BIR

IDENTITY THEFT RESOURCE CENTER

2025 Business Impact Report

This report was made possible through the support of ***Mitek****.*

ITRC IDENTITY THEFT RESOURCE CENTER

DECEMBER 2025

CONTENTS

THE NEW FRONTLINE:
Small Business Cybersecurity in the Era of AI

APPENDIX

INTRODUCTION
from the President

In the *2025 Consumer Impact Report* (CIR) published in October, we called out a dramatic increase in the financial and emotional impacts on victims of identity theft, fraud and scams. The results of our research into the impacts of cybercrimes on small businesses reveal an equally troubling and unsustainable trend at the core of the American economy.

While the data is comprehensive and often complex, the story it tells is simple: small businesses (the vast majority of U.S. businesses) are under a relentless and evolving digital siege. The economic consequences of these attacks are now rippling through the marketplace in the form of ***direct price increases for consumers***.

The survey responses reveal that a staggering 81 percent (81%) of small businesses have suffered a security or data breach within the last year. Most of these businesses experienced multiple attacks, with threat actors deploying increasingly sophisticated methods, including a significant number of AI-powered attacks cited as a root cause in more than 41 percent (41%) of incidents.

> *"I think the technology is just too new, and we don't know all the pitfalls. I choose not to be a cyber crash-dummy." –Small Business Leader*

The financial fallout from these breaches in the past year has been substantial. More than half of the affected businesses reported losses between $250,000 and $1 million. For a small business, such a loss can be catastrophic. However, the most critical finding of our research is how businesses are forced to absorb these costs.

While many are drawing from cash reserves or relying on cyber insurance proceeds, a significant portion – nearly 40 percent (40%) – are raising prices on their goods and services.

> *"My social security number was used for a really big purchase worth thousands of dollars." –Small Business Leader*

In effect, the rising cost of cybersecurity and the financial damage from data breaches are creating a hidden "cyber tax" that is being passed directly to consumers – the very people who are also directly impacted by the loss of their personal information (and financial resources) to identity criminals.

This shadow tax creates a drag on the U.S. economy, fuels inflation and places a disproportionate burden on the small businesses that generate jobs and sustain communities. These businesses, which generally lack the resources of their larger enterprise counterparts, are being forced to choose between investing in growth, keeping prices low and defending against an ever-present digital threat.

The current landscape is not a fair fight. We are at a point where the resilience of our national economy is increasingly linked to the cybersecurity of our small business community.

The data in this report should serve as a wake-up call that it is time for a serious dialogue about the role of public policy in leveling the playing field. We need to explore state and federal initiatives, along with public-private partnerships, to alleviate this burden.

> *"I had a man call and say he was from the IRS and that I needed to pay a certain amount of money right away or I would be arrested." –Small Business Leader*

We can no longer treat cybersecurity as a cost of doing business that falls solely on the shoulders of individual entrepreneurs and their customers (and employees) whose lives and livelihoods are impacted. It is a national economic imperative that requires a coordinated and strategic response.

If you have questions about the findings in this report, don't hesitate to email me at JamesPres@IDTheftCenter.org.

James E. Lee
President, Identity Theft Resource Center

GLOSSARY

For purposes of this report, the ITRC uses standard industry terms as defined by the National Institute of Standards & Technology (NIST), as well as specific definitions developed by the ITRC.

ACCOUNT TAKEOVER (ATO)

When an unauthorized person gains control of an existing account. ATO includes financial accounts such as bank accounts or non-financial accounts such as social media accounts.

CASES

Instances of identity compromise or misuse reported by people who contact the ITRC Contact Center.

CONTACTS

Individuals who contacted the ITRC Contact Center for any reason, including prevention as well as instances of identity compromise and misuse.

DATA BREACH

A data event where personal information is removed by malicious action or by an error from a database or system where it was created, collected, processed or maintained.

DATA EXPOSURE

An event where personal information is available for viewing or download but NOT copied or removed from the database or system where it was created, collected, processed or maintained.

IDENTITY COMPROMISE

When a person's personally identifiable information (PII) has been exposed in a data breach, a cybersecurity failure, or because of a scam, but has not yet been misused.

IDENTITY CRIMES

The use of stolen personally identifiable information (PII) to commit a crime.

IDENTITY FRAUD

The use of stolen personally identifiable information (PII) to commit fraud.

IDENTITY MISUSE

The use of someone's stolen personally identifiable information (PII) to commit identity fraud (open accounts, take over accounts, commit a crime, obtain employment, etc.).

IDENTITY THEFT

The act of stealing someone's personal information.

NEW ACCOUNT FRAUD

Opening new credit card or bank accounts using stolen personally identifiable information (PII).

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personal information such as name, date of birth, driver's license number, Social Security number, etc. The definition of PII varies by state, but often includes logins and passwords.

SOCIAL ENGINEERING TECHNIQUES

Using personal interactions and emotional manipulation to entice someone to willingly give a criminal their personally identifiable information (PII).

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 August 2025, covering the previous 12 months unless otherwise noted in a specific question.

The online questionnaire was completed by 662 people selected by SurveyMonkey. The respondents met the criteria of being a small business owner or executive at a company of 500 or fewer employees, including solopreneurs and gig workers.

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 concentration in financial services, technology, manufacturing and retail entities.

Figure 2 | *Employee Count*

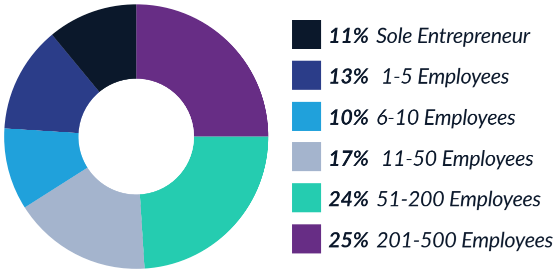


Figure 3 | *Job Title*

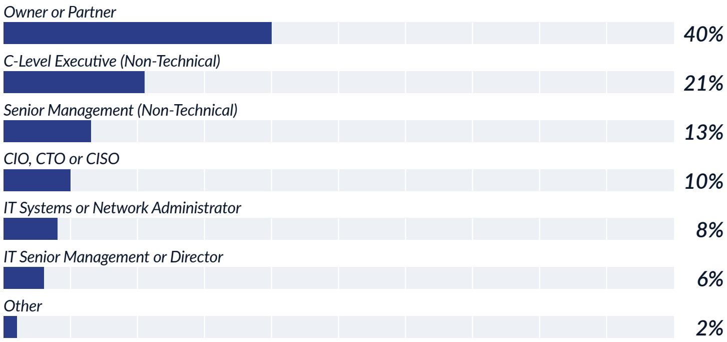
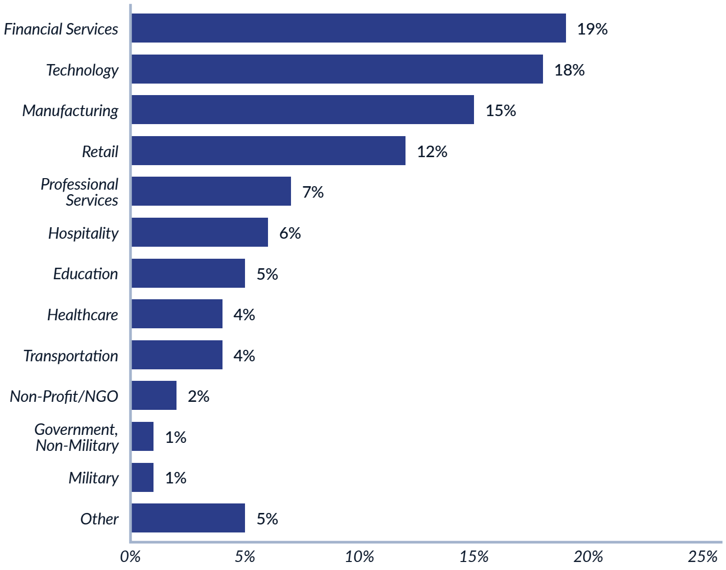


Figure 1 | *Industry*



KEY TAKEAWAYS

TAKEAWAY #1

Cyberattacks are a Near-Universal Threat, With a Shift Toward AI-Powered Attacks

Eighty-one percent (81%) of small businesses (SBs) reported suffering a security breach, a data breach or both in the past year. Artificial Intelligence (AI) powered attacks were identified as a root cause in more than 40 percent (40%) of cyber events, a pivot from internal risks to external, technologically advanced adversaries.

TAKEAWAY #2

The Financial Cost of Cybercrime is Being Passed Directly to Consumers

A significant number of businesses are raising prices on goods and services to cover the costs of cyberattacks, creating a hidden “cyber tax” that helps fuel inflation.

TAKEAWAY #3

Business Leaders’ Confidence in Their Cybersecurity Preparedness Has Collapsed

The percentage of SB leaders who felt “very prepared” for a cyberattack plummeted in 2025 – largely driven by the emergence of new, sophisticated threats, including AI-powered attacks.

TAKEAWAY #4

There is a Dangerous Disconnect Between the Perceptions of Risk and the Adoption of Basic Security Controls

Despite a heightened sense of alarm among business leaders, the implementation of critical security measures, such as Multi-Factor Authentication (MFA), has declined.

TAKEAWAY #5

Small Business Leaders Have Mixed Opinions About Artificial Intelligence (AI)

The vast majority of SB leaders are planning for AI-driven attacks and would embrace AI security tools, but are split over who should be responsible for protecting people from AI-enabled cybercrime.

BIR

IDENTITY THEFT RESOURCE CENTER

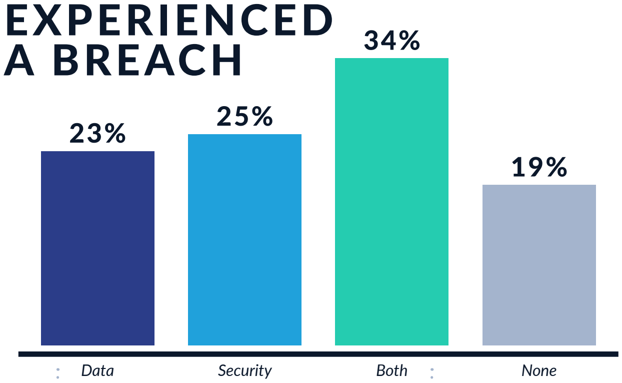
2025 Business Impact Report

The *2025 Business Impact Report* explores the trends of small businesses, ranging from single-employee companies to organizations with 500 employees. The report findings highlight significant changes in cyber habits from small business leaders in a wide range of industries.

ITRC | IDENTITY THEFT RESOURCE CENTER

SMALL BUSINESSES WHO

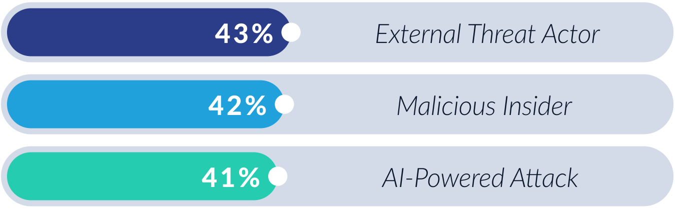
EXPERIENCED A BREACH



*Small businesses reporting a breach **remained the same** year-over-year.*

TOP ROOT CAUSES REPORTED BY SMALL BUSINESSES

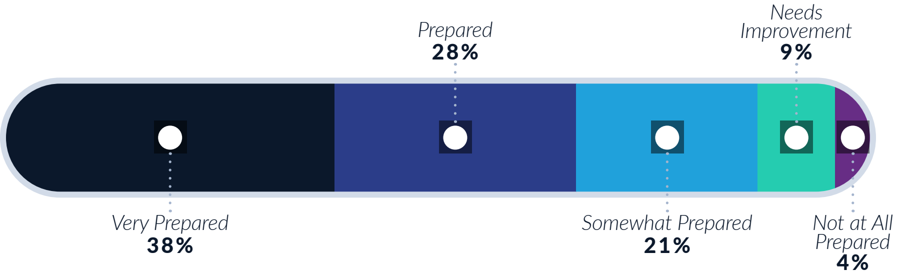
DUE TO A SECURITY OR DATA INCIDENT



*While other root causes are down from 2024, the emergence of **AI-powered attacks in 2025 shows a big pivot** from internal risks to external, technologically-advanced threats.*

PREPAREDNESS TO PROTECT OR RECOVER

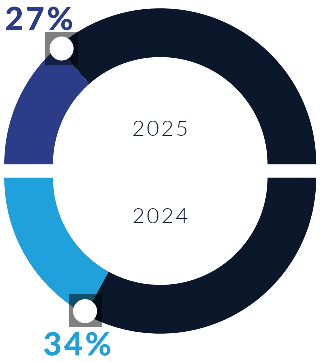
From a Cyberattack or Data Breach



*Small businesses reporting they feel "very prepared" **decreased by 18 percentage points** from 2024.*

DECLINE IN MFA ADOPTION

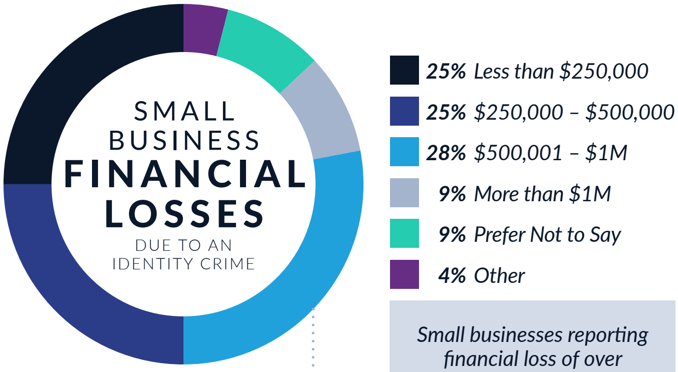
FOR INTERNAL SYSTEMS BY SMALL BUSINESSESS



*This **seven (7) percentage point decrease** represents a critical vulnerability within small businesses.*

SMALL BUSINESS FINANCIAL LOSSES

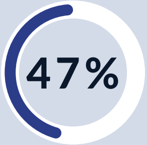
DUE TO AN IDENTITY CRIME



*Small businesses reporting financial loss of over $500,000 **increased by one (1) percentage point** year-over-year.*

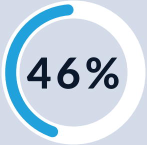
TOP FINANCIAL RECOVERY METHODS

Reported by Small Businesses Due to a Cyber Incident



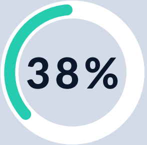
Cash Reserves

Down Three (3) Percentage Points From 2024



Cyber Insurance Proceeds

Down Ten (10) Percentage Points From 2024



Raised Prices

*New Category in 2025, Also Known as a **"Cyber Tax"***

Mitek

*This report was made possible through the support of **Mitek**.*

THE NEW FRONTLINE:

Small Business Cybersecurity in the Era of AI

OVERVIEW

The Business Impact section of the ITRC's *Business Impact Report* (BIR) presents a comprehensive analysis of the evolving cybersecurity landscape for Small Businesses (SBs), drawing upon a comparative analysis of survey data from 2024 and 2025 collected and analyzed by the Identity Theft Resource Center (ITRC). The findings reveal a dramatic and concerning shift in the nature of cyber threats, the profound business impacts of these incidents and the strategic adjustments required for survival and resilience.

The analysis indicates that while the overall prevalence of cyber incidents remains alarmingly high, the character of these attacks has fundamentally changed over time. The primary threat has pivoted from malicious insiders to external, technologically sophisticated adversaries leveraging Artificial Intelligence (AI). In 2025, AI-powered attacks emerged as a root cause in more than 40 percent (40%) of reported incidents, a development that has impacted the confidence of SB leaders. The percentage of leaders feeling "very prepared" for an attack dropped significantly from 56.5 percent (56.5%) in 2024 to just 38.4 percent (38.4%) in 2025.

This crisis of confidence is occurring alongside an evolving cyber insurance market, with SBs reporting a decreased reliance on insurance proceeds to cover the substantial financial damages, which most often fall within a range of $250,000 to $1 million USD per incident. Consequently, a growing number of businesses are forced to pass these costs directly to consumers by raising prices, signaling a broadening economic impact of cybercrime. The operational consequences are equally severe, with rising employee turnover post-incident suggesting financial strain and talent loss are creating a cycle of increasing vulnerability.

Unfortunately, this heightened state of alarm has not translated into a renewed focus on foundational security controls. The adoption of critical measures like Multi-Factor Authentication (MFA) has declined year-over-year. This suggests a state where leaders, overwhelmed by the complexity of new threats, are neglecting the very basics that provide an effective defense.

The ITRC suggests SBs pivot their defensive strategies to address the new reality of scalable, AI-driven external threats while simultaneously recommitting to the mastery of cybersecurity fundamentals. The path forward requires a three-pronged approach: building a robust human firewall through leadership and training, fortifying technical defenses with a focus on access control and system hardening and establishing a resilient crisis management capability through a well-rehearsed Incident Response Plan (IRP). For SBs, cybersecurity is no longer an IT issue; it is a fundamental pillar of business survival.

THE EVOLVING CYBER THREAT LANDSCAPE

for Small Businesses (2024–2025)

The operational environment for small and medium-sized businesses has undergone a seismic shift, with the cybersecurity threat landscape evolving at an unprecedented pace. An analysis of survey data from business leaders in 2024 and 2025 reveals that the challenge is not merely one of increasing volume, but of a fundamental transformation in the nature, origin and impact of cyberattacks. This section provides a detailed comparative analysis of these two periods, charting the emergence of new threats, the escalating consequences of compromise and the profound psychological impact on business leadership.

THE WIDENING ATTACK SURFACE

The data confirms that experiencing a cyber incident is now a near-universal aspect of operating a small business. In 2024, 81.1 percent (81.1%) of SBs reported having experienced either a security or data breach within the preceding 12 months. This figure held steady in 2025, with 81 percent (81%) of respondents reporting an incident, indicating that being a target of cybercrime is the rule, not the exception.[1]

While the overall prevalence of attacks remained constant, the frequency of incidents among victimized businesses shows a notable shift. As detailed in Figure 4, there was a significant increase in the proportion of businesses that experienced only a single incident, rising from 23.6 percent (23.6%) in 2024 to 34.4 percent (34.4%) in 2025. Conversely, the percentage of businesses suffering from repeat attacks declined. The proportion of victims hit three times fell from 30.7 percent (30.7%) to 24.4 percent (24.4%), and those hit four or more times dropped from 18.3 percent (18.3%) to 11.5 percent (11.5%) over the same period.

Figure 4 | *Year-Over-Year Comparison of Cyber Incidents in SBs (2024 vs. 2025)*

	2024 Percentage Responses	*2025 Percentage Responses*	*Year-Over-Year Change (Percentage Points)*
Yes, Experienced a Breach *(Security, Data, Both)*	81.1%	81.0%	-0.1
Experienced 1 Breach	23.6%	34.4%	+10.8
Experienced 2 Breaches	27.4%	29.7%	+2.3
Experienced 3 Breaches	30.7%	24.4%	-6.3
Experienced 4 or More Breaches	18.3%	11.5%	-6.8

This trend suggests a change in attacker methodology. The high, stable prevalence rate, combined with a move toward single-incident attacks, points to a "spray and pray" model becoming more dominant. Attackers, likely enabled by scalable and automated tools, are casting a wider net to maximize the number of unique victims for immediate financial gain, a hallmark of ransomware campaigns which disproportionately target SBs.[2]

Rather than investing resources to establish persistent access for long-term exploitation, which is more common in attacks against larger enterprises, threat actors appear to be focusing on opportunistic, high-volume strikes.

This alters the risk calculus for SBs, shifting the primary challenge from defending against a determined, persistent adversary to repelling a continuous barrage of single-shot attacks from a multitude of sources.

THE SHIFTING NATURE OF ATTACKS

The most significant trend identified in the year-over-year data is a fundamental pivot in the root cause of cyber incidents. This change marks a transition from a threat landscape largely dominated by internal, human-centric risks to one defined by external, technologically advanced and highly scalable attacks.

In 2024, the “malicious insider (employee or contractor)” was the most-cited root cause of a breach, identified by 50.6 percent (50.6%) of affected SBs.[1] By 2025, this figure had fallen by nearly nine percentage points to 41.8 percent (41.8%). It was surpassed by “external threat actor (hacker),” which rose to 42.8 percent (42.8%).[1]

> *“People calling claiming to be the police department with a warrant.” –Small Business Leader*

More strikingly, a new category introduced in the 2025 survey, “artificial intelligence (AI) powered attack,” debuted as a root cause for an eye-catching 41.3 percent (41.3%) of victims, nearly equaling the top two traditional causes.[1] This data, summarized in Figure 5, signals a watershed moment in the evolution of cyber threats against SBs.

The emergence of AI as a primary attack vector aligns with extensive industry analysis on the weaponization of generative AI for creating hyper-realistic phishing emails, deepfake audio and video, and adaptive malware.[4] These tools are effectively democratizing advanced attack capabilities that were once the domain of highly skilled actors.

The primary advantage of a malicious insider has always been their intimate knowledge of internal processes, communication styles and organizational hierarchies, allowing them to bypass defenses through trust and familiarity.[7] AI tools now allow external actors to replicate this advantage at scale. By scraping public data from social media and corporate websites, generative AI can craft highly personalized social engineering attacks that mimic the tone and context of legitimate internal communications.[4] Real-world incidents have demonstrated threat actors using AI-generated deepfake audio and video of CEOs to authorize fraudulent multimillion-dollar wire transfers – a tactic that directly usurps an insider’s position of trusted authority.[10]

This empowers external adversaries to launch attacks with the precision of an insider but without the need to recruit or become one, making the external threat environment exponentially more dangerous and necessitating a profound shift in defensive strategy.

Figure 5 | *Root Causes of Cyber Incidents – A Shifting Landscape, Year-Over-Year*

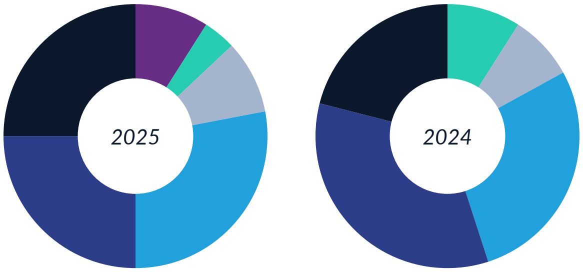
	2024 Percentage Responses	2025 Percentage Responses	Year-Over-Year Change (Percentage Points)
External Threat Actor *(Hacker)*	49.7%	42.8%	-6.9
Malicious Insider *(Employee or Contractor)*	50.6%	41.8%	-8.8
Artificial Intelligence (AI) Powered Attack	–	41.3%	–
Remote Worker	41.0%	26.8%	-14.2
Third-Party Vendor was Attacked	37.6%	29.6%	-8.0
Software Flaw	29.8%	22.5%	-7.3
Ransomware Attack	26.7%	18.8%	-7.9
Insecure Cloud Environment	29.0%	18.8%	-10.2

THE ESCALATING COST OF COMPROMISE

The financial and operational fallout from a successful cyberattack remains severe and capable of threatening the viability of any small business. In 2025, 62.5 percent (62.5%) of breached SBs reported a total financial impact—including lost revenue, remediation costs and fines—of more than $250,000. Within that group, more than a third of all victims (36.7%) faced costs exceeding $500,000.[1]

These figures represent a slight increase in the most catastrophic outcomes compared to 2024, where 35.6 percent (35.6%) of victims reported impacts over $500,000.[1]

Figure 6 | *Approximate Monetary Impacts Due to Identity Crime, Year-Over-Year*



2025		2024
25%	Less than $250,000	21%
25%	$250,000 – $500,000	34%
28%	$500,001 – $1M	28%
9%	More than $1M	8%
4%	Other	9%
9%	Prefer Not to Say	-

Beyond the direct monetary losses, the secondary operational impacts are profound and reveal a worsening trend in one key area. While the reported instances of “loss of customer trust” (47.6 percent (47.6%) in 2024 vs. 39.6 percent (39.6%) in 2025) and “loss of revenue” (45.5 percent (45.5%) in 2024 vs. 37 percent (37%) in 2025) saw a moderate decrease, the rate of “increased employee turnover” (referred to as “regrettable employee turnover” in 2024) held steady at a high level, reported by 42.3 percent (42.3%) of victims in 2024 and 37.4 percent (37.4%) in 2025.[1]

FUNDING RECOVERY

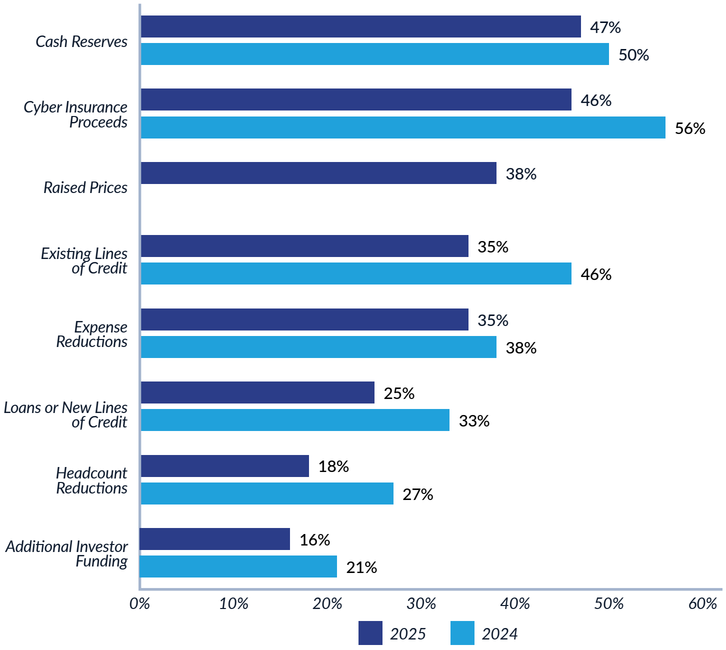
The mechanisms through which SBs finance their recovery from a cyber incident are undergoing a significant transformation, pointing to structural shifts in the cyber risk market. In 2024, “cyber insurance proceeds” were the single most-cited source of funding, used by 55.9 percent (55.9%) of affected businesses. By 2025, this figure had fallen significantly to 46.3 percent (46.3%).

> *“The email looked like a trusted source.” –Small Business Leader*

This decline in reliance on insurance coincides with SBs reporting increased friction in the insurance market; 30.7 percent (30.7%) of victims in 2024 and 23.8 percent (23.8%) in 2025 cited “difficulty obtaining or renewing cyber insurance” as a post-breach issue.[1] This suggests that as the frequency and cost of claims have risen, insurers have responded by adjusting underwriting standards.

As the insurance backstop becomes less reliable/available, SBs are being forced to find alternative ways to cover their losses. While tapping cash reserves (49.9 percent (49.9%) in 2024, 46.8 percent (46.8%) in 2025) and existing lines of credit (46.3 percent (46.3%) in 2024, 34.9 percent (34.9%) in 2025) remain common, a new and telling response appeared in the 2025 survey: 38.3 percent (38.3%) of businesses reported they “raised prices” to address the financial impacts of an incident.

Figure 7 | *Funding Recovery Due to Cyber Incident, Year-Over-Year*



This development indicates that the costs of cybercrime are no longer being absorbed solely by businesses and their insurers but are now being systematically passed on to consumers.

This represents a significant, inflationary macroeconomic ripple effect stemming directly from the worsening cyber threat landscape for small businesses.

A DANGEROUS DISCONNECT

The most striking psychological trend revealed by the survey data is a collapse in the self-assessed preparedness of SB leaders. In 2024, a majority of leaders (56.5%) felt “very prepared” to protect their organization against a cyberattack or recover from a data breach. By 2025, that figure had plummeted by more than 18 percentage points to just 38.4 percent (38.4%).

This is not a gradual erosion of confidence but a major shift in perception, indicating that leaders have become acutely aware that the threat landscape has evolved beyond their current capabilities. This newfound anxiety is driven in part by the rapid emergence of AI-powered attacks, with 80 percent (80%) of leaders in 2025 stating that threats from AI are influencing their security plans.

However, this heightened sense of alarm has not catalyzed a corresponding improvement in the adoption of basic security controls. In fact, the 2025 data reveals a dangerous disconnect between perceived risk and protection.

The implementation of MFA for internal systems – a simple, highly effective control championed by cybersecurity authorities like CISA[13] – actually *decreased* from 33.6 percent (33.6%) in 2024 to 27.2 percent (27.2%) in the past year. While some of this decline is undoubtedly related to the increased deployment of passkey technology, the decrease in internal and external MFA usage (down nine percentage points YoY), combined with reduced investment in new cybersecurity tools overall (down 15 percentage points YoY), far exceeds the offset in passkey adoption.

> *“I didn’t fall for it. I called the company directly to confirm if it was actually them.” –Small Business Leader*

BEST PRACTICES

for Cyberattack and Data Breach Prevention

In an environment of escalating and evolving threats, a reactive security posture is a blueprint for failure. Active defenses, grounded in established frameworks and a commitment to fundamental cyber hygiene, are a sustainable path to resilience for SBs.

This section synthesizes authoritative guidance from the National Institute of Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA) and the Small Business Administration (SBA) into an actionable blueprint for prevention. The recommendations are structured around the core functions of the NIST Cybersecurity Framework: Govern, Identify, Protect, Detect, Respond and Recover[15], and are based on the findings from the ITRC's *2025 BIR*.

BUILDING A HUMAN FIREWALL:

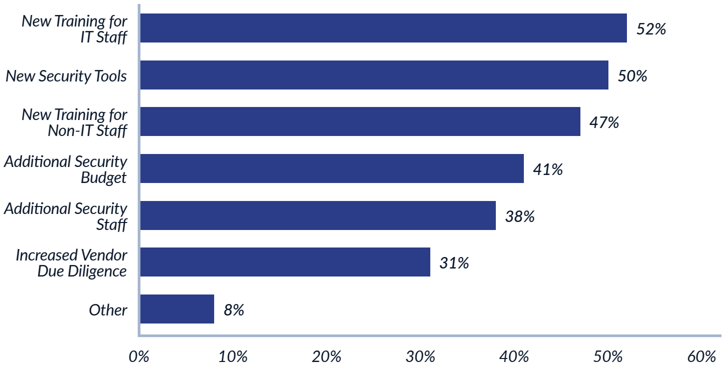
Leadership, Culture and Training

Technology is a critical component of cybersecurity, but it is not a replacement for a well-trained and cyber-aware staff. The most effective defense begins with people. CISA's Cyber Essentials guidance emphasizes that true security is rooted in a top-down "Culture of Cyber Readiness".[19] This culture must be championed by the Leaders, who are responsible for establishing cybersecurity as a core business objective, not merely an IT function.[13]

This leadership commitment must translate into a program of continuous and engaging employee training.

The need for this investment is clearly recognized by SBs themselves; in the aftermath of a breach, 46.7 percent (46.7%) of victimized businesses in 2025 implemented new training for their non-IT staff, acknowledging it as a key deficiency.[1]

Figure 8 | *Steps Taken to Prevent Further Security or Data Breaches, 2025*



Annual, check-the-box security awareness sessions are no longer sufficient. Training must be frequent and relevant, focusing on the modern threats employees face daily, including sophisticated phishing emails, targeted social engineering and the emerging challenge of AI-driven deception.[20] The goal of this training is to minimize the risk of human error, which the *Verizon Data Breach Investigations* Report (DBIR) consistently identifies as a contributing factor in the majority of successful breaches.[3]

FORTIFYING THE GATES:

Foundational Technical Controls

While a strong security culture is the foundation, it must be supported by a robust set of technical controls designed to make successful attacks as difficult and costly as possible for adversaries.

> *"They acted like they were a customer and wanted to get account information." –Small Business Leader*

ACCESS CONTROL

The principle of least privilege is a cornerstone of effective security. Employees should be granted access only to the data, systems and applications they absolutely require to perform their job functions.[20] This limits the potential damage an attacker can inflict if they compromise a user's account.

The single most critical access control for any SB to implement is **MFA**. MFA requires users to provide two or more verification factors to gain access, making it significantly harder for attackers to use stolen passwords. CISA, the Federal Communications Commission (FCC) and the SBA all strongly advocate for mandating MFA wherever possible, with the highest priority on remote access systems, administrative accounts and critical cloud services.[13]

SBs have a range of accessible MFA options, from free authenticator apps (e.g., Google Authenticator) to SMS codes and physical hardware tokens.[24] The alarming decline in MFA adoption for internal systems, from 33.6 percent (33.6%) in 2024 to just 27.2 percent (27.2%) in 2025, represents a critical, high-priority vulnerability that SBs must address immediately.[1]

NETWORK SECURITY

The network perimeter must be hardened to prevent unauthorized entry. This involves several key actions:

+ **FIREWALL CONFIGURATION**
  Firewalls should be configured with a "deny by default" rule set, meaning all traffic is blocked unless it is explicitly permitted for a legitimate business purpose.

+ **SECURE WI-FI**
  Workplace Wi-Fi networks must be secured with strong encryption (WPA2 or WPA3) and should be configured not to broadcast their network name (SSID), making them less visible to attackers.[20]

+ **NETWORK SEGMENTATION**
  Where possible, networks should be segmented into smaller, isolated zones. This contains the spread of an attack, preventing an intruder who compromises a less sensitive part of the network (like a guest Wi-Fi) from moving laterally to access critical systems like financial records or customer databases.[23]

APPLICATION SECURITY

Attackers frequently gain entry by exploiting known vulnerabilities in software for which a patch is already available. A diligent patch management program is, therefore, a simple yet powerful defense. All operating systems, web browsers and business applications must be kept up-to-date with the latest security patches. Enabling automatic updates wherever possible is a highly effective strategy to close these windows of opportunity for attackers.[13] This is particularly crucial given that vulnerability exploitation is one of the primary initial attack vectors identified in the ITRC's annual *DBR*, the *Verizon DBIR*[31] and the *IBM Cost of Data Breaches Report*.

Zero Day software flaws are also increasingly the attack vector "du jour" as threat actors increasingly rely on AI to find and exploit unknown vulnerabilities. Rule-based runtime protection and remediation tools block attacks and apply virtual patches to secure applications dramatically reduce or eliminate the risk of certain attacks.

> *"Fraudulent emails and texts indicating that I had purchased a service and that money had been transferred from my bank account." –Small Business Leader*

DATA PROTECTION

Protecting data is the ultimate goal, which means two practices are essential:

- **BACKUPS**
  Critical business data – including financial records, customer information and intellectual property – must be backed up regularly. A robust backup strategy involves maintaining multiple copies, with at least one stored offline (e.g., on a disconnected hard drive) and one offsite (e.g., in a secure cloud service). This is the most effective defense against ransomware, as it allows the business to restore its data without paying a ransom.[13]

- **ENCRYPTION**
  Data should be encrypted both "at rest" (when stored on servers and laptops) and "in transit" (when being transmitted across the network or internet). Modern operating systems have built-in tools for full-disk encryption that should be enabled on all company devices, especially laptops, which are at high risk of being lost or stolen.[13]

> *"I get them in my email all the time…but my full-time job gives us training, so I follow that in my side gig, and so far, I've been able to avoid buying into phishing scams, etc." –Small Business Leader*

MITIGATING THE INSIDER THREAT

While the threat from external, AI-powered actors is growing rapidly, the risk posed by insiders – both malicious and unintentional – remains significant. In 2025, 41.8 percent (41.8%) of breached SBs still pointed to a malicious insider as a root cause.[1] A comprehensive insider threat program, drawing on guidance from NIST and CISA, should include several key components.[7]

The program begins with pre-employment screening, including background checks for employees who will have access to sensitive information or systems.[23] During employment, the principles of least privilege and network segmentation are critical for limiting the potential scope of an insider's actions. It is also essential to maintain visibility into user activity through system and network logging, which allows security personnel to establish a baseline of normal behavior and more easily detect suspicious deviations.[23]

Finally, the program must include robust offboarding procedures. When an employee leaves the company, for any reason, all of their access credentials – to physical locations, networks, applications and cloud services—must be immediately and completely revoked to prevent post-employment misuse.[23]

COUNTERING AI-POWERED ATTACKS

The emergence of AI as a top-tier threat vector requires an evolution in defensive strategies. This new frontier of attacks directly addresses the anxieties that have caused the crisis of confidence among SB leaders.[1] Countering these threats requires a multi-layered approach that combines technology, process and human awareness.

THREAT AWARENESS

> *"AI already lies. You cannot trust a liar." –Small Business Leader*

Leaders and employees must first understand the specific nature of AI-powered attacks they now face:

+ **HYPER-REALISTIC PHISHING**
  AI has reduced the time to produce an effective phishing lure from hours to minutes. Malicious Large Language Models (LLMs) like FraudGPT and WormGPT can generate perfectly grammatical, contextually aware and highly persuasive phishing emails at scale, bypassing traditional spam filters and fooling even savvy users.[33]

+ **DEEPFAKE IMPERSONATION**
  AI can be used to create deepfake audio and video that convincingly mimics the voice and appearance of a trusted individual, such as a CEO or a key vendor. This is used in "vishing" (voice phishing) attacks to authorize fraudulent wire transfers or trick employees into revealing sensitive credentials, as seen in several high-profile, multi-million-dollar corporate scams.[10]

+ **AUTOMATED RECONNAISSANCE**
  AI tools can rapidly scan an organization's digital footprint for vulnerabilities and gather intelligence from public sources to craft highly targeted attacks.[4]

DEFENSIVE STRATEGIES

+ **TECHINICAL DEFENSES**
  The first line of defense is to fight AI with AI. SBs should consider adopting modern security solutions that incorporate AI and machine learning. These tools go beyond traditional signature-based detection and use behavioral analysis to identify anomalous activity on the network or endpoints that could indicate a sophisticated attack.[4] Advanced email security gateways with AI-driven content analysis are also better equipped to detect the nuances of AI-generated phishing messages.[36]

+ **PROCESS-BASED DEFENSES**
  Technology alone cannot stop a convincing deepfake. The most effective defense against AI-driven impersonation is a robust, non-technical verification process.

SBs must implement and strictly enforce a policy of **out-of-band verification** for any sensitive request, particularly those involving financial transactions or changes to access privileges. For example, if a CEO appears to request an urgent wire transfer via a video call or email, the employee must be required to verify the request through a separate, pre-established communication channel, such as a phone call to the CEO's known personal number or an in-person confirmation.[10] This simple, procedural step short-circuits the deception.

+ HUMAN DEFENSES

Employee security training must be updated to address these new threats. Staff should be educated on the tell-tale signs of AI-generated content, such as subtle visual artifacts in deepfake videos, the lack of emotional nuance in a cloned voice or the unnaturally perfect grammar of an AI-crafted email. Fostering a culture of healthy skepticism, where employees feel empowered to question and verify unusual or urgent requests, is vitally important.[4] NIST has created a checklist to help small business leaders build a cyber-safe culture.

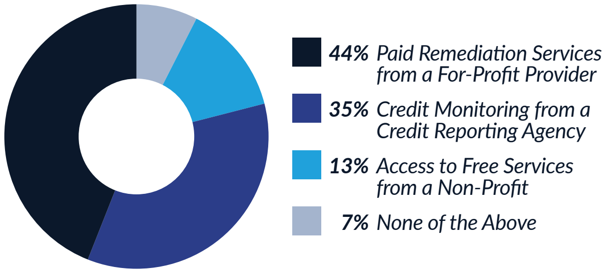
WHEN AN ATTACK SUCCEEDS

How an organization reacts during and after a security or data breach can have a greater impact on its long-term reputation and customer loyalty than the incident itself. A response characterized by transparency, timeliness and empathy can build trust, while a secretive or defensive response can destroy it.

The 2025 survey data shows that SBs largely understand this imperative. An overwhelming 89 percent (89%) of businesses that suffered a data breach notified their customers and other impacted individuals. This kind of active communication is a critical first step.

The decision of what to offer those affected is the next strategic consideration. A significant number of these businesses chose to offer remediation services, with 35.1 percent (35.1%) providing credit monitoring and 44.5 percent (44.5%) offering paid remediation services from a third-party provider.

Figure 9 | *Remediation Services to Customers After Breach, 2025*

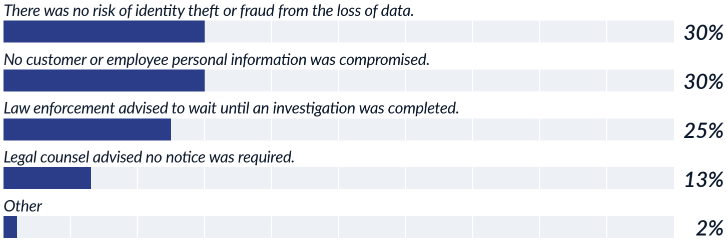


Often mandated by state laws for large enterprises, offering tangible support to victims may fall outside the requirements of a state data breach notification law for SBs. Nevertheless, the data shows that providing for breach victims is a standard practice for mitigating the loss of customer trust, which remained a top concern for 39.6 percent (39.6%) of breached SBs in 2025.

> *"Would not use AI exclusively." –Small Business Leader*

For the small percentage of businesses that did not send notifications, the primary reasons cited were that no customer or employee personal information was compromised (30.2%) or that there was no perceived risk of identity theft from the lost data (30.2%). While these may be valid technical assessments, the decision not to notify must always be made in close consultation with legal counsel to ensure compliance with the complex web of state and federal data breach notification laws and regulations.

Figure 10 | *Reasons for Not Notifying Customers After Breach, 2025*



NAVIGATING THE FUTURE OF SB CYBERSECURITY

The findings of this report paint a stark picture of a new and challenging era for small and medium-sized businesses. The cybersecurity landscape has fundamentally, and perhaps irrevocably, changed.

The era of predictable, human-scale threats has been superseded by a new reality of automated, intelligent and massively scalable attacks powered by AI. This technological shift has not only altered the methods of attack but has also profoundly impacted the financial stability, operational resilience and confidence of SB leaders.

> *"I really do not trust AI at all." –Small Business Leader*

Survival in this new environment is not a matter of finding a single technological solution. It demands a holistic and strategic commitment to building a resilient organization. The path forward is clear and rests on three core pillars:

+ **A CULTURE OF SECURITY**
  Resilience begins with people. Leadership must champion cybersecurity as a core business value, fostering a culture of vigilance and empowering every employee, through continuous training and support, to become part of a "human firewall."

+ **MASTERY OF THE FUNDAMENTALS**
  In the face of overwhelming complexity, the most powerful response is a renewed focus on the basics. Rigorous implementation of foundational controls – MFA, diligent patch management, robust data backups and the principle of least privilege – remains the most effective and highest-return investment an SB can make in its defense.

+ **PREPAREDNESS FOR CRISIS**
  Acknowledging that prevention can fail is not a sign of weakness but of strategic maturity. A well-documented, comprehensive and regularly rehearsed Incident Response Plan is the essential blueprint for navigating a crisis, minimizing damage and ensuring a swift recovery.

The threats facing SBs are daunting, but they are not insurmountable. The strategies for building resilience are well-established and accessible. For those leaders who can move past the fear and commit to a strategic, active approach, the future, while challenging, remains secure.

EDITOR'S NOTE & WORKS CITED

EDITOR'S NOTE

This report was written with the assistance of Google's Gemini AI. Gemini was used to identify secondary research and information related to the findings in the ITRC's 2025 Small Business Impact survey. The analysis of the survey findings was conducted by human beings. Gemini identified the following sources that were used in the development of this report.

WHEN AN ATTACK SUCCEEDS

1. 2024 ITRC Small Business Impact Survey
   2025 ITRC Small Business Impact Survey

2. Verizon DBIR: Small Businesses Bearing the Brunt of Ransomware Attacks

3. 2025 Verizon Data Breach Investigations Report, *Keepnet Labs*

4. Most Common AI-Powered Cyberattacks, *CrowdStrike*

5. The Dark Side of AI: What Small Businesses Need to Know About Emerging Cyber Attacks

6. AI-Driven Phishing And Deep Fakes: The Future Of Digital Fraud, *Forbes*

7. Insider Threat Best Practices Guide, 3rd Edition, *SIFMA*

8. Insider Threat Mitigation, *Cybersecurity and Infrastructure Security Agency*

9. AI Phishing Attacks: How Big is the Threat? (+Infographic), *Hoxhunt* | *Accessed August 27, 2025*

10. Top 10 Examples of Deepfake Across the Internet, *HyperVerge* | *Accessed August 27, 2025*

11. 7 Deepfake Attacks Examples: Deepfake CEO Scams, *Eftsure US* | *Accessed August 27, 2025*

12. Are successful deepfake scams more common than we realize?, *IBM* | *Accessed August 27, 2025*

13. Cyber Guidance for Small Businesses, *CISA* | *Accessed August 27, 2025*

14. CISA Small Business Protections Against Cyber Attacks, *First Western Trust* | *Accessed August 27, 2025*

15. The NIST Small Business Information Security Fundamentals Guide | *Accessed August 27, 2025*

16. NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide | *Accessed August 27, 2025*

17. NIST Cybersecurity Best Practices, *Sprinto* | *Accessed August 27, 2025*

18. NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide | *Accessed August 27, 2025*

19. Cyber Essentials, *CISA* | *Accessed August 27, 2025*

20. Cybersecurity for Small Businesses, *Federal Communications Commission* | *Accessed August 27, 2025*

21. In Today's Economy, Cyber Safety Is Critical to Small Business Success | *Accessed August 27, 2025*

22. Strengthen your cybersecurity, *U.S. Small Business Administration* | *Accessed August 27, 2025*

23. 14 ways to protect your business from insider threats, *PDQ* | *Accessed August 27, 2025*

24. A Small Business Guide to Implementing Multi-Factor Authentication (MFA), *Abacus* | *Accessed August 27, 2025*

25. 8 Multi-Factor Authentication (MFA) Types: A Complete Overview, *Frontegg* | *Accessed August 27, 2025*

26. Types of Multi-Factor Authentication & How to Pick the Best, *LoginRadius* | *Accessed August 27, 2025*

27. How to Configure a Firewall in 5 Steps, *Security Metrics* *Accessed August 27, 2025*

28. Understanding and Establishing Important Firewall Rules for Small Business Security | *Accessed August 27, 2025*

29. Cyber Safety Tips for Small Business Owners | *Accessed August 27, 2025*

30. Protect Your Small Business from Cybersecurity Attacks *Accessed August 27, 2025*

31. Verizon's 2025 Data Breach Investigations Report: Alarming surge in cyberattacks through third-parties, News Release | *Accessed August 27, 2025*

32. What Is an Insider Threat? Definition, Types, and Prevention, *Fortinet* | *Accessed August 27, 2025*

33. The Rise of AI-Powered Phishing 2025 [Plus What to Do About it?], *CybelAngel* | *Accessed August 27, 2025*

34. The Rise of AI Phishing and What it Means for the Future of Scammers - Transactional Email API Service For Developers, *Mailgun* | *Accessed August 27, 2025*

35. Cyber Attacks on Small Businesses in 2025, *Defense Guide* *Accessed August 27, 2025*

36. Artificial Intelligence (AI) in Cybersecurity: The Future of Threat Defense, *Fortinet* | *Accessed August 27, 2025*

37. AI-Powered Cyberattacks - How to Detect, Prevent, & Defend Against Intelligent Threats | *Accessed August 27, 2025*

38. Incident Response Plan (IRP) Basics, *CISA* | *Accessed August 27, 2025*

39. Top 8 Incident Response Plan Templates, *BlueVoyant* *Accessed August 27, 2025*

40. How To Create an Incident Response Plan For Small Business, *PurpleSec* | *Accessed August 27, 2025*

41. Small Business Guide: Response & Recovery, *NCSC.GOV.UK* | *Accessed August 27, 2025*

ABOUT
ITRC & Mitek

IDENTITY THEFT RESOURCE CENTER

Founded in 1999, the Identity Theft Resource Center® (ITRC) is a national nonprofit organization established to empower and guide consumers, victims, business and government to minimize risk and mitigate the impact of identity compromise and crime. Through public and private support, the ITRC provides no-cost victim assistance and consumer education through its website live-chat IDTheftCenter.org and toll-free phone number 888.400.5530. The ITRC also equips consumers and businesses with information about recent data breaches through its data breach tracking tool. The ITRC offers help to specific populations, including the deaf/hard of hearing and blind/low vision communities.

MITEK

Mitek Systems protects what's real across digital interactions in a world of evolving threats. Mitek helps businesses verify identities, prevent fraud before it happens, and deliver secure, seamless digital experiences in the face of rapidly advancing AI-generated threats. From account opening to authentication and deposit, Mitek's technology safeguards critical digital interactions. More than 7,000 organizations rely on Mitek to protect their most important customer connections and stay ahead of emerging risks. Learn more at MitekSystems.com.

BIR

IDENTITY THEFT RESOURCE CENTER

2025 Business Impact Report

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, contact the ITRC by email at BIR@IDTheftCenter.org.

FOR MEDIA

For any media-related inquiries, please email Media@IDTheftCenter.org.

CONTRIBUTORS

Thanks to the team responsible for the *2025 ITRC Business Impact Report*:

Analysis & Editorial – James E. Lee
Layout & Design – Meagan Lechleiter

This report was made possible through the support of ***Mitek****.*

IDENTITY THEFT RESOURCE CENTER

DECEMBER 2025

APPENDIX

2025 SMALL BUSINESS IMPACT SURVEY

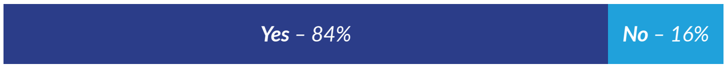
Survey Results

Demographics

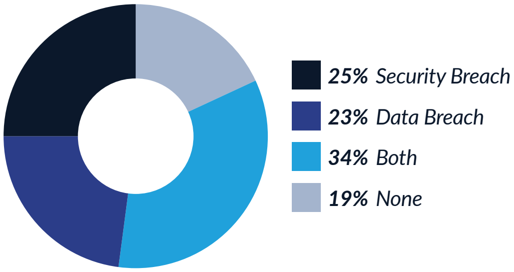
2025 SMALL BUSINESS IMPACT SURVEY

SURVEY RESULTS

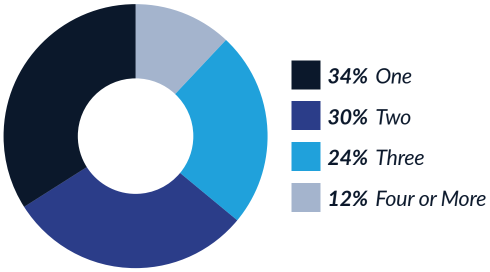
Q1 | *Are you an owner or leader of a small business with fewer than 500 employees, including solopreneurs and gig workers?*



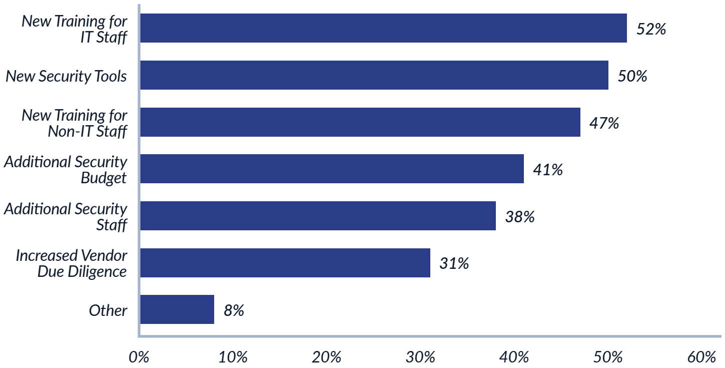
Q2 | *Has your company experienced a security or data breach in the past 12 months?*



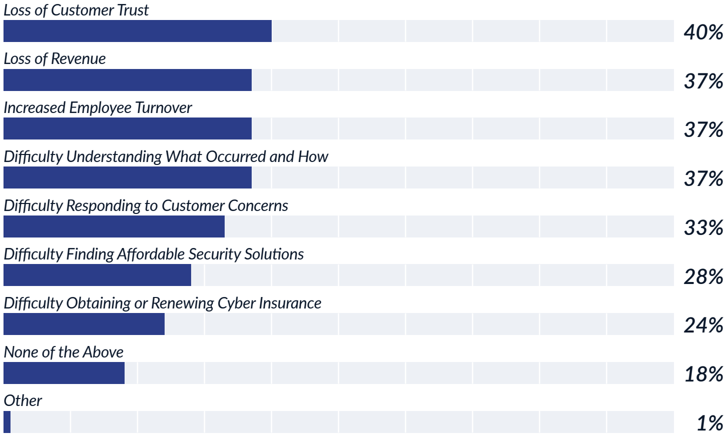
Q3 | *How many data or security incidents have you experienced in the past 12 months?*



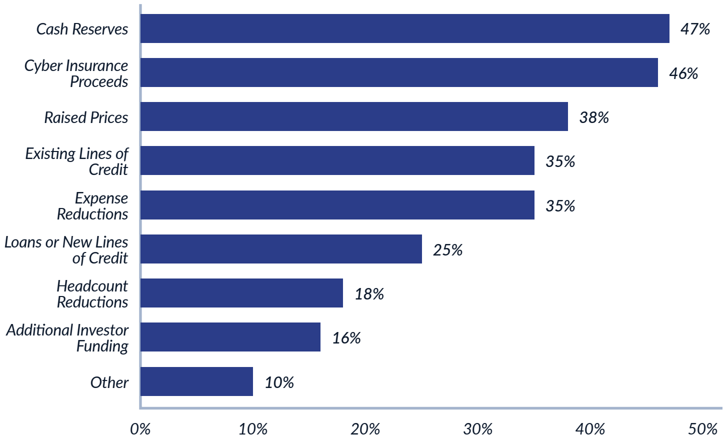
Q4 | *What steps have you taken to prevent additional security or data breaches in the future? Check all that apply.*



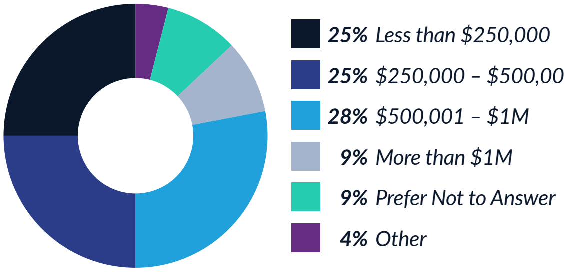
Q5 | *Did you experience any of the following issues after your cyber incident? Select all that apply.*



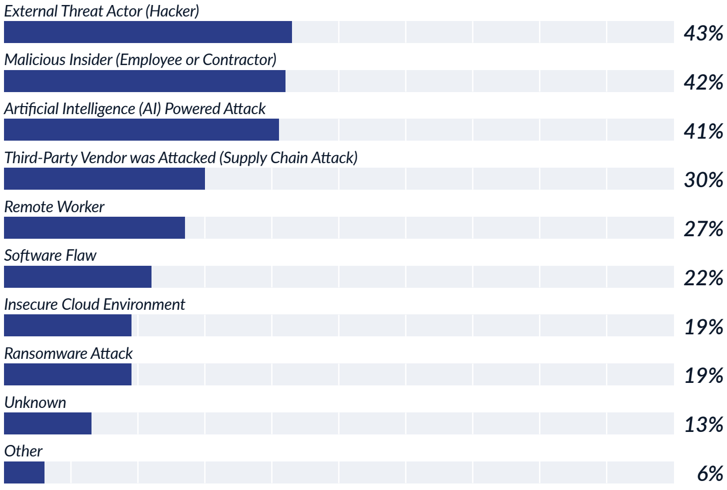
Q6 | *How did you address the financial impacts of the security/data or scam incident? Select all that apply.*



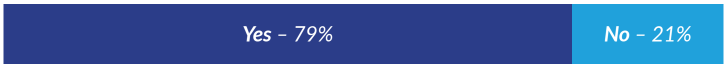
Q7 | *What was the approximate total financial impact of the security/data breach or scam, including lost revenue, lost customers, legal costs, fines and penalties, insurance, marketing costs, improved security, etc.?*



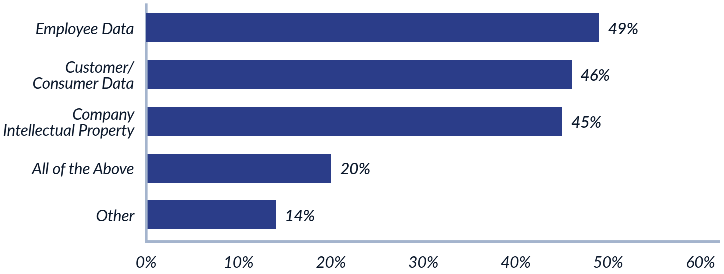
Q8 | *What was the root cause(s) of the recent security or data incident? Check all that apply.*



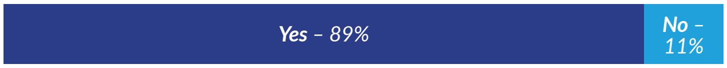
Q9 | *Have you been the target or victim of a phishing, impersonation, or other identity-related scam involving a fraudulent text, email, voicemail, or phone/video call in the past 12 months?*



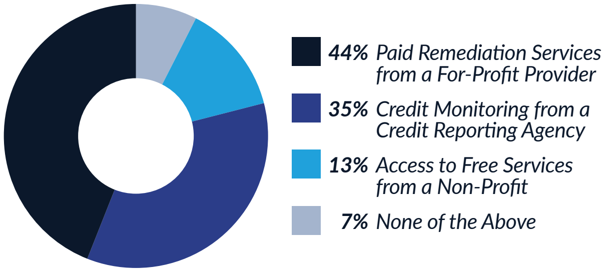
Q10 | *What data was compromised? Select all that apply.*



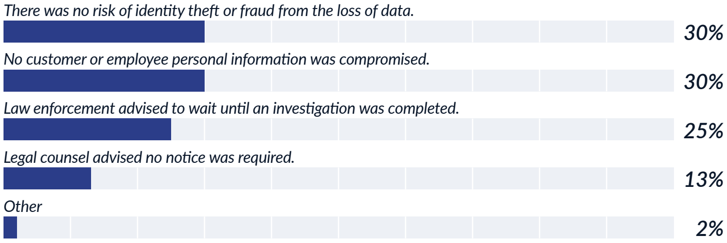
Q11 | *If you were the victim of a data breach, did you send a notice to alert customers and other people impacted by the incident?*



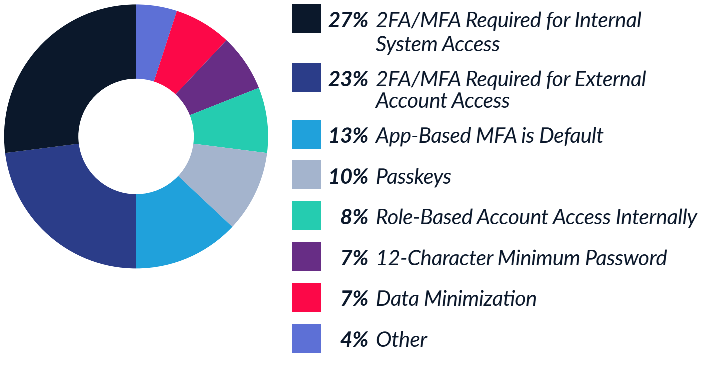
Q12 | *Did you offer remediation services to customers or consumers impacted by the breach?*



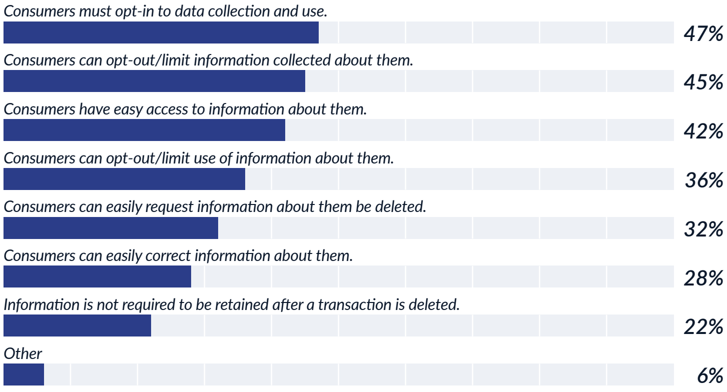
Q13 | *If you did not send a notice to customers or other impacted people after the incident, why not?*



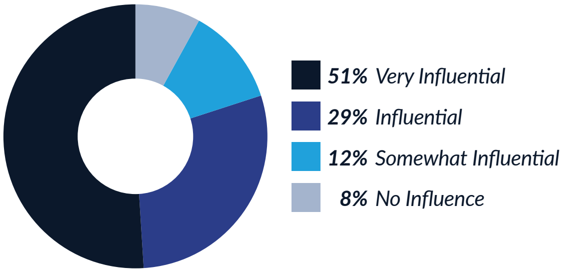
Q14 | *Do you currently utilize any of the following solutions to help protect business and customer data?*



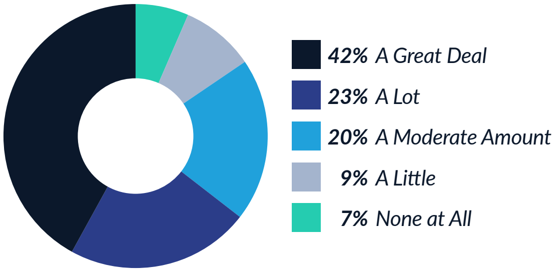
Q15 | *Do you follow any data privacy best practices? Select all that apply.*



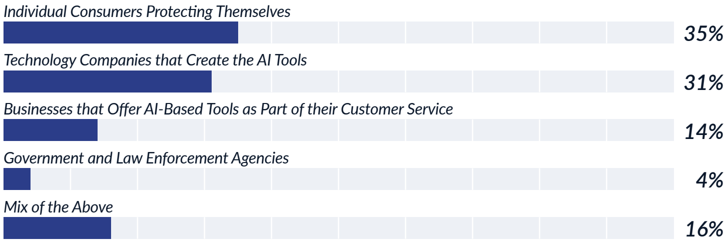
Q16 | *To what extent are threats from artificial intelligence (AI) technologies, such as malware, voice cloning, deepfakes or sophisticated phishing emails, influencing your security plans?*



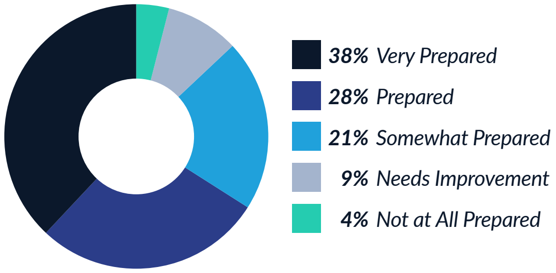
Q17 | *How much would you trust an AI-powered security system (e.g., AI fraud alerts from your bank, AI identity monitoring services, etc.) to protect your company from future attacks?*



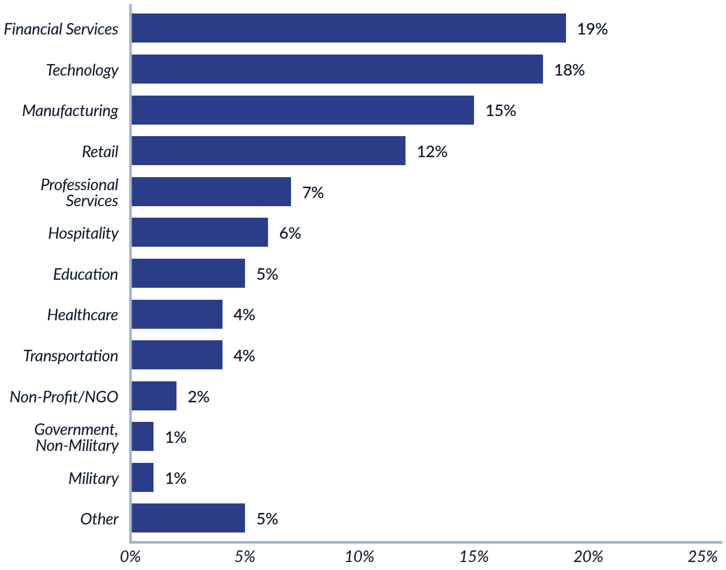
Q18 | *In your opinion, who should hold the primary responsibility for protecting people and organizations from AI-driven identity fraud?*



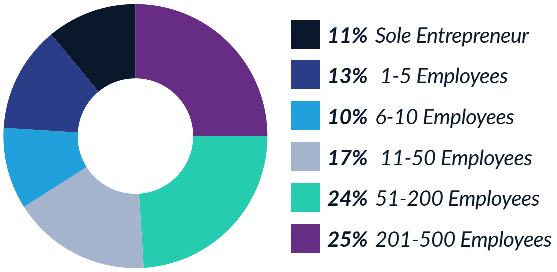
Q19 | *How well prepared are you to protect against a cyberattack or recover from a data breach?*



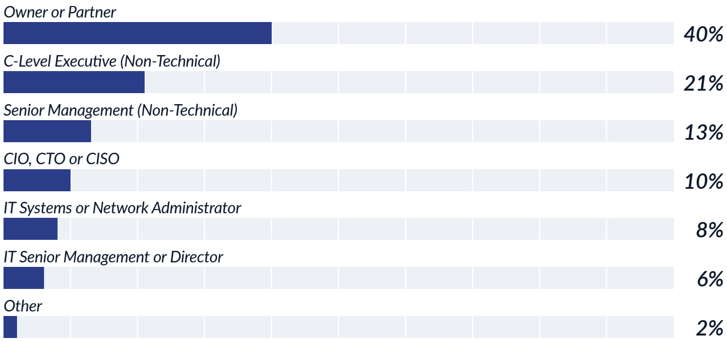
Q20 | *What is your industry?*



Q21 | *How many employees are in your company?*

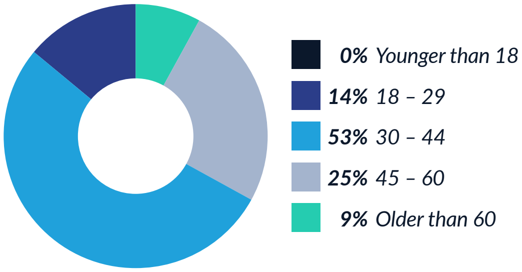


Q22 | *What is your title?*

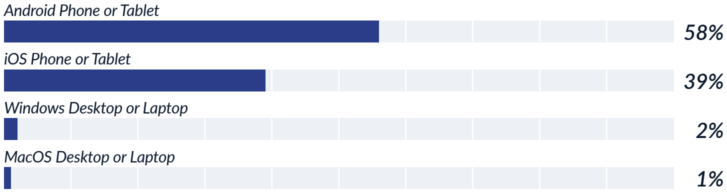


DEMOGRAPHICS

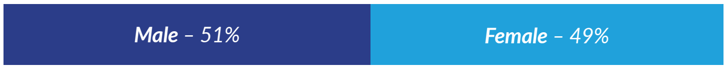
Age



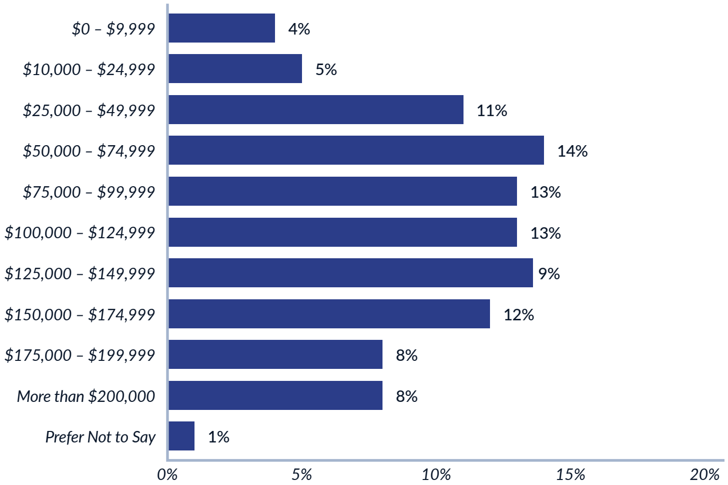
Device Type



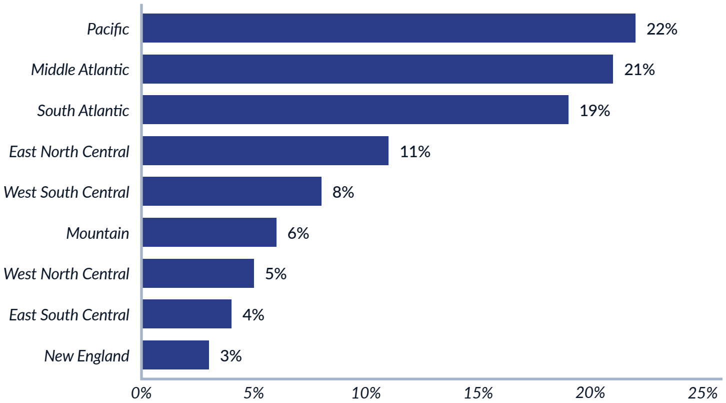
Gender



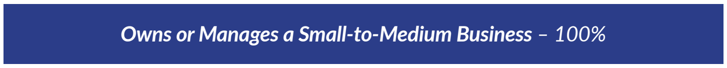
Household Income

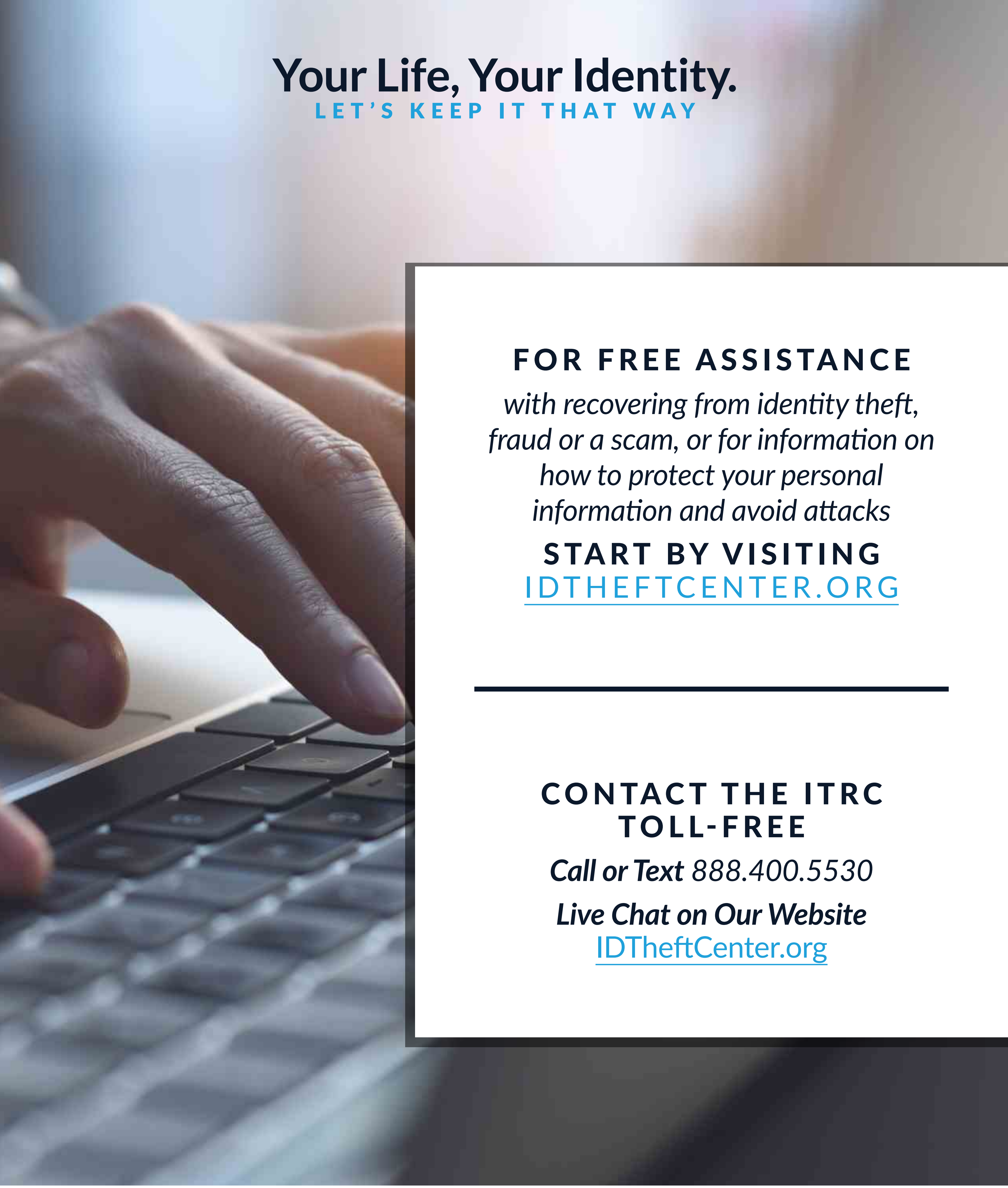


Major U.S. Region



Small-to-Medium Business





Your Life, Your Identity.

LET'S KEEP IT THAT WAY

FOR FREE ASSISTANCE

with recovering from identity theft, fraud or a scam, or for information on how to protect your personal information and avoid attacks

START BY VISITING

IDTHEFTCENTER.ORG

CONTACT THE ITRC TOLL-FREE

Call or Text *888.400.5530*

Live Chat on Our Website

IDTheftCenter.org

ITRC | IDENTITY THEFT RESOURCE CENTER