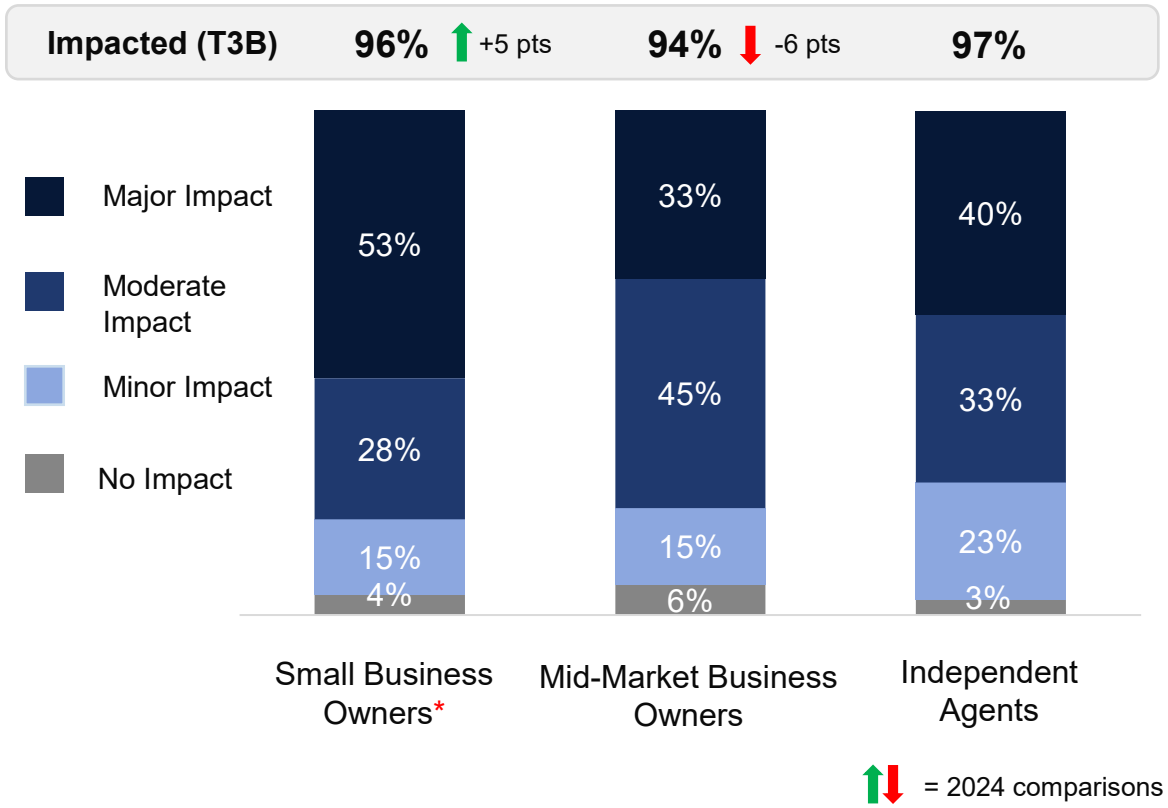
Cyberattack Impacted or Jeopardized Business Finances

(Shown: % Selected "Yes")



Cyberattack Negatively Impacted Customer Trust in Business

(Shown: % Selected)



Q41. Did the cyberattack impact or jeopardize your business' finances?
Q42. Did the cyberattack negatively impact customer trust or reputation in your business?
Base: Small Business Owners who have experienced a cyberattack (n=47), Mid-Market Business Owners who have experienced a cyberattack (n=185), and Independent Agents who have experienced a cyberattack (n=178)*

SBOs

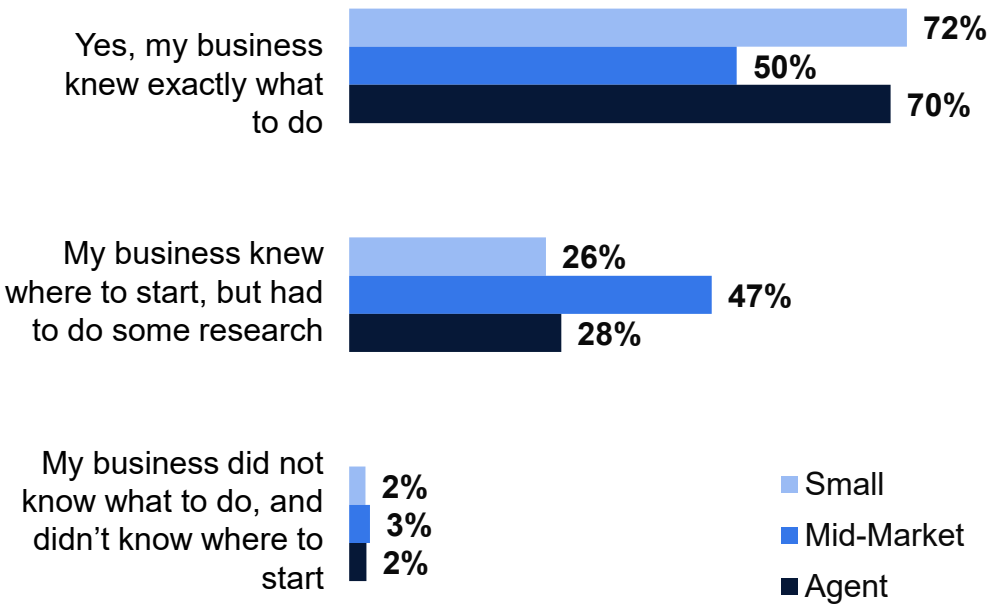
MMBOs

Agents

Only half of Mid-Market Business Owners were confident in their response – and while many are taking steps to prevent future issues, there is opportunity for better protection

Response to Cyberattack

(Shown: % Selected)



Steps Taken to Prevent Future Cyberattacks

(Shown: % Selected)

		SBOs	MMBOs	Agents
1	Requiring multi-factor authentication	34%	53%	42%
2	Adding regular password update requirements	34%	36%	31%
3	Updating our cybersecurity software	33%	46%	45%
4	Backing up data following stricter protocols	32%	37%	40%
5	Installing a new cybersecurity software	29%	35%	31%
6	Implementing procedures to verify requests involving payments, sensitive information, or account changes through a second communication channel	28%	25%	27%
7	Purchasing cyber insurance	26%	41%	35%
8	Requiring VPN use when on Wi-Fi outside of the workplace	26%	25%	27%
9	Establishing processes to verify the identity of callers, employees, vendors, or customers to guard against AI-generated impersonation	26%	27%	27%
10	Adding encryption features	26%	33%	35%

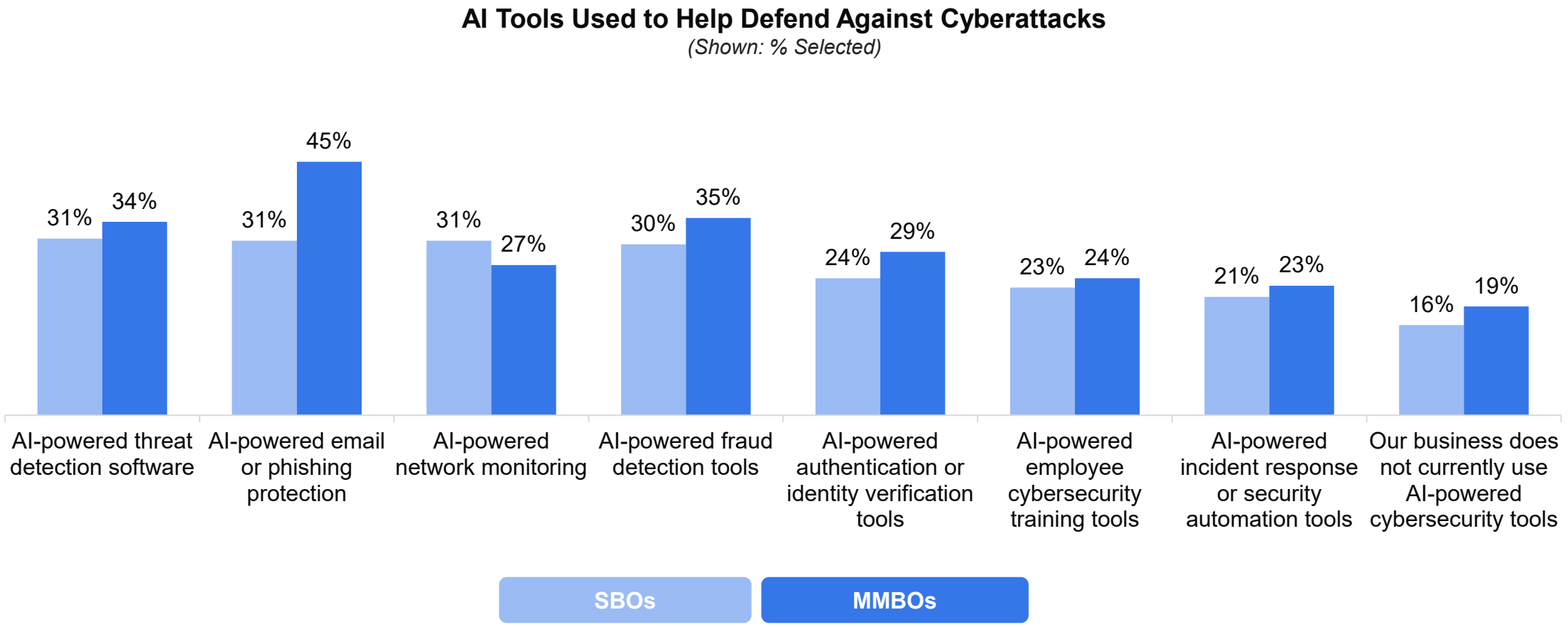
Highlighted text indicates significant difference between groups at the 95% confidence level

Q45. Did your business know what to do once you identified the attack? Base: Small Business Owners who have experienced a cyberattack (n=47), Mid-Market Business Owners who have experienced a cyberattack (n=185), and Independent Agents who have experienced a cyberattack (n=178) Q47. Thinking about if your business were to fall victim to cyberattacks in the future, which of the following are you taking to prevent future cyberattacks? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300), Independent Insurance Agents (n=300)*

SBOs

MMBOs

Most Business Owners are utilizing AI tools to some degree to defend against cyberattacks – with the most common use cases surrounding threat detection, email or phishing protection, network monitoring, and fraud detection



Q48. Which of the following AI-powered tools or technologies, if any, does your business use to help defend against cyberattacks? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

SBOs

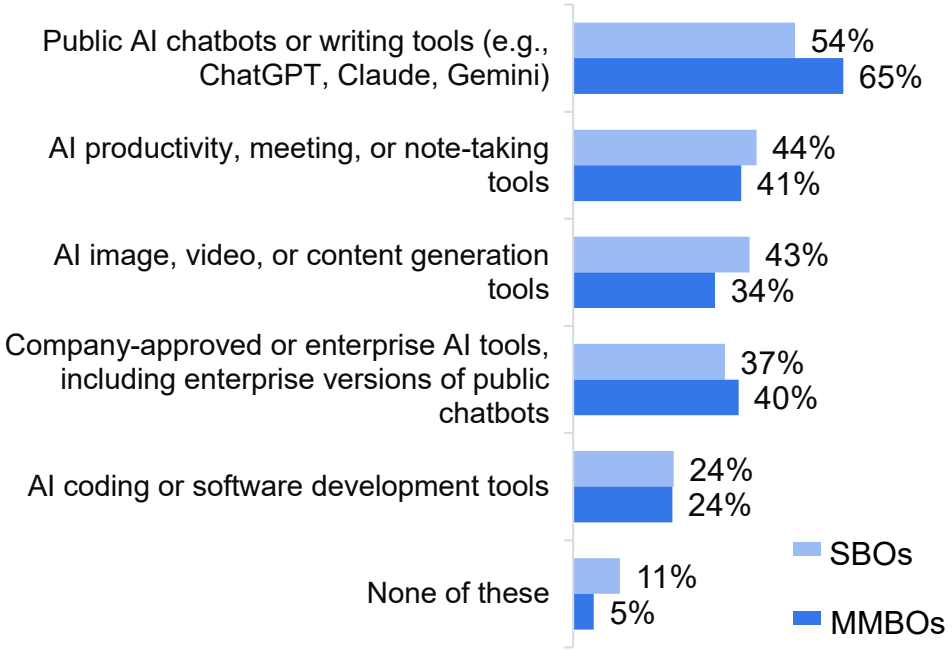
MMBOs

Around half of businesses are using public AI tools – however few have established written policies or offered training to support employee use

This reveals businesses are embracing AI faster than they're governing it. Additionally, 2 in 5 (39%) SBOs and 30% of MMBOs believe employees are using unauthorized AI tools for work.

AI Tools Used by Employees for Work-Related Tasks

(Shown: % Selected)



Governance or Management Implementations for AI Tools by Employees

(Shown: % Selected)

	SBOs	MMBOs
A written policy or guidelines for employee use of AI tools	35%	36%
Employee training on the responsible use of AI tools	35%	39%
Review or oversight of AI-generated content before it is shared externally	33%	18%
Restrictions on the use of public AI tools (e.g., ChatGPT, Claude, Gemini)	31%	19%
Rules about what company or customer information can be entered into AI tools	28%	26%
Procedures for verifying AI-generated information before it is used for business decisions	28%	21%
Regular reviews of AI-related cybersecurity, privacy, or compliance risks	27%	30%
Approval requirements before employees can use certain AI tools	26%	30%
A designated employee or team responsible for overseeing AI use	20%	21%
Our business has not implemented any policies, controls, or oversight related to AI use	12%	24%

SBOs

39% Believe employees are using unauthorized AI chatbots/tools for work

MMBOs

30% Believe employees are using unauthorized AI chatbots/tools for work

Q49. Which of the following types of AI tools are employees at your business currently using for work-related tasks? Q50. Do you believe employees at your company are using unauthorized AI chatbots/tools for work purposes? Q51. Which of the following, if any, has your business implemented to help govern or manage the use of AI tools by employees? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

A plurality of Business Owners believe time to recover from cyberattack to be up to 3 months, but are split on the ease of recovering costs

SBOs
MMBOs

Length of Time to Recover

(Shown: % Selected)

Anticipated Cost of Average Cyberattack

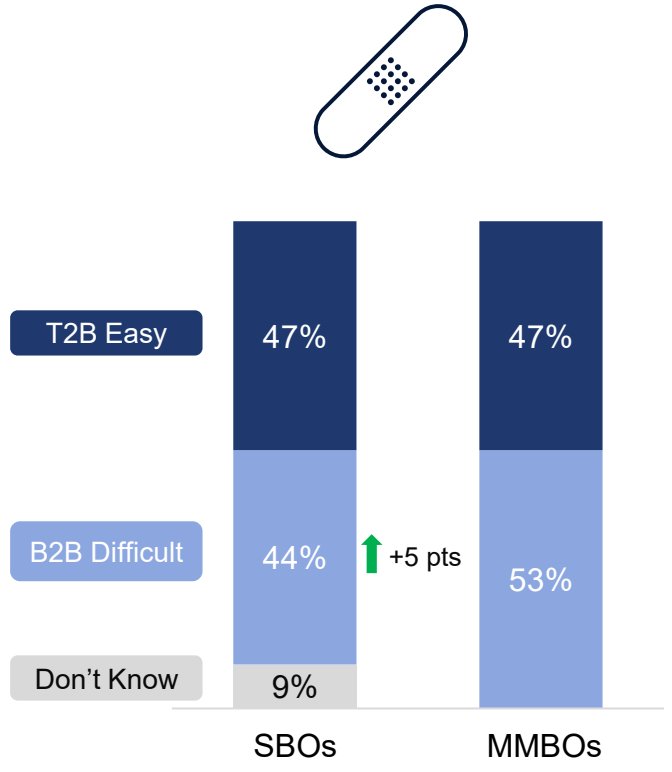
(Shown: % Selected)

	SBOs	MMBOs
Under $100	2%	0%
$100 – $499	5%	2%
$500 – $999	10%	9%
$1,000 – $4,999	20%	27%
$5,000 – $9,999	24%	19%
$10,000 – $49,999	20%	25%
$50,000 – $99,999	2%	10%
$100,000 – $249,000	1%	9%
$250,000+	2%	0%

Highlighted text indicates significant difference between groups at the 95% confidence level

Ease of Recovering Costs

(Shown: % Selected T2B Easy and B2B Difficult)



= 2024 comparisons

Q52. Thinking about if your business were to fall victim to a cyberattack in the future, how long do you anticipate recovering from a cyberattack would take? If you are unsure or don't know, please select that option. Q53. Thinking about if your business were to fall victim to a cyberattack in the future, how easy would it be to cover the costs of recovery? Q55. How much do you think it would cost for your business/you personally to recover from the average cyberattack/identity theft incident? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

SBOs

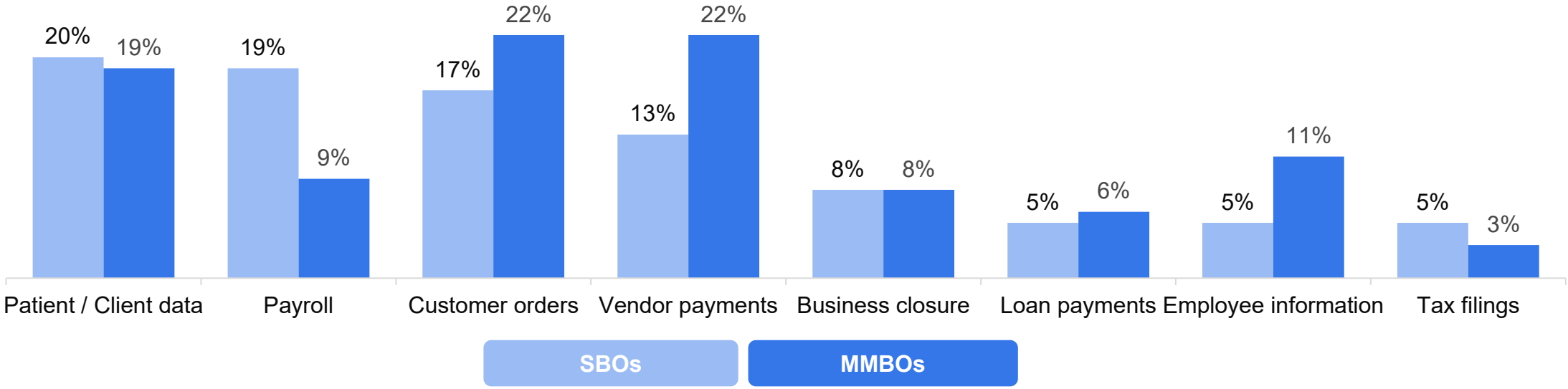
MMBOs

Were they to lose access to systems or funds for a week, Business Owners say client data would be most at risk

SBOs were more likely to say payroll would be most at risk, while MMBOs were more likely to say vendor payments.

If Your Business Lost Access to Systems or Funds for 1 Week Due to a Cyberattack, Which Would be Most at Risk?

(Shown: % Selected)



Q54. If your business lost access to systems or funds for one week due to a cyberattack, which would be most at risk? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

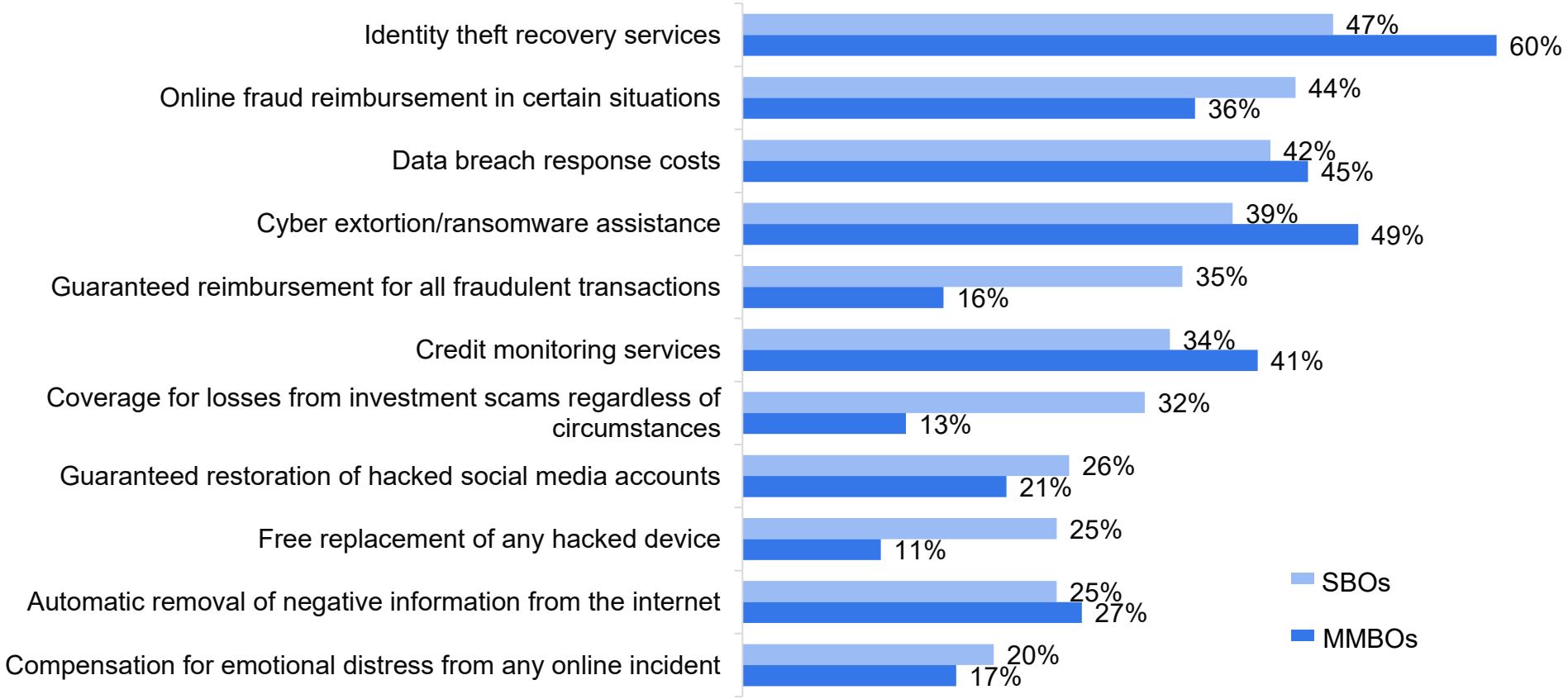
SBOs

MMBOs

Identity theft recovery is seen as a baseline provision of cyber insurance; MMBOs expect assistance with extortion and credit monitoring, SBOs expect coverage of fraud reimbursement and data breach response costs

Knowledge of What Cyber Insurance Covers

(Shown: % Selected)



Q58. To the best of your knowledge what does cyber insurance cover? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

SBOs

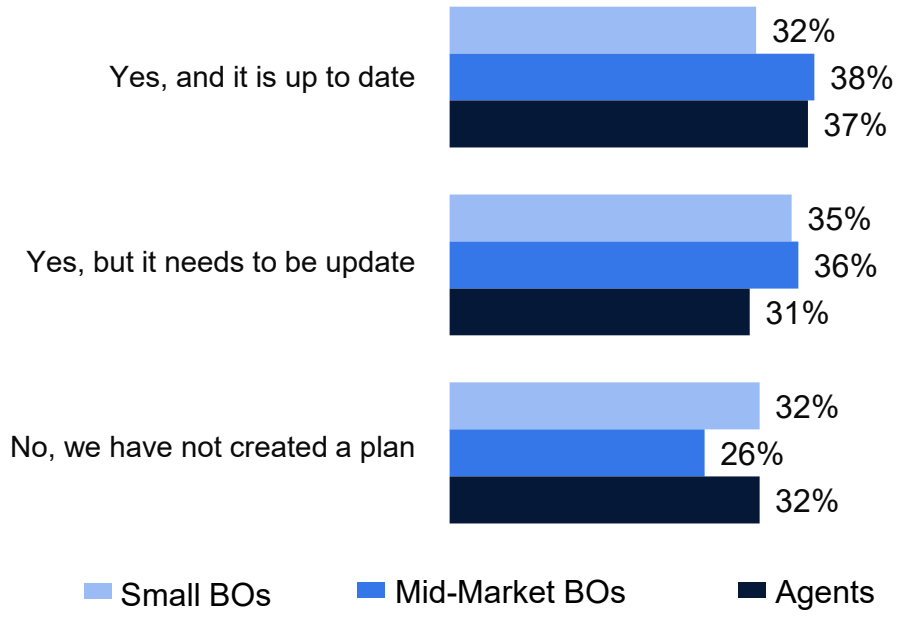
MMBOs

Agents

One third of audiences have an updated response plan for a cyberattack in place, with proactive monitoring being the most cited instruction

Incident Response Plan in Place

(Shown: % Selected)



Incident Response Plan Instructions in Place

(Shown: % Selected "Yes")

	Small Business Owners	Mid-Market Business Owners	Agents
Proactive monitoring and reporting	**77%**	**78%**	**71%**
Consultations with legal counsel	**67%**	**54%**	**58%**
Incident reporting procedures to government regulatory agencies	**65%**	**57%**	**63%**
Crisis response simulations	**62%**	**46%**	**44%**

Highlighted text indicates significant difference between groups at the 95% confidence level

Q59. Has your company created an incident response plan in the event of a cyberattack or data breach? Q60. Does your company's incident response plan include instructions for each of the following? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300), Independent Insurance Agents (n=300)

SBOs

MMBOs

Nine in 10 Small Business Owners trust that their cyber insurance would take care of their needs in the event of a cyberattack

Two-thirds of SBOs admit they haven't given much thought to what they'd do after a cyberattack.

Response if a Cyberattack Occurred

(Shown: % Selected T2B Agree)

	Small Business Owners	Mid-Market Business Owners
I trust that my cyber insurance coverage would take care of all my needs	90%*	77%*
I'm confident my business would retain its customers/reputation after the attack	79%	73%
I would know where and how to begin the recovery process after the attack	72%	78%
I'm confident that I could recover all my losses from the attack	70%	64%
I trust that my employees would know what to do if they were victims of a cyberattack	69%	70%
I haven't given much thought to what I would do if I fell victim to a cyberattack	66%	39%
Right now, I have all the resources I would need to recover any losses from the attack	62%	61%
I trust that my non-cyber insurance coverages would take care of all my needs	61%	36%

Highlighted text indicates significant difference between groups at the 95% confidence level

*Q61. Thinking about how you would respond if your business were to fall victim to a cyberattack, how much do you agree or disagree with the following statements? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300) (*asked only to those with cyber insurance)*

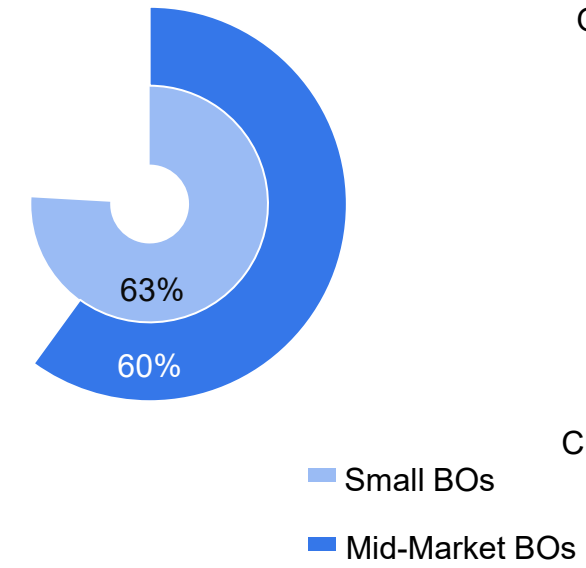
SBOs

MMBOs

Small BOs are more likely to outsource the recovery process, and less likely to employ their own dedicated IT or cybersecurity team

Would Hire / Outsource if Business Fell Victim to a Cyberattack

(Shown: % Selected "Yes")



Cybersecurity Roles Employed

(Shown: % Selected "Yes")

% of Overall IT Budget Allocated To Cybersecurity Needs

(Shown: % Selected)

	Small Business Owners	Mid-Market Business Owners
0%	10%	2%
1% - 9%	15%	42%
10% - 19%	28%	38%
20% - 29%	15%	8%
30% - 39%	17%	8%
40% - 49%	9%	1%
50% - 59%	4%	0%
60% - 69%	2%	0%
70% - 79%	1%	0%
80% - 89%	0%	0%
90% - 100%	0%	0%

Highlighted text indicates significant difference at the 95% confidence level

Q62. If your business were to fall victim to a cyberattack, would you hire or outsource someone to lead the recovery process for you? // Q80. Does your business currently employ the following roles relating to cybersecurity? // Q81. About what percent of your business's overall IT budget is dedicated to cybersecurity, including cyber insurance and any third-party vendors? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

Interest in cyberattack protections is overwhelming among Business Owners

SBOs

MMBOs

Interest in Cyberattack Protection Resources or Products

(Shown: % Selected T2B Interested)

	SBOs	MMBOs
Business / Computer System Interruption protection	**92%**	**84%**
Data compromise protection	**91%** +5 pts since 2024	**90%** -6 pts since 2024
Identity recovery protection	**90%**	**88%** -6 pts since 2024
Network Security Liability protection	**89%**	**87%** -7 pts since 2024
Misdirected Payment Fraud protection	**88%**	**85%** -6 pts since 2024
Cyber Extortion protection	**87%** +8 pts since 2024	**89%** -5 pts since 2024
Dependent Computer System Interruption protection	**87%**	**71%**
Dependent Computer System Failure protection	**84%**	**69%**
Electronic Media Liability protection	**82%**	**82%** -8 pts since 2024

Highlighted text indicates significant difference between groups at the 95% confidence level

Q63. How interested would you be in purchasing each of the following resources or products to protect against cyberattacks? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

** Definitions available in notes section*

Nearly two thirds of Agents are having cybersecurity threat conversations with commercial line customers often or always, but less than half with personal lines customers

Frequency of Conversations With Clients About Protecting Against Potential Cybersecurity Threats
(Shown: % Selected T2B Often/Always)

44%

Of Independent Agents have conversations with personal lines customers about protecting themselves / their business from potential cybersecurity threats often or always

62%

Of Independent Agents have conversations with commercial lines customers about protecting themselves / their business from potential cybersecurity threats often or always

Level of Resources Provided to Employees to Counsel Customers on Cyberattacks and Cyber Insurance Solutions
(Shown: % Selected)

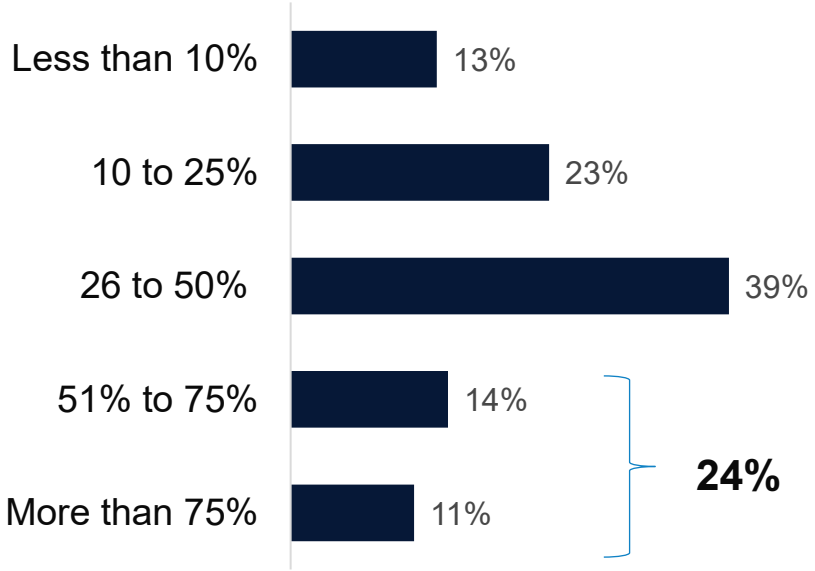
No resources are provided	8%
Few resources are provided	33%
Some resources are provided	40%
Plenty of resources are provided	19%
Some + Plenty NET	**59%**

Q64. Now thinking about your clients, how often do you have conversations with clients about protecting themselves/their business from potential cybersecurity threats?
Q65. Which of the following best describes the level of resources you provide your employees to counsel customers on cyberattacks and cyber insurance solutions? Base: Independent Insurance Agents (n=300)

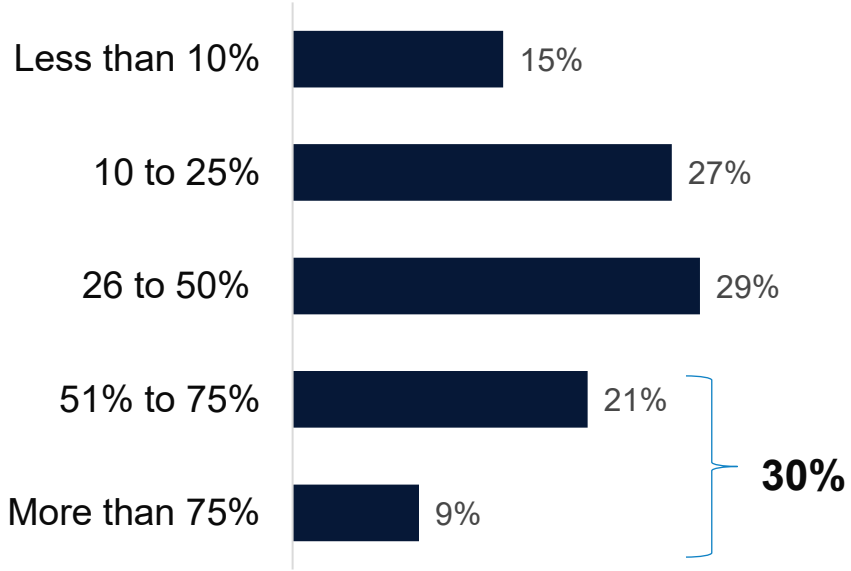
Agents say few of their commercial clients are keeping pace with evolving cyber risk

Less than at third of commercial clients have an incident response plan or keep cyber coverage up to date.

Percentage of Commercial Clients With an Incident Response Plan
(Shown: % Selected)



Percentage of Commercial Clients Who Keep Their Cyber Coverage Level Up to Date
(Shown: % Selected)



Q67. About how many of your commercial clients have created an incident response plan in the event of a cyberattack or data breach? // Q68. About how many of your commercial clients keep their cyber coverage level up to date with the evolving landscape? Base: Independent Insurance Agents (n=300)

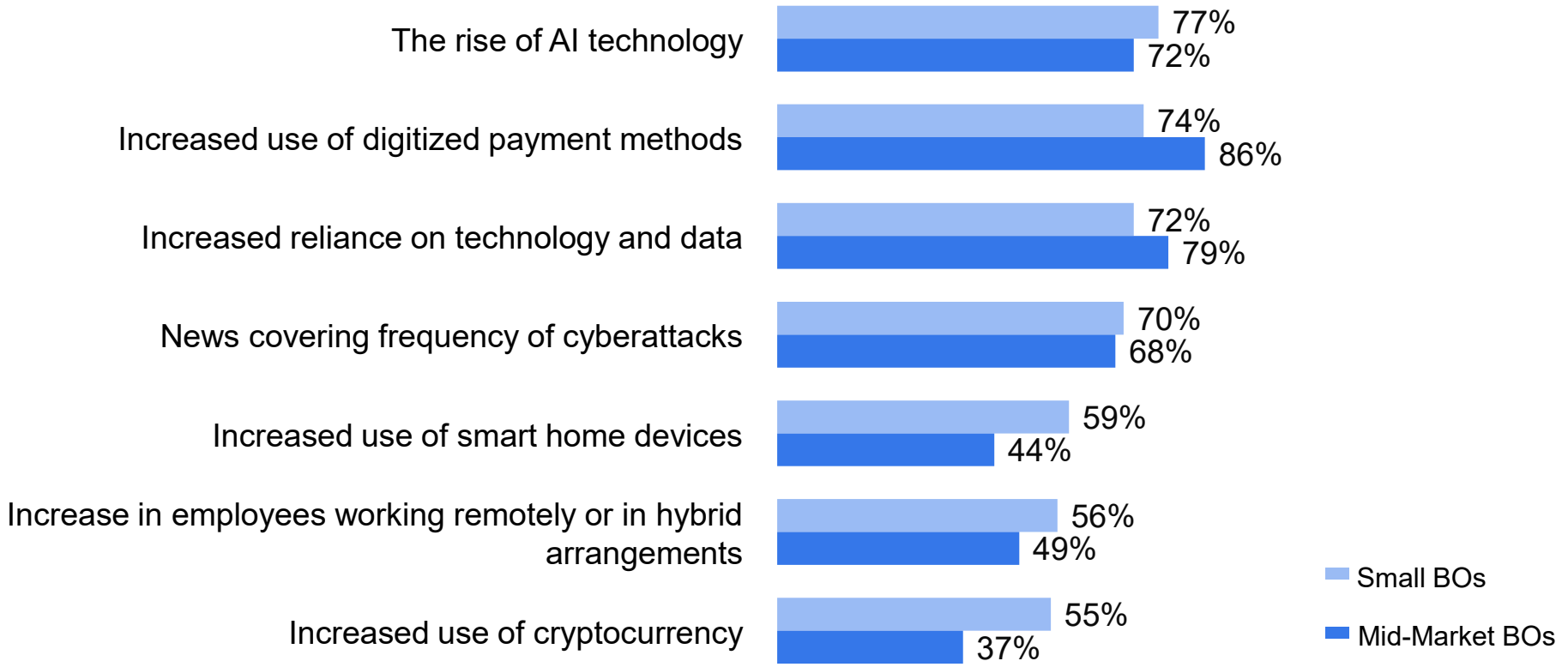
SBOs

MMBOs

Business Owners similarly feel more likely to purchase cyber insurance because of reliance on tech and rise in AI

Impact on Likelihood to Purchase Cyber Insurance Coverage

(Shown: % Selected T2B More Likely)

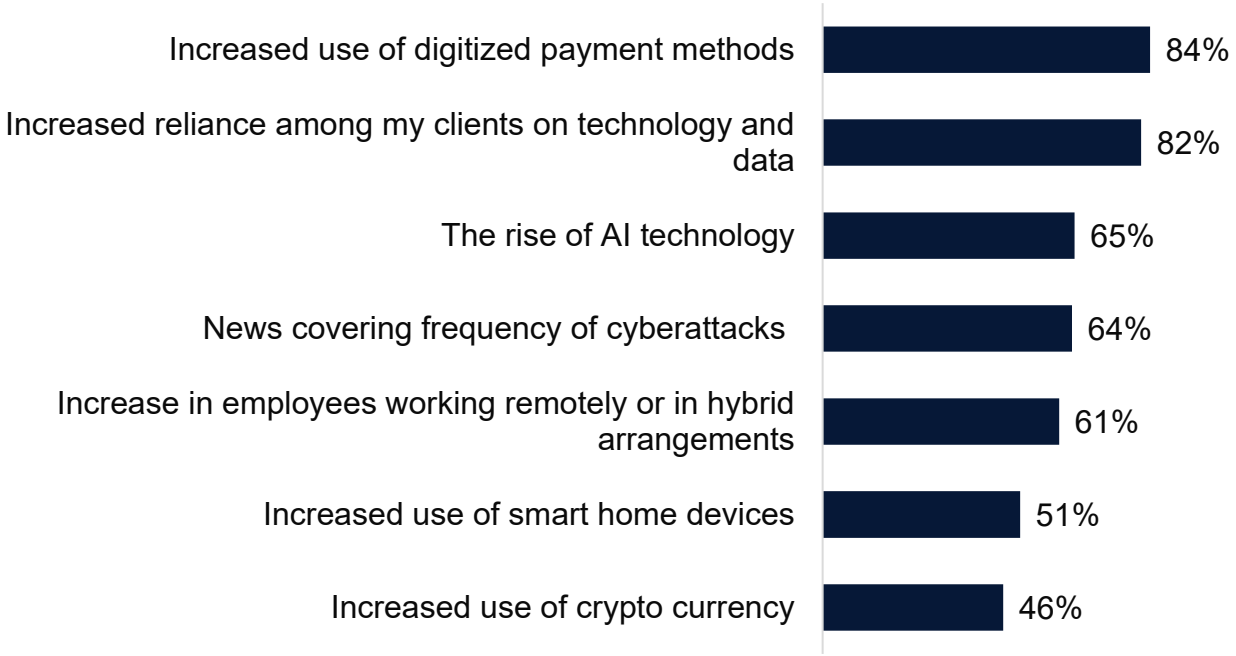


Q78. Have each of the following events made you more or less likely to purchase cybers risk insurance or expand your current level of cyber insurance coverage? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300)

The rise of AI, reliance on technology, and payment digitization have all made Agents more likely to recommend cyber insurance coverage

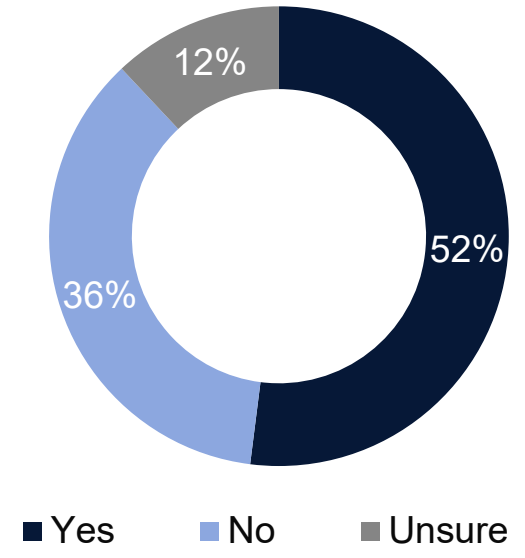
Impact on Likelihood of Encouraging Clients to Purchase or Increase Cyber Insurance Coverage

(Shown: % Selected T2B Likely)



Observed Increase in Scams or Fraud Attempts that Use Generative AI In the Past 12 Months

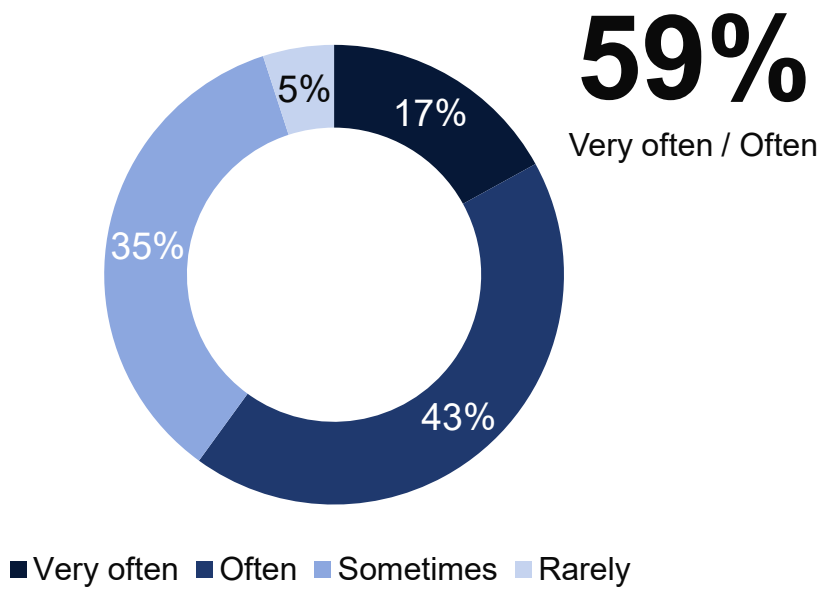
(Shown: % Selected)



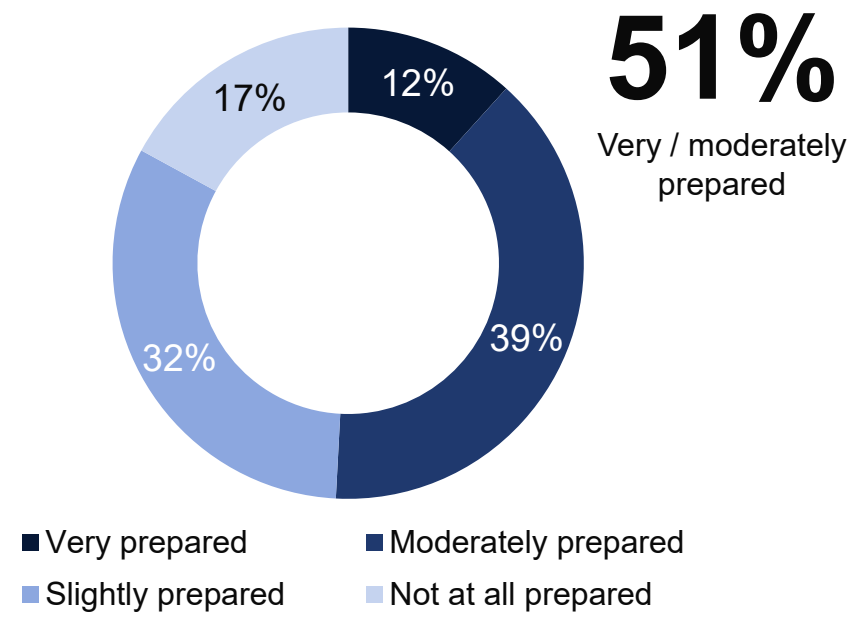
Q69. Have you observed an increase in claims related to scams or fraud attempts that use generative AI technology in the past 12 months? // Q79. Have each of the following events made you more or less likely to encourage your clients to purchase or increase their level of cyber insurance coverage? Base: Independent Insurance Agents (n=300)

Agents say only about half of clients are prepared to identify and respond to AI-powered cyber threats

Frequency of Clients Asking about AI-powered Scams, Cyber threats, or Cybersecurity Risks
(Shown: % Selected)



Preparedness of Clients to Identify and Respond to AI-powered Cyber threats
(Shown: % Selected)



Q70. How frequently are your clients asking questions about AI-powered scams, cyber threats, or cybersecurity risks? Q71. In your opinion, how prepared are your clients to identify and respond to AI-powered cyber threats? Base: Independent Insurance Agents (n=300)

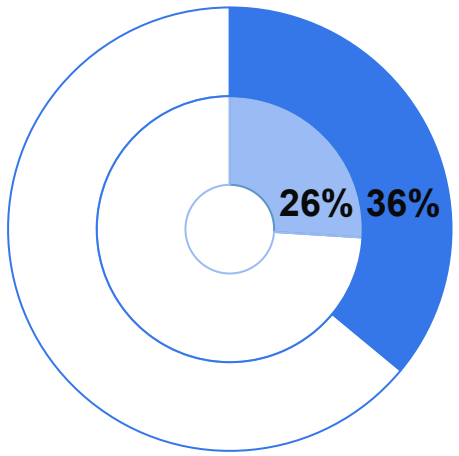
SBOs

MMBOs

More than a quarter of Business Owners have been targeted by an AI fraud attempt, particularly email impersonations or phishing attempts

Company Targeted By an AI Scam / Fraud Attempt Using Generative AI Within the Past 12 Months

(Shown: % Selected "Yes")



Description of Generative AI Scam / Fraud Attempt

(Shown: % Selected T2B "Yes", Among those targeted by a Gen AI fraud attempt)

	SBOs	MMBOs
Email impersonating a business owner, executive, employee, customer, or vendor	26%	17%
AI-generated customer support, vendor, or business inquiry designed to obtain information	15%	4%
Attempt to gain access to company accounts, systems, or credentials using AI-generated content	13%	13%
AI-generated phishing email, text message, or chat message	12%	24%
Fraudulent request for payment, wire transfer, gift cards, or financial information	10%	17%
Deepfake video or image impersonating a business owner, employee, customer, or vendor	9%	6%
Fake job applicant, resume, or candidate generated using AI	8%	6%
Phone call using AI-generated or cloned voice technology	6%	13%

Highlighted text indicates significant difference between groups at the 95% confidence level

Q72. Has your company been targeted by a scam or fraud attempt that used generative AI within the past 12 months? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300) Q73. You mentioned your business has been targeted by a scam or fraud attempt that used generative AI. Which of the following best describes the attack? Base: Small Business Owners who have been targeted by a Gen AI fraud attempt (n=78), Mid-Market Business Owners who have been targeted by a Gen AI fraud attempt (n=109)*

SBOs

MMBOs

Agents

AI is moving cyber insurance from a consideration to a business imperative

Audiences overwhelming agree that AI has made cyber crimes more accessible, effective, and widespread.

Perceptions of Generative AI Scams / Fraud Attempts

(Shown: % Selected T2B Agree)

	Small Business Owners	Mid-Market Business Owners	Agents
AI is making it easier for cybercriminals to launch attacks at scale	90%	93%	92%
AI is making it easier for attackers to identify vulnerabilities	90%	88%	87%
AI-enabled cyberattacks have become increasingly sophisticated over the past 12 months	89%	87%	90%
I need more information and resources about how best to protect my business from AI-enabled cyberattacks	88%	75%	N/A
AI is lowering the barriers for less-skilled attackers to carry out cyberattacks	83%	82%	85%
I'm very concerned about the threat of these attacks to my business	80%	84%	89%

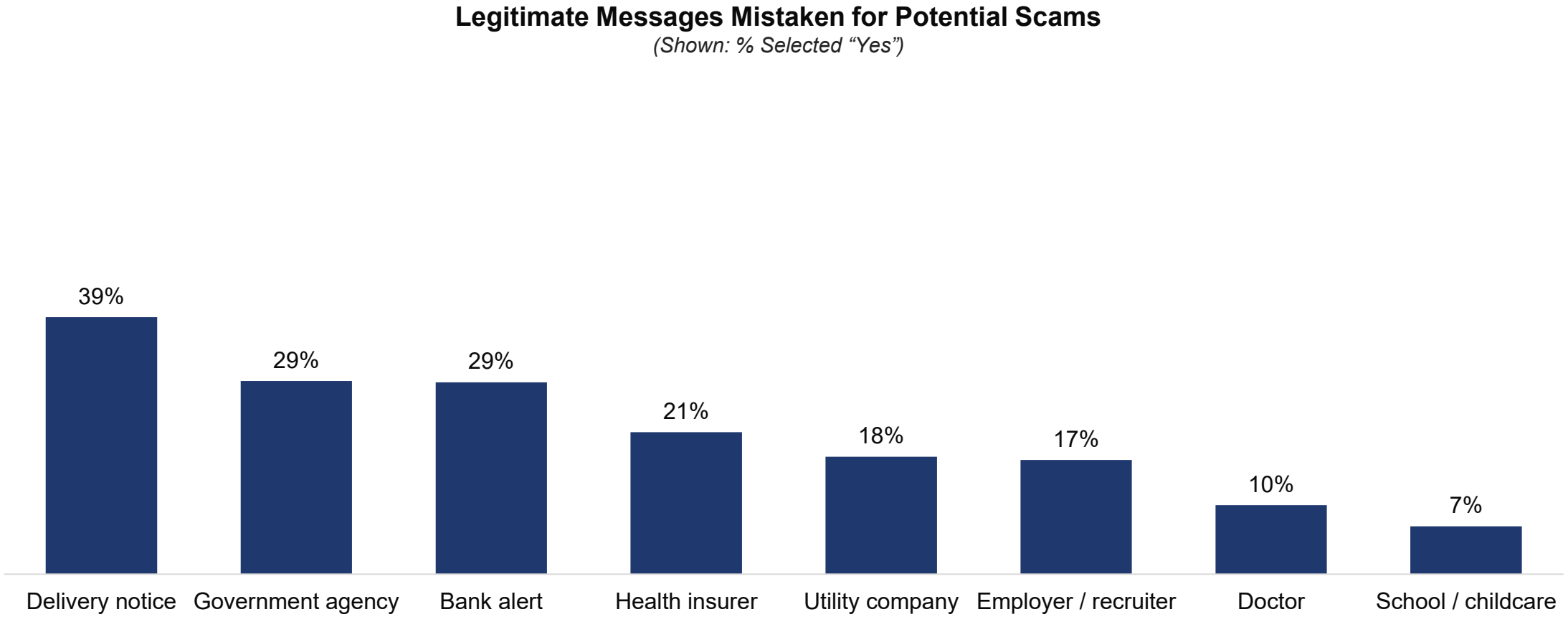
62% *Of Agents agree (T2B) that they need more information/resources on how to protect their clients from AI-enabled cyberattacks*

Q74. How much do you agree or disagree with the following statements about scams or fraud attempts that use generative AI? Base: Small Business Owners (n=300), Mid-Market Business Owners (n=300), Independent Insurance Agents (n=300)

Nationwide®

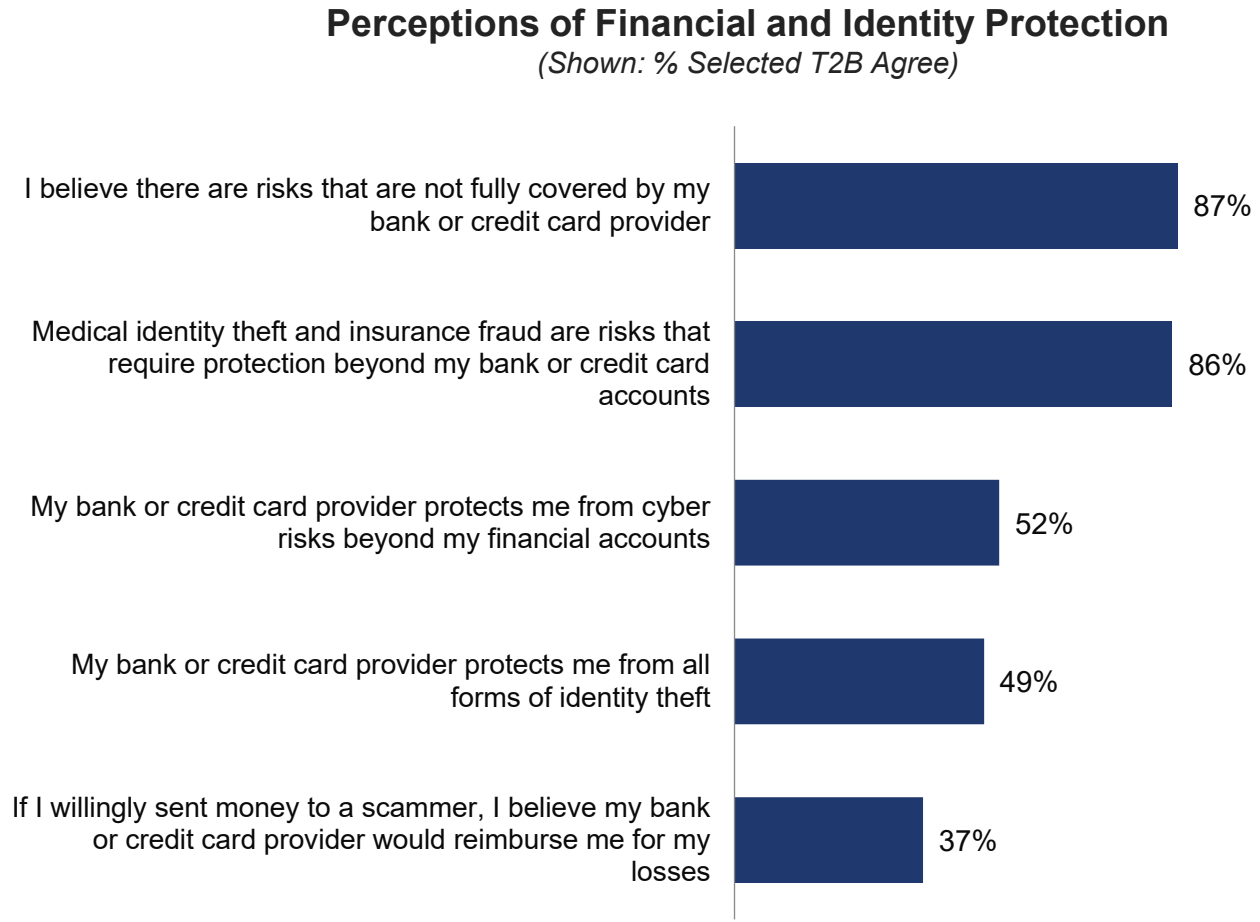
Additional Data: Consumers

Nearly 4 in 10 consumers have ignored or delayed responding to a legitimate delivery notice over scam concerns



Q12. Have you ignored or delayed responding to a legitimate message from any of the following sources because you suspected it was a scam or cybersecurity threat? Base: Consumers (n=1,000)

While most recognize limits to their bank/credit card provider's protection, around half overestimate the protection it provides for cyber risks and identity theft



Q30. How much do you agree or disagree with the following statements? Base: Consumers (n=1,000)

Additional Data: Business Owners & Agents

Agents report widespread cyberattack concern, especially among commercial clients

In their experience, the businesses that consider or purchase cyber insurance do so largely because they have witnessed similar businesses become victims of cyberattacks or they are well informed about these threats.

Client Concern about Cyberattacks

(Shown: % Selected Extremely/Moderately Concerned)

Concerned about a potential cyberattack on their client / client's business

62%

of Personal lines customers

79%

of Commercial lines customers

Why Businesses Consider or Purchase Cyber Insurance

(Shown: % Selected)

		Independent Insurance Agents
1	They have witnessed similar businesses become victims of cyberattacks	**64%**
2	They are well-informed about cyberattacks and are thinking ahead	**61%**
3	They have read articles in the news warning about cyberattacks	**50%**
4	They are concerned about the increased use of AI technology to support cyberattacks	**46%**
5	They are recently the victim of a cyberattack	**40%**
6	They do not trust their employees to avoid a cyberattack	**20%**

Q32: In general, how concerned do you think your clients are about potential cyberattacks (on themselves personally or their business)? Q35. In your experience, why do businesses consider or purchase cyber risk insurance? Please select all that apply. Base: Independent Insurance Agents (n=300)

SBOs

MMBOs

Agents

Phishing and email compromises are the top ways businesses and Agents were infiltrated; Most had cyber insurance at the time the attacks occurred – though Agents were less likely

How Cyberattack Infiltrated Business

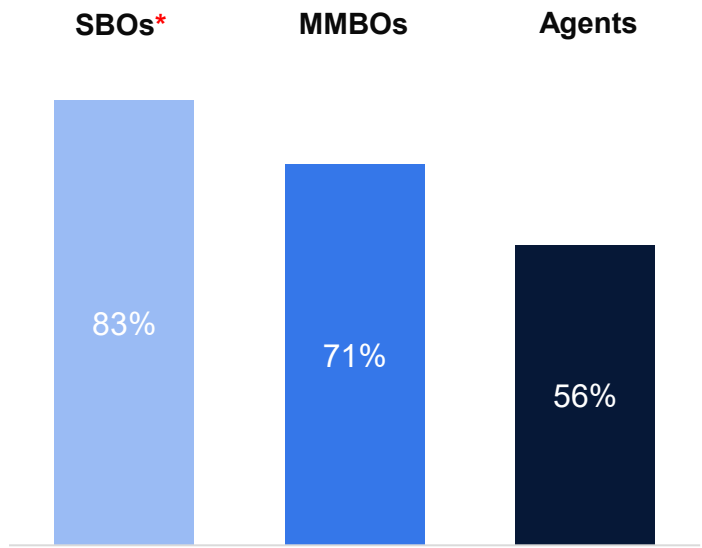
(Shown: % Selected)

		Small*	Mid-Market	Agents
1	Phishing	47%	52%	48%
2	Accidental data loss	36%	16%	15%
3	Email compromise (including AI-generated emails or impersonation attempts)	34%	50%	48%
4	Social engineering, impersonation, or other attempts to manipulate employees (including AI-generated messages, voice cloning, or deepfakes)	32%	36%	30%
5	Compromised credentials	32%	32%	28%
6	Lost or stolen devices	28%	15%	14%
7	Malicious employees / contractors	21%	12%	9%
8	Vulnerabilities from a vendor or third-party software	21%	16%	12%
9	Digital supply chain breach	21%	25%	14%
10	System error	21%	15%	9%
11	Physical security compromise	17%	15%	12%

Highlighted text indicates significant difference between groups at the 95% confidence level

Cyber Insurance Status at Time of Cyberattack

(Shown: % Selected T2B "Had cyber insurance", among those who have experienced a cyberattack)*



Q43. Which of the following best describes your situation when the cyberattack occurred?
Q44. Based on what you currently know, how did the cyberattack infiltrate your business? Base: Small Business Owners who have experienced a cyberattack (n=47), Mid-Market Business Owners who have experienced a cyberattack (n=185), and Independent Agents who have experienced a cyberattack (n=178)*

9 in 10 Agents agree that clients view them as a credible source of cybersecurity information

Agent Perceptions of Client Cybersecurity Knowledge

(Shown: % Selected T2B Agree)

AI technology is making my clients more susceptible to cyber threats	**94%**
My clients view me as a credible source of information when it comes to cybersecurity	**90%**
I feel confident talking to my clients about their cyber vulnerabilities and coverages to protect them	**87%**
I'm concerned about the lack of knowledge among my clients around cybersecurity in general	**80%**
I feel confident explaining the differences between identity theft protection and personal cyber insurance coverage to my clients	**77%**
Many of my clients are unaware of their exposure to cyberattacks	**76%**
Many of my clients are unsure of what is covered in a cyber insurance policy	**74%**
Many of my clients are not even aware that cyber insurance exists	**49%**

Q75. How much do you agree or disagree with each of the following statements? Base: Independent Agents (300)

9 in 10 Independent Agents are recommending cyber insurance to their customers

Recommendation of Cyber Insurance

(Shown: % Selected "Yes")

89%

Of Independent Agents regularly recommend cyber insurance to their customers

Agent Perceptions of Client Cybersecurity Knowledge

(Shown: Open-End Verbatims)

"I usually tell them to think of identity theft protection as a service that helps restore your identity after it is being compromised, whereas personal cyber insurance provides financial protection for covered cyber related events."

"The key difference is that identity theft protection helps restore who you are after identity fraud, while personal cyber insurance helps protect what you may lose financially from covered cyber incidents."

Q76. Do you regularly recommend cyber insurance to your customers?
Q77. In a sentence or two, how would you explain the difference between identity theft protection and personal cyber insurance coverage to a customer? Base: Independent Insurance Agents (n=300)