OCTOBER 2023

ITRC | IDENTITY THEFT RESOURCE CENTER

2023 BUSINESS IMPACT REPORT

idtheftcenter.org • 1-888-400-5530

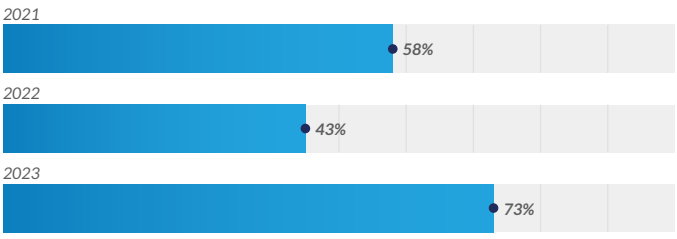
Table of Contents

CEO Letter

Once upon a time, it was true that small businesses and solopreneurs were not a favorite target for cybercriminals. Attackers tended to go for larger, data-rich organizations with lots of cash and thousands of employees, where the law of averages meant it was easier to find someone to fall for a phishing attack.

That hasn't been true since at least 2020, and the past year has seen a big jump in the number of attacks targeting small businesses. In our third annual *ITRC Business Impact Report*, 73 percent (73%) of owners or leaders of SMBs shared they had experienced a data breach, a cyberattack, or both in the previous 12 months. That follows a year when there was a slight dip in attacks against smaller businesses.
Figure 1

Figure 1 | *Data Breaches, Cyberattacks, or Both, Reported by SMBs*



These trends follow the same patterns the ITRC has seen in consumer impacts and data breaches: a peak year of attacks in 2021 with a small reduction in 2022 due to a variety of factors, including the Russian invasion of Ukraine and disruption in the cryptocurrency markets. Since then, much like the legitimate stock market, the identity crime markets have adjusted to conditions that resulted in fewer attacks in 2022 and rebounded with a vengeance in 2023.

As you will see in the pages that follow, the number of first-time attacks against small businesses jumped 18 percentage points compared to 2022. At the same time, more SMB leaders believe they are ready to take on cyber attackers. In 2022, 70 percent (70%) of SMBs believed they were ready to defend against a cyberattack or data breach. This year, the number was 85 percent (85%).

One new area we probed in 2023 was the concept of new or emerging data security tools. As you'll notice, the uptake of new solutions such as Multi-Factor Authentication (MFA) and practices like data minimization were slow to gain acceptance. Utilization ranged from 34 percent (34%) for MFA to 20 percent (20%) for newer tools such as passkeys that were known to be effective protections.

Likewise, privacy protections were yet to break fully into the mainstream. The ability to opt-out of data collection or to have information deleted about you remained far less than 40 percent (40%), even as more states moved toward adopting their own comprehensive privacy laws.

SMB leaders are more focused on data security and privacy protection than ever. That's great news, but we still have a tremendous amount of work to do. We are going to set an all-time high for data breaches this year and more than likely will experience a tsunami of identity fraud in the months and years to follow.

We need to accelerate the transition to newer protections and continue to develop new resources to assist victims based on solid research and clear evidence similar to our recent study of identity crimes in Black communities. This one-two combination of enhanced protections and targeted victim support will help us adjust to the ever-changing and relentless threats from cybercriminals.

Our hope is that you will use the information presented here and the tools the ITRC offers to help your SMB defend against cyberattacks and respond to the data compromises that we know are inevitable. If you have questions or need assistance, just ask. If you have suggestions, please share those ideas, too. Just send an email to communications@idtheftcenter.org.

Eva Velasquez, *CEO*

Identity Theft Resource Center
October 2023

Methodology

The ITRC, using the SurveyMonkey platform, 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 September 2023, covering the previous 12 months (unless otherwise noted in a specific question).

The online questionnaire was completed by 551 individuals; 276 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. One hundred ninety-nine (199) reported being the victim of a cyberattack, a data breach or both in the past 12 months.

This year's report reflects responses from businesses ranging from single-employee companies to organizations with 500 employees. The responses also reflect a wide range of industries with a slight concentration in retail entities.

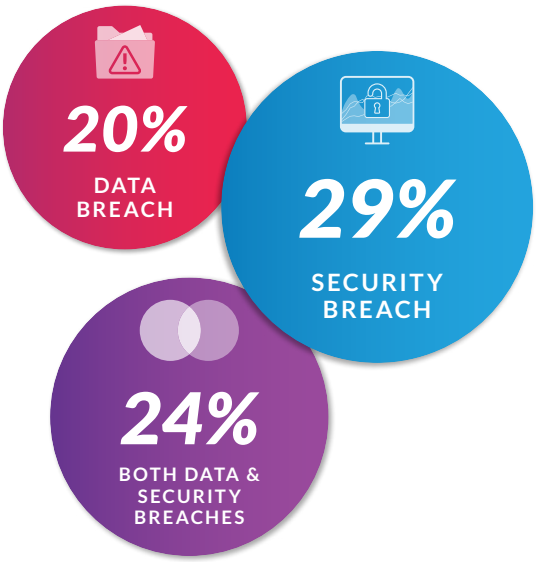
Number of Employees

- **8%** Solo Entrepreneur
- **24%** 1-5 Employees
- **12%** 6-10 Employees
- **25%** 11-50 Employees
- **21%** 51-200 Employees
- **10%** 201-500 Employees

Top Industries

RETAIL	21%
FINANCIAL SERVICES	12%
TECHNOLOGY	12%
MANUFACTURING	11%
OTHER	9%
HOSPITALITY	7%
HEALTHCARE	7%

Type of Cyberattack



Position Titles

2023 BUSINESS IMPACT REPORT

idtheftcenter.org • 1-888-400-5530

*Our **2023 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 551 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.*

ITRC | IDENTITY THEFT RESOURCE CENTER

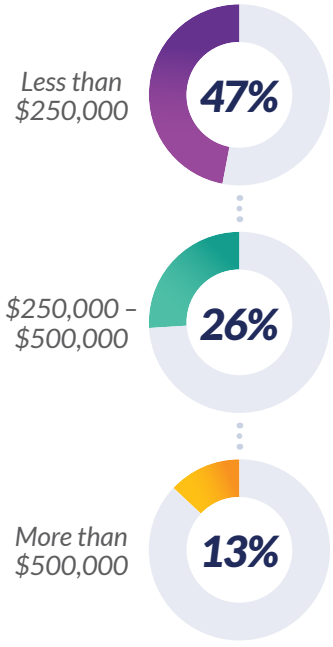
Cyberattacks Experienced by Small Businesses in the Past Year

- **20%** Data Breach
- **29%** Security Breach
- **24%** Both
- **28%** No Cyberattack

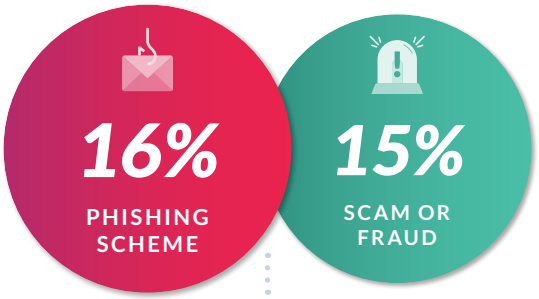
28 Percentage Point Increase
SINCE 2022

Financial Impact Due to Cybercrimes

Though we saw an increase of 4% in financial impacts totaling less than $250,000 since 2022, overall financial impacts due to cybercrimes continues to drop compared to previous years.



Rising Root Causes of Attacks



3 Percentage Point Increase
SINCE 2022

Top Root Causes in 2023

EXTERNAL ATTACKERS – 30%
16 Percentage Point Decrease from 2022

MALICIOUS INSIDERS – 30%
Same Year-Over-Year

THIRD-PARTY VENDORS – 24%
14 Percentage Point Decrease from 2022

REMOTE WORKERS – 21%
8 Percentage Point Decrease from 2022

Customer & Business Data Protection

CUSTOMER DATA

2FA & MFA Required for Access

Must Opt-In to Data Collection & Use

Can Opt-Out or Limit Information Collected

BUSINESS DATA

2FA & MFA Required for Access

Role-Based Account Access Internally

12-Character Minimum Required

50% of Small Businesses
Surveyed Reported Taking Steps to Prevent Future Breaches

65%
Provided New Training for Staff
IT & NON-IT STAFF

54%
Added Additional Security
STAFF & BUDGET

53%
Implemented New Security Tools

Summary of Key Findings

Summary and Analysis of 2023 Key Findings

First-Time Questions

Summary and Analysis of 2023 Key Findings

Small business leaders who responded to the ITRC's 2023 Business Impact Survey described a security and data protection landscape that reflects the same broad trends reflected in the ITRC's other research: an overall increase in identity and cybercrimes. The 2023 research recorded the highest level of businesses reporting attacks (73%) in the three-year history of the BIR.
Figure 2

Despite the strong negative trends, small business owners continue to project an air of extreme confidence about their ability to respond to the threats they face and the options for recovery when an attack is successful. While 70 percent (70%) of 2022 respondents said they were prepared to protect against a cyberattack or recover from a data breach, 85 percent (85%) of respondents in 2023 expressed they were ready to respond to a cyber event.
Figure 3

Employee and consumer data continue to be the most impacted categories of information impacted by a breach.
Figure 4

The number of organizations reporting first-time attacks was flat compared to 2022 (43%).
Figure 5

Figure 2 | *Types of Cyberattacks, 2023*

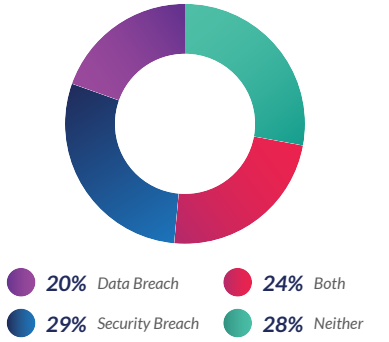


Figure 3 | *Ability to Respond to a Cyberattack, 2023*

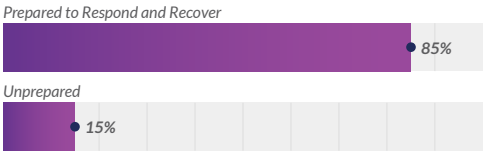


Figure 4 | *Compromised Data in Small Businesses*

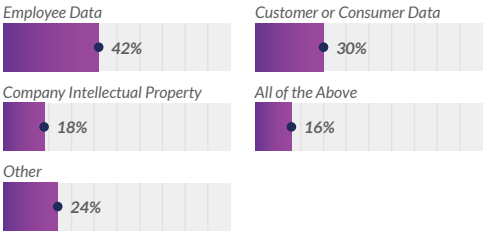
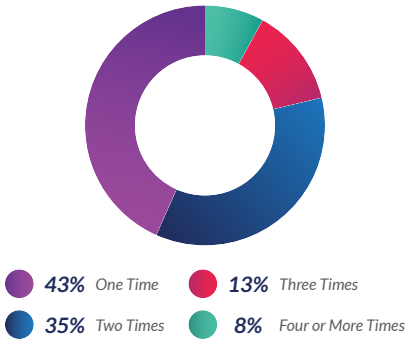


Figure 5 | *Number of Incidents Experienced*



The root cause of breaches shifted in 2023 compared to previous years, with external attackers, malicious employees, remote workers, and Third-Party Vendors taking the top slots but at reduced rates. Breaches caused by Phishing and Scams increased in keeping with broad trends.
Figure 6

The financial impacts of cyber breaches continued to drop compared to previous years, with more SMBs reporting losses of <$250,000 and fewer reporting higher dollar-value events.
Figure7

Cyber insurance emerged as the primary source of recovery funding (33%), followed by cash reserves. There was a slight uptick in headcount reductions (13%) as a means of addressing the costs of a breach.
Figure 8

Figure 6 | *Root Causes of Breaches in 2023*

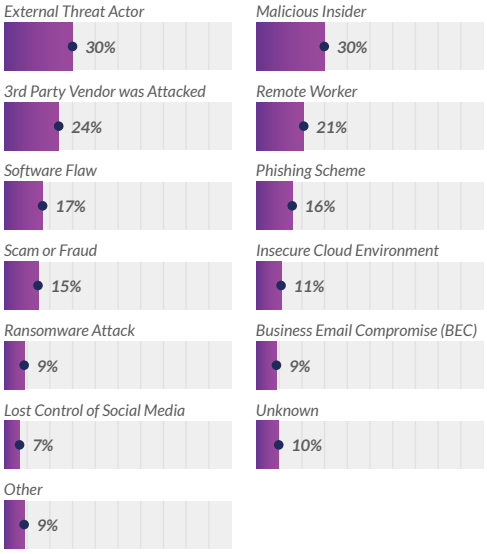


Figure 7 | *Financial Impact of Attack*

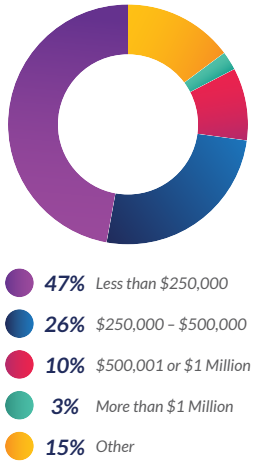
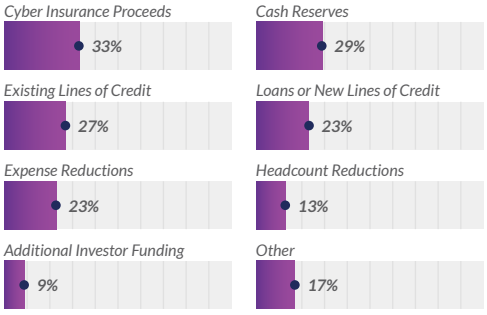


Figure 8 | *Financial Recovery After an Attack*



The vast majority of organizations that experienced a data breach sent notices to impacted consumers (83%), but 17 percent (17%) did not.
Figure 9

The most common reason given for delaying or not issuing a breach notice was at the request of law enforcement (50%), followed by a finding that no personal information was exposed (38%) or a self-determination that there was no risk of harm from the type of data compromised (21%).
Figure 10

With more organizations issuing data breach notices, more entities also offered a wider range of recovery services that included credit monitoring (44%), paid identity recovery services (47%), and access to free services via a non-profit (27%). Approximately 13 percent (13%) offered no services.
Figure 11

Slightly fewer organizations reported revenue losses (42%) as a result of cyber events. However, more businesses saw other impacts, including more customers losing trust (32%), higher regrettable employee turnover (32%) and increased difficulty in understanding what happened.
Figure 12

Figure 9 | *Alert to Customers of Incident*

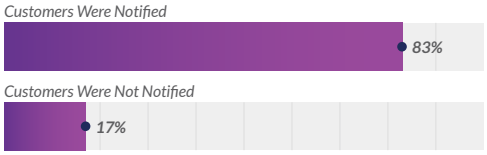


Figure 10 | *Reasons for Not Alerting Customers*

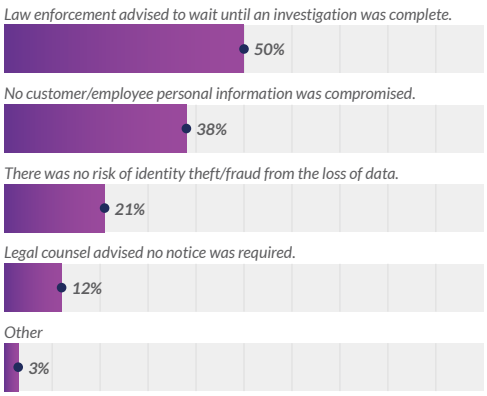


Figure 11 | *Remediation Services Offered to Affected*

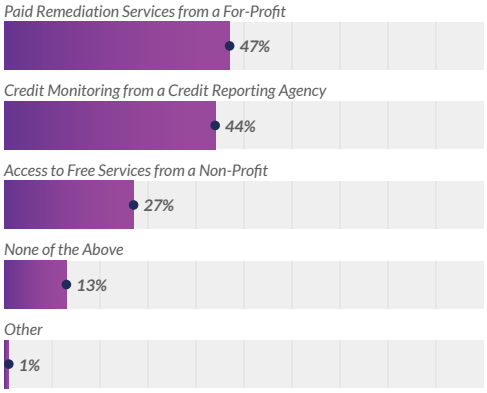
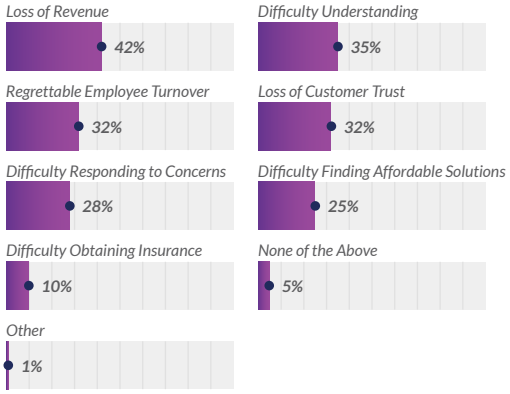


Figure 12 | *Problems Following Cyber Incident*



First-Time Questions

Each year, the ITRC explores new topics that relate to cybersecurity and data protection. In 2022, we explored the rise of social media account takeover and the relationship with identity fraud. In this report, we asked SMB leaders about the latest best practices for account access and for data use based on the rise of comprehensive data privacy and security laws at the state level in the absence of a national privacy law.

The findings show a slow rate of adoption for a variety of well-established best practices as well as new technology or processes that protect personal and business information. The vast majority of SMBs have not utilized tools such as Multi-Factor Authentication (MFA) for employee or customer use, mandatory strong passwords, or role-based access for employee access to sensitive data. Adoption rates range between 34 percent (34%) and 20 percent (20%) depending on the solution.
Figure 13

The *2023 Business Impact Report* shows similar rates of adoption for consumer data collection, use, and storage designed to protect personal information and privacy. Adoption rates range from 37 percent (37%) to 21 percent (21%), driven, in part, by state laws that require data best practices, including data access, opt-in to data collection, opt-out of data sales, and rights to correct and delete certain types of information.
Figure 14

The information gathered this year will form the basis for follow-up research in 2024 to explore the barriers to adoption of best practices.

Figure 13 | *Current Protective Measures*

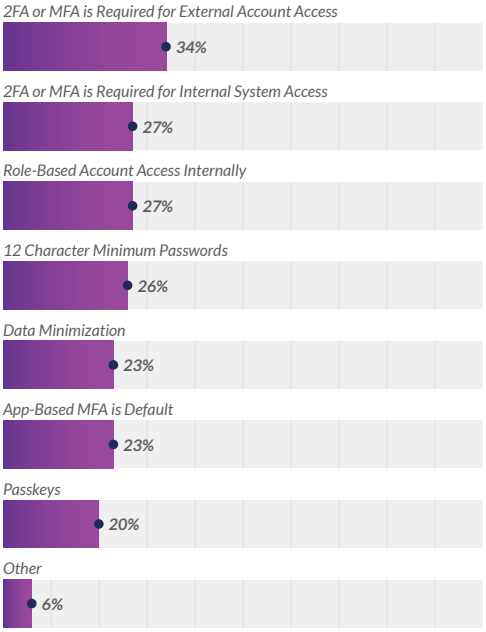
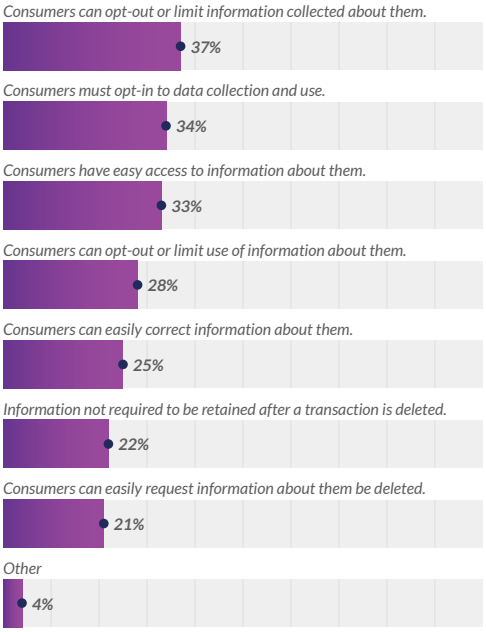


Figure 14 | *Data Privacy Best Practices Followed*



A Word About Supply Chain Data Breaches

The number of data compromises in 2023 will represent a single-year record. As this report is released in October, more than 2,100 data compromises have been reported in 2023 – far exceeding the previous annual record high of 1,862 set in 2021. More than 1,300 organizations have been impacted to date by attacks against just 87 vendors, many of which are SMBs who are part of the supply chain of larger organizations.

Increased due diligence by organizations prompted by cyber insurance requirements, state privacy laws, and federal regulations is creating demand for information about past data breach events and near real-time alerts as new breaches are discovered. The ITRC has created a breach alert solution for organizations of all sizes that will help satisfy corporate and legal requirements for understanding the cybersecurity history and performance of vendors (and vendors' vendors).

For more information about Breach Alert for Business, contact ***Dorinda Miller***, *Director of Business Developement*.

2023 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, email ***dorinda@idtheftcenter.org***.

For Media

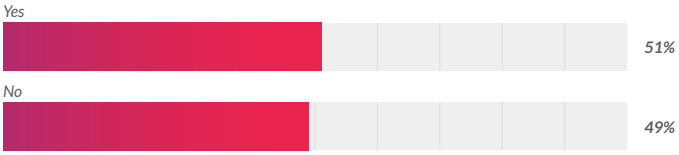
For any media-related inquiries, please email ***media@idtheftcenter.org***.

Appendix

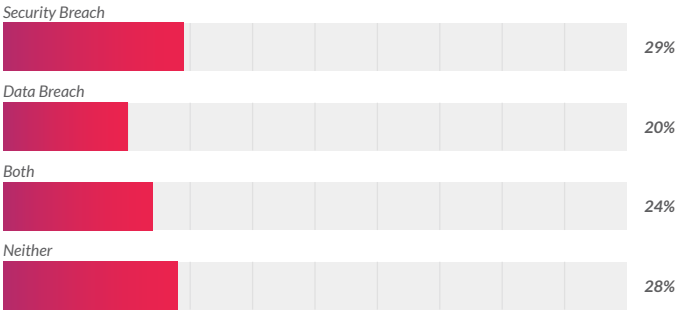
The ITRC, using the SurveyMonkey platform, conducted an online survey to explore the impacts of cybercrimes on small businesses as defined by the U.S. Small Business Administration. The survey was conducted in September 2023.

2023 Business Impact Study

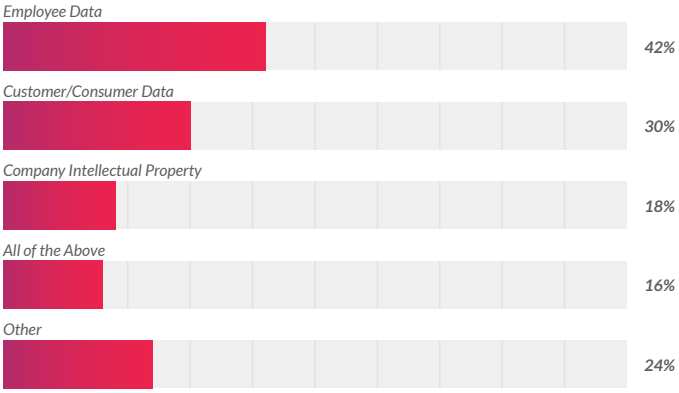
Are you the owner or leader of a small business with fewer than 500 employees, including solopreneurs and gig workers?



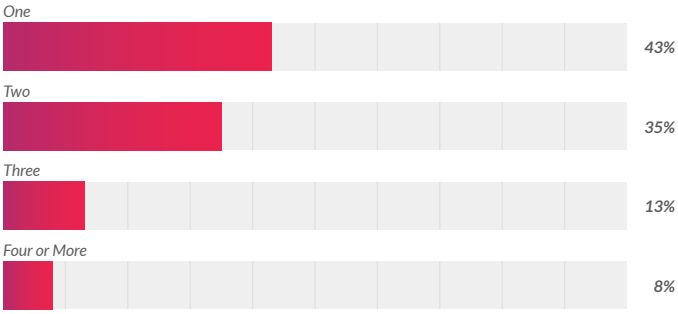
Has your company experienced a security or data breach in the past 12 months?



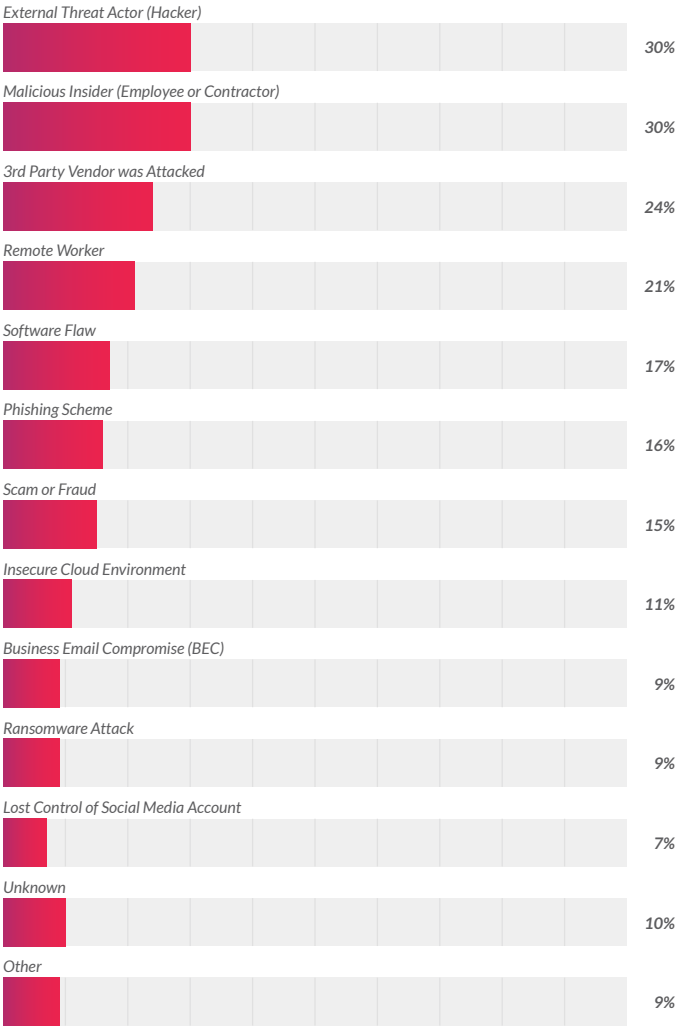
What data was compromised? Select all that apply.



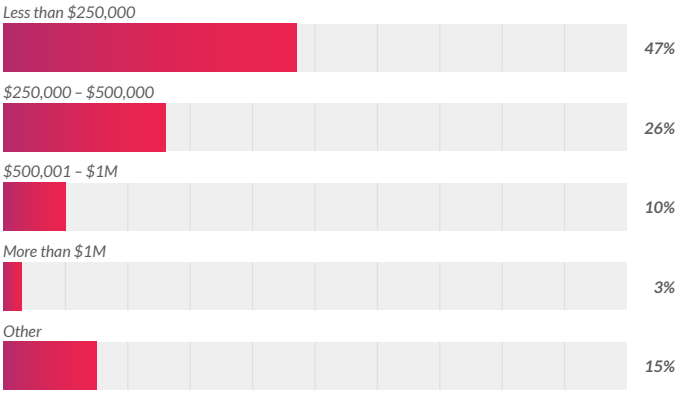
How many times have you experienced a data or security incident?



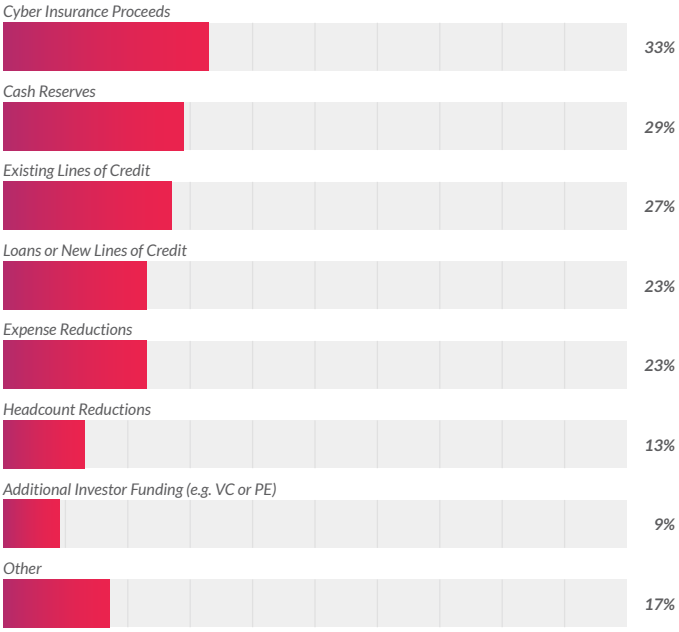
What was the root cause(s) of the recent data or security incident? Select all that apply.



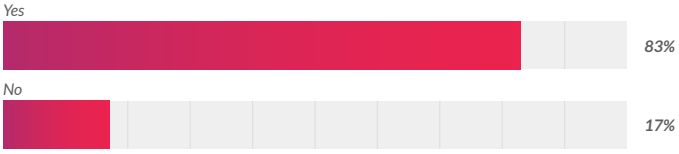
What was the approximate total financial impact of the security or data breach, including lost revenue, lost customers, legal costs, fines and penalties, insurance, marketing costs, improved security, etc.?



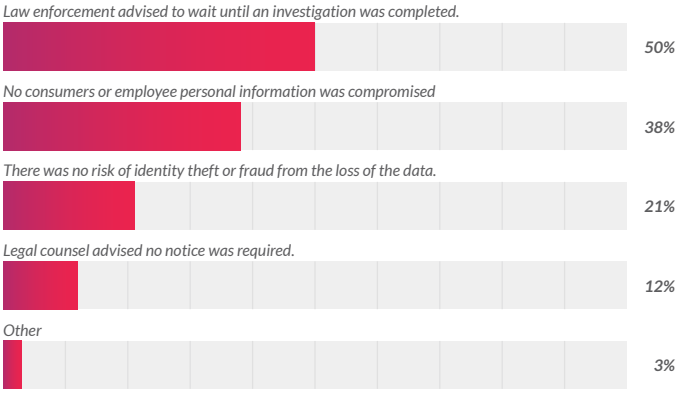
How did you address the financial impacts of the data or security incident? Select all that apply.



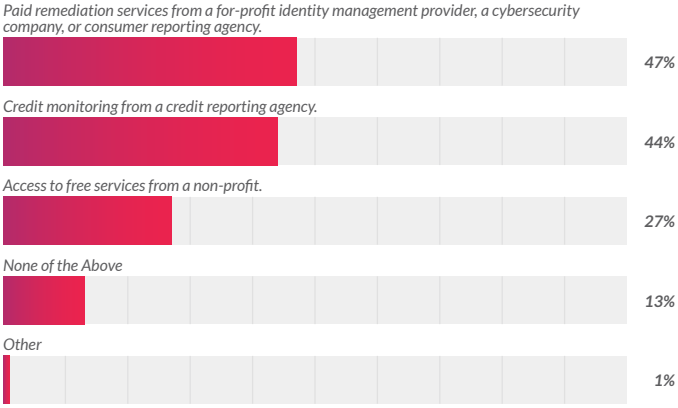
Did you send a breach notice to alert consumers of the incident?



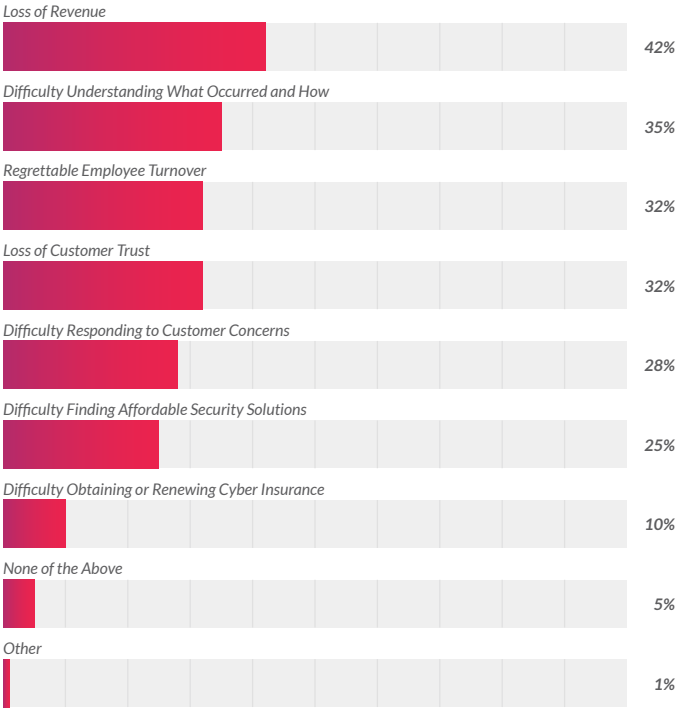
Why didn't you send a breach notice after the incident?



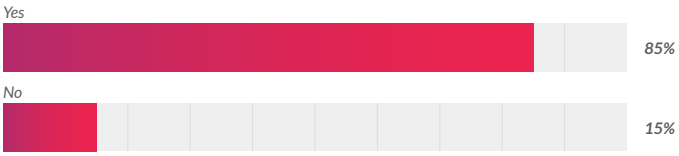
Did you offer any of the following remediation services to customers or consumers impacted by the breach?



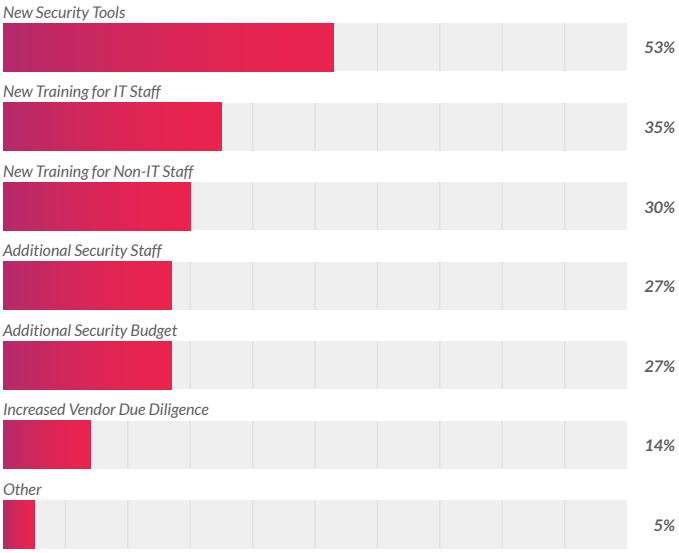
Did you experience any of the following issues following your cyber incident? Select all that apply.



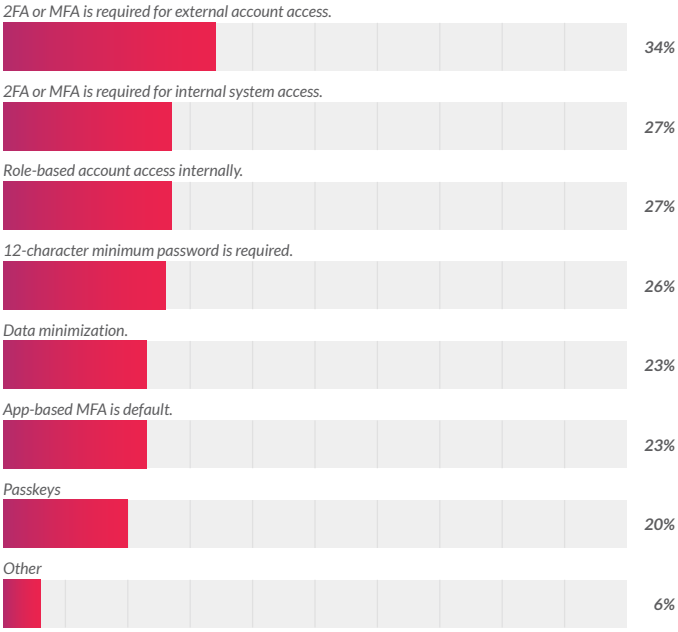
Are you prepared to protect against a cyberattack or recover from a data breach?



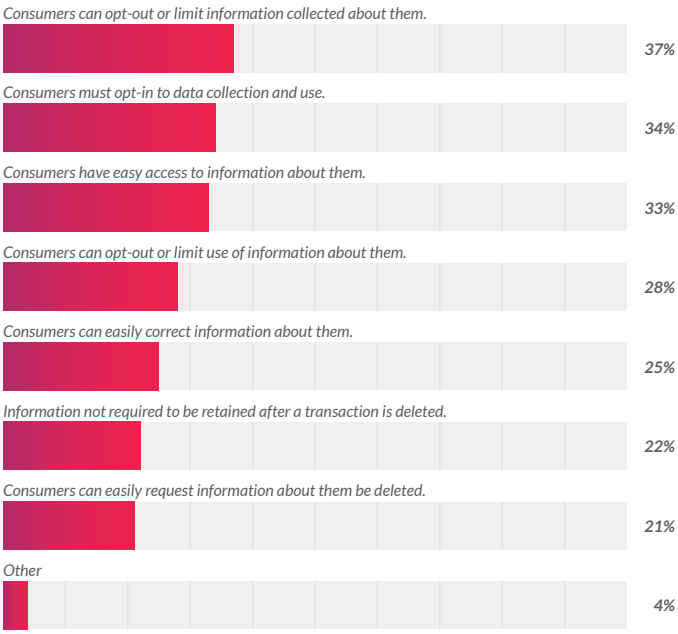
What steps have you taken to prevent future security or data breaches? Select all that apply.



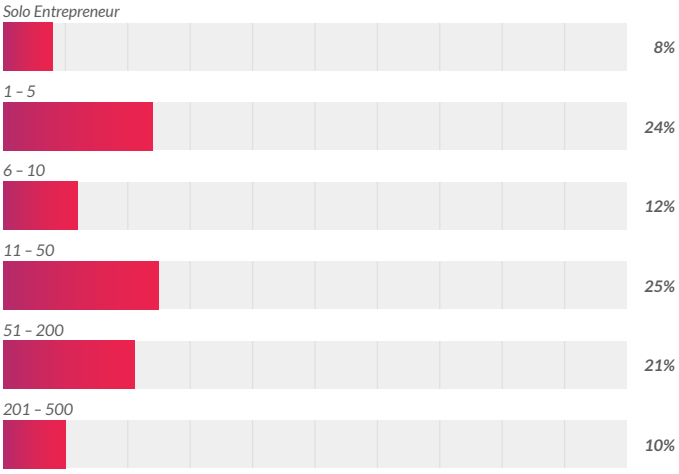
Do you currently utilize any of the following solutions to help protect business and consumer data?



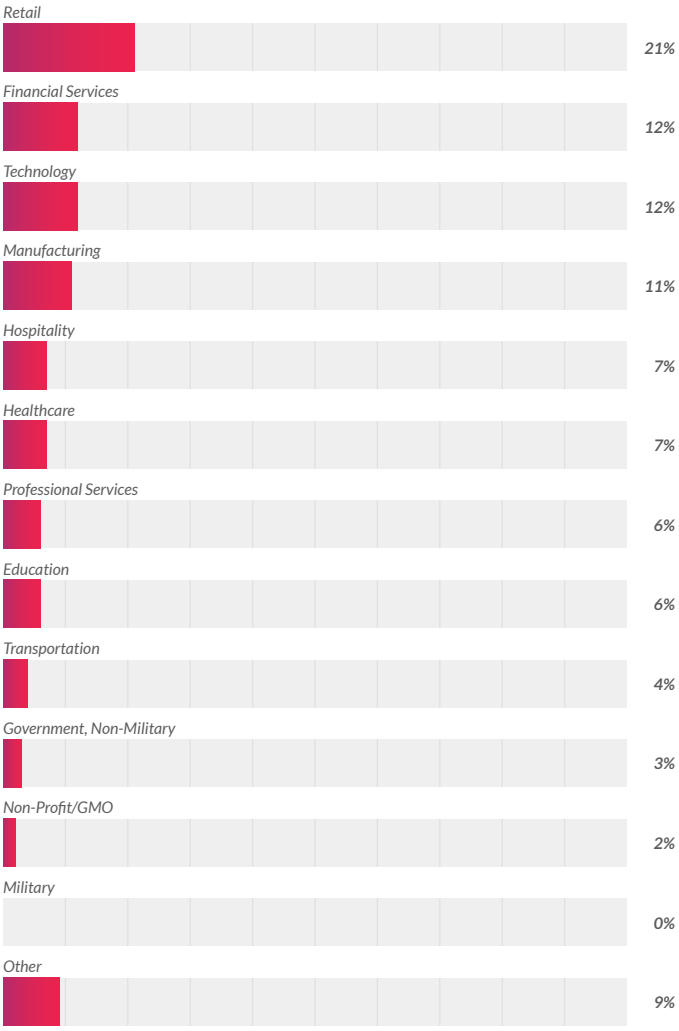
Do you follow any of the following data privacy best practices? Select all that apply.



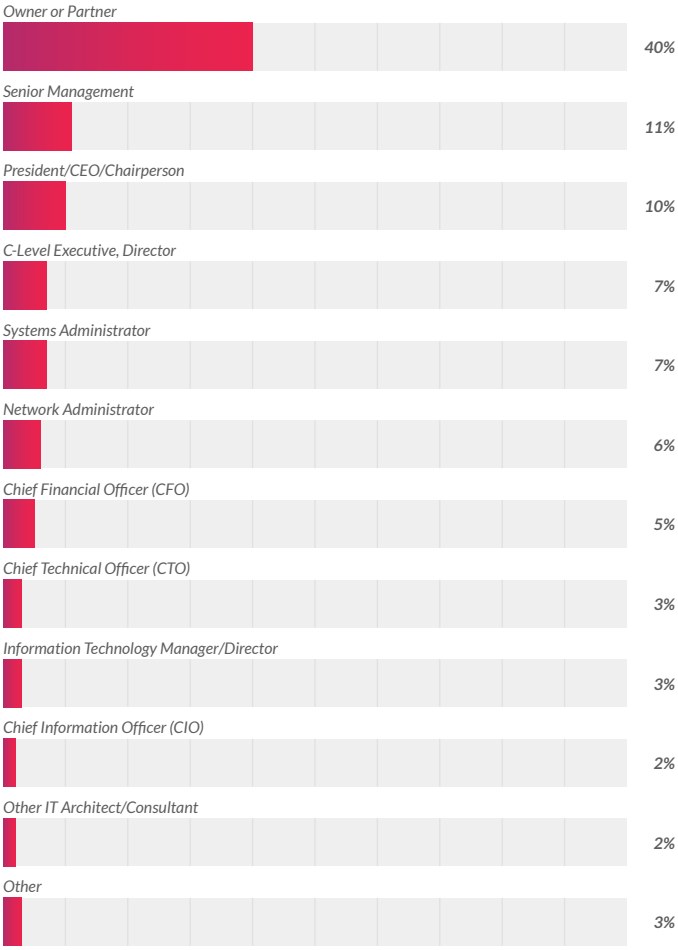
How many employees are in your company?



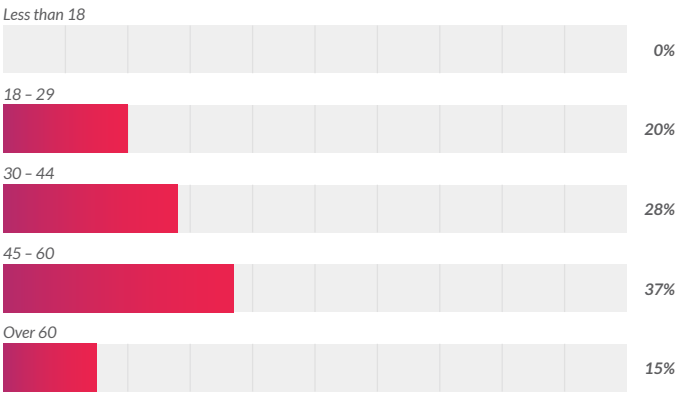
What is your industry?



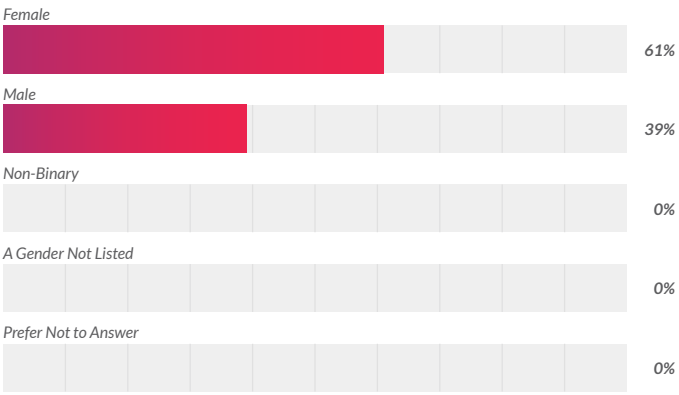
What is your title?



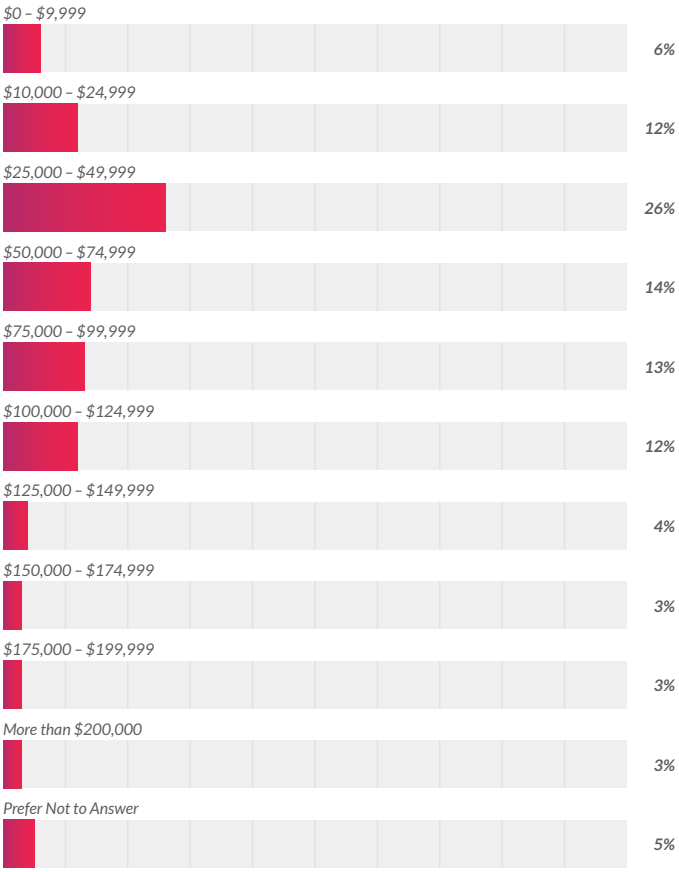
Age



Gender



Household Income



Region