Nationwide®

September 2024

Nationwide Cybersecurity

Survey Report – Business Owners

SURVEY METHODOLOGY

Audiences	Sample Size	Methodology	Timing
Small Business Owners *Owners of small businesses, defined as 1-50 employees and less than $10M in annual revenue*	**N=400**	**20-Minute Online Survey**	**Survey Fielded July 26th – August 14th, 2024**
Mid-Market Business Owners *Owners of middle-market businesses, defined as 50-500 employees or $10M-$500M in annual revenue*	**N=400**		
Commercial Lines-Focused Independent Insurance Agents *Mix of Principals, Producers, and CSRs; At least 50% of agency business must be from commercial lines products/accounts*	**N=400**		

Roughly 3 in 4 Business Owners are concerned about cyberattacks on their businesses – with Small BOs reporting higher levels of concern since 2022

The top reasons for concern include the recent increase in cyberattacks, digital supply chain vulnerabilities, the lack of preventative IT measures to avert attacks, and the proliferation of new avenues for system breaches since the pandemic began. Additionally, compared to 2023, more small business owners are concerned about potential cyberattacks.

Concern about Cyberattacks

(Shown % Selected Extremely/Moderately Concerned)

At least moderately concerned about a potential cyberattack on their business

69% +16 pts since 2022

Of Small Business Owners

77% -2 pts since 2022

Of Mid-Market Business Owners

Why Businesses are Concerned about Cyberattacks

(Shown % Select)

		Small	Mid-Market
1	Cyberattacks have been increasingly common in the last few years	53%	67%
2	With a digital supply chain, there are more devices than ever vulnerable to cyberattacks	31%	28%
3	There are not enough IT measures in place to effectively prevent cyberattacks	24%	20%
4	The pandemic has been a catalyst for new ways to breach our system (for example through remote working, digitized point of sales systems, etc.)	24%	37%
5	I do not have cyber risk insurance	24%	24%
6	The data our business collects has not been properly examined for cyberthreats	20%	22%
7	It is very difficult to find cybersecurity experts to protect my business	19%	27%
8	I don't think I understand enough about cybersecurity to protect my business	19%	17%
9	I'm concerned there may be increased cyberattacks stemming from the war in Ukraine	18%	25%
10	Maintenance of our IT systems is not conducted regularly enough	16%	27%
11	I do not trust that my employees are diligent enough to fend off all cyberattacks	16%	10%

Q1a. 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? // Q2a. 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 (n=400), Mid-Market Business Owners (n=400)

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

Roughly 2 in 3 Agents report their clients are concerned about potential cyberattacks

When asked why businesses consider cyber insurance, most agents say their clients are well-informed about cyber threats and have kept up with news articles warning about potential attacks. About half of agents also report they continuously discuss the need for cyber insurance.

Client Concern about Cyberattacks

(Shown % Selected Extremely/Moderately Concerned)

My clients are at least moderately concerned about a potential cyberattack on their business

65%

Of Independent Insurance Agents

Why Businesses Consider or Purchase Cyber Insurance

(Shown % Select)

		Independent Insurance Agents
1	They are well-informed about cyberattacks and are thinking ahead	**60%**
2	They have read articles in the news warning about cyberattacks	**56%**
3	I continuously discuss the need for cyber risk insurance	**51%**
4	They have witnessed similar businesses become victims of cyberattacks	**48%**
5	They were recently the victim of a cyberattack	**47%**
6	They do not trust their employees to avoid a cyberattack	**14%**
7	I'm rarely approached about cyber insurance, so we don't discuss it	**1%**

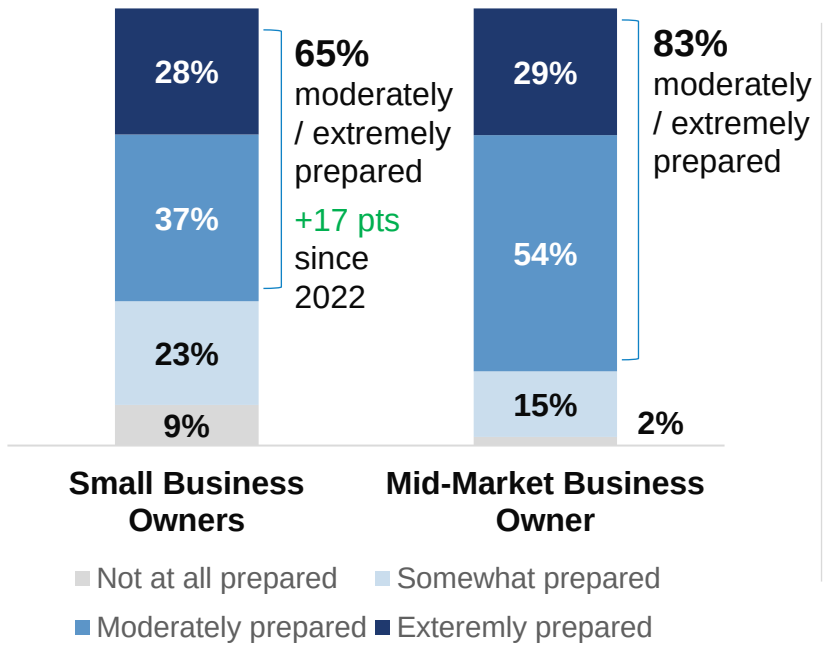
Q1b: In general, how concerned do you think your clients are about potential cyberattacks (on themselves personally or their business)? // Q3. In your experience, why do businesses consider or purchase cyber risk insurance? Please select all that apply. Base: Independent Insurance Agents (n=400)

Mid-Market Business Owners feel more prepared than Small Business Owners for a cyberattack – likely due to proactive cybersecurity training measures

Small and Mid-Market Business Owners are equally as likely to send phishing test emails to employees at least every few months, however Mid-Market Business Owners are more likely to hold formal cybersecurity training on an annual basis compared to Small Business Owners.

Preparedness for Preventing a Cyberattack

(Shown % Select)



Cybersecurity Training Actions Taken

(Shown % Select)

Sending Phishing Test Emails to Employees

Small Business Owners

36% sent at least every few months

Mid-Market Business Owners

35% sent at least every few months

Providing Formal Cybersecurity Training

Small Business Owners

71% offered training at least annually

Mid-Market Business Owners

95% offered training at least annually

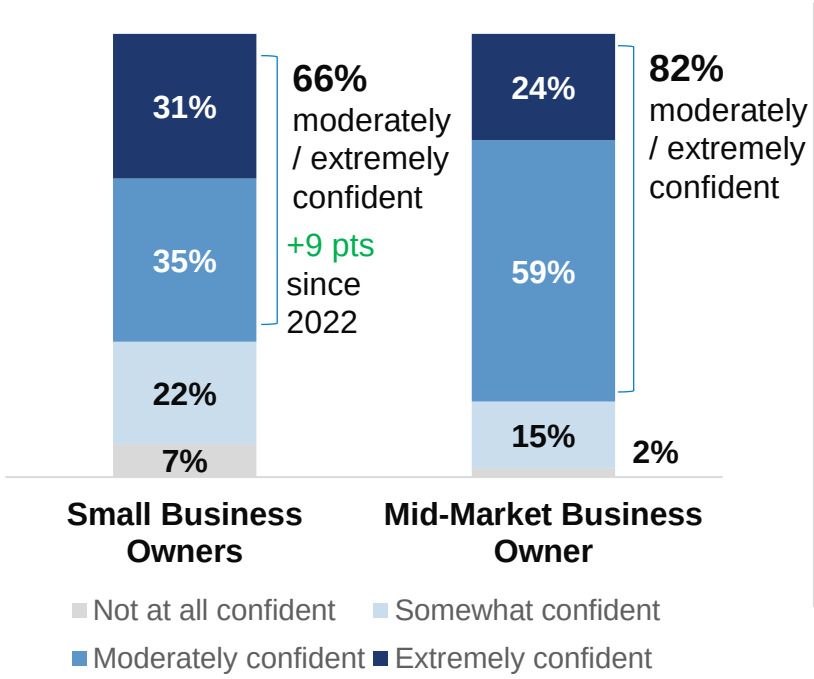
Q4. How often does your business do each of the following regarding employees' cybersecurity roles and responsibilities? // Q12. How prepared is your business in preventing a cyberattack? Base: Small Business Owners (n=400), Mid-Market Business Owners (n=400)

Over 8 in 10 Mid-Market Business Owners are at least moderately confident their business would recover in the event of a cyberattack

However, small business owners are more trusting of their cyber coverage and more confident that their business would retain its reputation after an attack.

Confidence in their Business's Ability to Recover

(Shown % Select)



Response if a Cyberattack Occurred

(Shown % Select T2B Agree)

	Small Business Owners	Mid-Market Business Owners
I trust that my cyber insurance coverage would take care of all my needs	**89%**	**74%**
I'm confident my business would retain its customers/reputation after the attack	**87%**	**77%**
I'm confident that I could recover all my losses from the attack	**76%**	**73%**
I would know where and how to begin the recovery process after the attack	**75%**	**81%**
Right now, I have all the resources I would need to recover any losses from the attack	**74%**	**70%**
I trust that my non-cyber insurance coverages would take care of all my needs	**66%**	**45%**
I haven't given much thought to what I would do if I fell victim to a cyberattack	**66%**	**43%**

Q5. How confident are you in your business's ability to recover from a cyberattack? // Q19. 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=400), Mid-Market Business Owners (n=400)

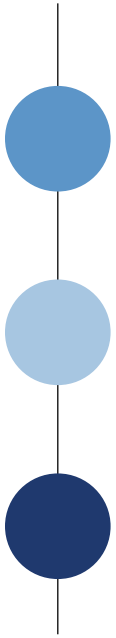
Highlighted text indicates significant difference between groups at the 95% confidence level

Over half of Mid-Market Business Owners have been a victim of a cyberattack

Independent Agents and Mid-Market Business Owners are more likely to have experienced an array of cybersecurity threats while Small Business Owners mostly reported instances of phishing, data breaches, malware, and business email compromise.

Experienced a Cyberattack

(Shown % Select 'Yes')



23% Small Business Owners

+9 pts since 2022

56% Mid-Market Business Owners

+9 pts since 2022

49% Independent Agents

*Low sample, directional only

Cybersecurity Threats Experienced

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

		Small*	Mid-Market	Agents
1	Data breach	27%	40%	50%
2	Ransomware	19%	34%	36%
3	Password attacks	19%	29%	42%
4	Phishing	28%	23%	24%
5	Malware such as viruses and trojan horses	22%	18%	21%
6	Identification theft	20%	13%	20%
7	Malware on Mobile Point of Sale applications	14%	15%	19%
8	Business email compromise	22%	14%	15%
9	Digital tax fraud	13%	13%	19%
10	IoT security breaches	14%	15%	15%
11	Digital unemployment fraud	5%	14%	19%
12	Attacks on the digital supply chain	19%	13%	13%
13	Deepfakes	12%	13%	14%
14	Fake job postings	13%	7%	18%
15	Denial of Service (DoS) attacks	10%	7%	17%
16	Sim card swap	13%	2%	11%

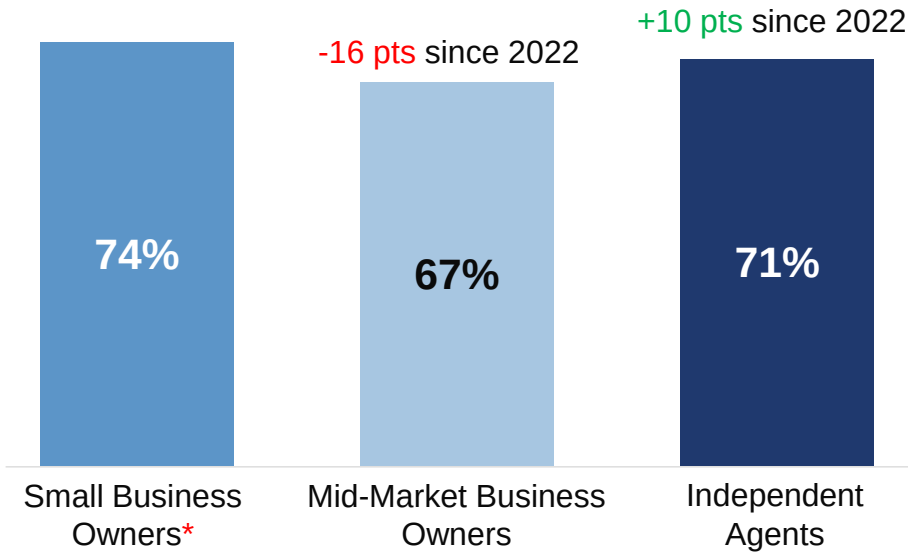
Q7. Has your business / Have you personally ever been a victim of a cyberattack? // Q8. Which, if any, of the following cybersecurity threats has your business / have you experienced? Please select all that apply. Base: Small Business Owners (n=400), Mid-Market Business Owners (n=400), Independent Insurance Agents (n=400), Small Business Owners who have experienced a cyberattack (n=93), Mid-Market Business Owners who have experienced a cyberattack (n=224), and Independent Agents who have experienced a cyberattack (n=195)*

Business Owners and Agents overwhelmingly agree cyberattacks have jeopardized their business and negatively impacted customer trust

Of those who have experienced a cyberattack, nearly all respondents across both business owners and agents report the attack had a negative impact on customer trust or reputation.

Cyberattack Impacted or Jeopardized Business Finances

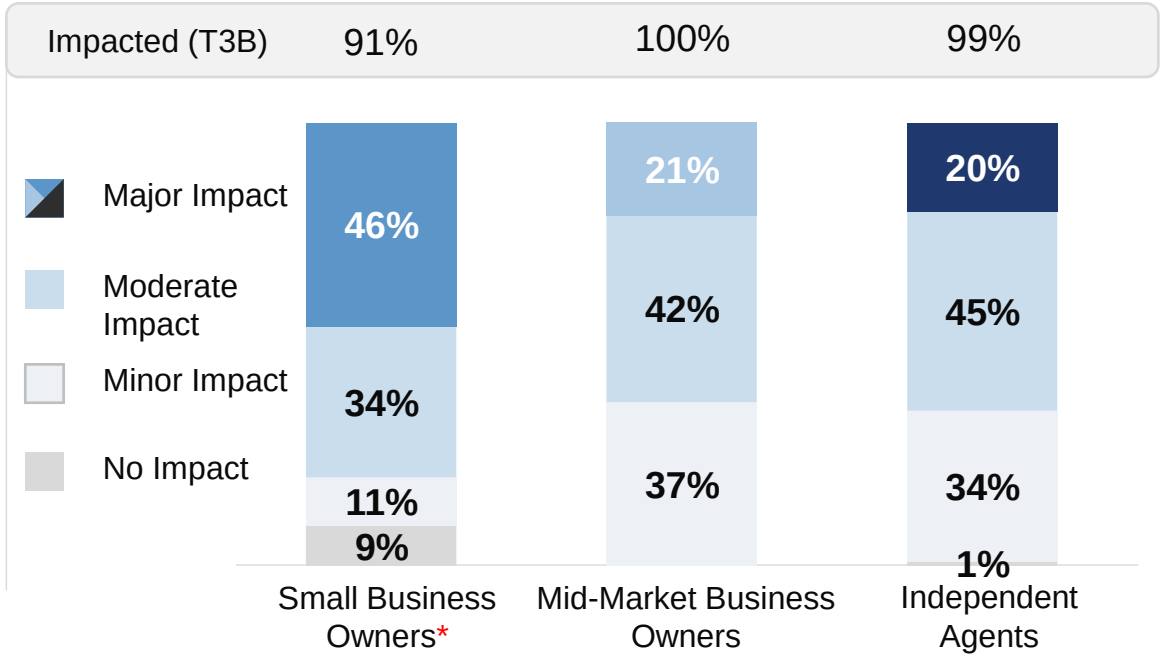
(Shown % Select 'Yes')



*Low sample, directional only

Cyberattack Negatively Impacted Customer Trust in Business

(Shown % Select)



Q9a. Did the cyberattack impact or jeopardize your business / your personal finances? // Q9b. Did the cyberattack negatively impact customer trust or reputation in your business? Base: Small Business Owners who have experienced a cyberattack (n=93), Mid-Market Business Owners who have experienced a cyberattack (n=224), and Independent Agents who have experienced a cyberattack (n=195)*

Email Compromise and Phishing are the main sources of business cyberattacks

Of those who have experienced a cyberattack, small business owners are most likely to have had cyber insurance when the attack occurred.

How Cyberattack Infiltrated Business

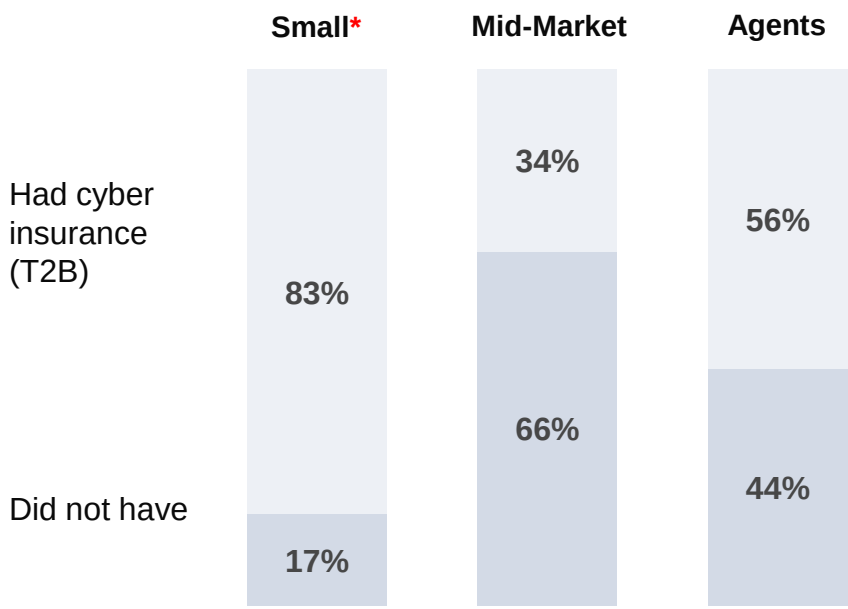
(Shown % Select)

		Small*	Mid-Market	Agents
1	Email compromise	12%	20%	15%
2	Phishing	17%	13%	18%
3	Accidental data loss	9%	15%	10%
4	Compromised credentials	9%	13%	12%
5	Malicious insiders	4%	13%	9%
6	System error	11%	6%	12%
7	Vulnerabilities from a vendor or third-party software	5%	5%	7%
8	Physical security compromise	13%	5%	3%
9	Lost or stolen devices	10%	3%	5%
10	Social engineering, impersonation, or other attempts to manipulate employees	5%	4%	5%
11	Cloud misconfiguration	4%	3%	5%

*Low sample, directional only

Cyber Insurance Status at Time of Cyberattack

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



Q10. Which of the following best describes your situation when the cyberattack occurred? // Q10a. Based on what you currently know, how did the cyberattack infiltrate your business? Base: Small Business Owners who have experienced a cyberattack (n=93), Mid-Market Business Owners who have experienced a cyberattack (n=224), and Independent Agents who have experienced a cyberattack (n=195)*

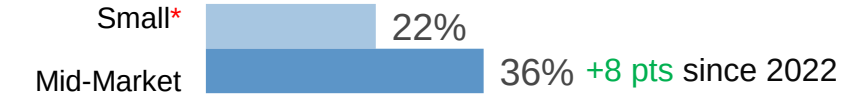
Most Business Owners say they knew exactly what to do in response to a previous cyberattack, however Mid-Market owners are taking more steps to prevent future attacks

Response to Cyberattack

(Shown % Select)

Yes, my business knew exactly what to do

My business knew where to start, but had to do some research



My business did not know what to do, and didn't know where to start

*Low sample, directional only

Steps Taken to Prevent Future Cyberattacks

(Shown % Select)

		Small	Mid-Market
1	Using only secured Wi-Fi connection	**41%**	**42%**
2	Updating our cybersecurity software	**41%**	**46%**
3	Backing up data following stricter protocols	**36%**	**43%**
4	Requiring multi-factor authentication	**34%**	**45%**
5	Blocking unsecured websites and social media	**33%**	**32%**
6	Adding regular password update requirements	**32%**	**45%**
7	Installing a new cybersecurity software	**29%**	**35%**
8	Adding encryption features	**26%**	**55%**
9	Providing additional training to employees	**25%**	**44%**
10	Requiring admin rights	**24%**	**32%**
11	Requiring VPN when on Wi-Fi outside of workplace	**23%**	**32%**
12	Purchasing cyber insurance	**21%**	**38%**
13	Developing an incident response plan	**19%**	**44%**
14	Asking my insurance agent for advice and information about insurance	**18%**	**20%**
15	Patching more frequently	**16%**	**31%**
16	Appointing a security expert	**15%**	**43%**
17	Increasing my cyber insurance coverage amounts	**13%**	**21%**

Q11. Did your business know what to do once you identified the attack? Base: Small Business Owners who have experienced a cyberattack (n=93), Mid-Market Business Owners who have experienced a cyberattack (n=224), and Independent Agents who have experienced a cyberattack (n=195) // Q12a_2024. 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=400), Mid-Market Business Owners (n=400)*

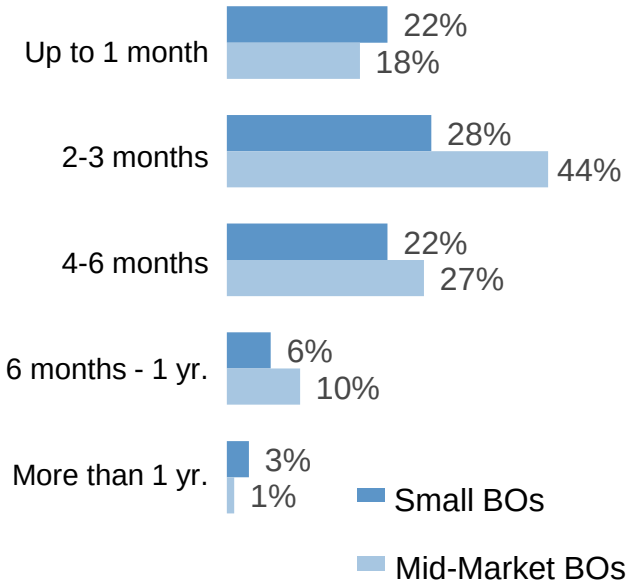
Highlighted text indicates significant difference between groups at the 95% confidence level

1 in 5 Small Business Owners believe recovering from a cyberattack would cost $5,000 or more

However, MMBOs are more likely to think recovering costs will be difficult compared to Small Business Owners.

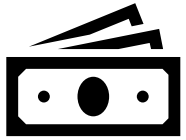
Length of Time to Recover

(Shown % Select)



Anticipated Cost of Average Cyberattack

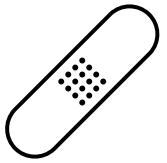
(Shown % Select)



	Small Business Owners	Mid-Market Business Owners
Under $100	3%	1%
$100-$499	7%	4%
$500-$749	9%	14%
$750-$999	11%	23%
$1,000-$1,999	18%	23%
$2,000-$2,999	14%	14%
$3,000-$3,999	11%	14%
$4,000-$4,999	8%	5%
$5,000+	21%	4%

Ease of Recovering Costs

(Shown Top 2 Box Easy and Bottom 2 Box Difficult)



Easy (T2B)

Small Business Owners: 51%
+16 pts since 2022

Mid-Market Business Owners: 49%
-14 pts since 2022

Difficult (B2B)

Small Business Owners: 39%

Mid-Market Business Owners: 50%

Q13. 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. // Q14a. 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? // Q14b. 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=400), Mid-Market Business Owners (n=400)

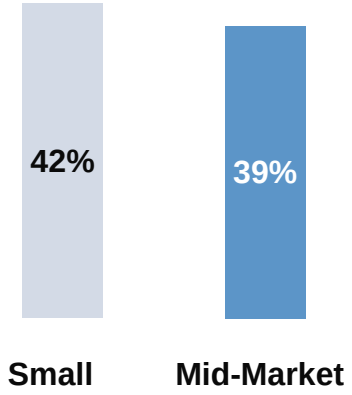
Highlighted text indicates significant difference between groups at the 95% confidence level

Only 2 in 5 Business Owners currently have cyber insurance; Those who do not are confident in their current cybersecurity software or feel coverage is too costly

However, the majority of business owners say they would be interested in offerings like insurers working directly with security service providers to manage claims and discounts based on cyber defense preparation.

Cyber Insurance Ownership

(Shown % Select)



Why Business Don't Buy Cyber Insurance

(Shown % Select)

		Small	Mid-Market
1	I feel that my current cybersecurity software provides sufficient protection	24%	51%
2	Cyber insurance is too costly	32%	29%
3	I don't know enough about cyber insurance	37%	17%
4	My insurance agent has never recommended it to me	24%	24%
5	I have trained my employees sufficiently to protect my business from a cyberattack	13%	33%
6	I did not know cyber insurance was available	27%	8%
7	I do not feel that my business will be affected by a cyberattack	16%	17%
8	I don't feel cyber insurance is worth the money	12%	19%
9	I have outsourced my cybersecurity function, so I am not worried	8%	10%
10	I had cyber insurance in the past and I didn't find it useful	6%	7%

Interest in Cyber Insurance Offerings

(Shown % Select, T2B 'Interested')

A system where the insurer directly works with a security service provider to manage a claim	78%	85%
Discount offers based on a track record of better cyber defense preparation	78%	84%
Cyber defense preparation programs and resources	77%	83%
Cyberattack defense simulation exercises	74%	79%

Q14. Does your business purchase cyber insurance? // Q3a. As a business owner, how interested would you be in an insurer offering the following to better defend your enterprise against cyberattacks? Base: Small Business Owners (n=400), Mid-Market Business Owners (n=400) // Q15. Why don't you currently have cyber insurance? Base: Small Business Owners without cyber risk insurance (n=220), and Mid-Market Business Owners without cyber risk insurance (n=246)

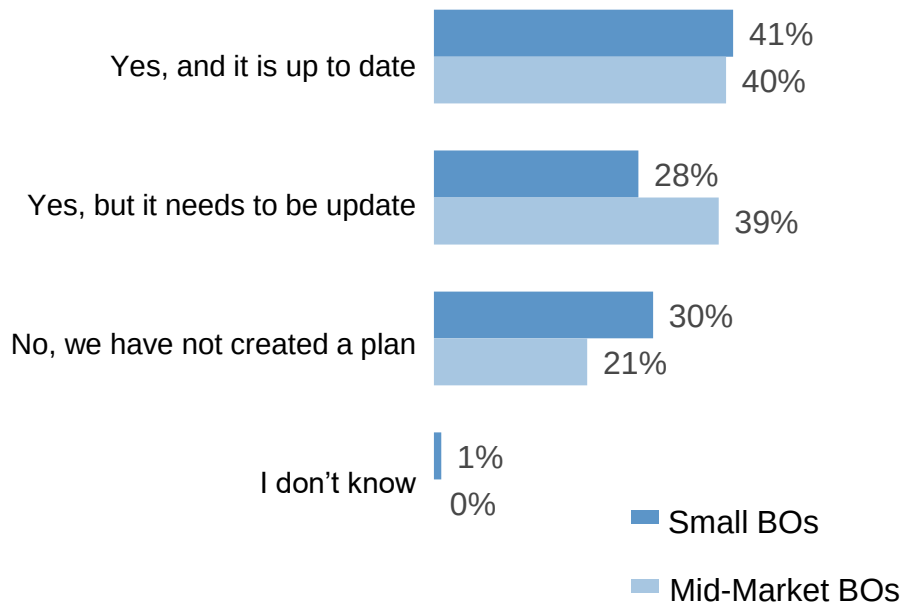
Highlighted text indicates significant difference between groups at the 95% confidence level

Most Businesses have created an incident response plan in the event of a cyberattack or data breach – although many owners report their plans need to be updated

Mid-Market Business Owners are more likely to say their company's incident response plan includes instructions for Incident reporting procedures to government regulatory agencies, consultations with legal counsel, and table-top training exercises.

Incident Response Plan in Place

(Shown % Select)



Incident Response Plan Instructions in Place

(Shown % Select)

	Small Business Owners	Mid-Market Business Owners
Proactive monitoring and reporting	75%	78%
Incident reporting procedures to government regulatory agencies	68%	82%
Consultations with legal counsel	61%	81%
Table-top training exercises	57%	68%

Q15a_2024. Has your company created an incident response plan in the event of a cyberattack or data breach? Q15b_2024. Does your company's incident response plan include instructions for each of the following? Base: Small Business Owners (n=400), Mid-Market Business Owners (n=400)

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

Most Small and Mid-Market Business Owners are interested in a range of cyber protection resources or products – and interest has increased across almost all resources since 2022

Interest in Cyberattack Protection Resources or Products

(Shown Top 2 Box Interested)

	Small Business Owners		Mid-Market Business Owners	
Identity Recovery protection*	**89%**	+14 pts since 2022	**94%**	+7 pts since 2022
Computer Fraud protection*	**88%**	+13 pts since 2022	**95%**	
Computer Attack protection*	**87%**	+14 pts since 2022	**93%**	+5 pts since 2022
Data compromise protection*	**86%**	+19 pts since 2022	**96%**	+8 pts since 2022
Network Security Liability protection*	**86%**	+23 pts since 2022	**94%**	
Misdirected Payment Fraud protection*	**85%**	+23 pts since 2022	**91%**	+5 pts since 2022
Cyber Extortion protection*	**79%**	+20 pts since 2022	**94%**	+7 pts since 2022
Electronic Media Liability protection*	**79%**	+25 pts since 2022	**90%**	+5 pts since 2022

Q20a. How interested would you be in purchasing each of the following resources or products to protect against cyberattacks? Base: Small Business Owners (n=400), Mid-Market Business Owners (n=400)

** Definition available in notes section*

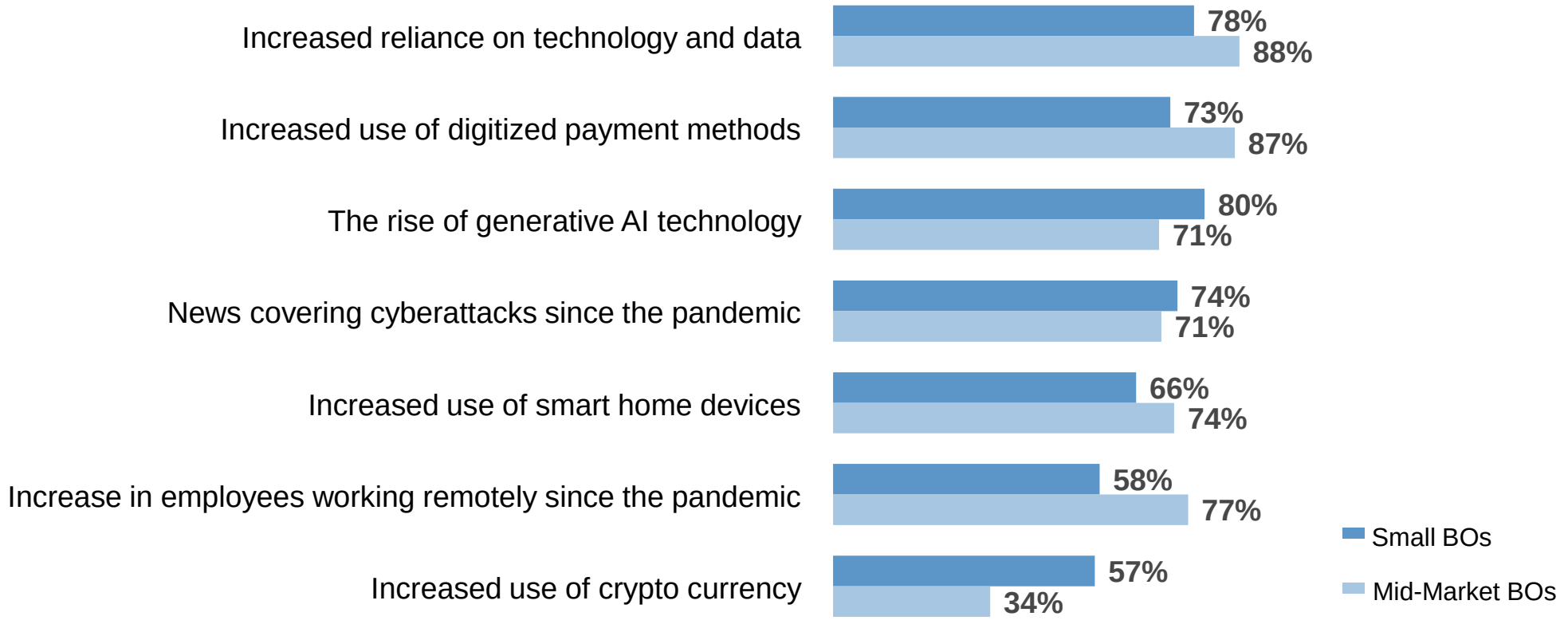
Highlighted text indicates significant difference between groups at the 95% confidence level

Increased reliance on technology and digital payment methods have made Business Owners more likely to consider purchasing cyber insurance

8 in 10 Small Business Owners say the rise of generative AI has made them more likely to purchase coverage.

Impact on Likelihood to Purchase Cyber Insurance Coverage

(Shown Top 2 Box More Likely)



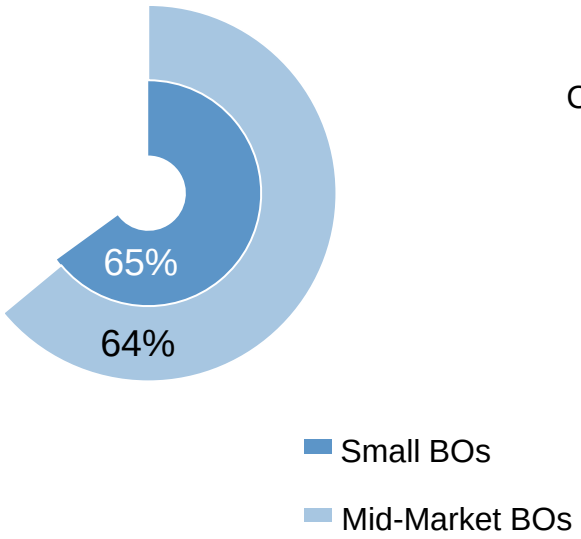
Q33a. Have each of the following events made you more or less likely to purchase cybers risk insurance or expand your current level of cyber insurance coverage? Base: Small Business Owners (n=400), Mid-Market Business Owners (n=400),

Despite many businesses having cybersecurity roles employed like IT departments or risk managers, nearly 2 in 3 report they would hire or outsource in the event of a cyberattack

Additionally, most businesses dedicate 1 to 30 percent of their business' overall IT budget to cybersecurity needs like insurance or third-party vendors.

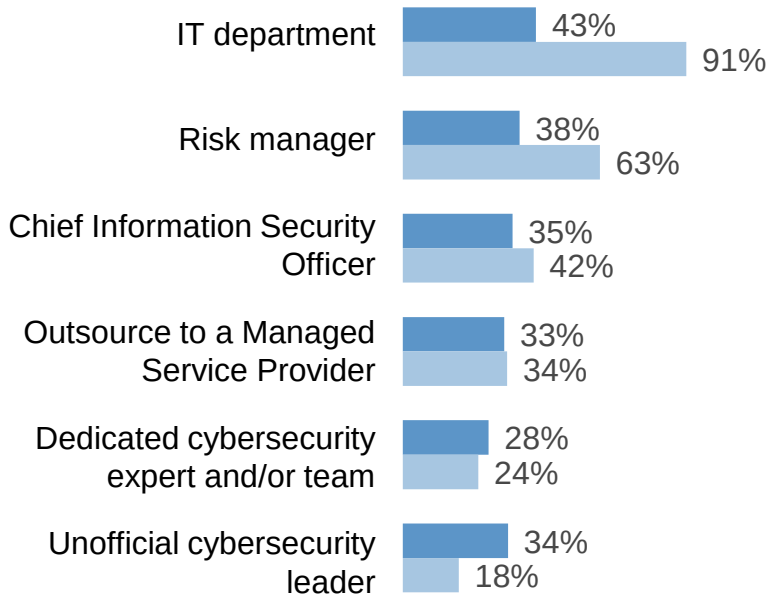
Would Hire / Outsource if Business Fell Victim to a Cyberattack

(Shown % Select, 'Yes')



Cybersecurity Roles Employed

(Shown % Select)



% of Overall IT Budget Allocated To Cybersecurity Needs

(Shown % Select)

	Small Business Owners	Mid-Market Business Owners
0%	10%	2%
1% - 9%	23%	23%
10% - 19%	20%	47%
20% - 29%	15%	22%
30% - 39%	14%	4%
40% - 49%	5%	2%
50% - 59%	5%	0%
60% - 69%	2%	0%
70% - 79%	5%	0%
80% - 89%	2%	0%
90% - 100%	1%	0%

Q18. If your business were to fall victim to a cyberattack, would you hire or outsource someone to lead the recovery process for you? // Q34. Does your business currently employ the following roles relating to cybersecurity? // Q35. 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=400), Mid-Market Business Owners (n=400)

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

Over 7 in 10 Business Owners say their business is fully compliant with data protection and sharing regulations – and keeps up to date on the latest regulations

Additionally, considering the recent CrowdStrike software update that caused a global outage of many Microsoft Windows-run machines, most Business Owners, especially Mid-Market, are still confident in cybersecurity firms to provide software that will protect their data.

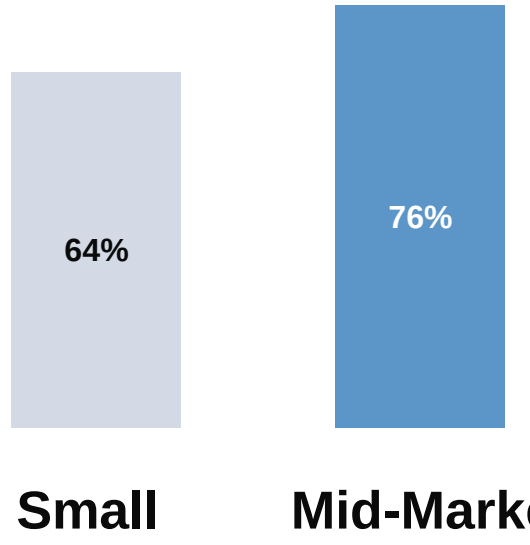
Data Protection and Regulatory Compliance

(Shown % Select T2B 'Agree')

	Small	Mid-Market
My business is fully compliant with data protection and sharing regulations in the state(s) where it operates	86%	71%
My business keeps up to date on the latest government data sharing and data protection regulations	78%	78%
If my business had a data breach I would know how to respond based on the regulatory guidelines	75%	79%
My business has a good understanding of how data protection regulations can vary between states	72%	72%

Confidence in Cybersecurity Firms to Provide Software that Will Protect Data – Considering Recent CrowdStrike Incident

(Shown % Select, T2B 'Confident')



Q14c_2024. How much do you agree or disagree with the following statements? // Q14d_2024. As you may have seen, read, heard, or been impacted by, a recent faulty CrowdStrike security software update caused a global outage of many Microsoft Windows-run machines, leading to numerous global systems being affected such as airlines, banks, and businesses. With this in mind, how confident are you in cybersecurity firms to provide software that will protect your data? Base: Small Business Owners (n=400), Mid-Market Business Owners (n=400)

Over 2 in 3 Independent Agents report often discussing cybersecurity threats with their clients; Almost the same provide resources to employees to counsel customers on cyberattacks and cyber insurance solutions

Data Protection and Regulatory Compliance
(Shown % Select T2B 'Agree')

I have a good understanding of how data protection regulations can vary between states	90%
I keep up to date on the latest government data sharing and data protection regulations in the state(s) where my clients operate	84%

Frequency of Client Counsel About Data Protection / Sharing Regulations
(Shown Top 2 Box 'Often/Always')

70%

Of Independent Agents counsel or provide information to their clients about ways to stay compliant with data protection and data sharing regulations in the state(s) where they operate often or always

Q24_2024. How much do you agree or disagree with the following statements? // Q25_2024. How often do you counsel or provide information to your clients about ways to stay compliant with data protection and data sharing regulations in the state(s) where they operate? Base: Independent Insurance Agents (n=400)

Over 2 in 3 Independent Agents report often discussing cybersecurity threats with their clients; Almost the same provide resources to employees to counsel customers on cyberattacks and cyber insurance solutions

Frequency of Conversations With Clients About Protecting Against Potential Cybersecurity Threats
(Shown Top 2 Box 'Often/Always')

69%

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

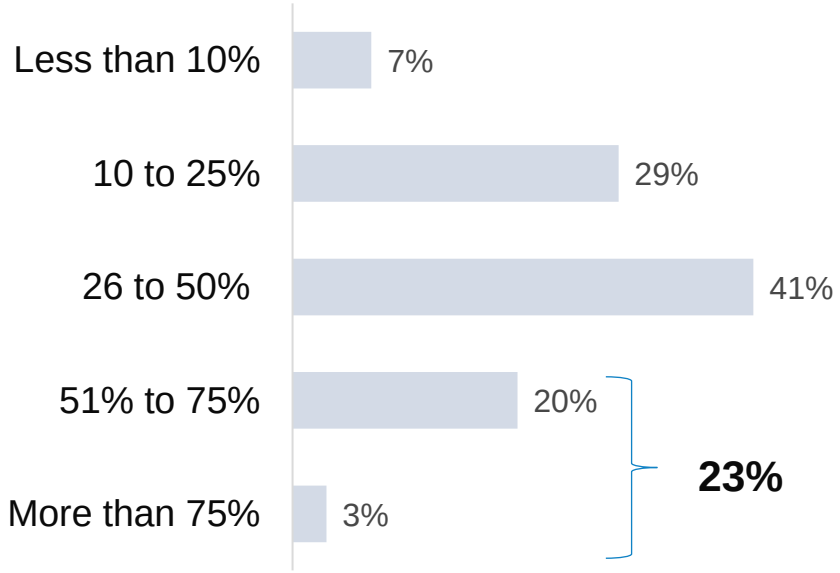
Level of Resources Provided to Employees to Counsel Customers on Cyberattacks and Cyber Insurance Solutions
(Shown % Select)

No resources are provided	10%
Few resources are provided	23%
Some resources are provided	48%
Plenty of resources are provided	19%
Some + Plenty NET	**67%**

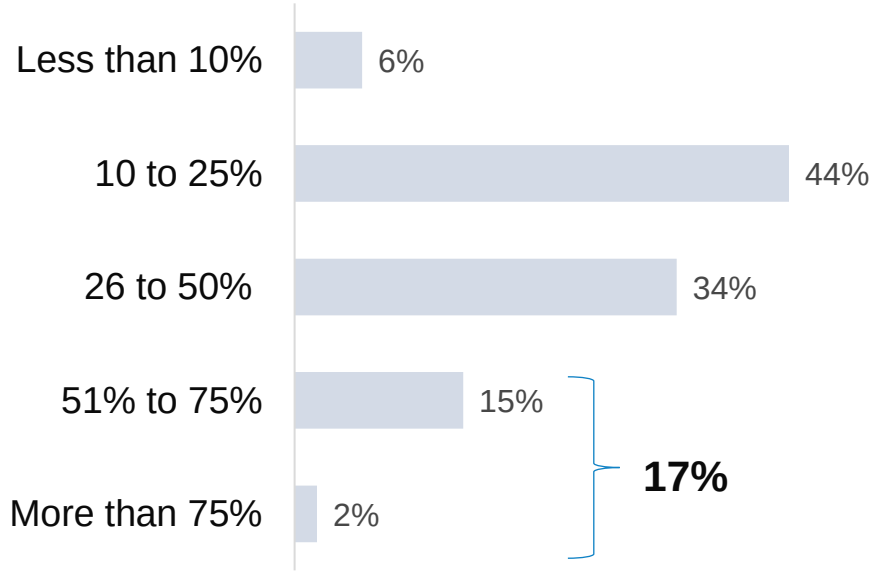
Q21. Now thinking about your clients, how often do you have conversations with clients about protecting themselves/their business from potential cybersecurity threats? // Q22a. In your opinion, how prepared is the average business owner client for a potential cybersecurity attack? // Q23A. Which of the 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=400)

Most Agents report that less than half of their commercial clients have created an incident response plan or keep their cyber coverage level up to date with the evolving landscape

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



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



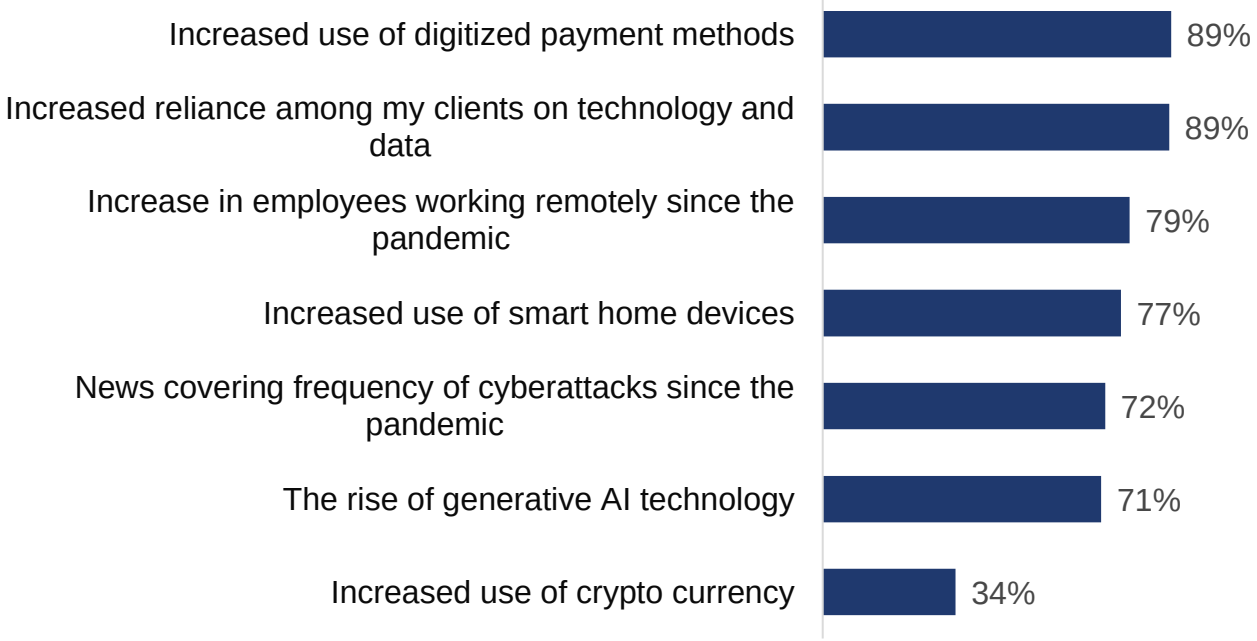
Q26_2024. About how many of your commercial clients have created an incident response plan in the event of a cyberattack or data breach? // Q27_2024. About how many of your commercial clients keep their cyber coverage level up to date with the evolving landscape? Base: Independent Insurance Agents (n=400)

Increased client reliance on technology and digital payment methods has prompted Agents to encourage clients to purchase or increase their cyber coverage

7 in 10 Agents also say the rise of generative AI technology has been a factor – with over a third observing an increase in scams or fraud attempts that use generative ai in the past 12 months.

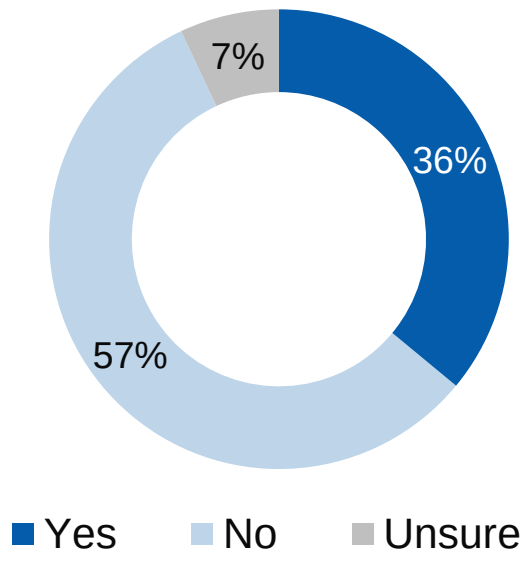
Impact on Likelihood of Encouraging Clients to Purchase or Increase Cyber Insurance Coverage

(Shown Top 2 Box Likely)



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

(Shown % Select)



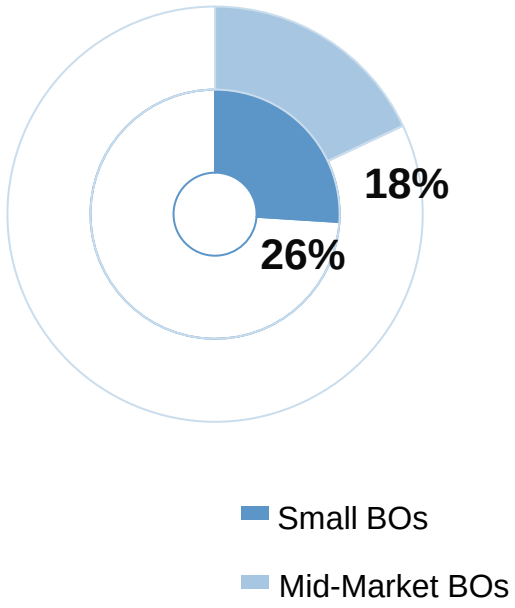
Q28_2024. Have you observed an increase in claims related to scams or fraud attempts that use generative AI technology in the past 12 months? // Q33B. Have each of the following events made you more or less likely to encourage your clients to purchase or increase their level of cyber insurance coverage? Base: Independent Insurance Agents (n=400)

More so than Mid-Market Business Owners, about a quarter of Small Business Owners report their company was targeted by a Generative AI fraud attempt within the past year

Of those targeted by a Gen AI fraud attempt, most describe the attack as an email impersonation of the business owner or another senior employee.

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

(Shown % Select, 'Yes')



Description of Generative AI Scam / Fraud Attempt

(Shown Top 2 Box ' Agree', Among those targeted by a Gen AI fraud attempt)

	Small Business Owners	Mid-Market Business Owners*
Email impersonation of the business owner or another senior employee	**55%**	**53%**
Phishing using an AI chatbot	**14%**	**32%**
Deepfake audio or video of the business owner or another senior employee	**26%**	**3%**
Fake candidate for a job posting	**5%**	**12%**

*Low sample, directional only

Q30_2024. 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=400), Mid-Market Business Owners (n=400) // Q31_2024. 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=104), Mid-Market Business Owners who have been targeted by a Gen AI fraud attempt (n=73)*

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

Business Owners and Agents alike are highly concerned about the threat of Generative AI fraud attempts – and are in need of more information and resources to better protect their businesses from these attacks

Additionally, half of Small Business Owners have personally been fooled by a deepfake image or video in the past 12 months.

Perceptions of Generative AI Scams / Fraud Attempts

(Shown % Select T2B Agree)

	Small Business Owners	Mid-Market Business Owners	Independent Agents
These attacks have become increasingly sophisticated over the past 12 months	**90%**	**93%**	**91%**
I need more information and resources about how best to protect my business from these attacks	**90%**	**88%**	**87%**
I'm very concerned about the threat of these attacks to my business	**81%**	**87%**	**87%**
I have personally been fooled by a deepfake image or video in the past 12 months	**52%**	**16%**	**15%**

Q31A_2024. 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=400), Mid-Market Business Owners (n=400), Independent Insurance Agents (n=400)