OCTOBER 2022

2022 BUSINESS IMPACT REPORT

idtheftcenter.org • 1-888-400-5530

ITRC | IDENTITY THEFT RESOURCE CENTER

Table of Contents

CEO Letter

Welcome to the Identity Theft Resource Center's second Business Impact Report (BIR), the first follow-up to our 2021 look at the impacts of identity crimes on small businesses including gig workers and solopreneurs. And, my, what a difference one year makes in terms of the trends and impacts on the businesses and individuals that make up the largest part of the U.S. economy.

This time in 2021 we were closing-in on the highest number of data breaches ever recorded in the U.S. – 1,862 – and small businesses and solopreneurs were not exempt from being targeted by cybercriminals. At the time, we reported:

More than half *(57%) of small businesses had experienced a security breach, a data breach, or both.*

Three-fourths *have experienced 2 or more breaches.*

One-third *have experienced 3 or more breaches.*

Nearly half *(45%) of small businesses spent between $250K-$500K to cover costs of their breaches;* ***17%*** *spent between $500K-$1M.*

As you will see in the pages that follow, the past 12 months have seen some improvements when it comes to the impacts of identity crimes and cyberattacks against small businesses. For example, fewer small businesses say they have experienced a data breach, a security breach, or both. Even the number of repeat victims has dropped slightly.

Any expense related to a cybercrime is too high, but small business leaders also report the costs associated with addressing a data or security breach are less severe year-over-year.

For example, the number of businesses losing less than $250,000 grew, while fewer companies report losing between $250,000 and $1 million. That's especially important in the current economic climate where rising costs of labor, products, and delivery are challenging businesses of every size.

But not all the news is hopeful. Just as consumers are increasingly the targets of social media account takeover attacks, so are small businesses. Half of the owners and executives who responded to our survey said they had lost control of a social media account to a cybercriminal and nearly 90 percent had lost revenue as a result. You'll find the full details in this report.

To help understand the dynamic nature of identity crimes against small businesses, we asked many of the same questions of business owners and leaders that we did in 2021. We also asked several first-time questions resulting in some powerful insights:

More than 45% *of businesses lost revenue.*

Nearly 30% *lost customer trust and had difficulty responding to customer concerns.*

More than 40% *struggled to understand what happened and why.*

This year's data raises two important questions:
Why are impacts less severe? **and** ***Is this a trend or a blip?***

We have plenty of evidence that points to why we're seeing small business owners report fewer cyber events:

There are fewer U.S. data breaches being reported overall this year compared to 2021.

The ongoing conflict in Ukraine and the downturn in cryptocurrency markets have reduced the activity of Russia-based cybercrime groups.

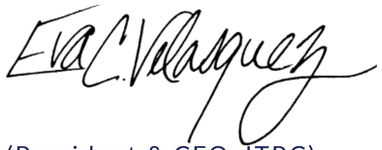
Small businesses are increasing their investment in new security tools, IT staff, and IT staff training (even though they are spending less on overall staff cybersecurity training).

As a result, small business owners and leaders are overwhelmingly confident they are prepared to defend against a cyber event. We'll know in 2023 if these statistics and confidence levels are one-time events or true trends.

Just as with our Consumer Impact Report (CIR), Trends in Identity Report (TIR), and our annual Data Breach Report (DBR), behind every statistic that follows are people. People who are trying to support their families and the families of their employees. The resources stolen by a cybercriminal are the same resources needed to sustain or grow a business to keep those families safe, healthy, and financially secure. I encourage you to think about that as you read this report.

I also encourage you to consider supporting the ITRC in our mission to provide free identity recovery support to the victims of identity crimes and compromises. To offer no-cost education assistance to help people avoid becoming a victim. I hope you will also consider taking advantage of the low-cost education and assistance tools for businesses of all sizes. Your teams and stakeholders will have access to personalized, concierge-level services to help them address their unique identity issues and questions – while helping to ensure our free victim services remain just that – free.

Eva C. Velasquez



(President & CEO, ITRC)

October 2022

Methodology

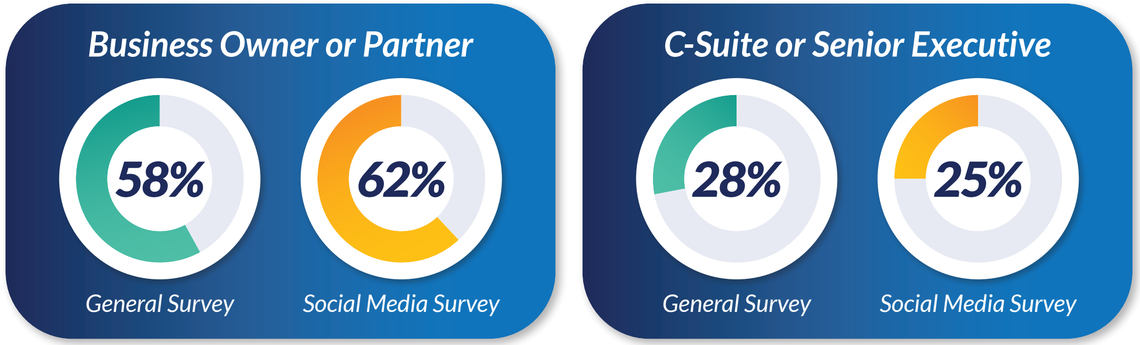
The ITRC, with the assistance of ***SurveyMonkey***, conducted an online survey to explore the impacts of cybercrimes on small businesses as defined by the U.S. Small Business Administration. The survey was conducted in August 2022 covering the 12 months from July 2021 to July 2022 unless otherwise noted in a specific question.

Two online questionnaires were completed by 447 individuals that met the criteria of being a person in a leadership position or an IT professional at a company of 500 or fewer employees including solopreneurs.

Number of Employees

Employee Position

What is the position of the employee who reported the breach?



2022 BUSINESS IMPACT REPORT

idtheftcenter.org • 1-888-400-5530

ITRC | IDENTITY THEFT RESOURCE CENTER

Our *2022 Business Impact Report* looks into what happens specifically to small businesses and solopreneurs following a data or security breach. For the report, the ITRC surveyed 447 small business owners, leaders, and employees to paint a picture of small organizations and individuals that are significantly impacted by cybercrimes, often multiple times in a short period of time.

In the event of another cyberattack or data breach...

70%

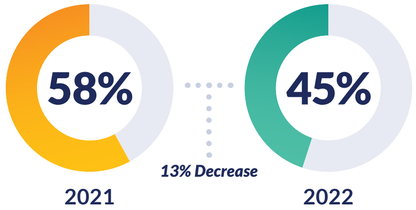
OF SMALL BUSINESSES CLAIM TO BE READY FOR AN ATTACK/BREACH

Cybersecurity Incidents Targeting Small Businesses

+61%

*Increase during the pandemic years of **2020** and **2021**.*

Reported Security Breaches, Data Breaches, or Both



Lost Revenue Due to Cybercrimes

***More than 45%** of small businesses reported a loss in revenue.*

*In the **past year**, the amount of lost revenue was generally reported as **lower** than in 2021.*

Exception: Victims of Social Media Account Takeovers

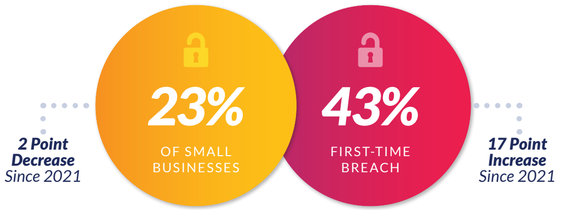
11 Point Increase** in Revenue Loss of **Less than $250K

***6 Point Decrease** in Revenue Loss Between $250K-$500K*

***More than 40%** of small businesses that reported a cybercrime struggled to understand what happened and why.*

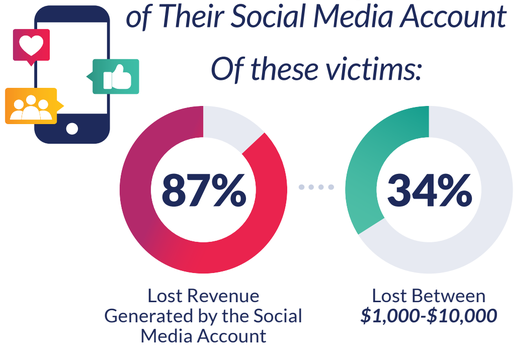
***Nearly 30% of small businesses** lost customer trust and/or had difficulty responding to customer concerns.*

Small Businesses Reported Experiencing a Breach



***50% of Small Businesses** Reported Losing Control of Their Social Media Account*

Of these victims:



"Losing control of our social media account impacted customer trust."

"Losing control of our social media account has affected the business drastically."

Analysis & Summary of 2022 Key Findings

Small business leaders who responded to the ITRC's Business Impact Survey generally describe an overall improved security and data protection landscape since the 2021 research. There is a level of awareness (and confidence) among small business owners, even in the smallest organizations, that reflects a better recognition of the threats they face and the options for recovery when an attack is successful.

Despite the slightly reduced impacts described by small business leaders, there are still significant risks. Half of the business leaders surveyed reported that cyberthieves had taken control of their social media accounts for as long as 30 days, costing 87% of the companies revenue.

Businesses also need to continue to implement or maintain comprehensive cybersecurity and data protection plans. One trend identified in this report, though, stands out as needing attention: Cybersecurity training for all employees.

Phishing and social engineering attacks aimed at employees and contractors with access to sensitive company or customer information are increasingly sophisticated. Given the volume and velocity of these attacks, now is not the time to reduce the training opportunities for non-IT employees. Yet, that is exactly the trend described by the small business leaders whose experiences are described here.

While any reduction in the impact of a cybercrime on a small business or individual is welcome and significant, it's also too early to tell if the improvements reflected here are medium or long-term trends or simply unique to the current environment.

Summary of Key Findings

Key Findings of General Victims

Security Impact | Financial Impact | Operational Impact

Social Media Takeover Attack Findings

Security Impact | Financial Impact | Operational Impact

Key Findings of General Victims

Small businesses who self-reported their security or data breach in a national survey.

Security Impact ***Financial Impact*** ***Operational Impact***

Has your company ever experienced a security or data breach?

Less than half (45%) of small businesses reported a security breach, a data breach, or both in the most recent survey, a steep reduction from the 58 percent (58%) that reported a cybercrime in the 2021 survey. The largest reduction was among businesses that reported both a cyberattack and data breach – a six percentage point drop.

2021

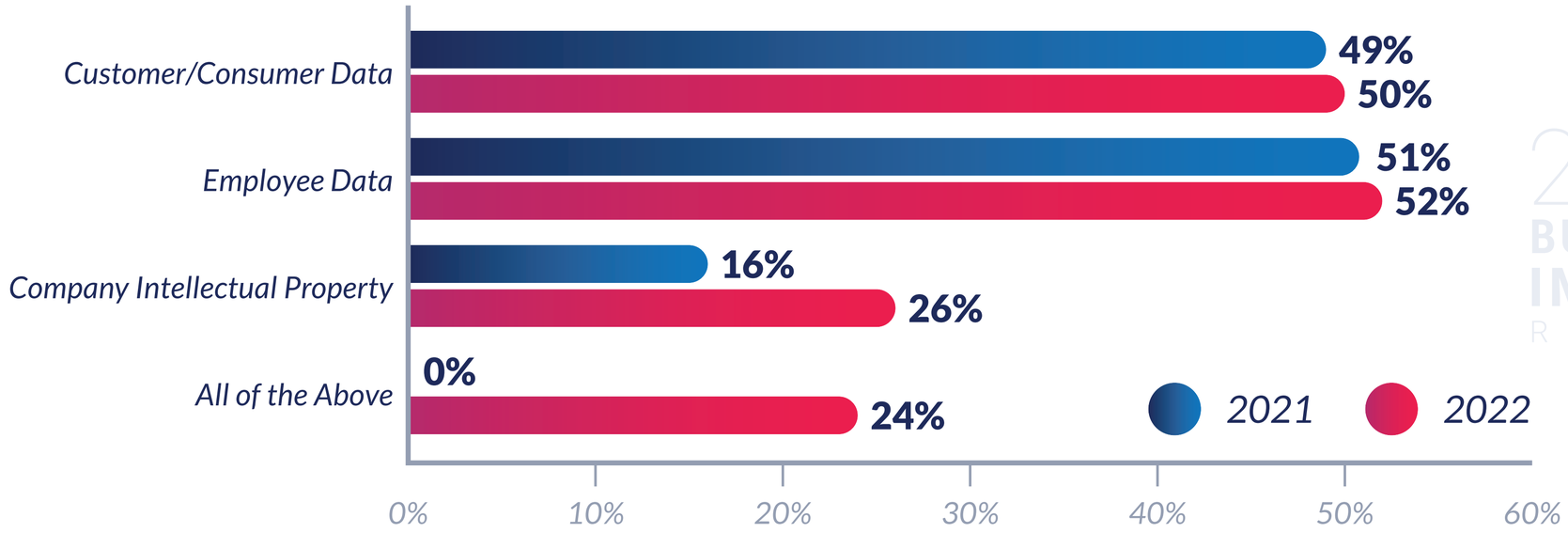
Data Breach	16%
Security Breach	22%
Both	20%
Have Not Experienced a Security or Data Breach	42%

2022

13%	Data Breach
18%	Security Breach
14%	Both
55%	Have Not Experienced a Security or Data Breach

What data was compromised?

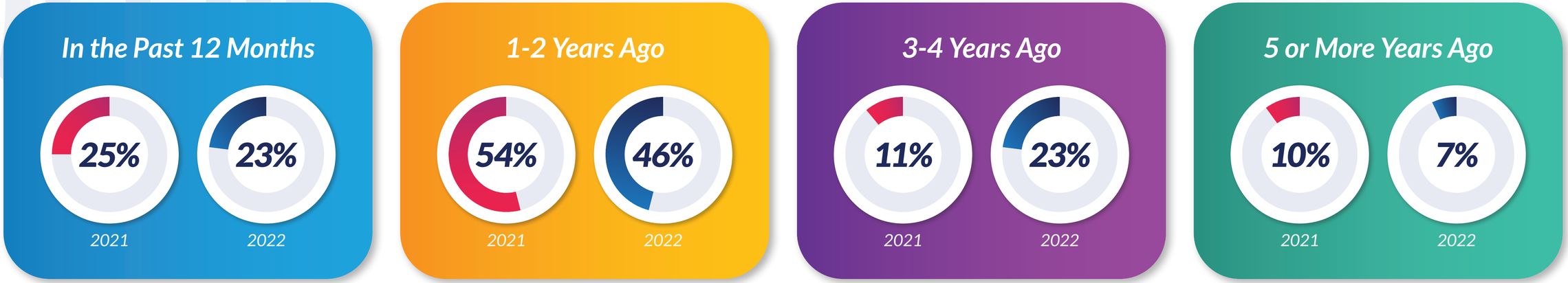
Employee (52%) and Customer (50%) data remained the most sought-after information by cybercriminals, but company intellectual property was the target in more than a quarter of incidents (26%), up from 16 percent (16%) in last year's report. The fact that employee data is compromised more often is consistent with the general trend of information that can be used to attack a business is more valuable to a threat actor.



2022 BUSINESS IMPACT REPORT

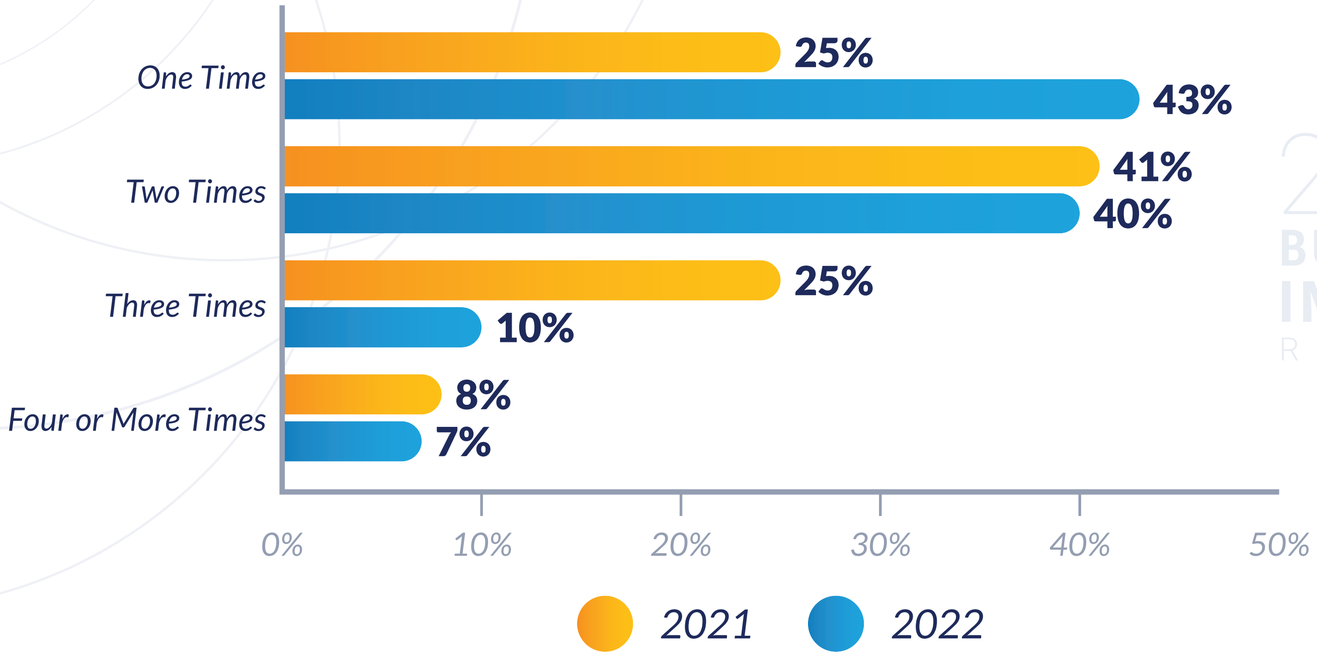
When did you experience the most recent data breach?

Fewer small businesses reported experiencing a data breach in the past 12 months – 23 percent (23%), a two percentage point reduction from 2021; the number of businesses reporting a first-time breach jumped 17 points year-over-year.



How many times have you experienced a data breach?

Companies suffering two data compromises over time declined one percentage point from 2021 but remained a very high 40 percent (40%) in total. Only ten percent (10%) reported being the victim of three data breaches, a 16-point drop from 2021; and businesses that reported being the victim of four or more data breaches dropped from eight percent (8%) to seven percent (7%) in this survey.

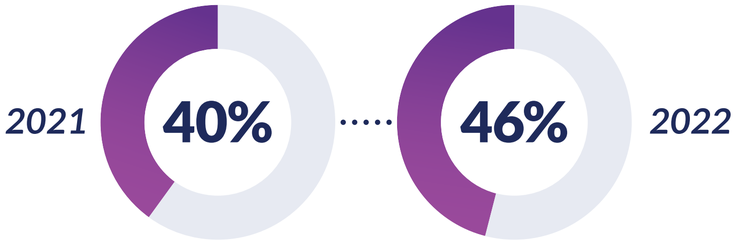


2022 BUSINESS IMPACT REPORT

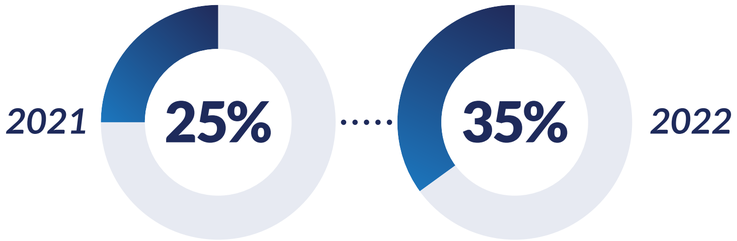
What was the root cause(s) of the most recent data breach?

External threat actors (hackers) remained the primary cause of data breaches at 46 percent (46%), a six percentage point increase over the previous year. However, compromises due to remote workers (35%) and third-party vendors (29%) both grew ten points due to the continued trend of working from home and supply chain attacks against smaller vendors as a means of gaining access to a larger company's data.

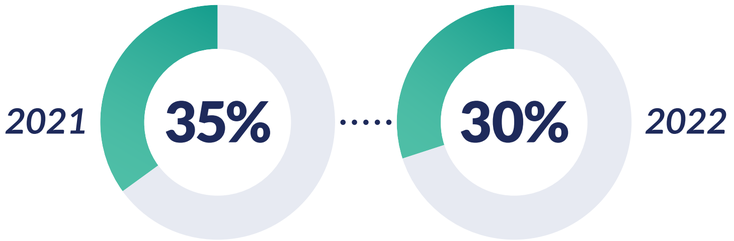
Data breaches caused by malicious insiders dropped five percentage points to 30 percent (30%) of compromises, and those caused by failing to secure a cloud environment also dropped from 22 percent (22%) in the previous report to 18 percent (18%) in this report.



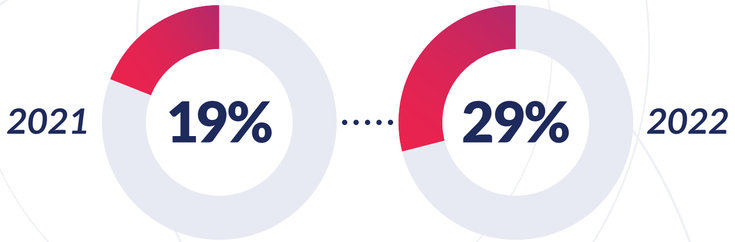
External Threat Actor (Hacker)



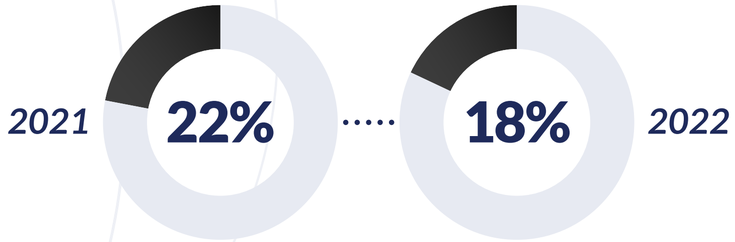
Remote Worker



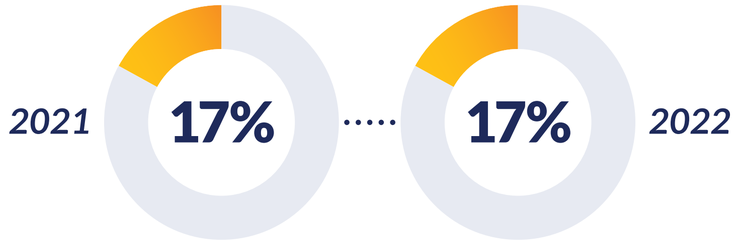
Malicious Insider (Employee or Contractor)



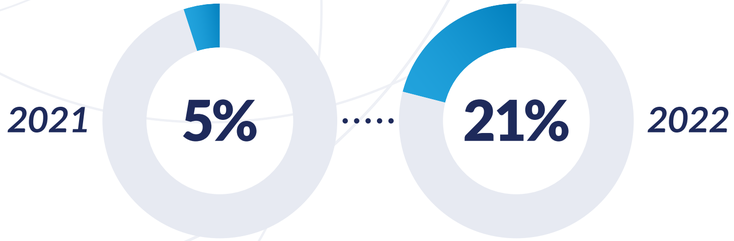
Third Party Vendor



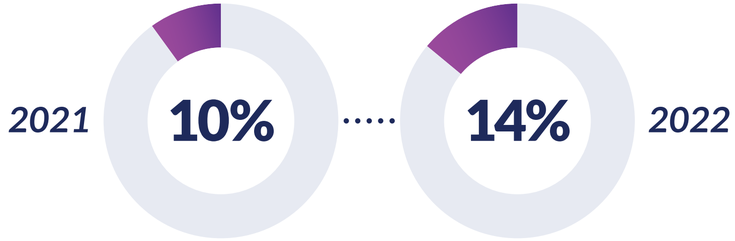
Failure to Secure a Cloud Environment



Failure to Patch a Known Software Flaw

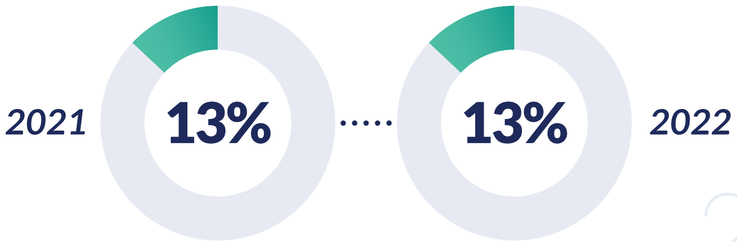


Human Error

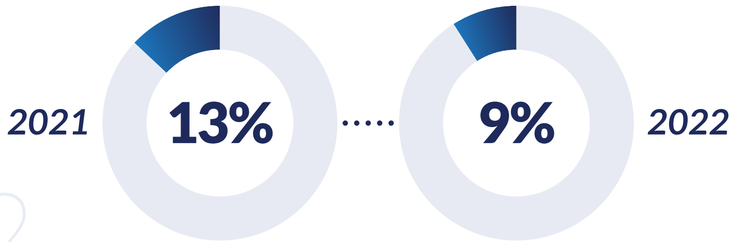


Ransomware Attack

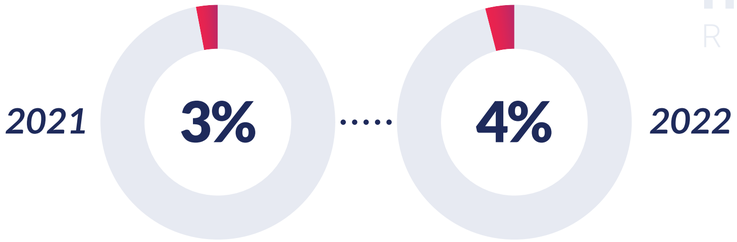
Findings 2 of 3



Phishing Scheme



System Error



Unknown

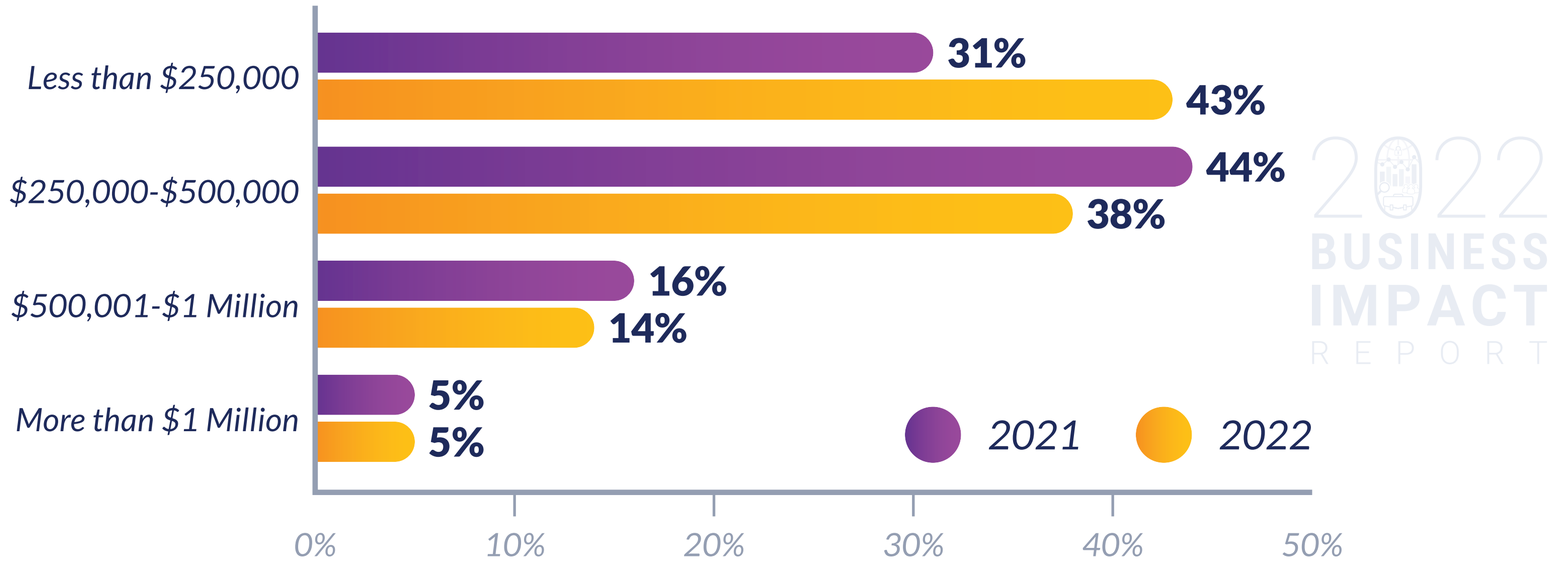
Other

Findings 3 of 3

Financial Impact

What was the approximate total financial impact of the security or data breach?

Small businesses generally lost less money as a result of a cyber incident in the past year. The number of companies paying less than $250,000 grew by 11 percentage points over 2021 to 43 percent (43%), while the number of businesses paying $250,000 to $500,000 dropped six points to 38 percent (38%). Small businesses paying between $500,000 to $1 million dropped two percentage points to 14 percent (14%); five percent (5%) of organizations saw impacts of more than $1 million, flat with the previous year.

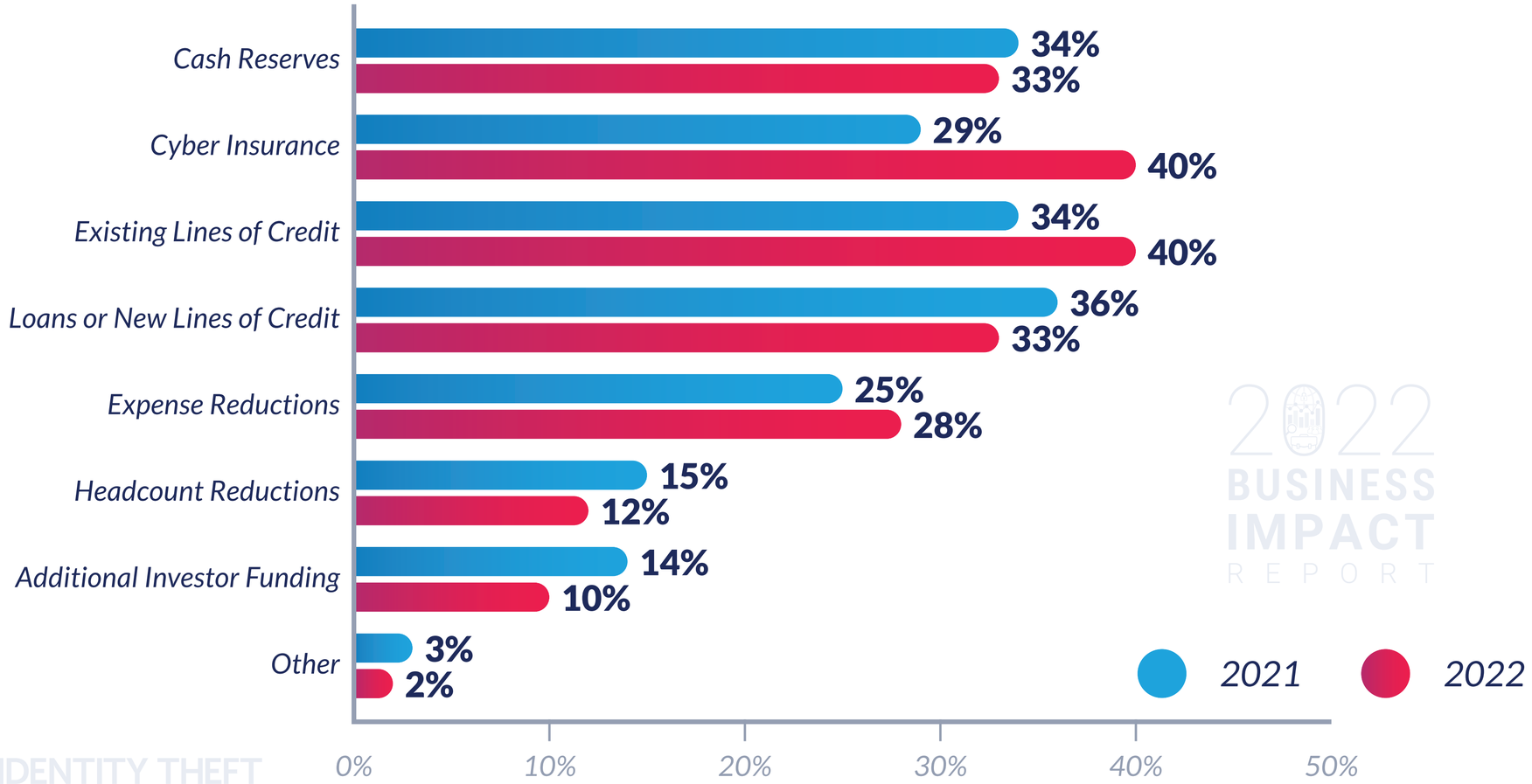


2022 BUSINESS IMPACT REPORT

Financial Impact

How did you address the financial impacts of the breach?

Small businesses relied more on cyber insurance and existing credit lines to cover the costs associated with a data or security breach – 40 percent (40%), respectively. That's a 12 percentage point hike in using insurance proceeds and a seven-point jump in existing credit use. The use of cash reserves, new lines of credit, and headcount reductions declined year-over-year.



2022 BUSINESS IMPACT REPORT

ITRC | IDENTITY THEFT RESOURCE CENTER

Operational Impact

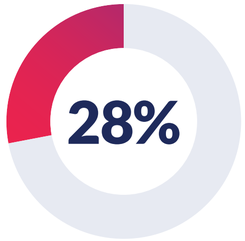
How long did it take your business to return to pre-breach levels of performance?

The pace of recovery from a breach increased in the past 12 months. More than one-third of small businesses – 35 percent (35%) – reported returning to pre-breach levels of performance within one (1) year, a 13 percentage point increase from 2021. Most companies – 41 percent (41%) – required between one to two years to fully recover, a decline of one point over the previous report.

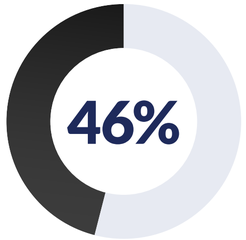
	2021	2022
Less than a Year	22%	35%
1-2 Years	42%	41%
3-5 Years	28%	19%
Have Not Fully Recovered	7%	4%
Other	1%	0%

Did you experience any of the following issues following your cyber incident?

The most significant impacts small business reported in the wake of a cyber incident is "loss of revenue" (46%), followed by "difficulty understanding what occurred & how" (41%), "loss of customer trust" and "difficulty responding to customer concerns" (28% respectively), and regrettable turnover (24%).

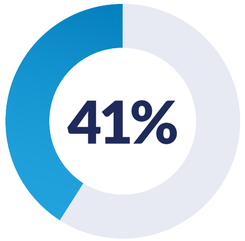


Loss of Customer Trust



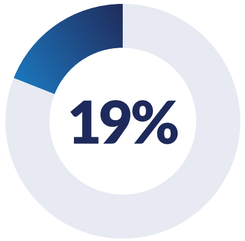
Loss of Revenue

Regrettable Employee Turnover

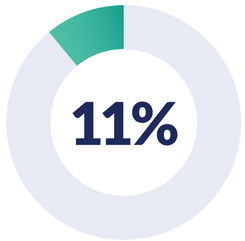


Difficulty Understanding What Occurred and How

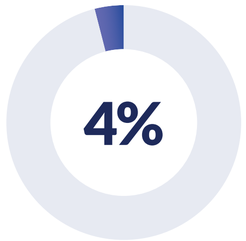
Difficulty Responding to Customer Concerns



Difficulty Finding Affordable Security Solutions



Difficulty Obtaining or Renewing Cyber Insurance



None of the Above

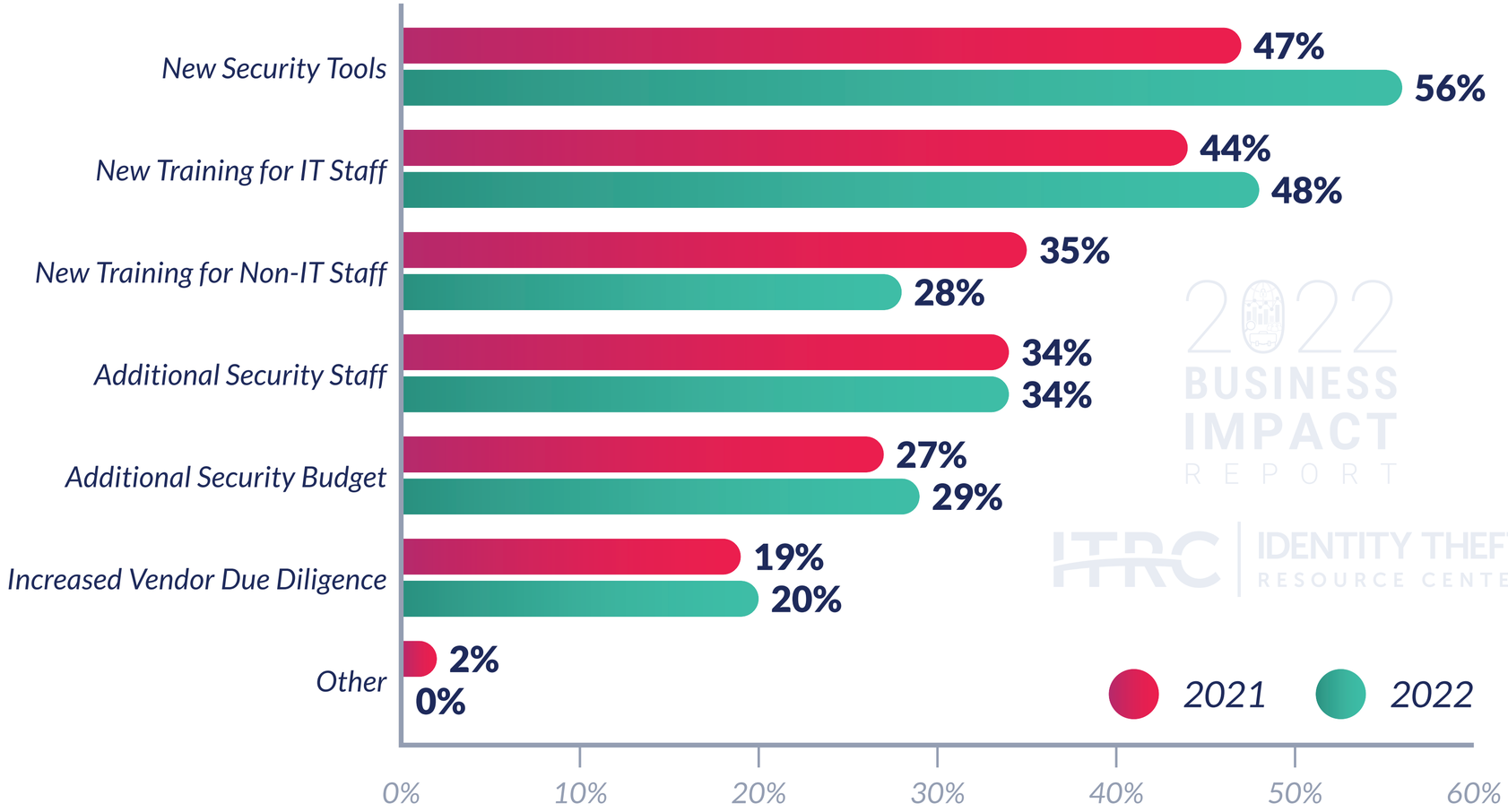
2022 BUSINESS IMPACT REPORT

ITRC | IDENTITY THEFT RESOURCE CENTER

Operational Impact

What steps have you taken to prevent future security or data breaches?

More than half of small businesses (56%) increased their spend on new security tools, and 48 percent (48%) invested in IT staff training but decreased new training for non-IT staff – down seven percentage points to 28 percent (28%) compared to the previous report. This reflects an overall trend of reducing security training for general employees to one annual security update for all team members.



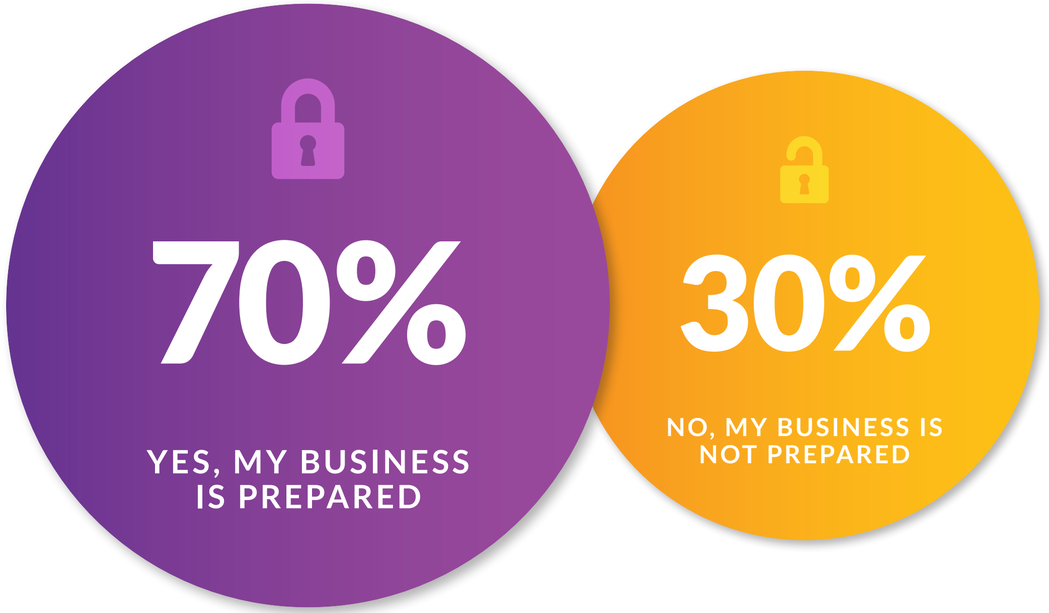
2022 BUSINESS IMPACT REPORT

ITRC | IDENTITY THEFT RESOURCE CENTER

Operational Impact

Are you prepared to protect against a cyberattack or recover from a data breach?

A large majority of small businesses – 70 percent (70%) – said they are ready to protect against a cyberattack or recover from a data breach.



ITRC | IDENTITY THEFT RESOURCE CENTER

2022 BUSINESS IMPACT REPORT

Social Media Takeover Attack Findings

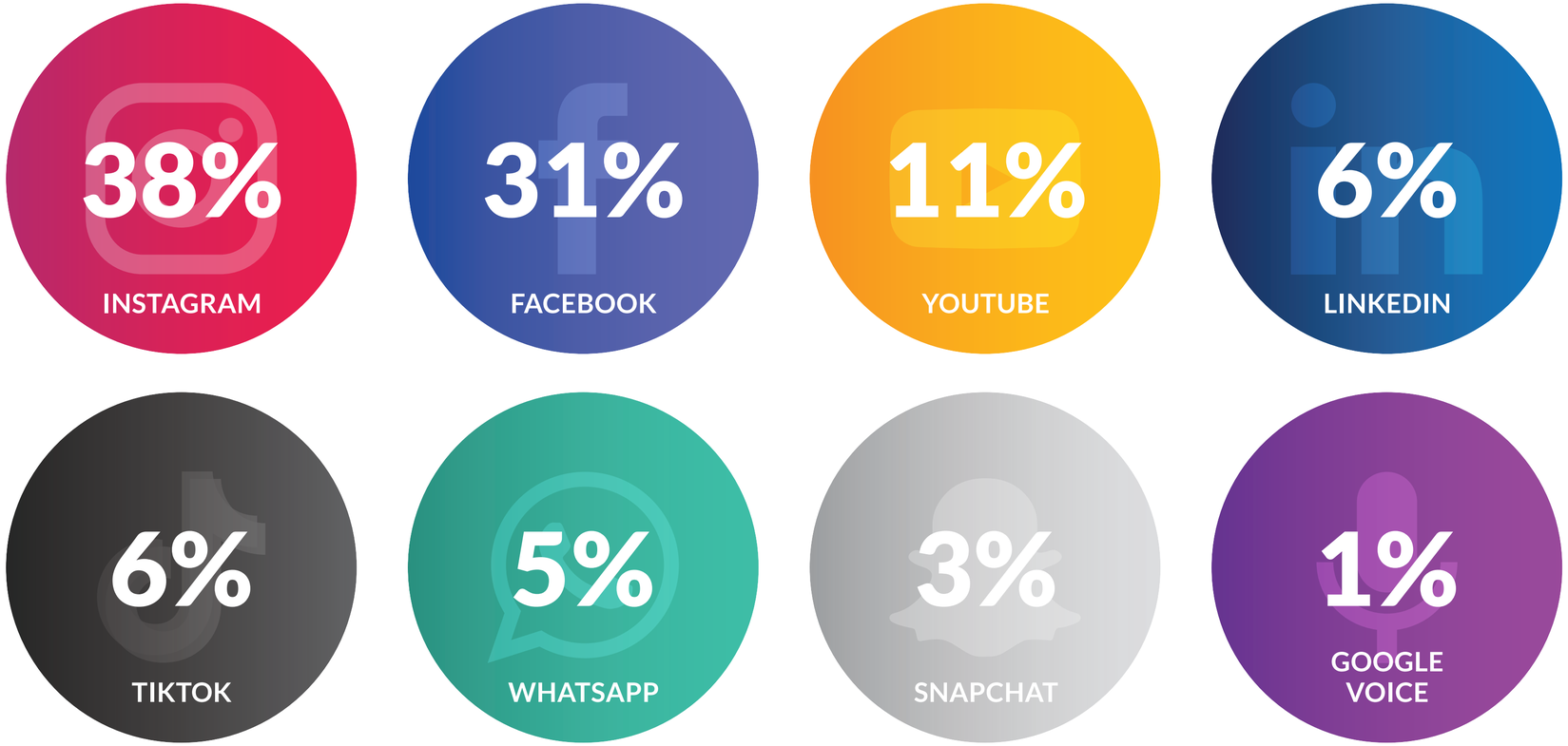
The ITRC described in the most recent Trends in Identity and Consumer Impact Reports the dramatic rise in social media account takeover attacks and the effect they have on consumers. Social media attacks reported to the ITRC jumped more than 1,000 percent (1,000%) in the past year and 27 percent (27%) of individual victims lost earnings from those accounts.

That finding prompted the ITRC to learn if a similar dynamic existed for small businesses. The results were startling.

Security Impact ***Financial Impact*** ***Operational Impact***

Which account(s) were compromised?

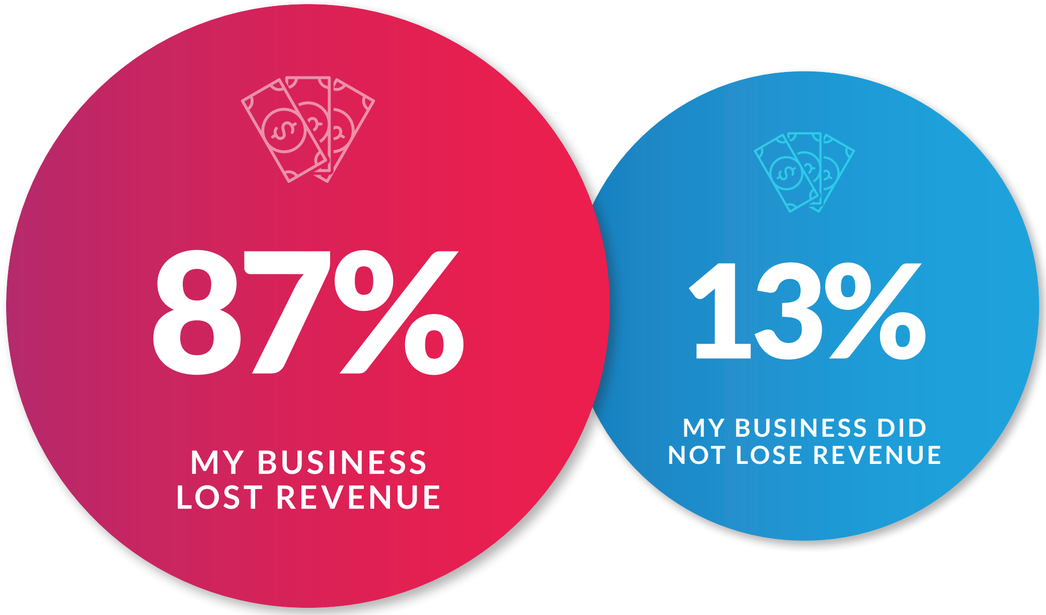
Instagram (38%) and Facebook (31%), both owned by Meta, were the most frequently compromised sites, followed by YouTube at 11 percent (11%).



Financial Impact

Did you lose revenue as a result of losing control of your social media account(s)?

Half of the respondents (50%) reported that their company's social media accounts were compromised in the past 12 months. Of those who lost control of their social media accounts, 87 percent (87%) also lost revenue.



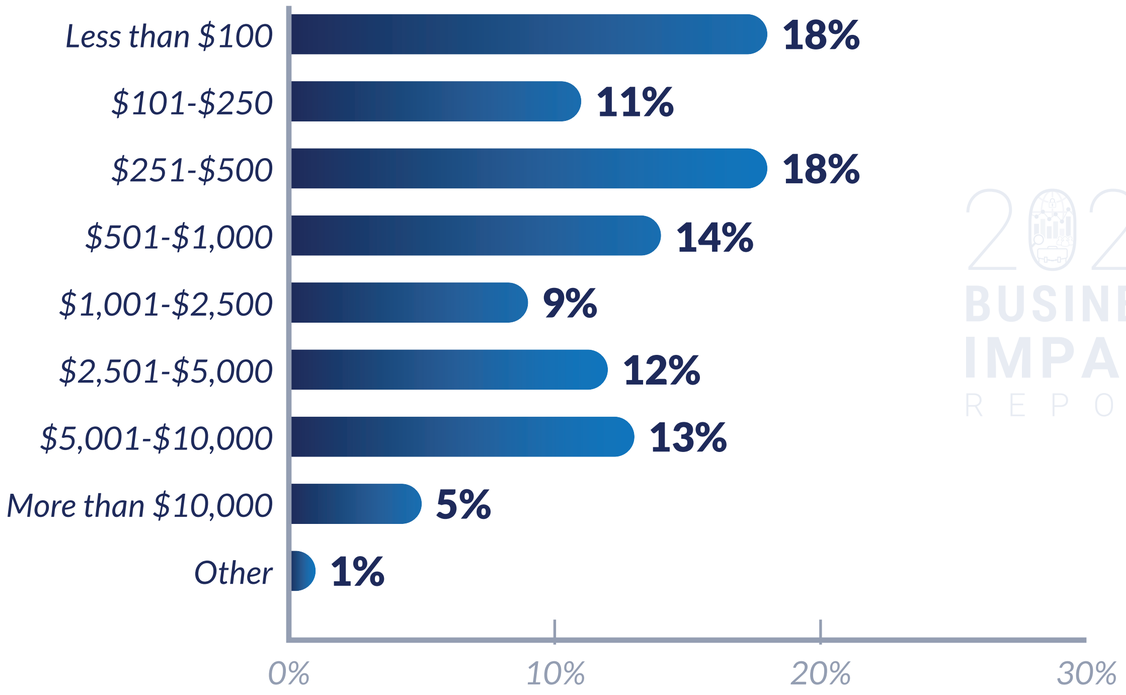
2022 BUSINESS IMPACT REPORT

ITRC | IDENTITY THEFT RESOURCE CENTER

Financial Impact

How much revenue did you and/or your customers/followers lose as a result of the social media account takeover?

More than 40 percent (40%) lost between $100-$1,000; One-third lost between $1,001-$10,000; five percent (5%) lost more than $10,000 to cybercriminals.



2022 BUSINESS IMPACT REPORT

Did the identity criminal take any of the following actions?

Attackers continued to post to the compromised company social media account in half of the cases; 38 percent (38%) of companies saw cybercriminals contact their customers/followers with scams; and, 11 percent (11%) of businesses said the attackers captured revenue from the social media platform.

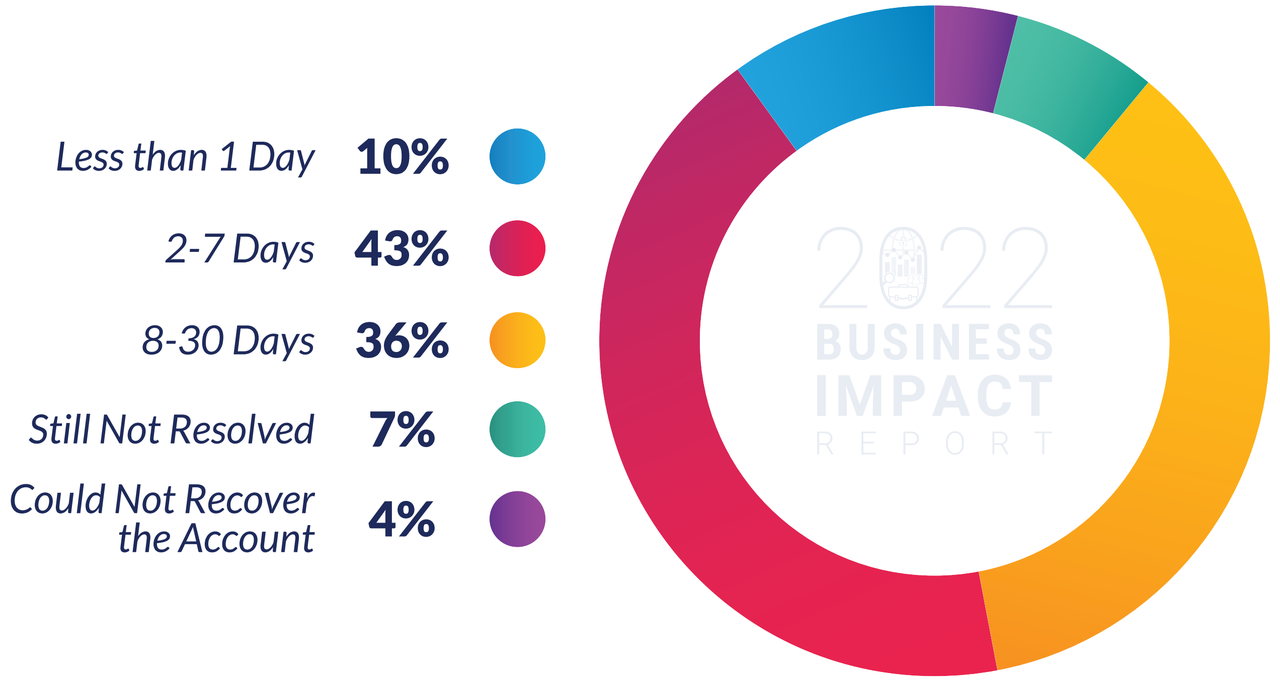
Continued to Post New Messages on the Account(s)	**50%**
Contacted Followers/ Customers with Similar Scam	**38%**
Captured Revenue Intended for Our Business	**11%**
Other	**1%**

ITRC | IDENTITY THEFT RESOURCE CENTER

Operational Impact

How long did it take you to recover your compromised account(s)?

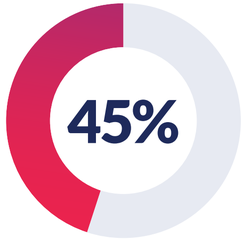
Unlike 70 percent (70%) of consumers who report they lose permanent access to their compromised social media accounts, 89 percent (89%) of small businesses are able to regain control of their accounts within 30 days.



ITRC | IDENTITY THEFT RESOURCE CENTER

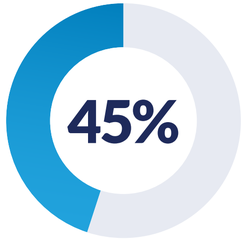
What was the root cause(s) of the account takeover?

More than half of the companies (51%) believe their accounts were compromised when someone responded to a direct message (DM) and 45 percent (45%) were the result of someone clicking on a phishing link or sharing account credentials who impersonated a friend. 29 percent (29%) reported the cybercriminal claimed to be a customer, prospect, or vendor.



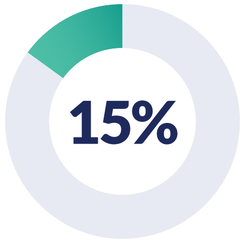
Someone Clicked on a Phishing Link

Someone Responded to a Direct Message



Someone Shared Account Credentials with a Person Who Claimed to be a Friend

Someone Shared Account Credentials with a Person Who Claimed to be a Potential Customer/ Vendor



Unknown

In the victims' words:

"Losing control of our social media account impacted customer trust."

"We have had to implement more precautions on opening attachments."

"I lost followers because the hacker messages scams to people."

"I am unable to post my product to my social media page."

"Losing control of our social media account has affected the business drastically."

2022 BUSINESS IMPACT REPORT

idtheftcenter.org • 1-888-400-5530

ITRC | IDENTITY THEFT RESOURCE CENTER

Consumer & Business Resources

The ITRC offers a variety of low-cost identity education, protection, and recovery services for small businesses as well as free victim assistance and education opportunities for consumers. To learn more, ***click here*** or contact the ITRC by email at ***communications@idtheftcenter.org***.

For Media

For any media-related inquiries, please email ***media@idtheftcenter.org***.

Appendix

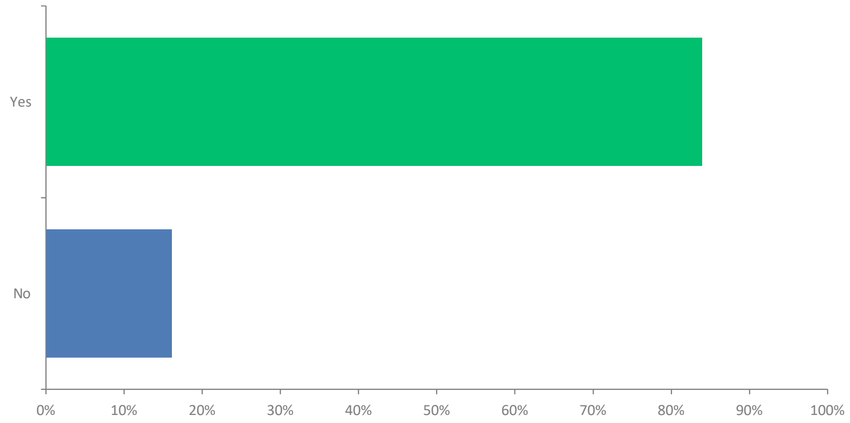
2022 Business Impact Study

Snap Social Media Survey

227

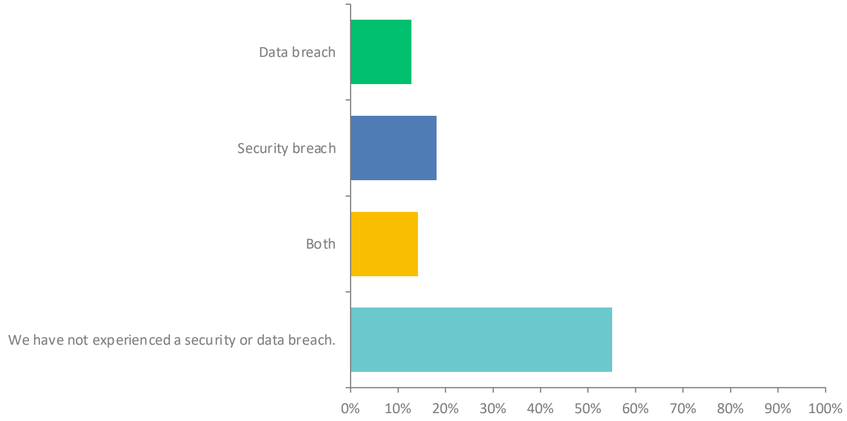
TOTAL RESPONSES

1. Are you an owner or leader of a small business, including single employee companies, with fewer than 500 employees?



ANSWER CHOICES	RESPONSES
Yes	83.93%
No	16.07%

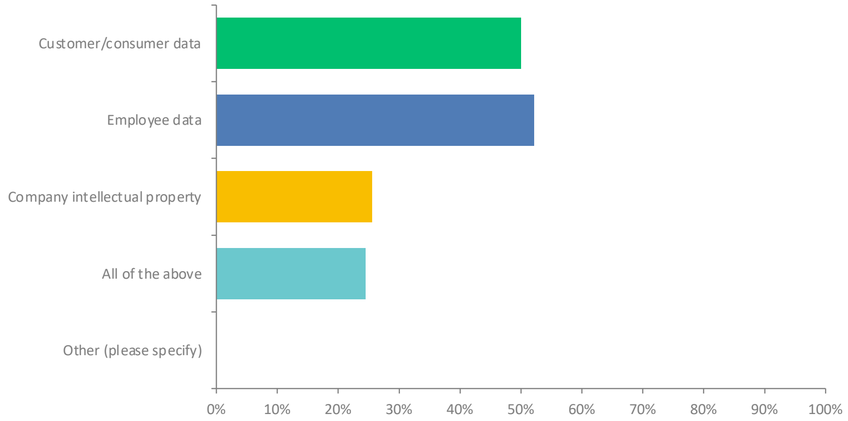
2. Has your company ever experienced a security or data breach?



ANSWER CHOICES	RESPONSES
Data breach	12.78%
Security breach	18.06%
Both	14.10%
We have not experienced a security or data breach.	55.07%

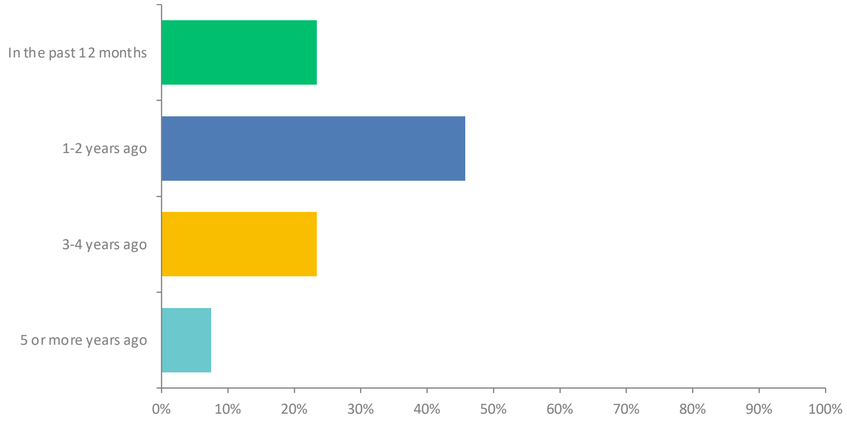
2022 BUSINESS IMPACT REPORT

3. What data was compromised? *(Check all that apply.)*



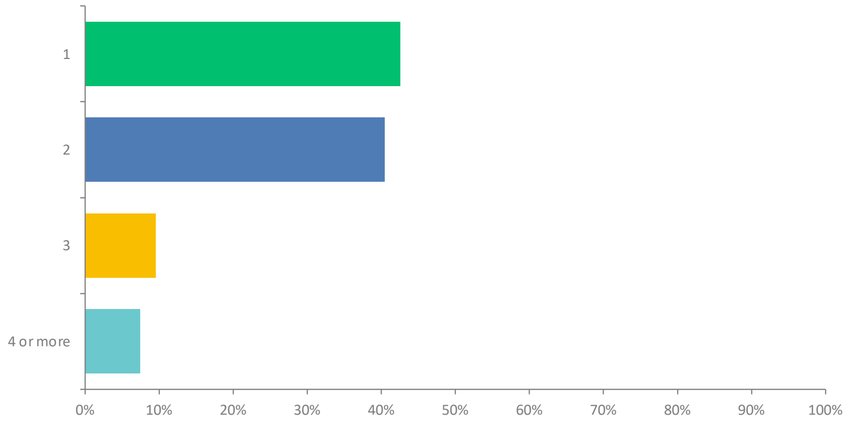
ANSWER CHOICES	RESPONSES
Customer/consumer data	50.0%
Employee data	52.13%
Company intellectual property	25.53%
All of the above	24.47%
Other (please specify)	0%

4. When did you experience the most recent data breach?



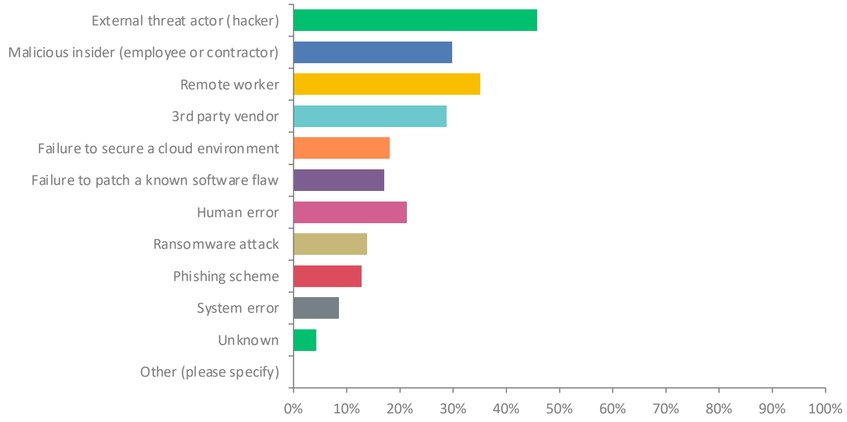
ANSWER CHOICES	RESPONSES
In the past 12 months	23.40%
1-2 years ago	45.74%
3-4 years ago	23.40%
5 or more years ago	7.45%

5. How many times have you experienced a data breach?



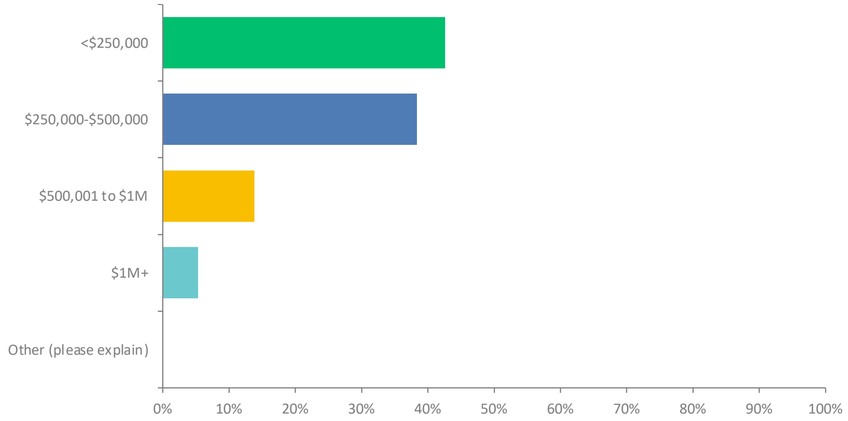
ANSWER CHOICES	RESPONSES
1	42.55%
2	40.43%
3	9.57%
4 or more	7.45%

6. What was the root cause(s) of the most recent data breach? *(Check all that apply.)*



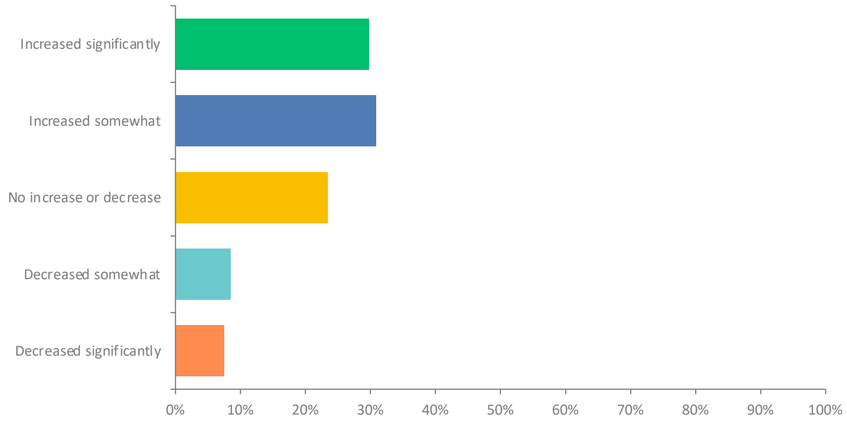
ANSWER CHOICES	RESPONSES
External threat actor (hacker)	45.74%
Malicious insider (employee or contractor)	29.79%
Remote worker	35.11%
3rd party vendor	28.72%
Failure to secure a cloud environment	18.09%
Failure to patch a known software flaw	17.02%
Human error	21.28%
Ransomware attack	13.83%
Phishing scheme	12.77%
System error	8.51%
Unknown	4.26%
Other (please specify)	0%

7. What was the approximate total financial impact of the security or data breach, including lost revenue, lost customers, legal costs, fines & penalties, insurance, marketing costs, improved security, etc?



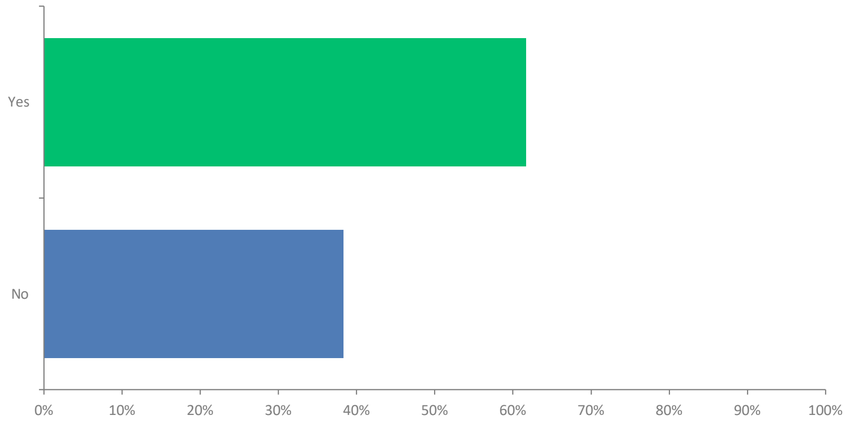
ANSWER CHOICES	RESPONSES
<$250,000	42.55%
$250,000-$500,000	38.30%
$500,001 to $1M	13.83%
$1M+	5.32%
Other (please explain)	0%

8. Did the number of security incidents increase, decrease, or stay the same during the pandemic years of 2020-2021?



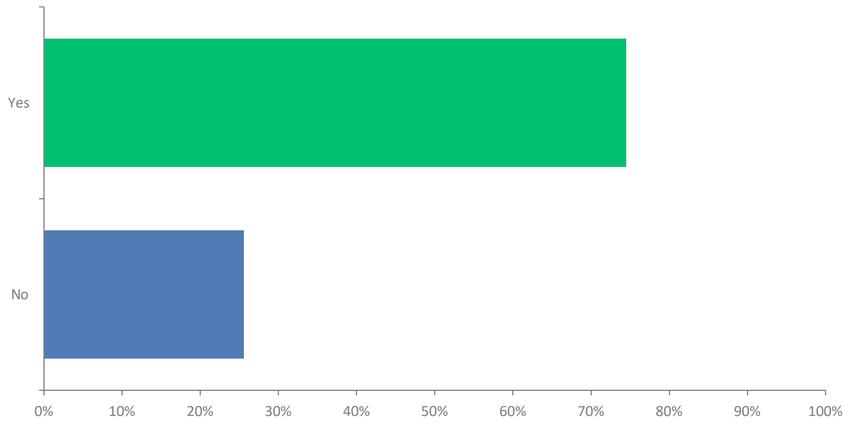
ANSWER CHOICES	RESPONSES
Increased significantly	29.79%
Increased somewhat	30.85%
No increase or decrease	23.40%
Decreased somewhat	8.51%
Decreased significantly	7.45%

9. Were you required to issue a public breach notice under state law or regulation?



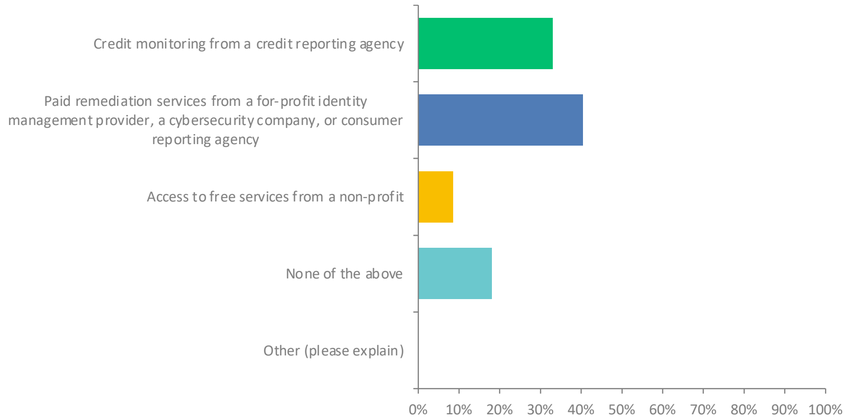
ANSWER CHOICES	RESPONSES
Yes	61.70%
No	38.30%

10. Did you provide a security or data breach notice to your customers or consumers even though you were not required to do so?



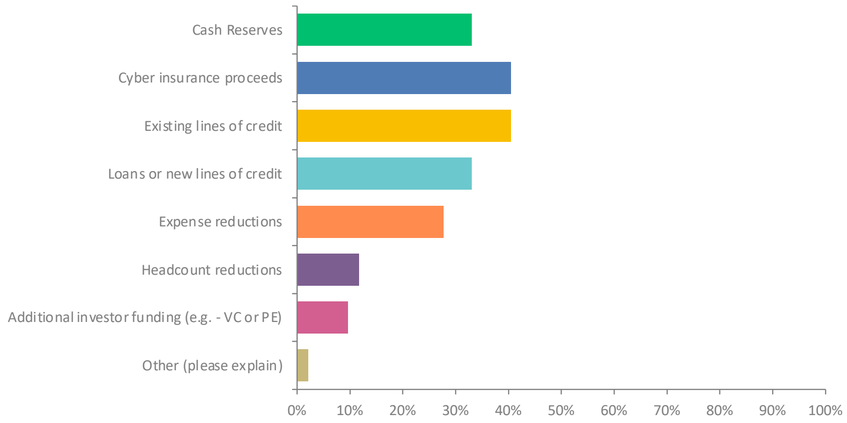
ANSWER CHOICES	RESPONSES
Yes	74.47%
No	25.53%

11. Did you offer remediation services to customers or consumers impacted by the breach?



ANSWER CHOICES	RESPONSES
Credit monitoring from a credit reporting agency	32.98%
Paid remediation services from a for-profit identity management provider, a cybersecurity company, or consumer reporting agency	40.43%
Access to free services from a non-profit	8.51%
None of the above	18.09%
Other (please explain)	0%

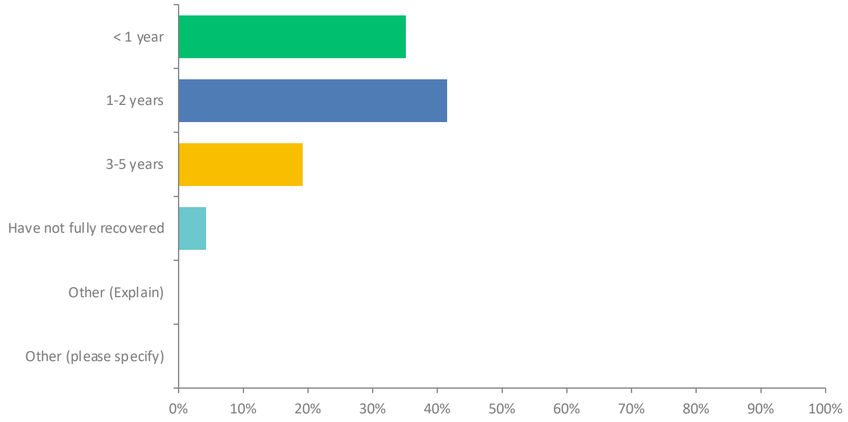
12. How did you address the financial impacts of the breach? *(Select all that apply.)*



ANSWER CHOICES	RESPONSES
Cash Reserves	32.98%
Cyber insurance proceeds	40.43%
Existing lines of credit	40.43%
Loans or new lines of credit	32.98%
Expense reductions	27.66%
Headcount reductions	11.70%
Additional investor funding (e.g. - VC or PE)	9.57%
Other (please explain)	2.13%

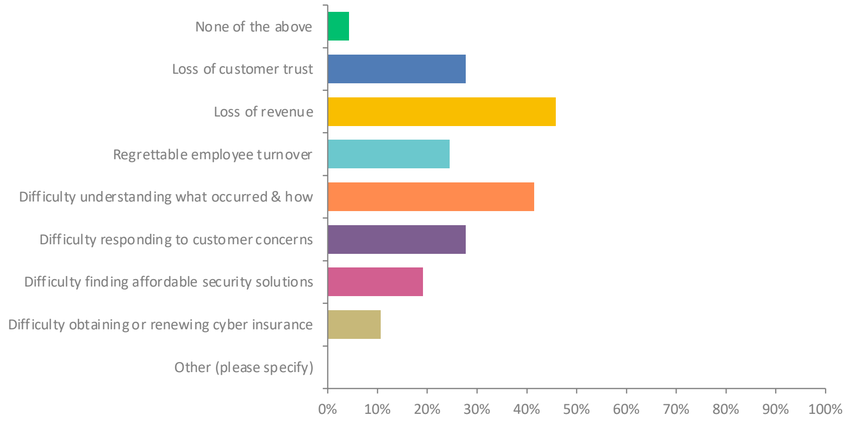
2022 BUSINESS IMPACT REPORT

13. How long did it take your business to return to pre-breach levels of performance?



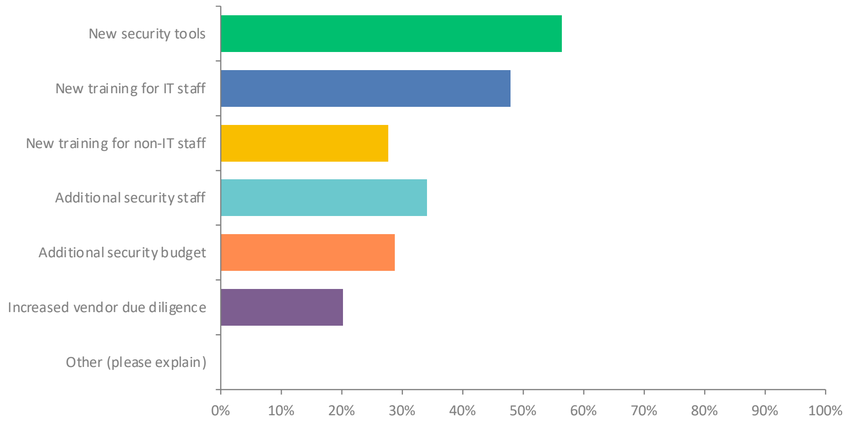
ANSWER CHOICES	RESPONSES
< 1 year	35.11%
1-2 years	41.49%
3-5 years	19.15%
Have not fully recovered	4.26%
Other (Explain)	0%
Other (please specify)	0%

14. Did you experience any of the following issues following your cyber incident?



ANSWER CHOICES	RESPONSES
None of the above	4.26%
Loss of customer trust	27.66%
Loss of revenue	45.74%
Regrettable employee turnover	24.47%
Difficulty understanding what occurred & how	41.49%
Difficulty responding to customer concerns	27.66%
Difficulty finding affordable security solutions	19.15%
Difficulty obtaining or renewing cyber insurance	10.64%
Other (please specify)	0%

15. What steps have you taken to prevent future security or data breaches? *(Check all that apply.)*

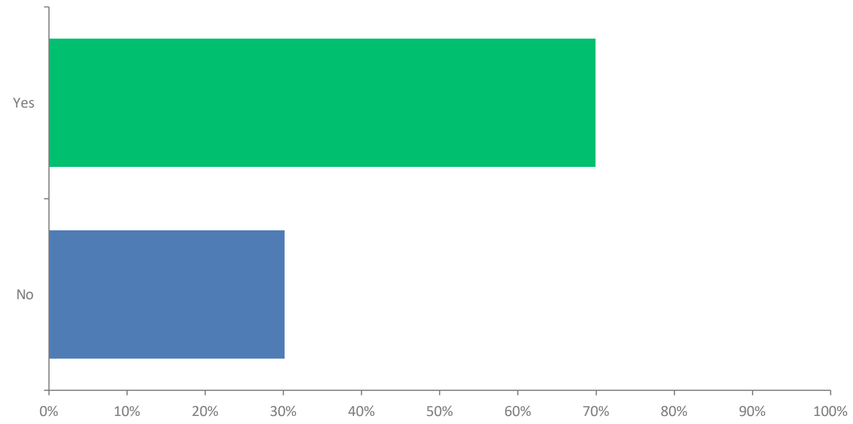


ANSWER CHOICES	RESPONSES
New security tools	56.38%
New training for IT staff	47.87%
New training for non-IT staff	27.66%
Additional security staff	34.04%
Additional security budget	28.72%
Increased vendor due diligence	20.21%
Other (please explain)	0%

16. Do you have any of the following solutions or programs in place as a means of preventing security or data breaches? *(Select all that apply.)*

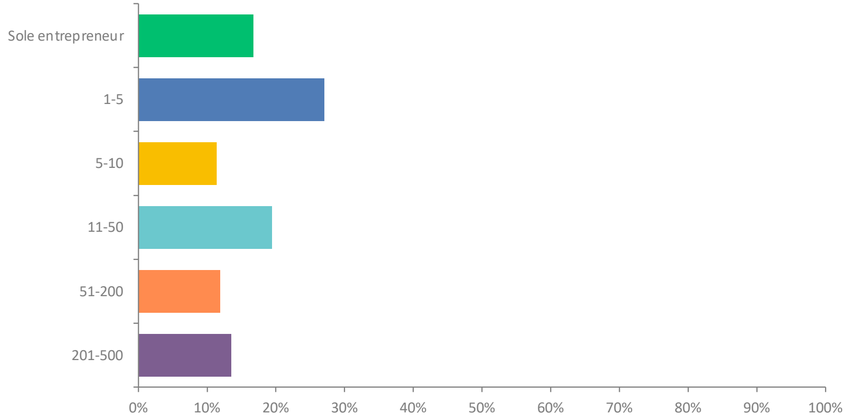
ANSWER CHOICES	RESPONSES
Annual security training for all staff	15.59%
Weekly/monthly/quarterly security updates with all staff	17.74%
Annual security updates with all staff	18.82%
Specialized training for remote workers	9.68%
Cybersecurity and/or Identity Protection services as an employee benefit	11.83%
An employee incentive/bounty for identifying vulnerabilities and/or vulnerable behaviors	5.38%
Other (please explain)	20.97%

17. Are you prepared to protect against a cyberattack or recover from a data breach?



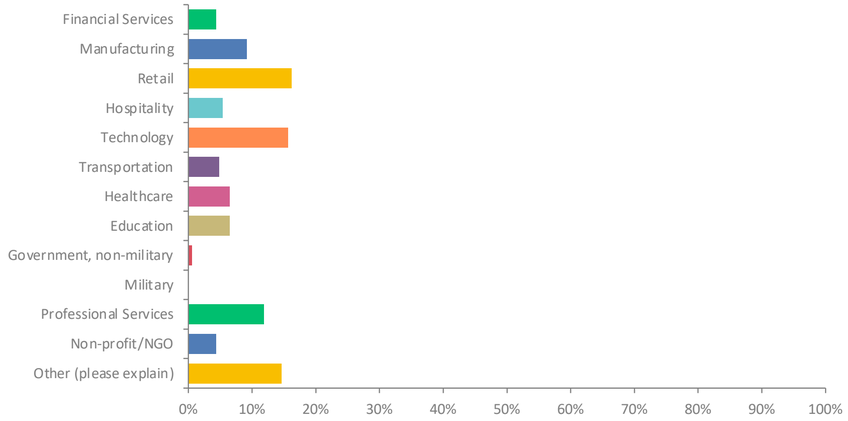
ANSWER CHOICES	RESPONSES
Yes	69.89%
No	30.11%

18. How many employees are in your company?



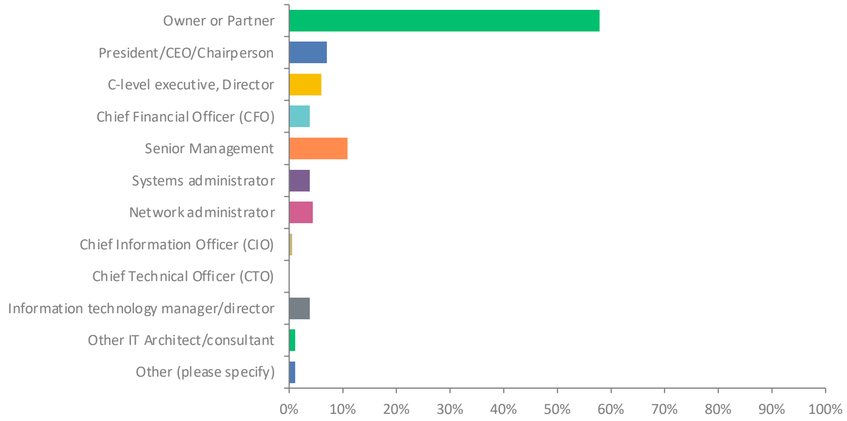
ANSWER CHOICES	RESPONSES
Sole entrepreneur	16.76%
1-5	27.03%
5-10	11.35%
11-50	19.46%
51-200	11.89%
201-500	13.51%

19. What is your industry?



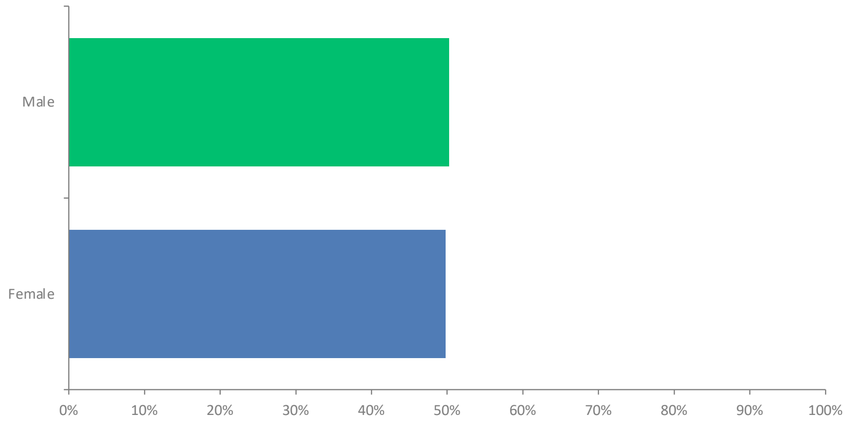
ANSWER CHOICES	RESPONSES
Financial Services	4.32%
Manufacturing	9.19%
Retail	16.22%
Hospitality	5.41%
Technology	15.68%
Transportation	4.86%
Healthcare	6.49%
Education	6.49%
Government, non-military	0.54%
Military	0%
Professional Services	11.89%
Non-profit/NGO	4.32%
Other (please explain)	14.59%

20. What is your title?



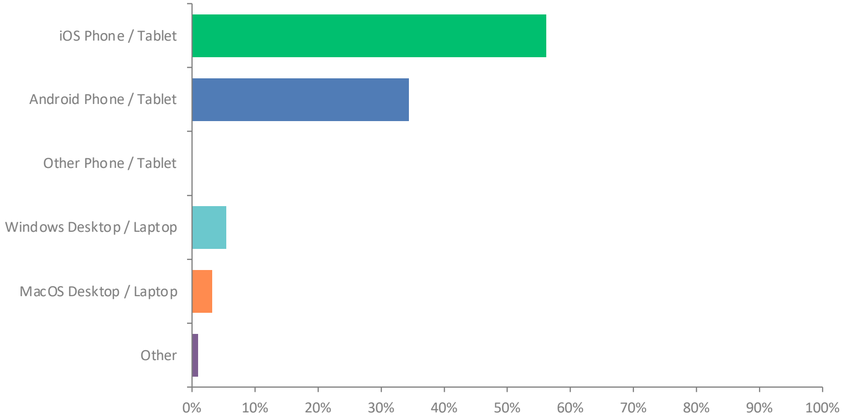
ANSWER CHOICES	RESPONSES
Owner or Partner	57.84%
President/CEO/Chairperson	7.03%
C-level executive, Director	5.95%
Chief Financial Officer (CFO)	3.78%
Senior Management	10.81%
Systems administrator	3.78%
Network administrator	4.32%
Chief Information Officer (CIO)	0.54%
Chief Technical Officer (CTO)	0%
Information technology manager/director	3.78%
Other IT Architect/consultant	1.08%
Other (please specify)	1.08%

21. Gender



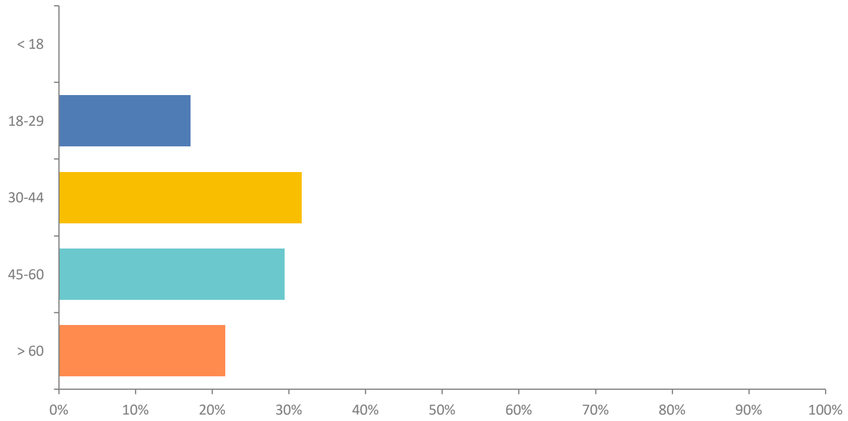
ANSWER CHOICES	RESPONSES
Male	50.23%
Female	49.77%

22. Device Type



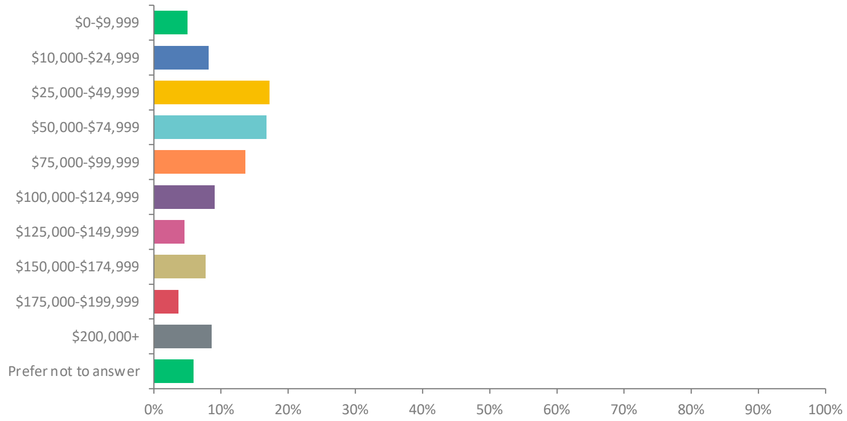
ANSWER CHOICES	RESPONSES
iOS Phone / Tablet	56.11%
Android Phone / Tablet	34.39%
Other Phone / Tablet	0%
Windows Desktop / Laptop	5.43%
MacOS Desktop / Laptop	3.17%
Other	0.90%

23. Age



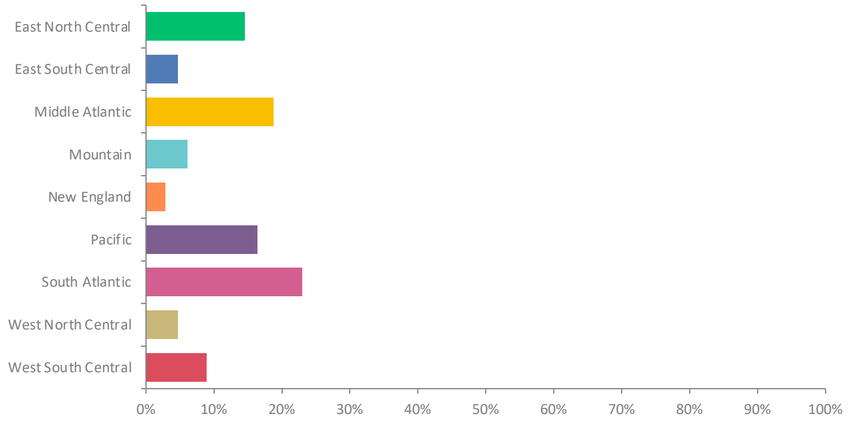
ANSWER CHOICES	RESPONSES
< 18	0%
18-29	17.19%
30-44	31.67%
45-60	29.41%
> 60	21.72%

24. Household Income



ANSWER CHOICES	RESPONSES
$0-$9,999	4.98%
$10,000-$24,999	8.14%
$25,000-$49,999	17.19%
$50,000-$74,999	16.74%
$75,000-$99,999	13.57%
$100,000-$124,999	9.05%
$125,000-$149,999	4.52%
$150,000-$174,999	7.69%
$175,000-$199,999	3.62%
$200,000+	8.60%
Prefer not to answer	5.88%

25. Region



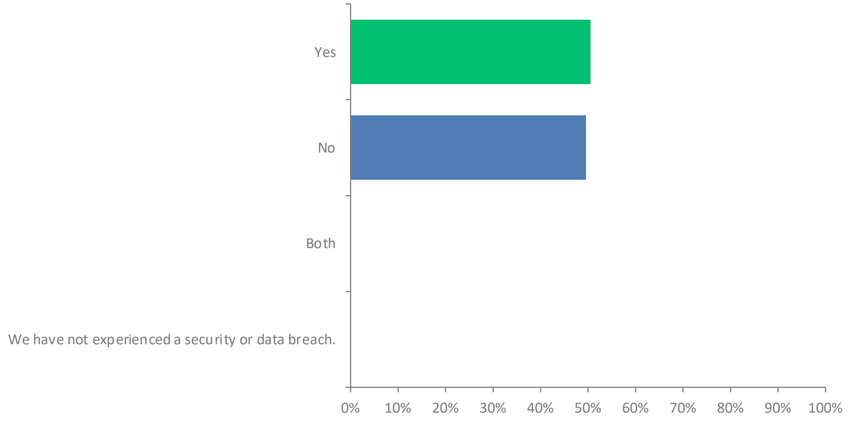
ANSWER CHOICES	RESPONSES
East North Central	14.55%
East South Central	4.69%
Middle Atlantic	18.78%
Mountain	6.10%
New England	2.82%
Pacific	16.43%
South Atlantic	23.00%
West North Central	4.69%
West South Central	8.92%

Snap Social Media Survey

220

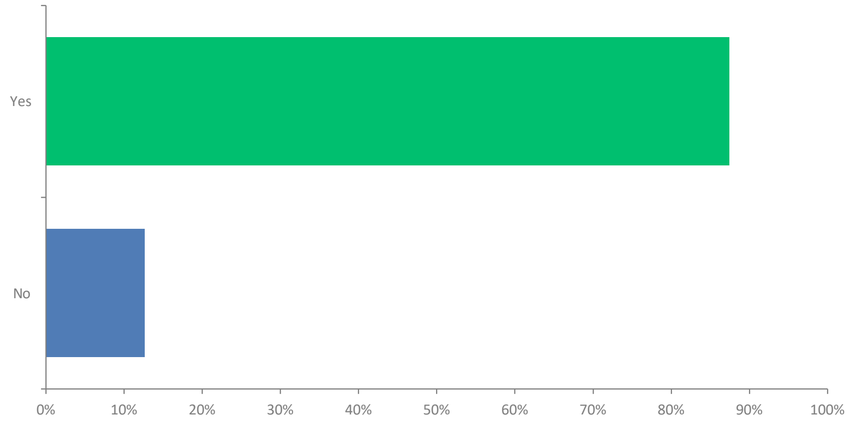
TOTAL RESPONSES

1. Have your company's social media account(s) been compromised or taken-over by an identity criminal?



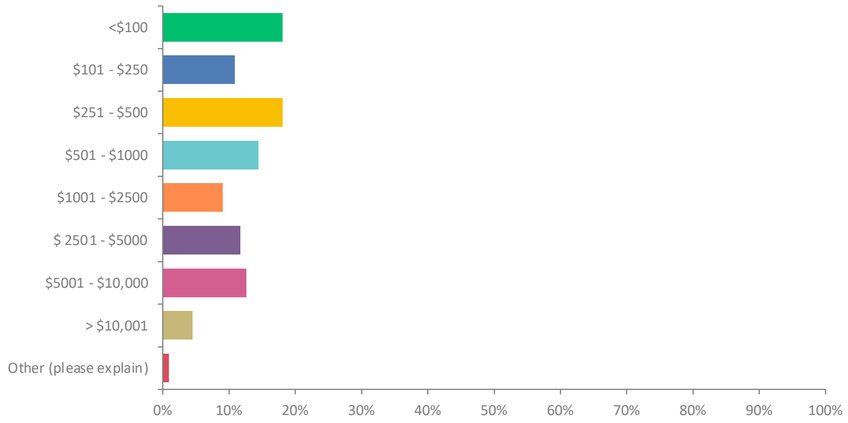
ANSWER CHOICES	RESPONSES
Yes	50.45%
No	49.55%
Both	0%
We have not experienced a security or data breach.	0%

2. Did you lose any revenue as a result of losing control of your social media account(s)?



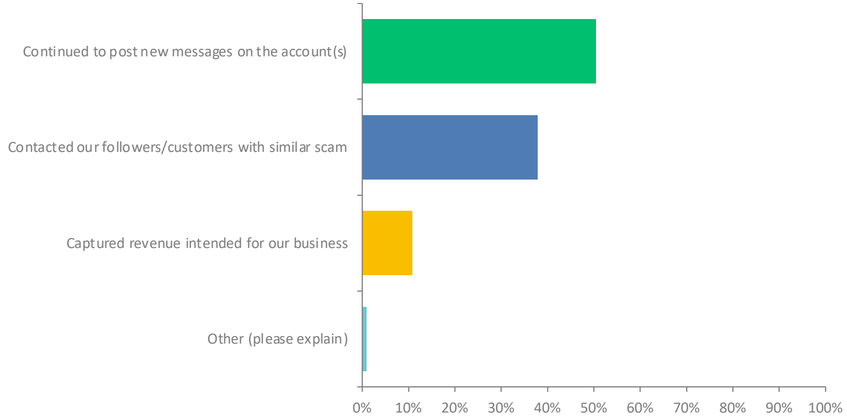
ANSWER CHOICES	RESPONSES
Yes	87.39%
No	12.61%

3. How much total revenue did you and/or your customers/ followers lose as a result of the social media account takeover?



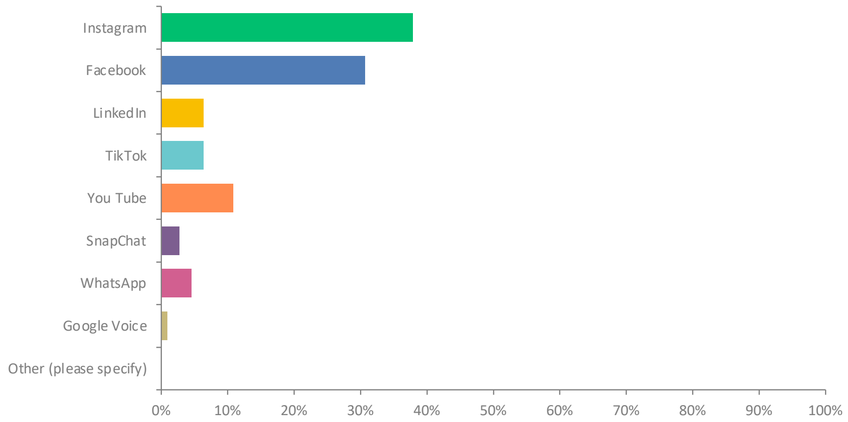
ANSWER CHOICES	RESPONSES
<$100	18.02%
$101 - $250	10.81%
$251 - $500	18.02%
$501 - $1000	14.41%
$1001 - $2500	9.01%
$ 2501 - $5000	11.71%
$5001 - $10,000	12.61%
> $10,001	4.50%
Other (please explain)	0.90%

4. Did the identity criminal take any of the following action?



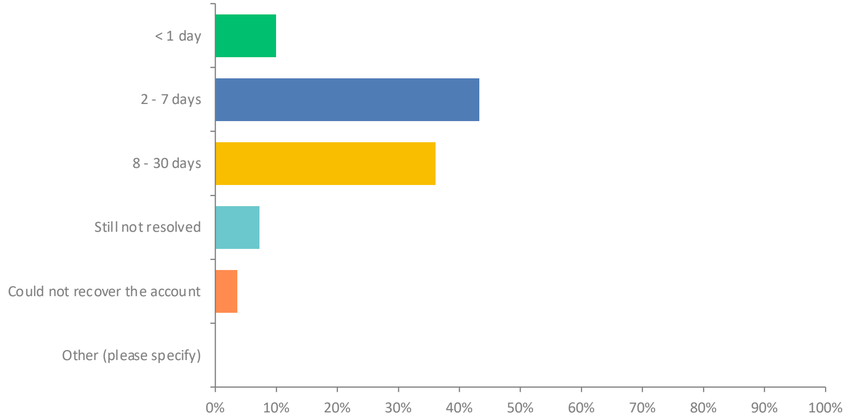
ANSWER CHOICES	RESPONSES
Continued to post new messages on the account(s)	50.45%
Contacted our followers/customers with similar scam	37.84%
Captured revenue intended for our business	10.81%
Other (please explain)	0.90%

5. Which account(s) were compromised? *(Check all that apply.)*



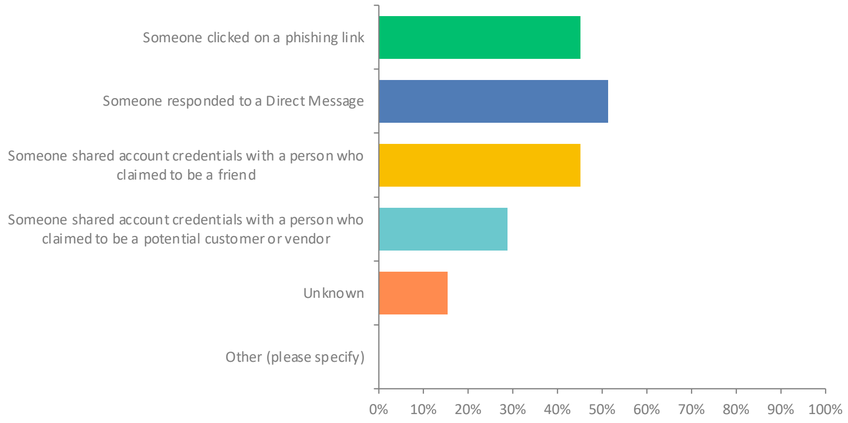
ANSWER CHOICES	RESPONSES
Instagram	37.84%
Facebook	30.63%
LinkedIn	6.31%
TikTok	6.31%
You Tube	10.81%
SnapChat	2.70%
WhatsApp	4.50%
Google Voice	0.90%

6. How long did it take you to recover your compromised account(s)?



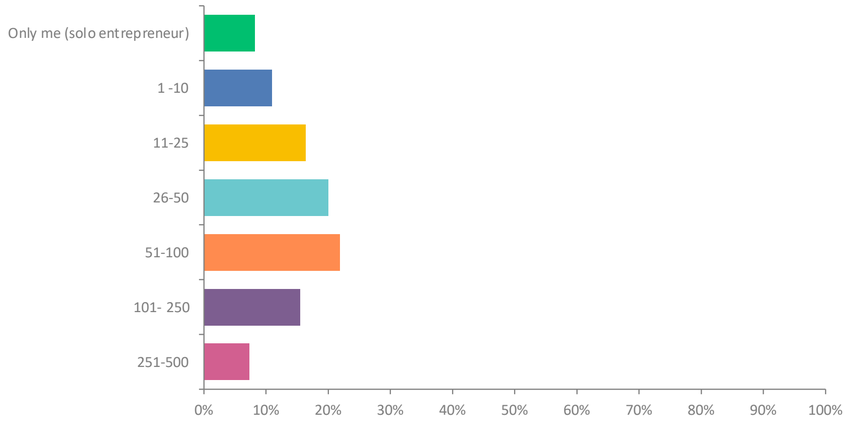
ANSWER CHOICES	RESPONSES
< 1 day	9.91%
2 - 7 days	43.24%
8 - 30 days	36.04%
Still not resolved	7.21%
Could not recover the account	3.60%
Other (please specify)	0%

7. What are the root cause(s) of the account takeover? *(Check all that apply.)*



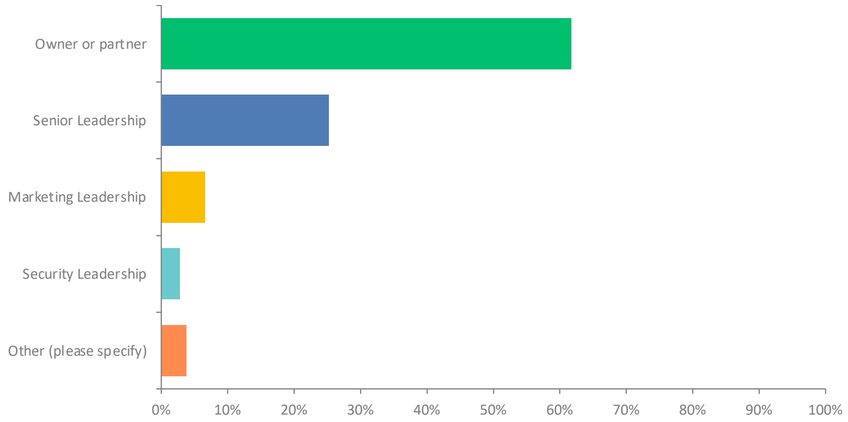
ANSWER CHOICES	RESPONSES
Someone clicked on a phishing link	45.05%
Someone responded to a Direct Message	51.35%
Someone shared account credentials with a person who claimed to be a friend	45.05%
Someone shared account credentials with a person who claimed to be a potential customer or vendor	28.83%
Unknown	15.32%
Other (please specify)	0%

8. How many employees, including you, are in your company?



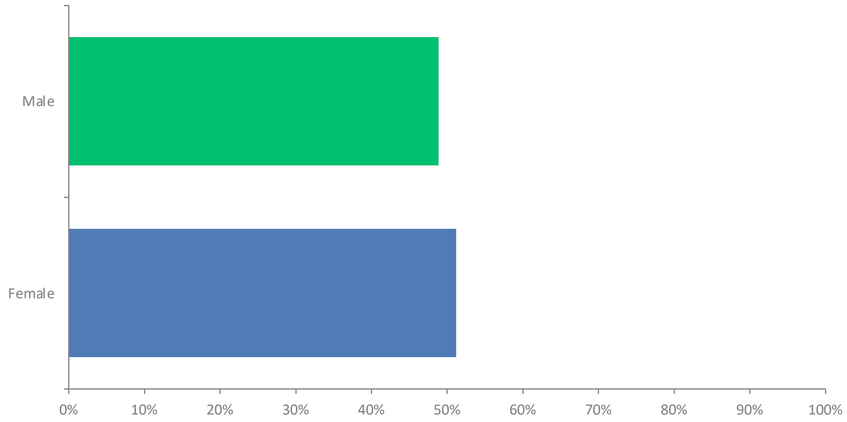
ANSWER CHOICES	RESPONSES
Only me (solo entrepreneur)	8.18%
1 -10	10.91%
11-25	16.36%
26-50	20.0%
51-100	21.82%
101- 250	15.45%
251-500	7.27%

9. What is your role?



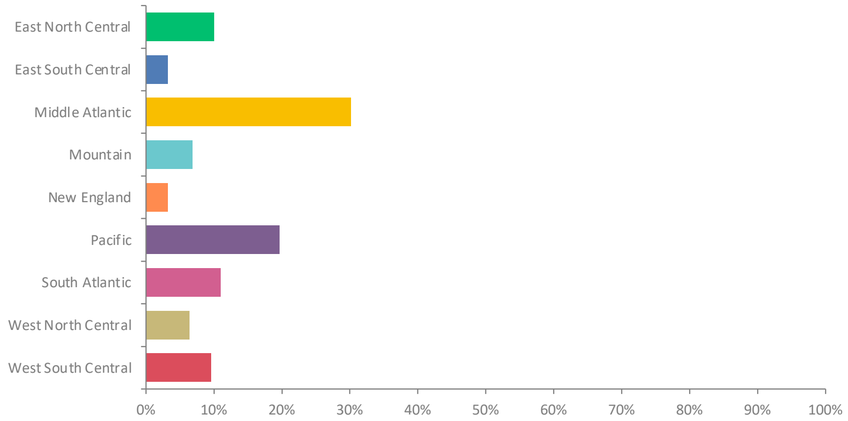
ANSWER CHOICES	RESPONSES
Owner or partner	61.68%
Senior Leadership	25.23%
Marketing Leadership	6.54%
Security Leadership	2.80%
Other (please specify)	3.74%

10. Gender



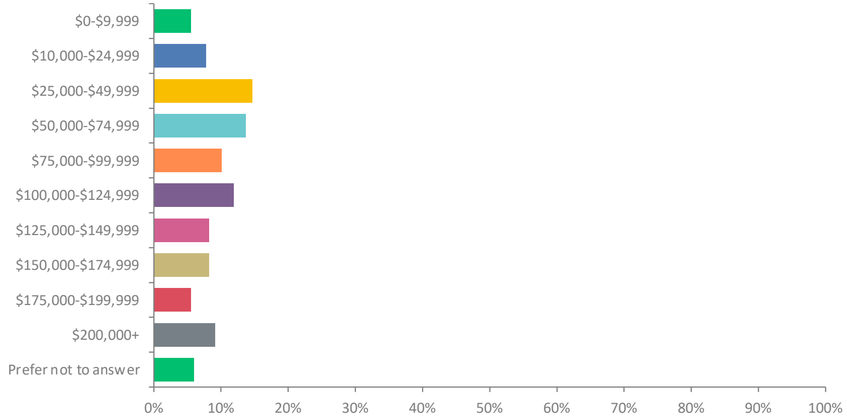
ANSWER CHOICES	RESPONSES
Male	48.86%
Female	51.14%

11. Region



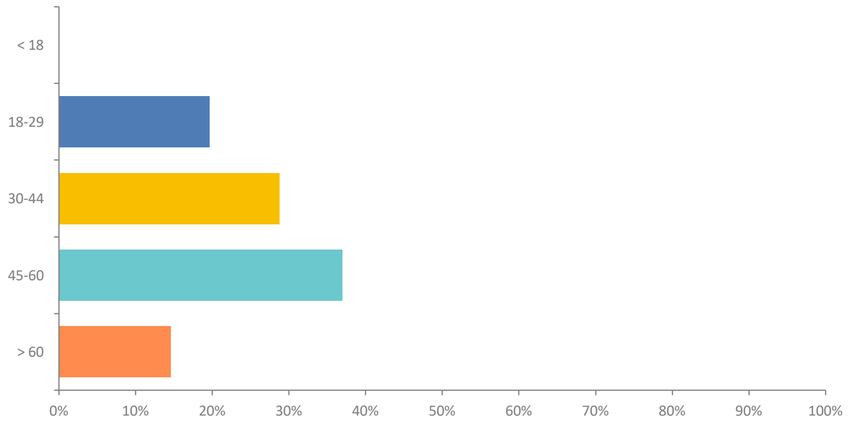
ANSWER CHOICES	RESPONSES
East North Central	10.05%
East South Central	3.20%
Middle Atlantic	30.14%
Mountain	6.85%
New England	3.20%
Pacific	19.63%
South Atlantic	10.96%
West North Central	6.39%
West South Central	9.59%

12. Household Income



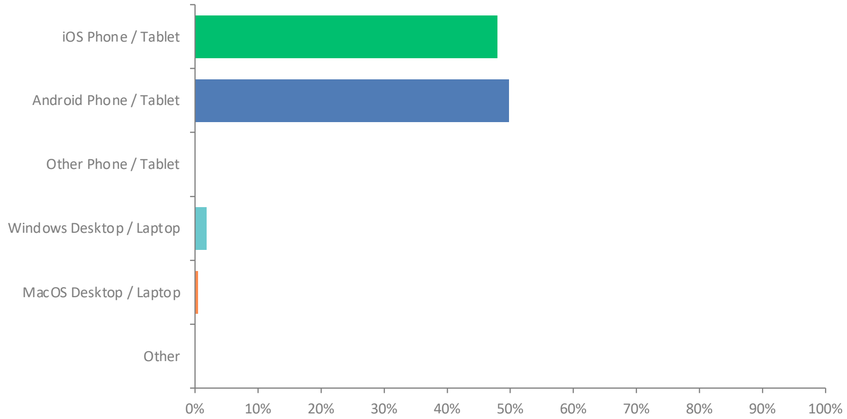
ANSWER CHOICES	RESPONSES
$0-$9,999	5.48%
$10,000-$24,999	7.76%
$25,000-$49,999	14.61%
$50,000-$74,999	13.70%
$75,000-$99,999	10.05%
$100,000-$124,999	11.87%
$125,000-$149,999	8.22%
$150,000-$174,999	8.22%
$175,000-$199,999	5.48%
$200,000+	9.13%
Prefer not to answer	5.94%

13. Age



ANSWER CHOICES	RESPONSES
< 18	0%
18-29	19.63%
30-44	28.77%
45-60	36.99%
> 60	14.61%

14. Device Type



ANSWER CHOICES	RESPONSES
iOS Phone / Tablet	47.95%
Android Phone / Tablet	49.77%
Other Phone / Tablet	0%
Windows Desktop / Laptop	1.83%
MacOS Desktop / Laptop	0.46%
Other	0%