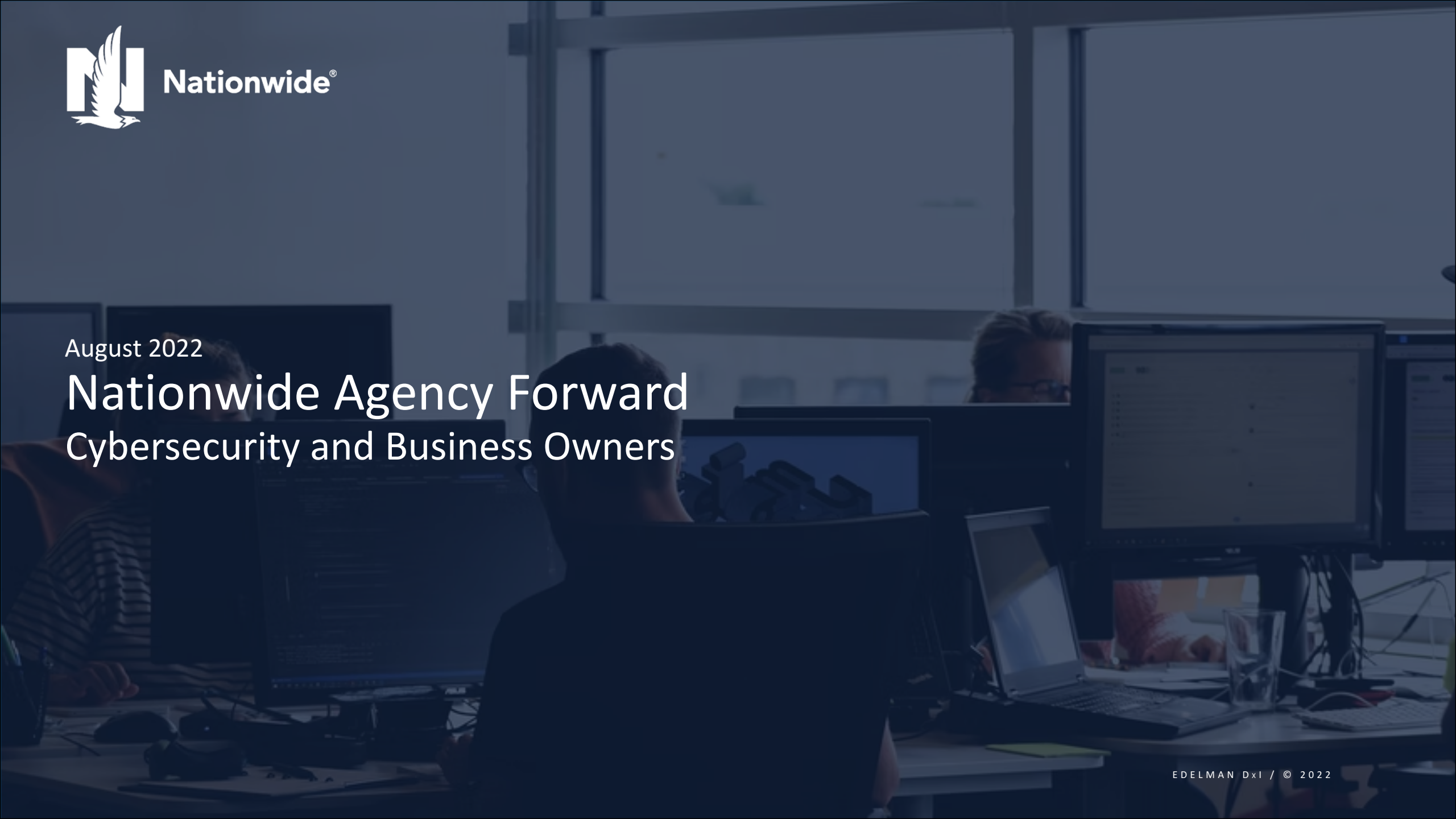


August 2022

# Nationwide Agency Forward

## Cybersecurity and Business Owners

# METHODOLOGY

| Audience | Sample Size | Methodology | Timing |
|---|---|---|---|
| Independent Insurance Agents<br>• Identify as an independent insurance agent<br>• Mix of principals, producers, and customer service reps<br>• Includes oversample of 100 agents who primarily sell commercial lines insurance (defined as >50% of sales from commercial lines) | n=430 | 20-minute Online Survey | Survey fielded July 27th – August 9th, 2022 |
| Small Business Owners<br>• Business owner of a company with 1-50 employees and less than $10M in revenue | n=400 | | |
| Mid-Market Business Owners<br>• Business owner of a company with either 51-500 employees or $10M-$500M in revenue or 20+ fleet vehicles | n=401 | | |

# KEY FINDINGS: Commercial Lines

## 1 Cybersecurity concern is up since 2020, with Mid-Market Business Owners significantly more concerned than Small Business Owners

Two-thirds of business owners are concerned about cyberattacks, including 79% of Mid-Market Business Owners (a 12-point increase since 2020) and 53% of Small Business Owners (up 15 points since 2020). Concern has risen due to increased frequency of attacks, perceived vulnerabilities in the digital supply chain, and the rise of remote working and other pandemic-era innovations that have opened new avenues for attacks.

## 2 Mid-market businesses are much more prepared to prevent cyberattacks than small businesses

83% of Mid-Market Business Owners feel prepared to prevent a cyberattack, compared to only 48% of Small Business Owners. This confidence may be because 94% of Mid-Market Business Owners provide their workers annual cybersecurity training and nearly 3 in 4 (71%) have cyber coverage. Just 28% of Small Business Owners report owning cyber insurance.

## 3 Small businesses lack knowledge of cyber best practices and insurance options

The top reasons Small Business Owners don't purchase cyber insurance are not knowing enough about it (40%) and not knowing cyber insurance was available to them (32%).

## 4 Both Small and Mid-Market Business Owners show strong interest in a range of cyber solutions and products

Business owners say an increased reliance on technology and data in businesses, adoption of digital payment methods and increased coverage of cyber attacks in the news cycle have made them more likely to consider purchasing cyber insurance. And when informed about cyber protection resources and products, both Small and Mid-Market Owners express strong interest – particularly in computer fraud, identity recovery, and computer attack protection.

# Detailed Findings

# Two-thirds of Business Owners are concerned about cyberattacks on their businesses, including almost 8 in 10 Mid-Market Business Owners

Top reasons for concern include the recent increase in cyberattacks, digital supply chain vulnerabilities, and the proliferation of new avenues for system breaches since the pandemic began. Additionally, 3-in-10 Small Business Owners point to a lack of cyber insurance and sufficient IT measures to prevent an attack.

## Concern about Cyberattacks

*(Shown % Selected Extremely/Moderately Concerned)*

At least moderately concerned about a potential cyberattack on their business

**53%** +15% since June 2020

Of Small business owners

**79%** +12% since June 2020

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 | 67% | 41% |
| 2 | With a digital supply chain, there are more devices than ever vulnerable to cyberattacks | 37% | 36% |
| 3 | The pandemic has been a catalyst for new ways to breach our system (for example through remote working, digitized point of sales systems, etc.) | 37% | 41% |
| 4 | I'm concerned there may be increased cyberattacks stemming from the war in Ukraine | 32% | 32% |
| 5 | There are not enough IT measures in place to effectively prevent cyberattacks | 30% | 20% |
| 6 | I do not have cyber risk insurance | 28% | 16% |
| 7 | I do not trust that my employees are diligent enough to fend off all cyberattacks | 19% | 15% |
| 8 | It is very difficult to find cybersecurity experts to protect my business | 18% | 31% |
| 9 | I don't think I understand enough about cybersecurity to protect my business | 18% | 21% |
| 10 | Maintenance of our IT systems is not conducted regularly enough | 18% | 33% |
| 11 | The data our business collects has not been properly examined for cyberthreats | 15% | 24% |

*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=401)*

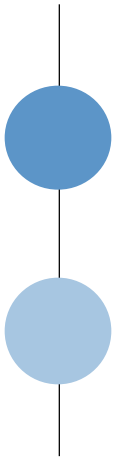
Highlighted text indicates significant difference between groups at the 95% confidence level

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

Mid-Market Business Owners were more likely to have experienced an array of cybersecurity threats while Small Business Owners mostly reported instances of phishing, password attacks, ransomware, malware, and business email compromise.

## Experienced a Cyberattack

*(Shown % Select 'Yes')*



14% Small Business Owners

47% Mid-Market Business Owners

*Low sample, directional only

## Cybersecurity Threats Experienced

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

| | | Small* | Mid-Market |
|---|---|---|---|
| 1 | Phishing | 27% | 27% |
| 2 | Password attacks | 30% | 28% |
| 3 | Data breach | 18% | 30% |
| 4 | Business Email Compromise | 27% | 33% |
| 5 | Ransomware | 29% | 22% |
| 6 | Malware such as viruses and trojan horses | 32% | 28% |
| 7 | Identification theft | 21% | 27% |
| 8 | Malware on Mobile Point of Sale applications | 16% | 30% |
| 9 | IoT or Internet of Things security breaches | 9% | 29% |
| 10 | Denial of Service (DoS) attacks | 14% | 22% |
| 11 | Digital unemployment fraud | 11% | 20% |
| 12 | Attacks on the digital supply chain | 9% | 25% |
| 13 | Deepfakes | 7% | 16% |
| 14 | Digital tax fraud | 4% | 19% |

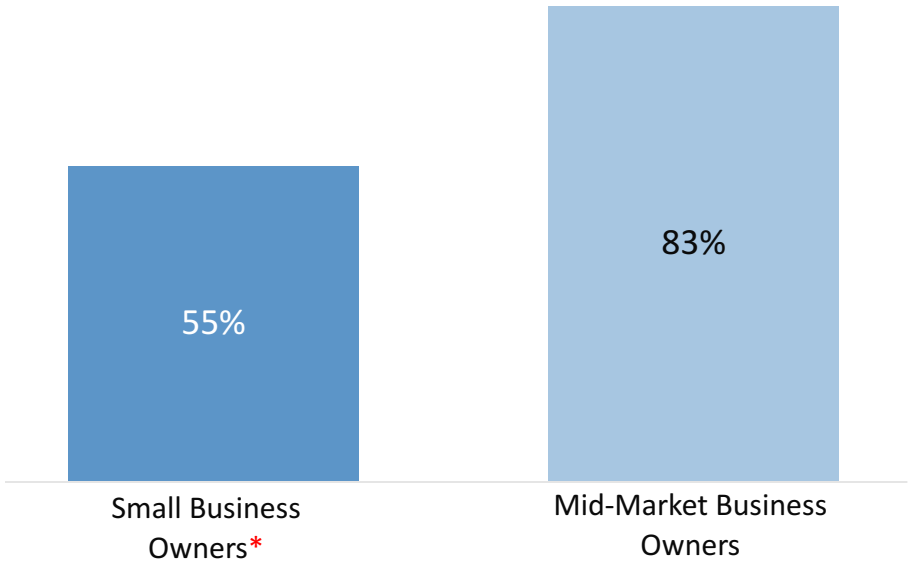
*Q7. Has your business / Have you personally ever been a victim of a cyberattack? // Q8. Which, if any, of the following cybersecurity threats has your business / have you experienced? Please select all that apply. Base: Small Business Owners (n=400), Mid-Market Business Owners (n=401), Small Business Owners who have experienced a cyberattack (n=56*), Mid-Market Business Owners who have experienced a cyberattack (n=187).*

# Mid-Market Business Owners overwhelmingly agree cyberattacks have jeopardized their business and negatively impacted customer trust

In contrast, just over half of Small Business Owners said the same.

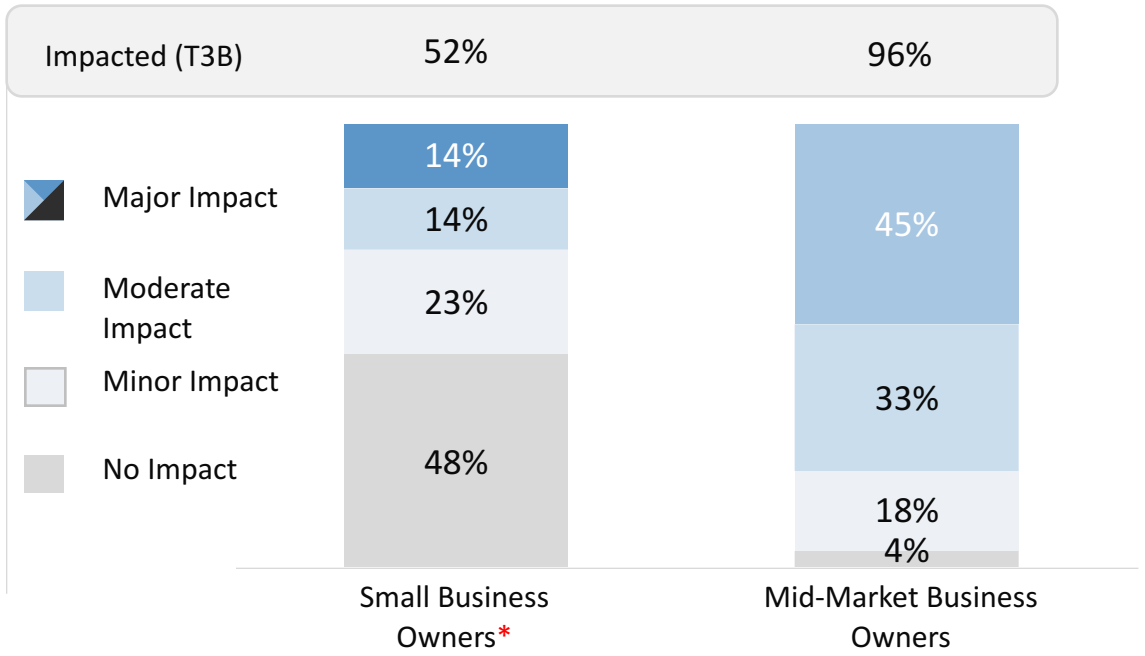
Cyberattack Impacted or Jeopardized Business Finances

*(Shown % Select 'Yes')*




Cyberattack Negatively Impacted Customer Trust in Business

*(Shown % Select )*




*Low sample, directional only

*Q9a. Did the cyberattack impact or jeopardize your business / your personal finances? // Q10. Which of the following best describes your situation when the cyberattack occurred? Base: Small Business Owners (n=56*), Mid-Market Business Owners (n=187).*

# Mid-Market Business Owners were more likely to know exactly what to do in response to a previous cyberattack and to subsequently invest further in cyber insurance coverage

## Response to Cyberattack

*(Shown % Select)*


*Low sample, directional only

## Steps Taken Since Experiencing Cyberattack

*(Shown % Select )*

| | | Small* | Mid-Market |
|---|---|---|---|
| 1 | Backed up data following stricter protocols | 41% | 29% |
| 2 | Provided additional training to employees | 38% | 30% |
| 3 | Updated our cybersecurity software | 38% | 30% |
| 4 | Installed a new cybersecurity software | 36% | 28% |
| 5 | Blocked unsecured websites and social media | 36% | 21% |
| 6 | Used only secured Wi-Fi connection | 34% | 30% |
| 7 | Required multi-factor authentication | 34% | 29% |
| 8 | Added regular password update requirements | 34% | 23% |
| 9 | Added encryption features | 30% | 27% |
| 10 | Required admin rights | 27% | 25% |
| 11 | Patched more frequently | 16% | 22% |
| 12 | Purchased cyber risk insurance | 14% | 22% |
| 13 | Asked my insurance agent for advice and information about insurance | 13% | 20% |
| 14 | Developed an incident response plan | 11% | 28% |
| 15 | Increased my cyber risk insurance coverage amounts | 11% | 26% |
| 16 | Appointed a security expert | 9% | 30% |

*Q11. Did your business know what to do once you identified the attack? // Q11a. Which, if any, of the following steps have you taken since experiencing a cyberattack to prevent future attacks? Please select all that apply. Base: Small Business Owners (n=56*), Mid-Market Business Owners (n=187)*

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

# Small Business Owners predict spending less time and lower costs recovering from a cyberattack compared to Mid-Market Business Owners

However, they are significantly more likely to think recovering costs will be difficult compared to Mid-Market 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 | 7% | 1% |
| $100-$499 | 15% | 5% |
| $500-$749 | 9% | 5% |
| $750-$999 | 9% | 12% |
| $1,000-$1,999 | 22% | 24% |
| $2,000-$2,999 | 10% | 22% |
| $3,000-$3,999 | 6% | 15% |
| $4,000-$4,999 | 5% | 5% |
| $5,000+ | 19% | 10% |

## Ease of Recovering Costs

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

Easy (T2B)

Small Business Owners: 35%

Mid-Market Business Owners: 63%

Difficult (B2B)

Small Business Owners: 52%

Mid-Market Business Owners: 34%

*Q12. Thinking about if your business/you personally 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. // Q13a. Thinking about if your business/you personally were to fall victim to a cyberattack in the future, how easy would it be to cover the costs of recovery? // Q13b. 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*

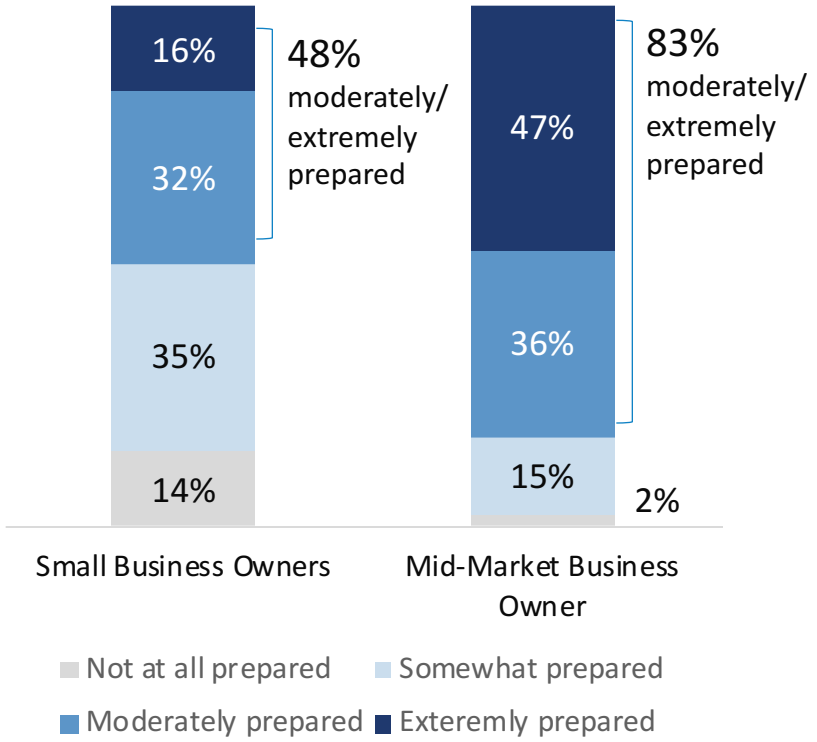
Highlighted text indicates significant difference between groups at the 95% confidence level

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

Mid-Market Business Owners are over twice as likely to send phishing test emails to employees at least every few months and nearly twice as 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

24% sent at least every few months

Mid-Market Business Owners

65% sent at least every few months

### *Providing Formal Cybersecurity Training*

Small Business Owners

56% offered training at least annually

Mid-Market Business Owners

94% offered training at least annually

*Q4. How often does your business do each of the following regarding employees' cybersecurity roles and responsibilities? // Q17. How prepared is your business in preventing a cyberattack? Base: Small Business Owners (n=400), Mid-Market Business Owners (n=401)*

# Half of Independent Agents report often discussing cybersecurity threats with their clients, almost the same share that believe their commercial clients are prepared to prevent one

**49%**

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

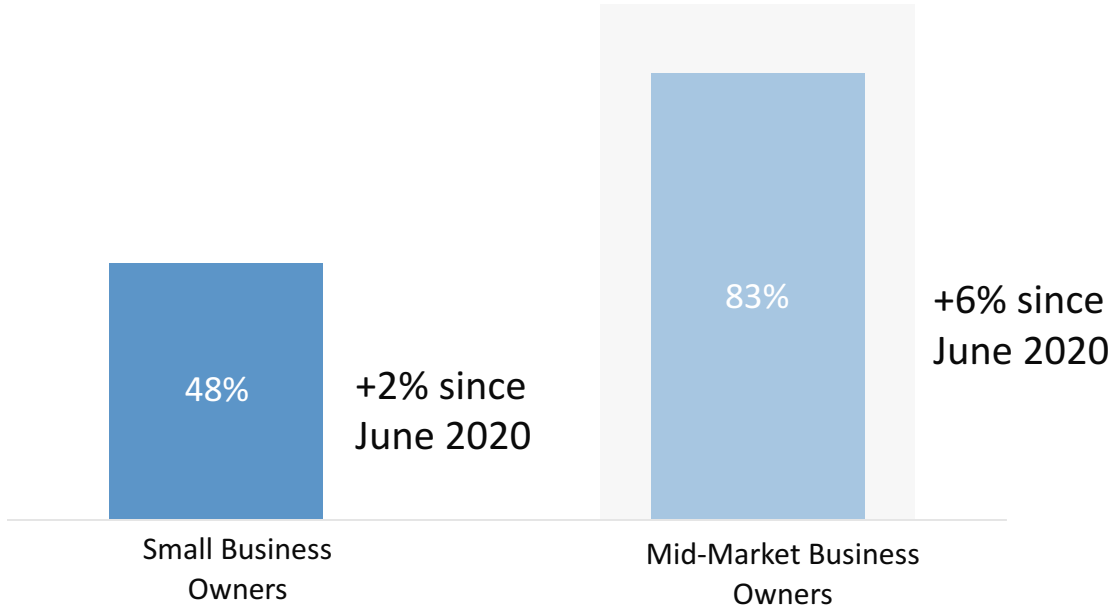
43% of Commercial Line Agents

**52%** +13% since June 2020

Of Independent Agents believe their commercial clients are prepared for a potential cybersecurity attack

Business Owners' Reported Preparedness for Preventing a Cyberattack

*(Shown Top 2 Box Prepared)*




*Q17. How prepared is your business in preventing a cyberattack? // 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? Base: Small Business Owners (n=400), Mid-Market Business Owners (n=401), Independent Insurance Agents (n=430), Commercial lines Agents (n=100)*

# Most Small and Mid-Market Business Owners are interested in a range of cyber protection resources or products

Interest in Cyberattack Protection Resources or Products

*(Shown Top 2 Box Interested)*

| | Small Business Owners | Mid-Market Business Owners |
|---|---|---|
| Computer Fraud protection* | 75% | 91% |
| Identity recovery protection* | 75% | 87% |
| Computer Attack protection* | 73% | 88% |
| Data compromise protection* | 67% | 88% |
| Network Security Liability protection* | 63% | 91% |
| Misdirected Payment Fraud protection* | 62% | 86% |
| Cyber Extortion protection* | 59% | 87% |
| Electronic Media Liability protection* | 54% | 85% |

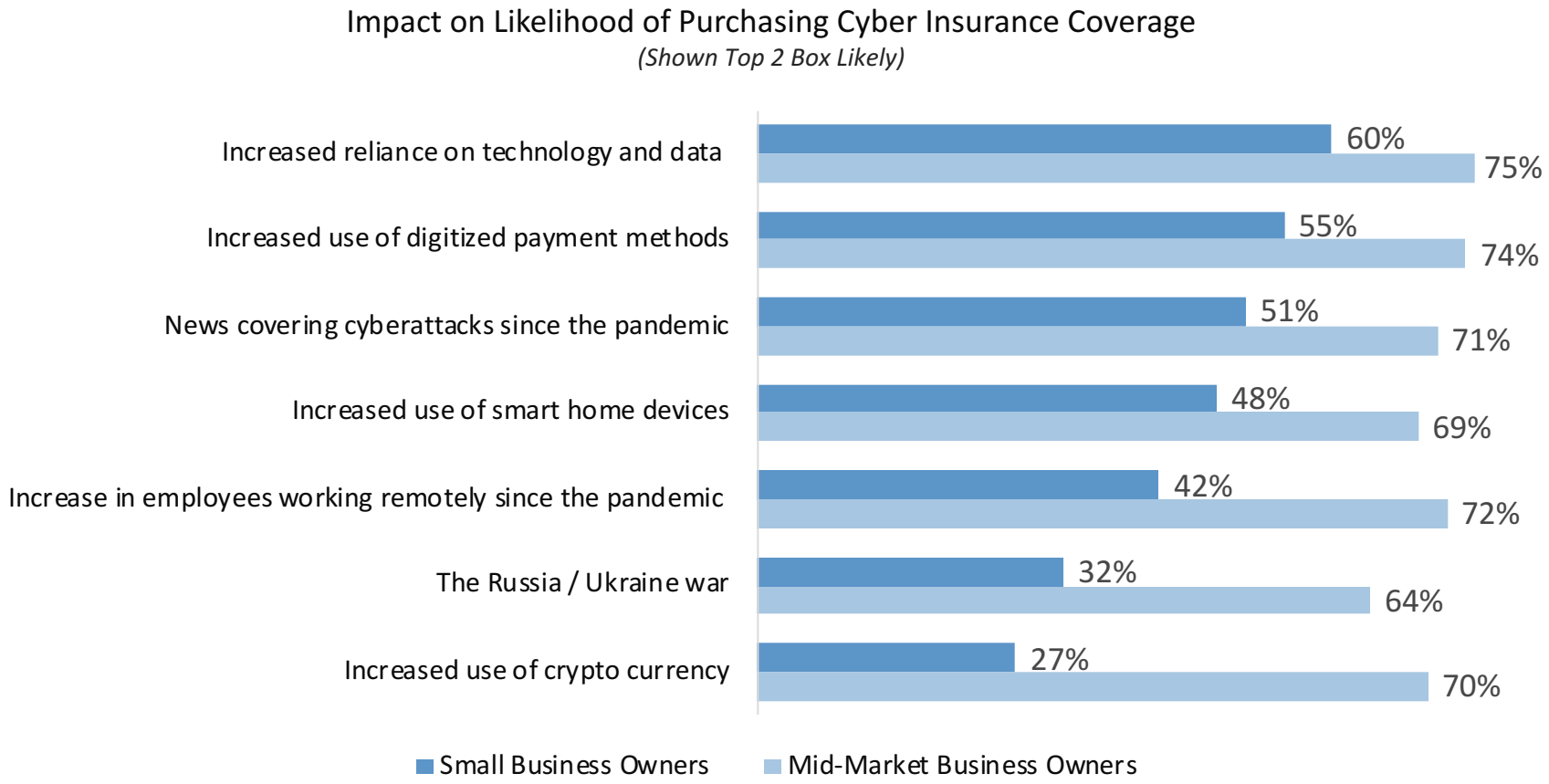
*Q20a. How interested would you be in purchasing each of the following resources or products to protect against cyberattacks? Base: Small Business Owners (n=400), Mid-Market Business Owners (n=401)*

** Definition available in notes section*

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

# Both Small and Mid-Market Business Owners say increased use of technology has made them more likely to purchase cyber insurance

Mid-Market Owners are much more likely than SBOs to say the same of increased remote work, the Russia/Ukraine War, and the increased adoption of crypto currencies.




*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=371), Mid-Market Business Owners (n=397)*