2021 BUSINESS AFTERMATH FINDINGS

Insights on Small Business Identity and Cybercrimes

ITRC | IDENTITY THEFT RESOURCE CENTER

21 Years of Service

idtheftcenter.org • 1-888-400-5530

Letter from the CEO

Eva C. Velasquez
(President & CEO, ITRC)
October 2021

Welcome to the Identity Theft Resource Center's inaugural Business Aftermath Report, a first-of-its-kind look at the impacts of identity crimes on small businesses including gig workers and solopreneurs. Like our earlier **2021 Consumer Aftermath Report** that focused on how identity crimes affect individuals, this eye-opening research shows the scope and scale of cyberattacks and identity compromises on the businesses least equipped to prevent or readily respond to a cybercrime.

When the ITRC was created in 1999, most identity crimes and data compromises were relatively simple. Lost or stolen documents, mail removed from curbside mailboxes, dumpster diving, and shoulder surfing were the norm. No one really considered businesses as victims of these crimes because they weren't the actual target, or the person harmed.

Not so today. Readers of our **notified data breach tracking tool** and reports know that most identity crimes today begin with a cyberattack against a business. Increasingly, those attacks are against small businesses that lack the staff, expertise, and resources to defend themselves.

Another change has occurred during the past 20 years that has a direct bearing on small businesses: There are a lot more of them, most of which have only one person in the company. There were 15M single person small businesses in 1997 according to the **U.S. Small Business Administration**. Today there are ~42M "solopreneurs" based on a 2019 report from the brand strategy group **Spencer Brenneman**. That number goes up to 57M if you include gig workers.

There is 15+ years of information from multiple sources about the impacts of identity and cybercrimes on large organizations that tend to have large staffs of cybersecurity professionals. There are no equivalent comprehensive studies on how businesses with employee headcounts of 0 to 500 employees, the official SBA definition of a small business, recover from cyber events.

That is, until today.

When we began to look to see how small businesses were being impacted by the rise in identity crimes and cyberattacks, we immediately realized there was very little statistically valid information. What information that did exist was often wrong or so outdated as to be less then useful. As a result, we set out to find accurate information by seeking input directly from the small business owners and leaders impacted by these crimes.

This is our first Business Aftermath Report and we're pleased to share what we've found with you. We want this to be a living document, though, that adapts and shifts over time to ensure we keep the focus where it belongs – on the victims of identity crimes including businesses. To that end, I hope you will share your thoughts on this report and provide suggestions on how we might improve it next year. Send me an email at **ceo@idtheftcenter.org**.

Just as with our Consumer Aftermath Report (CAR) 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.

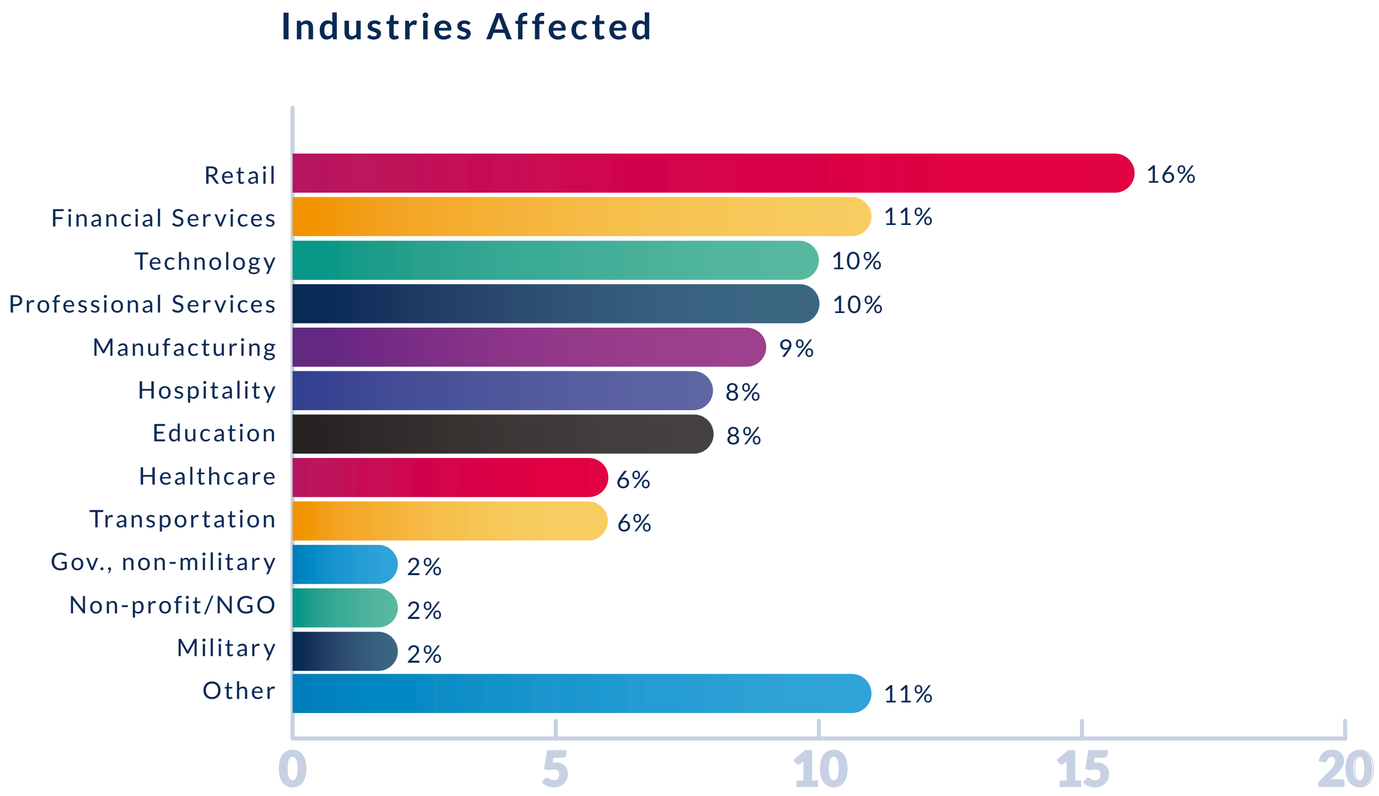
Methodology

The ITRC, with the assistance of SurveyMonkey (now Momentive) and DIG.Works, conducted two surveys to explore the impacts of cybercrimes on small businesses as defined by the U.S. Small Business Administration. Specifically, security and data breaches.

The SurveyMonkey online questionnaire was completed by 417 individuals that met the criteria of being a person in a leadership position or a IT professional at a company of 500 or fewer employees.

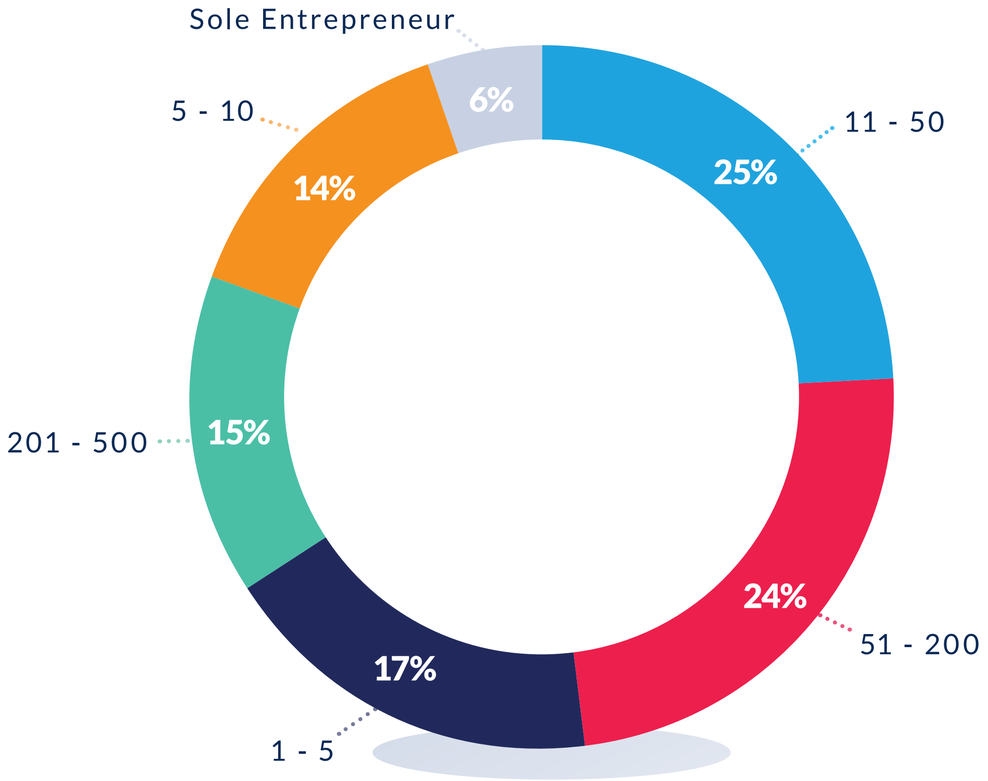
The DIG.Works findings resulted in 1,050 responses to an online survey of general consumers who were asked if they worked for an organization of 50 employees or less; and, if so, has their employer experienced a data breach. The results of these questions are reported separately.

Together, these surveys paint a portrait of small organizations and individuals that are significantly impacted by cybercrimes, often multiple times in relatively short periods of time.



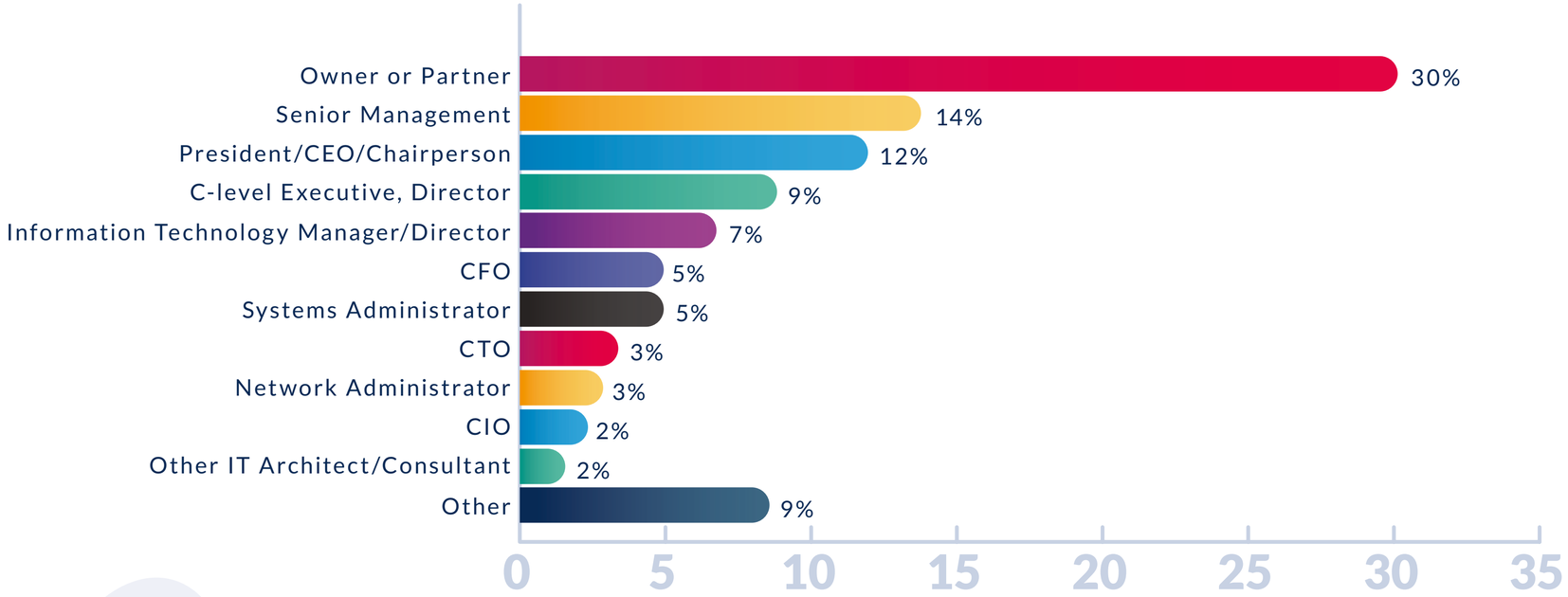
Top Responses

Company Employee Count



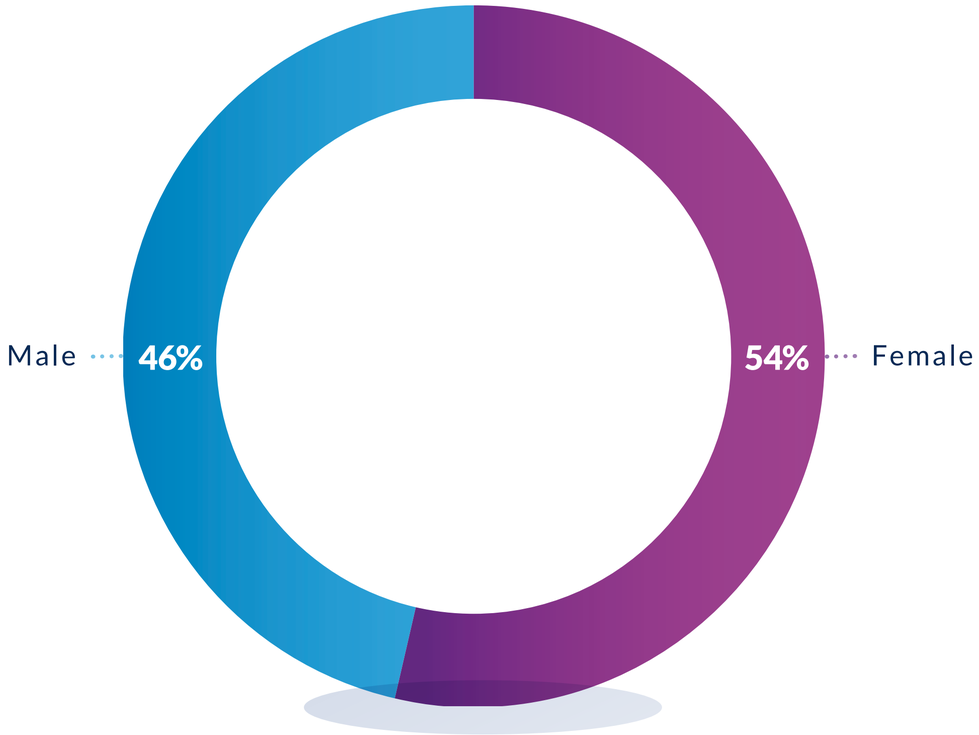
Top Responses

Title of Respondent (Position in Company)

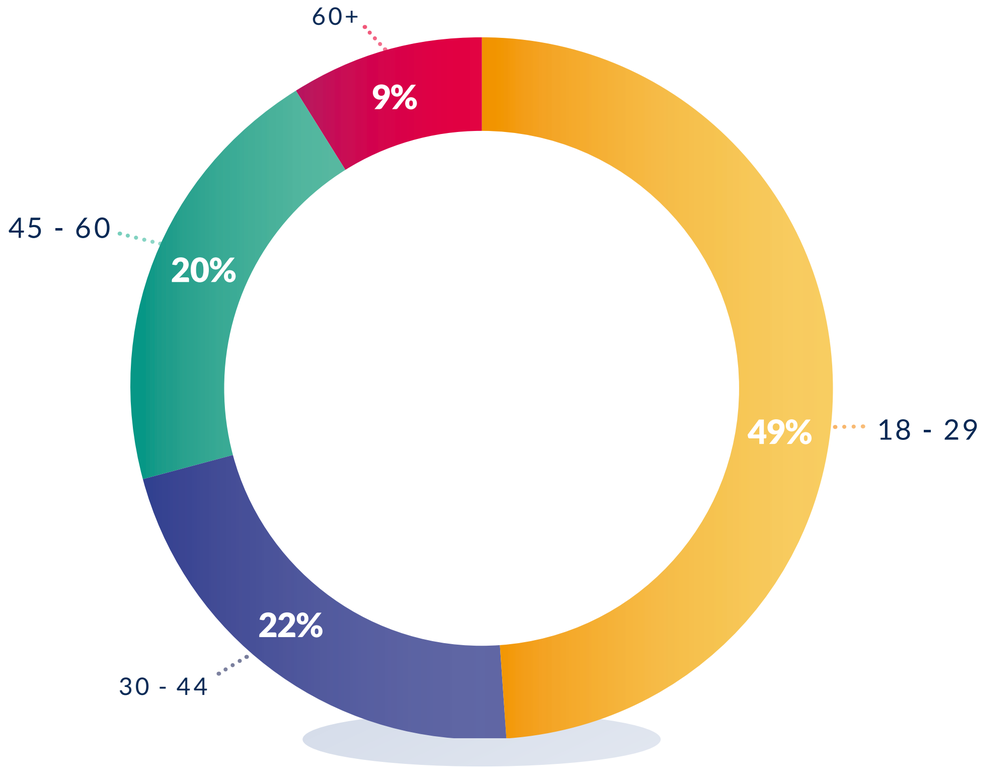


Top Responses

Gender of Respondent



Age of Respondent



2021 BUSINESS AFTERMATH FINDINGS

idtheftcenter.org • 1-888-400-5530

ITRC | IDENTITY THEFT™ RESOURCE CENTER
21 Years of Service

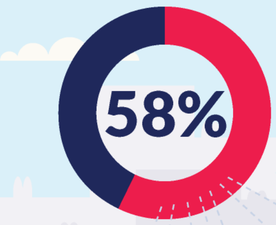
Welcome to the Identity Theft Resource Center's inaugural Business Aftermath Report, a first-of-its-kind look at the impacts of identity crimes on small businesses including gig workers and solopreneurs. For this report we surveyed small business owners, leaders, and employees to learn if, and how, they were impacted by security breaches, data breaches, or both.

How Big is Small Business?

- The U.S. Small Business Administration defines a small business as having fewer than 500 full-time employees.
- There at 31.7 small businesses in the U.S.
- 25.7 million small businesses have no employees.
- As many has 57 million people work as independent contractors (gig workers).

Sources: The U.S. Small Business Administration; Spencer Brenneman

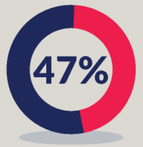
Please view our full report for methodology at idtheftcenter.org



MORE THAN HALF of **small businesses** have experienced at least one security breach or one data breach, **or both.**

have experienced **2 or more** breaches

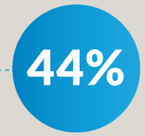
have experienced **3 or more** breaches



implemented new security tools to **prevent** future occurrences

of people who work for or own a small business say they have experienced **at least one data breach** or have been the **victim of identity theft.** *[According to DIG.Works]*

It's a **devastating** price tag for small businesses to cover their breach costs...



Paid between **$250K** and **$500K**

Paid between **$500K** and **$1M**

recovery time to return business to normal is a **slow process**

1 - 2 years for recovery

3 - 5 years for recovery

have not fully recovered

dipped into **cash reserves**

reduced staff to save on expenses

Incurred debt to cover costs

Key Findings

Scope and **Frequency**

More than half of small businesses have experienced at least one security breach or one data breach, **or both**

- **16%** — **data breach**
- **22%** — **security breach**
- **20%** — **both**

Small businesses have **frequently experienced** data breaches

- **25%** — **past 12 months**
- **54%** — **1 - 2 yrs**
- **11%** — **3 - 4 yrs**
- **10%** — **5+ yrs**

IT was identified as the cause of most security breaches

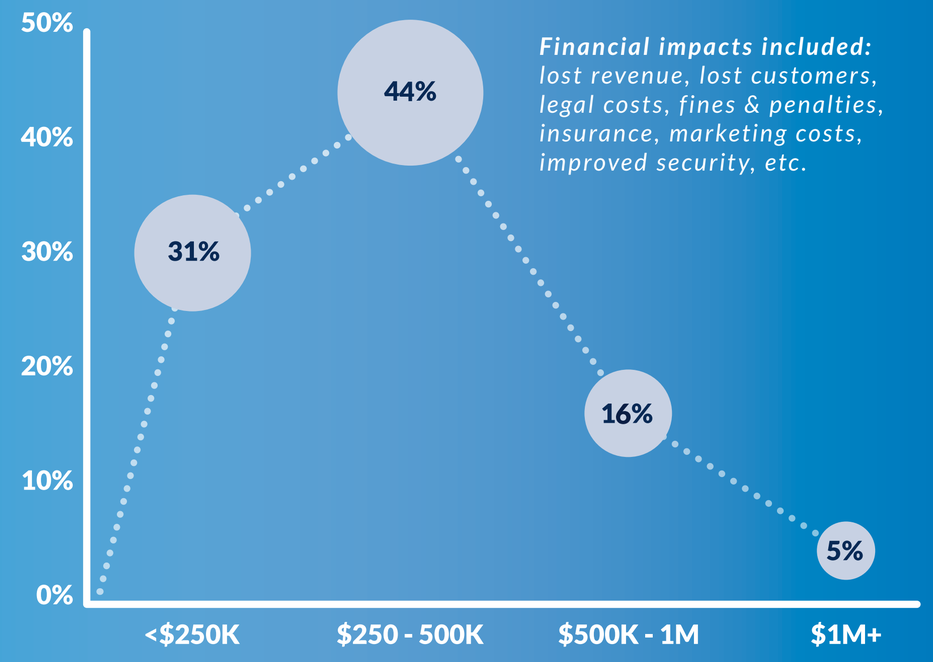
- **58%** — **information technology (IT)**
- **34%** — **operations technology (OT)**
- **8%** — **industrial internet of things (IoT)**

Financial Impact

Breaches forced small businesses to take **extreme measures and incur debt**

- **36%** took out loans or new lines of credit
- **34%** dipped into cash reserves
- **34%** utilized existing lines of credit, acquiring more debt
- **29%** utilized their cyber insurance proceeds
- **25%** reduced expenses
- **15%** reduced staff
- **14%** requested additional investor funding

Breaches financial impact on small businesses **could be detrimental to operations**



Financial impacts included: *lost revenue, lost customers, legal costs, fines & penalties, insurance, marketing costs, improved security, etc.*

Key Findings

Root Causes

External threats were the main cause of data breaches, followed closely by malicious insiders such as an employee

- **40%** external threat actor (hacker)
- **35%** malicious insider (employee or contractor)
- **25%** remote worker
- **22%** failure to secure a cloud environment
- **19%** third party vendor
- **17%** failure to patch known software flaw
- **13%** phishing scheme
- **13%** system error
- **10%** ransomeware attack
- **5%** human error
- **3%** unknown

Data at **Risk**

Customer and employee data is the **most compromised** PII

51%
employee data

49%
customer data

company intellectual property followed at 16%

Key Findings

Breach Response

Multiple breaches are a common occurrence for small business[1]

25%	41%	25%	8%
1 breach	2 breaches	3 breaches	4+ breaches

Post-breach measures to avoid repeat occurrences are important to small businesses

- **47%** implemented new security tools
- **44%** provided new training for IT staff
- **35%** provided new training for non-IT staff
- **34%** hired additional security staff
- **27%** increased budgets
- **19%** increased vendor due diligence

1. Dig.Works conducted pro-bono research for the ITRC on a variety of topics including data breaches at small businesses. Dig.Works findings were consistent with the ITRC's other results: 42 percent of SMB owners/employees responded that their business had experienced issues with data breaches / identity theft issues.

Remediation Services Offered

Breach notifications under state law were required

80% SAID **YES**

Of the **20%** who said they weren't required to send a breach notification...

***69%** did so anyway*

Types of **remediation offered**

- **54%** paid remediation services from a for-profit identity management provider, a cybersecurity company, or consumer reporting agency
- **29%** credit monitoring from a credit reporting agency
- **14%** access to free services from a non-profit
- **2%** none

Key Findings

Time to **Recover**

Time reported to return to **pre-breach** level performance

22%	42%	28%	7%
under 1 yr	**1 - 2 yrs**	**3 - 5 yrs**	**not fully recovered**

Small businesses are **enhancing** their **data protection procedures**

- **23%** have annual security training for staff
- **23%** have weekly/monthly/quarterly security updates with staff
- **14%** have annual security updates with staff
- **11%** offer Cybersecurity and/or ID Protection services as an employee benefit
- **10%** offer specialized training for remote workers
- **8%** implement employee incentives/bounty for alerting of ID vulnerabilities

2021 BUSINESS AFTERMATH FINDINGS

Insights on Small Business Identity and Cybercrimes

Acknowledgements

This report was created based on responses from small business owners, leaders, and employees using tools from SurveyMonkey (now Momentive) and from DIG. Works. Special thanks to Jonathan Sasse and Anders Steele of DIG.Works for their pro bono work on behalf of the ITRC to help increase awareness of the impact of identity crimes as well as ways to prevent them.

Consumer & Business Resources

For more information about low-cost identity education, protection, and recovery services for small businesses as well as the free services and education opportunities for consumers, visit idtheftcenter.org or by email at notified@idtheftcenter.org.

ITRC | IDENTITY THEFT RESOURCE CENTER
21 Years of Service

idtheftcenter.org • 1-888-400-5530

Coming Soon!

Annual Data Breach Report | January 2022

Sign up on our website for notifications

notified.idtheftcenter.org

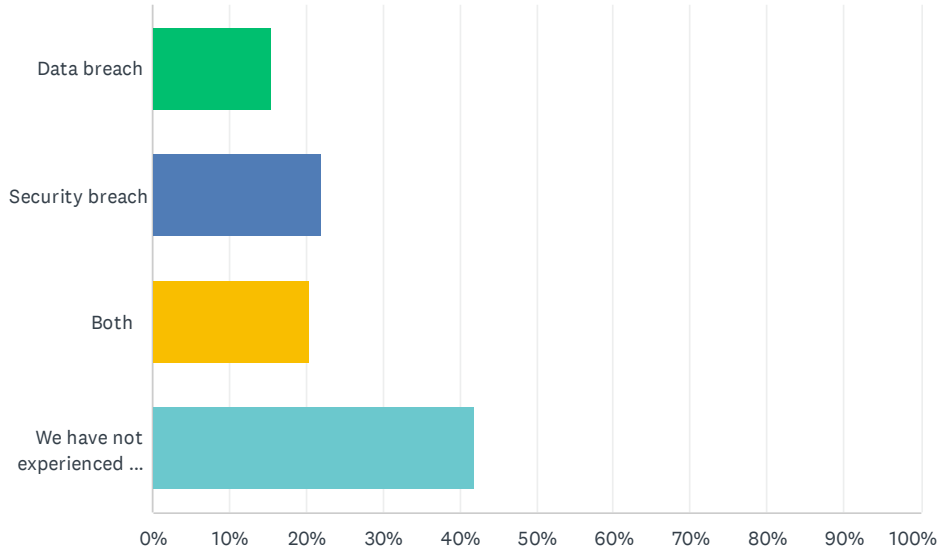
IDENTITY THEFT RESOURCE CENTER

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q1 Has your company ever experienced a security or data breach? *

Answered: 417 Skipped: 0



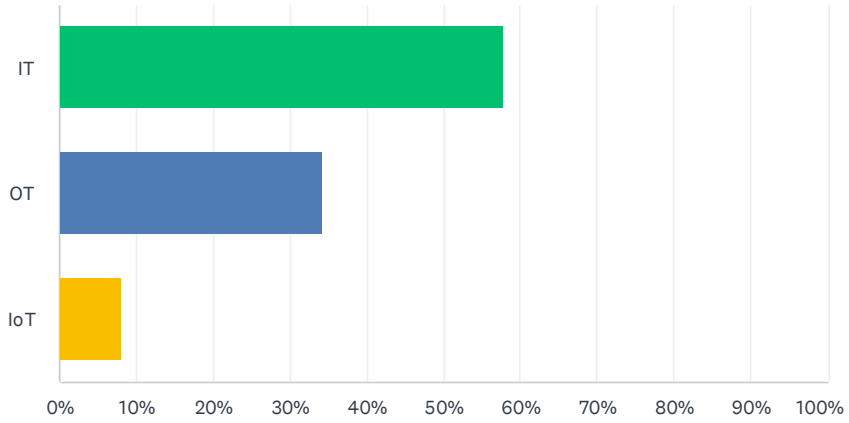
ANSWER CHOICES	RESPONSES
Data breach	15.59%
Security breach	22.06%
Both	20.38%
We have not experienced a security or data breach.	41.97%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q2 Did the security breach involve Information (IT) or Operational (OT) technologies?

Answered: 175 Skipped: 242



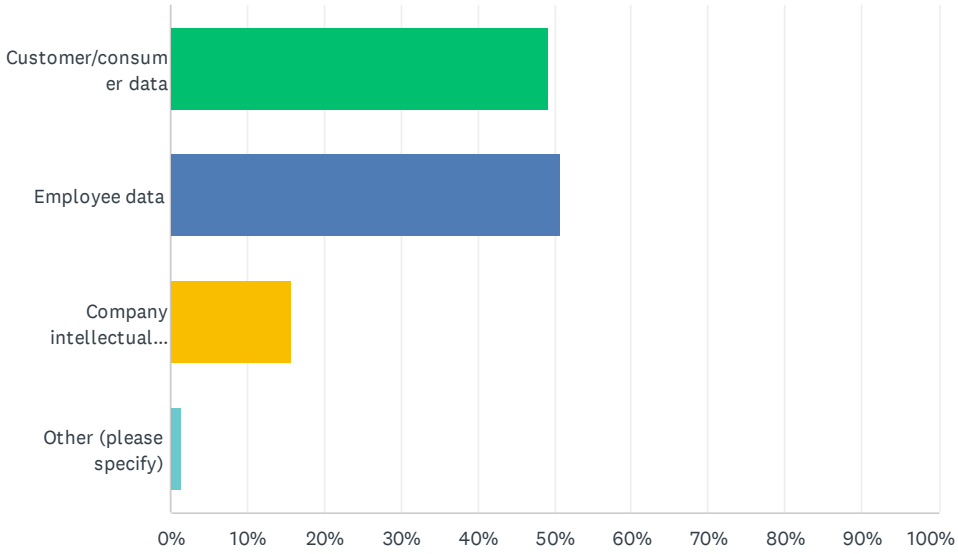
ANSWER CHOICES	RESPONSES
IT	57.71%
OT	34.29%
IoT	8.00%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q3 What data was compromised? * (Check all that apply)

Answered: 63 Skipped: 354



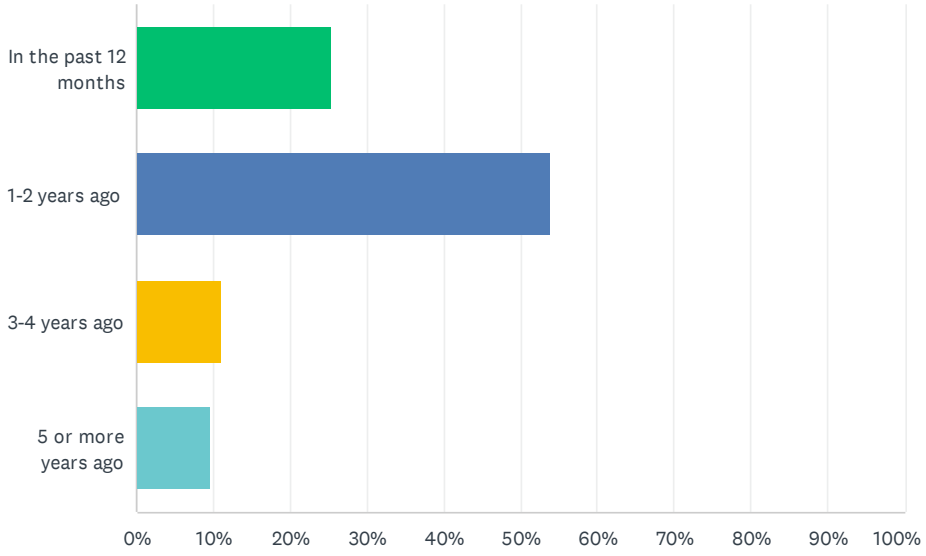
ANSWER CHOICES	RESPONSES
Customer/consumer data	49.21%
Employee data	50.79%
Company intellectual property	15.87%
Other (please specify)	1.59%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q4 When did you experience the most recent data breach? *

Answered: 63 Skipped: 354



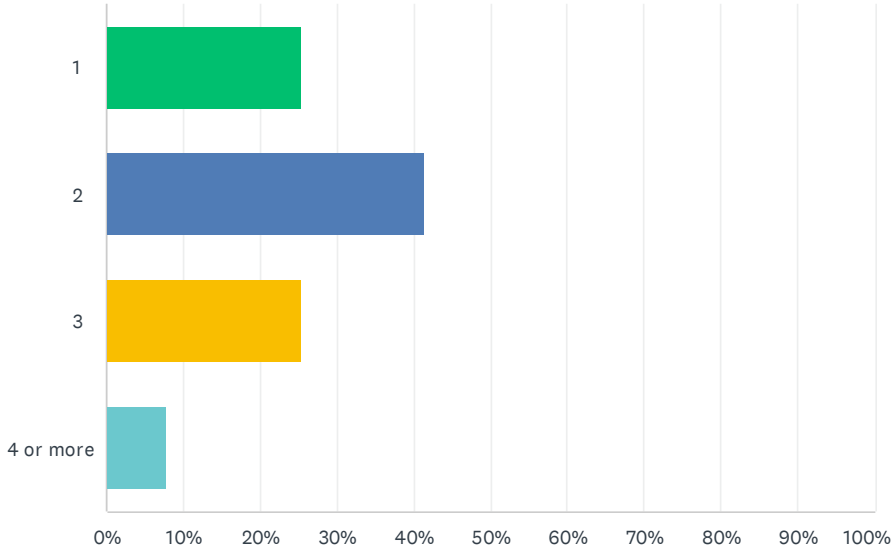
ANSWER CHOICES	RESPONSES
In the past 12 months	25.40%
1-2 years ago	53.97%
3-4 years ago	11.11%
5 or more years ago	9.52%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q5 How many times have you experienced a data breach?*

Answered: 63 Skipped: 354



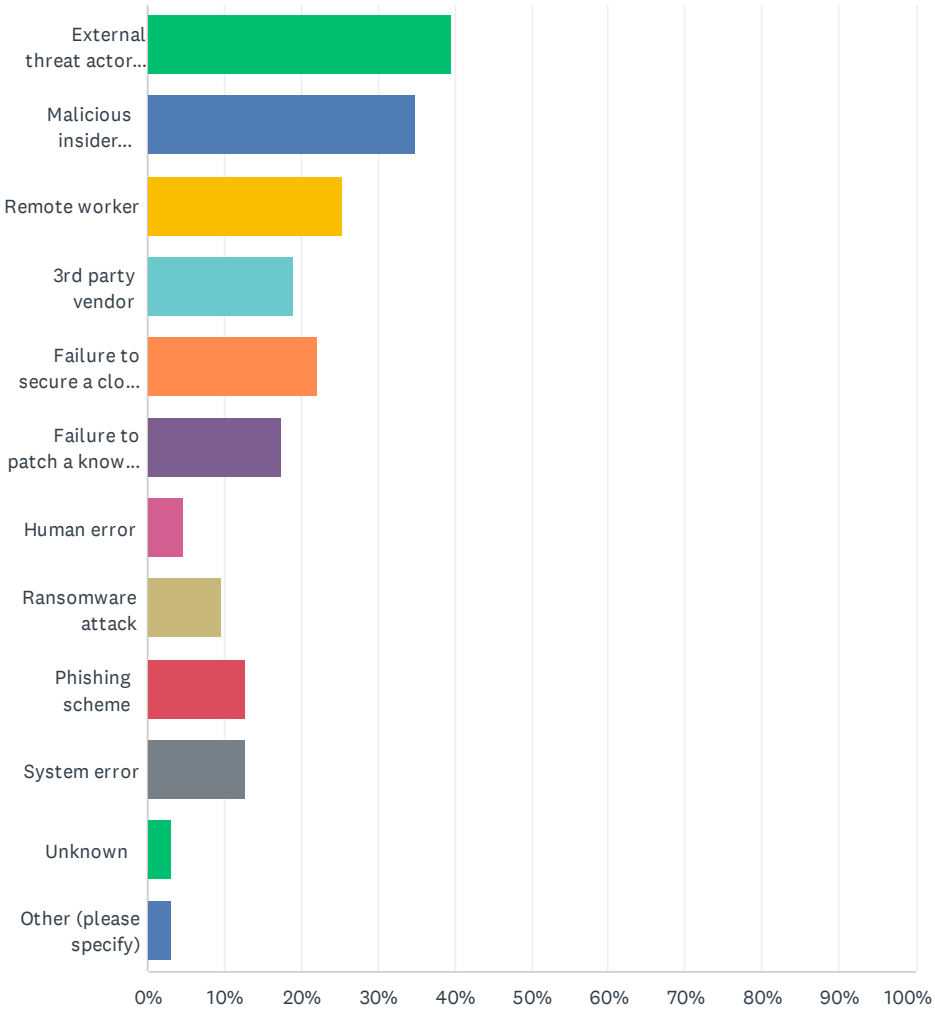
ANSWER CHOICES	RESPONSES
1	25.40%
2	41.27%
3	25.40%
4 or more	7.94%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q6 What was the root cause(s) of the data breach(es)? * (Check all that apply)

Answered: 63 Skipped: 354



(chart data continued on next page)

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

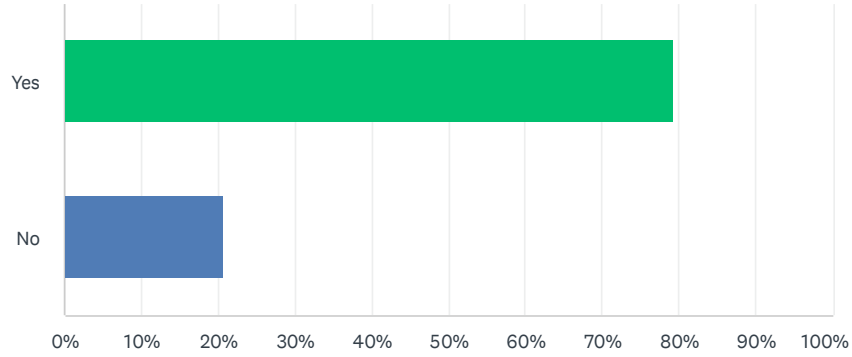
ANSWER CHOICES	RESPONSES
External threat actor (hacker)	39.68%
Malicious insider (employee or contractor)	34.92%
Remote worker	25.40%
3rd party vendor	19.05%
Failure to secure a cloud environment	22.22%
Failure to patch a known software flaw	17.46%
Human error	4.76%
Ransomware attack	9.52%
Phishing scheme	12.70%
System error	12.70%
Unknown	3.17%
Other (please specify)	3.17%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q7 Were you required to issue a public breach notice under state law or regulation? *

Answered: 63 Skipped: 354



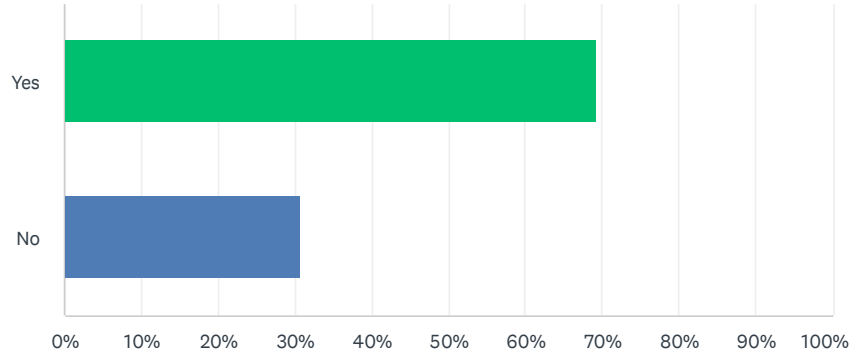
ANSWER CHOICES	RESPONSES
Yes	79.37%
No	20.63%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q8 Did you provide notice to your customers or consumers even though you were not required to do so?

Answered: 13 Skipped: 404



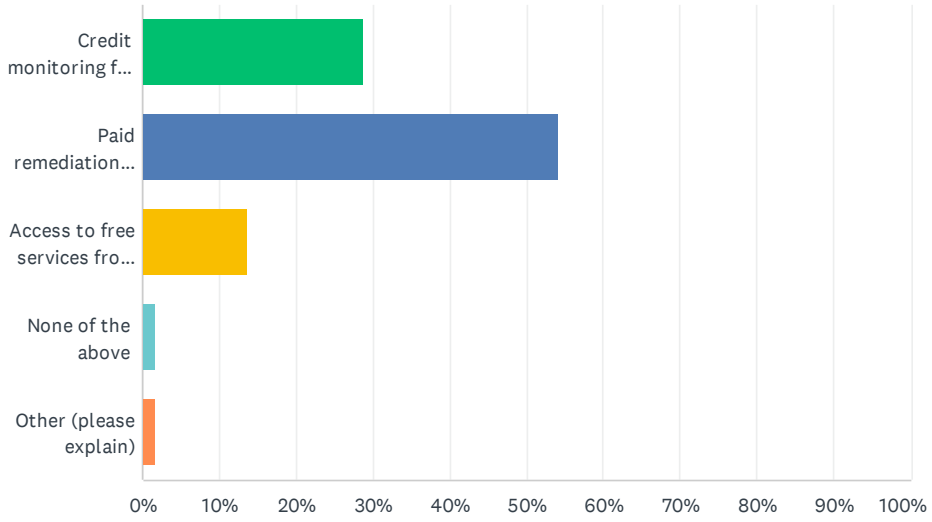
ANSWER CHOICES	RESPONSES
Yes	69.23%
No	30.77%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q9 Did you offer remediation services to customers or consumers impacted by the breach, such as:

Answered: 59 Skipped: 358



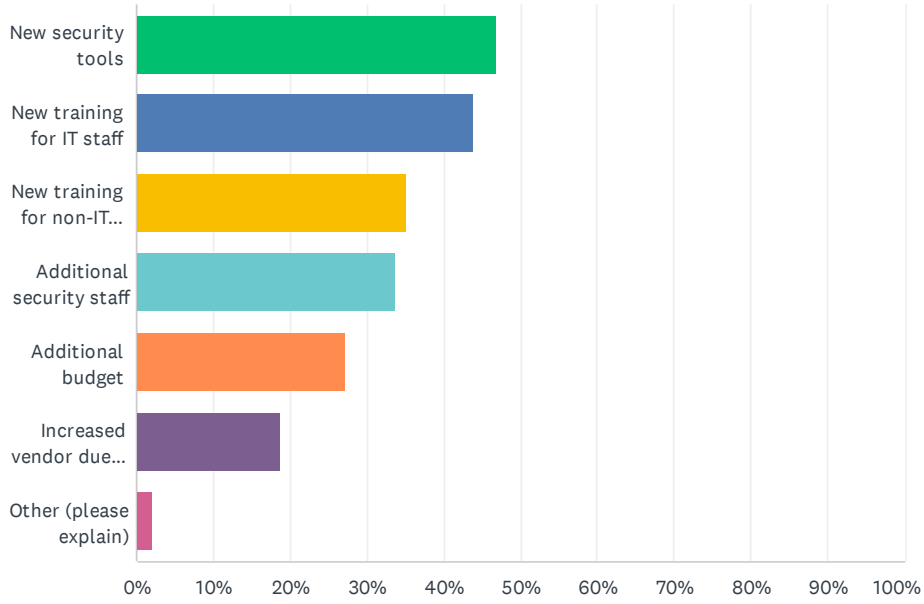
ANSWER CHOICES	RESPONSES
Credit monitoring from a credit reporting agency	28.81%
Paid remediation services from a for-profit identity management provider, a cybersecurity company, or consumer reporting agency	54.24%
Access to free services from a non-profit	13.56%
None of the above	1.69%
Other (please explain)	1.69%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q10 What steps have you taken to prevent a repeat occurrence? * (Check all that apply)

Answered: 228 Skipped: 189



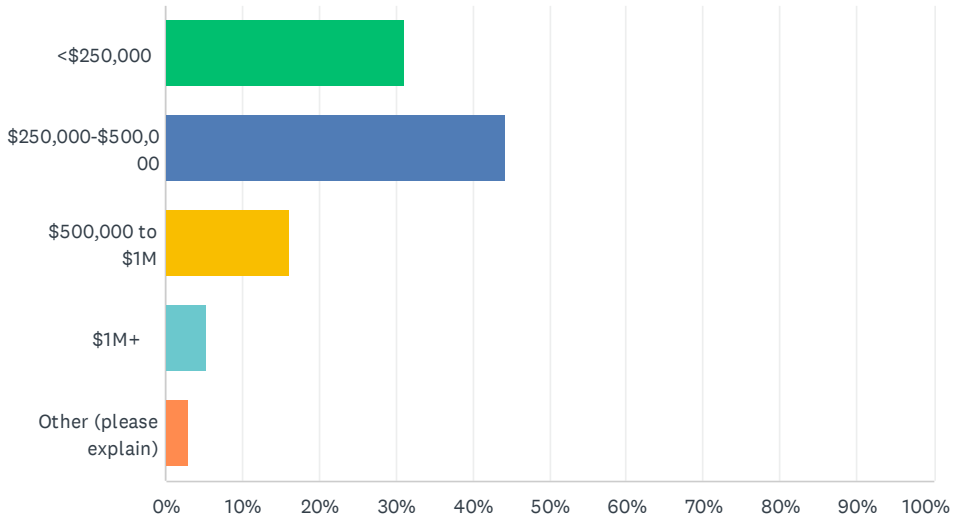
ANSWER CHOICES	RESPONSES
New security tools	46.93%
New training for IT staff	43.86%
New training for non-IT staff	35.09%
Additional security staff	33.77%
Additional budget	27.19%
Increased vendor due diligence	18.86%
Other (please explain)	2.19%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q11 What was the approximate total financial impact of the breach, including lost revenue, lost customers, legal costs, fines & penalties, insurance, marketing costs, improved security, etc?

Answered: 228 Skipped: 189



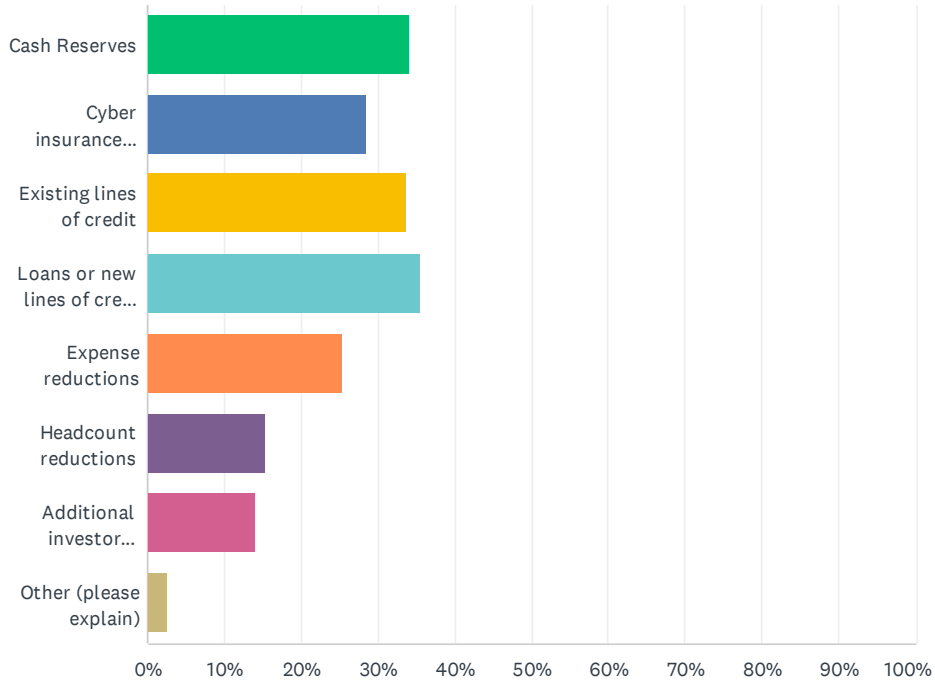
ANSWER CHOICES	RESPONSES
<$250,000	31.14%
$250,000-$500,000	44.30%
$500,000 to $1M	16.23%
$1M+	5.26%
Other (please explain)	3.07%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q12 How did you address the financial impacts of the breach? * (Select all that apply)

Answered: 228 Skipped: 189



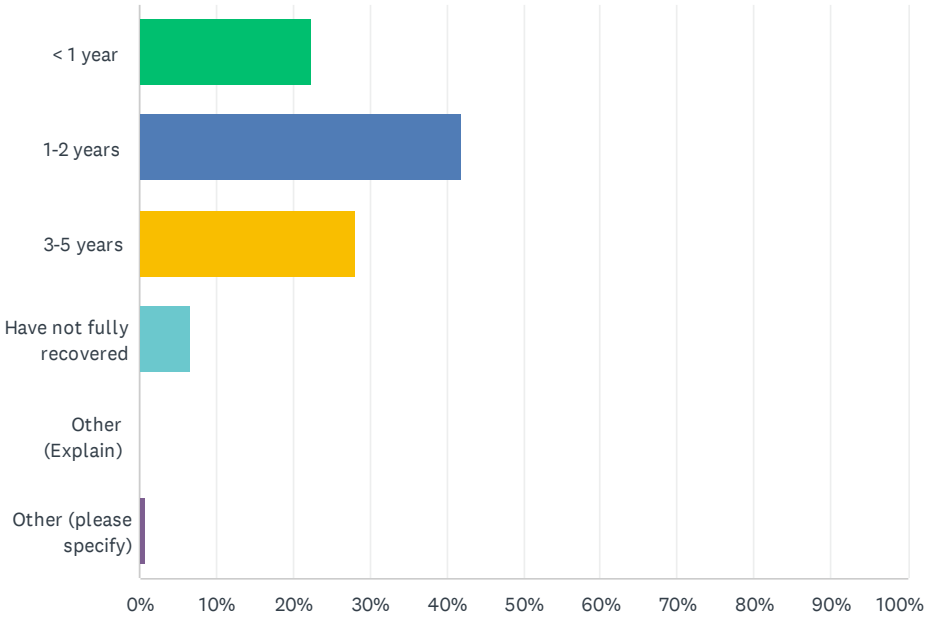
ANSWER CHOICES	RESPONSES
Cash Reserves	34.21%
Cyber insurance proceeds	28.51%
Existing lines of credit	33.77%
Loans or new lines of credit	35.53%
Expense reductions	25.44%
Headcount reductions	15.35%
Additional investor funding (e.g. - VC or PE)	14.04%
Other (please explain)	2.63%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q13 How long did it take your business to return to pre-breach levels of performance?

Answered: 228 Skipped: 189



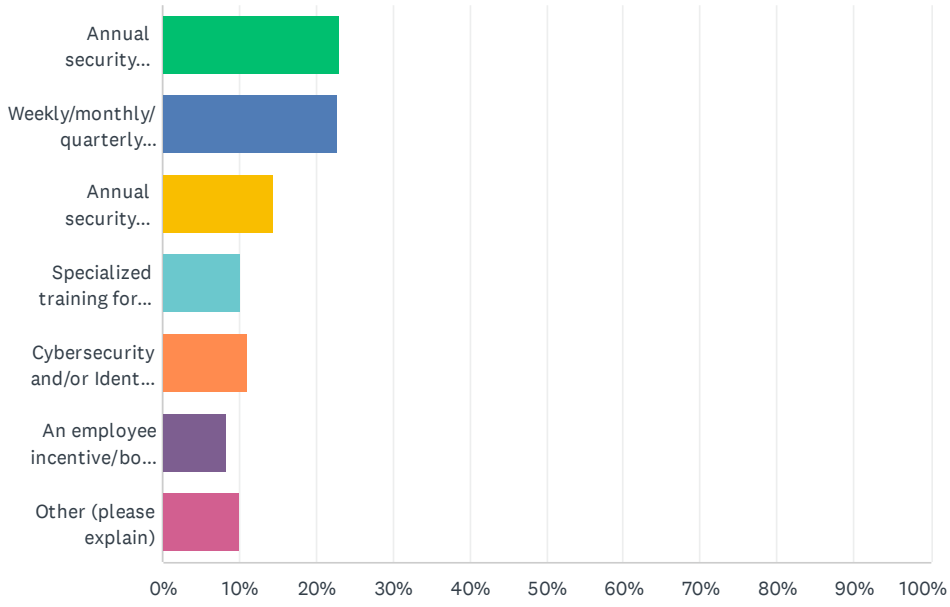
ANSWER CHOICES	RESPONSES
< 1 year	22.37%
1-2 years	42.11%
3-5 years	28.07%
Have not fully recovered	6.58%
Other (Explain)	0.00%
Other (please specify)	0.88%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q14 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)

Answered: 387 Skipped: 30



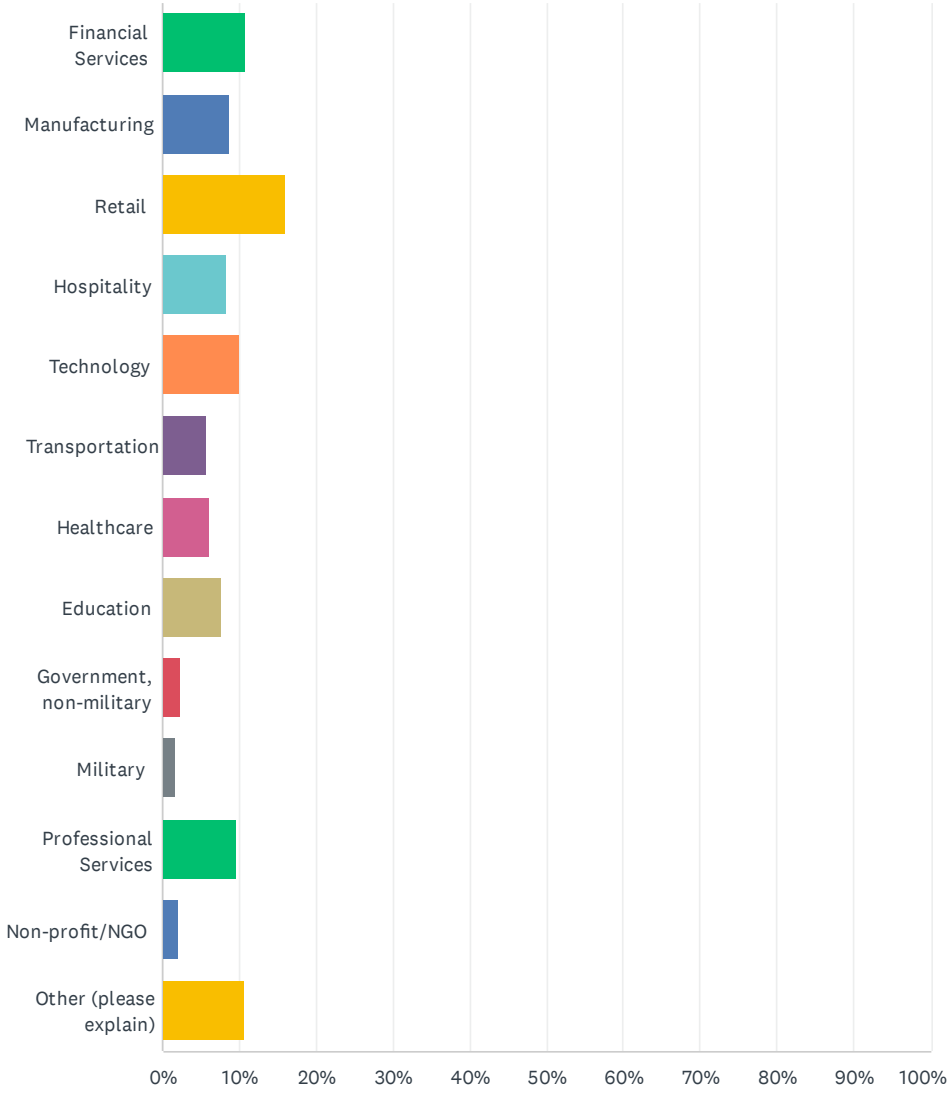
ANSWER CHOICES	RESPONSES
Annual security training for all staff	23.00%
Weekly/monthly/quarterly security updates with all staff	22.74%
Annual security updates with all staff	14.47%
Specialized training for remote workers	10.34%
Cybersecurity and/or Identity Protection services as an employee benefit	11.11%
An employee incentive/bounty for identifying vulnerabilities and/or vulnerable behaviors	8.27%
Other (please explain)	10.08%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q15 What is your industry? *

Answered: 387 Skipped: 30



(chart data continued on next page)

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

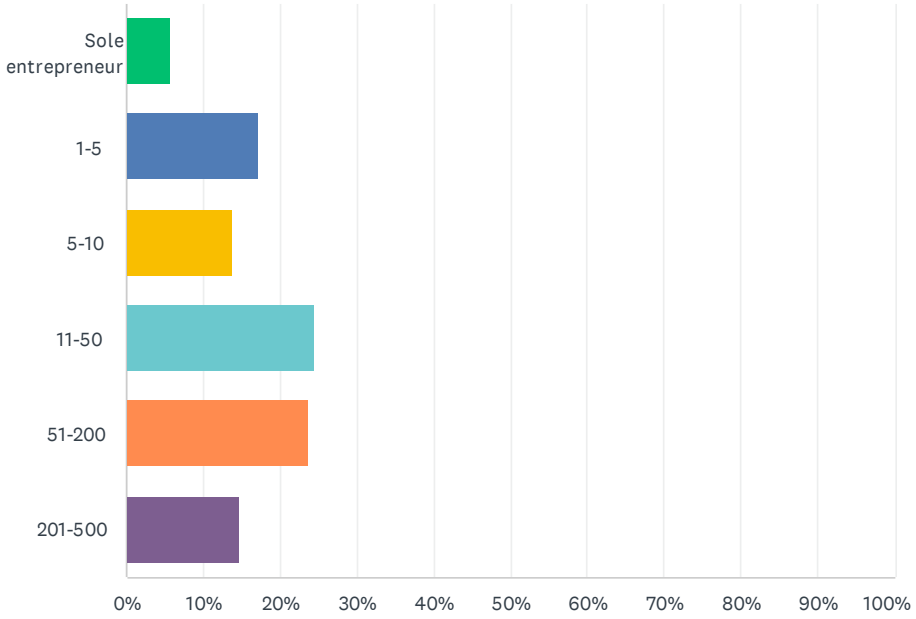
ANSWER CHOICES	RESPONSES
Financial Services	10.85%
Manufacturing	8.79%
Retail	16.02%
Hospitality	8.27%
Technology	10.08%
Transportation	5.68%
Healthcare	6.20%
Education	7.75%
Government, non-military	2.33%
Military	1.81%
Professional Services	9.56%
Non-profit/NGO	2.07%
Other (please explain)	10.59%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q16 How many employees are in your company?

Answered: 387 Skipped: 30



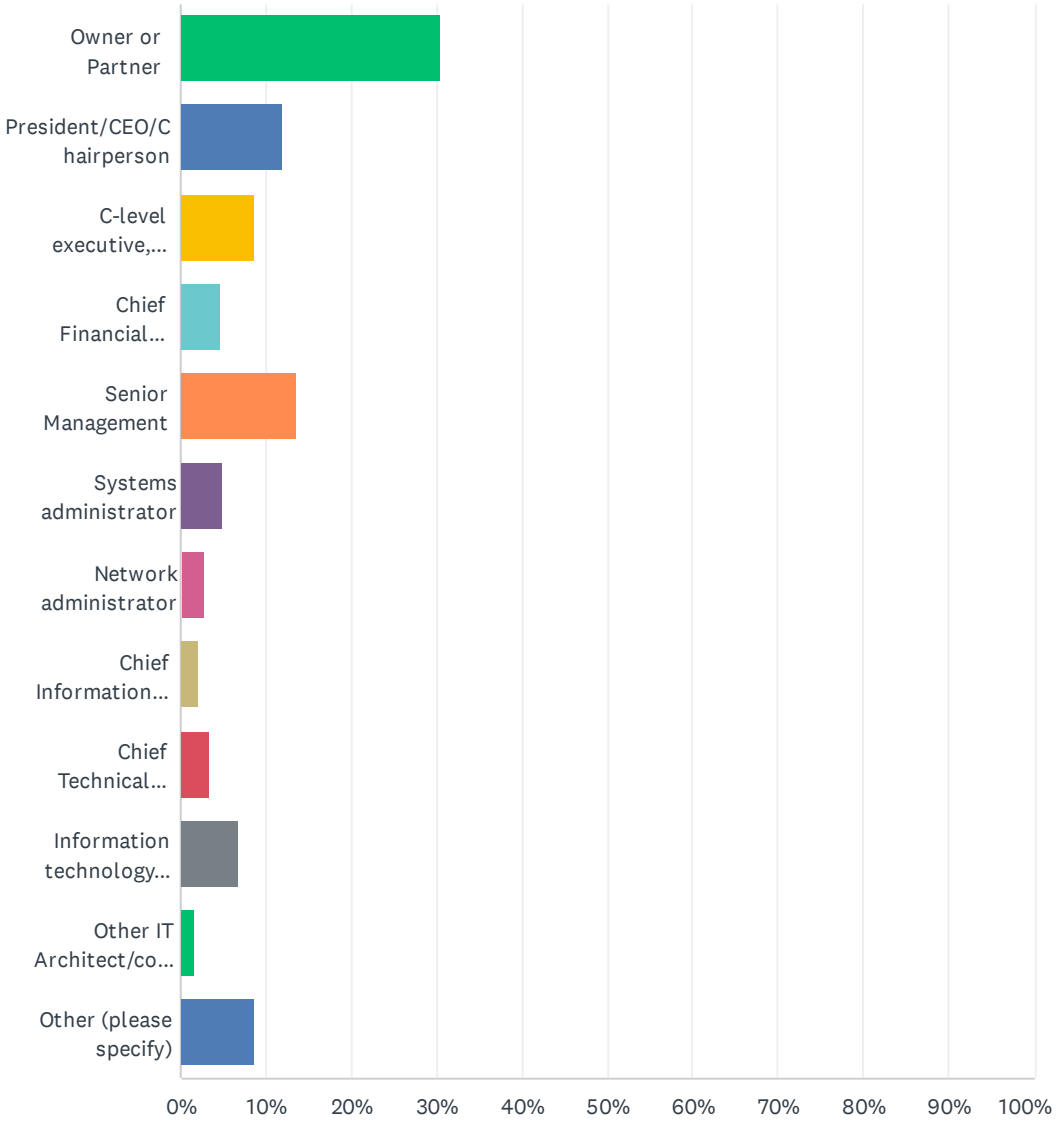
ANSWER CHOICES	RESPONSES
Sole entrepreneur	5.68%
1-5	17.31%
5-10	13.95%
11-50	24.55%
51-200	23.77%
201-500	14.73%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q17 What is your title?

Answered: 387 Skipped: 30



(chart data continued on next page)

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

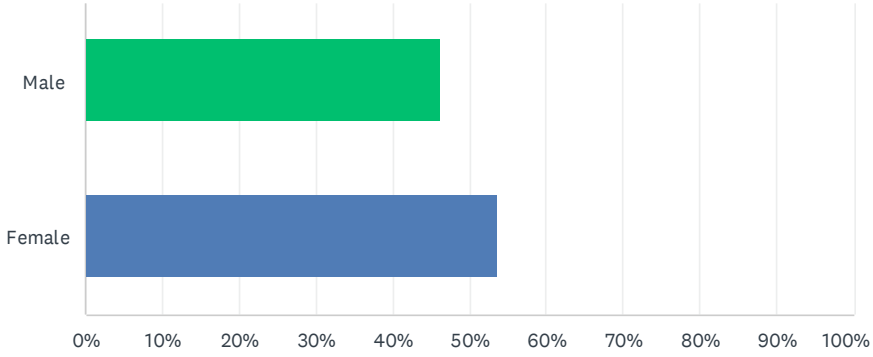
ANSWER CHOICES	RESPONSES
Owner or Partner	30.49%
President/CEO/Chairperson	11.89%
C-level executive, Director	8.79%
Chief Financial Officer (CFO)	4.65%
Senior Management	13.70%
Systems administrator	4.91%
Network administrator	2.84%
Chief Information Officer (CIO)	2.07%
Chief Technical Officer (CTO)	3.36%
Information technology manager/director	6.72%
Other IT Architect/consultant	1.81%
Other (please specify)	8.79%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q18 Gender

Answered: 350 Skipped: 67



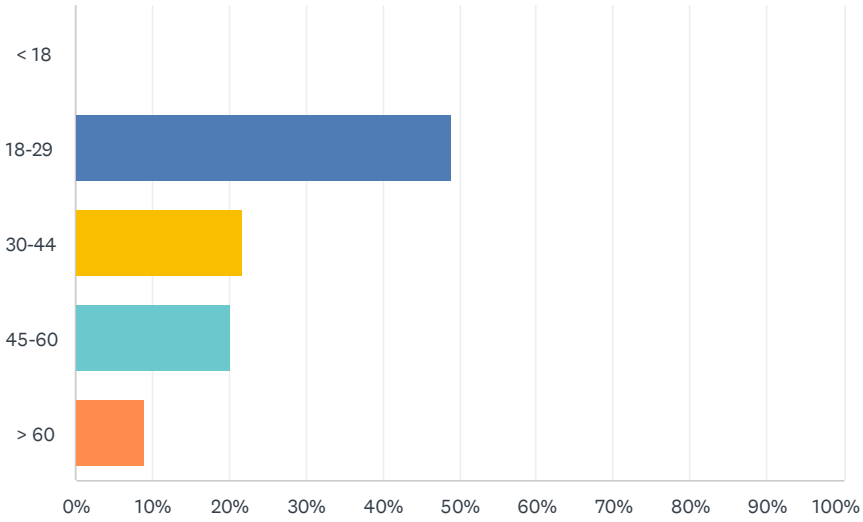
ANSWER CHOICES	RESPONSES
Male	46.29%
Female	53.71%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q19 Age

Answered: 350 Skipped: 67



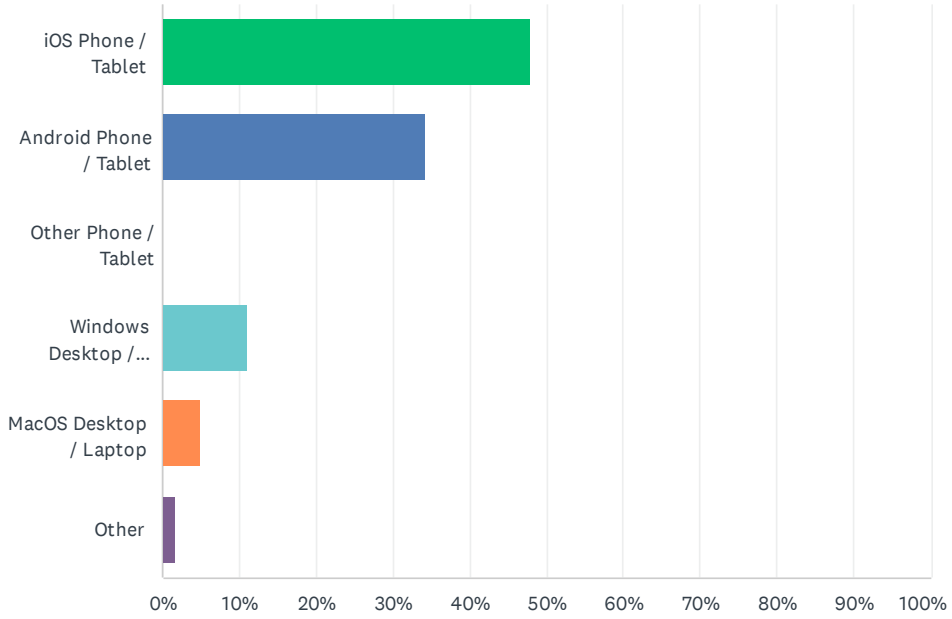
ANSWER CHOICES	RESPONSES
< 18	0.00%
18-29	49.14%
30-44	21.71%
45-60	20.29%
> 60	8.86%

2021 **Business Aftermath** Study

Insights on Small Business Identity Cybercrimes

Q20 Device Type

Answered: 350 Skipped: 67



ANSWER CHOICES	RESPONSES
iOS Phone / Tablet	48.00%
Android Phone / Tablet	34.29%
Other Phone / Tablet	0.00%
Windows Desktop / Laptop	11.14%
MacOS Desktop / Laptop	4.86%
Other	1.71%