TRI COUNTIES BANK | RESEARCH

Small Businesses and Cybersecurity

Results of a nationwide survey of small business owners on cyberattacks, cybersecurity measures, and related topics.

tri counties bank

California's *local* bank

Introduction

Tri Counties Bank's commitment to California communities includes equipping businesses with insights on the issues most critical to success in today's marketplace. We are proud to share our latest research report, Small Businesses and Cybersecurity.

This report examines how small business owners are addressing cyberattacks, the potential effects on their businesses, and the broader cybersecurity considerations influencing their decisions.

This research was conducted through a survey administered by The Harris Poll, a leading global market research firm. The study gathered perspectives from more than 300 small business owners representing a diverse range of industries across the United States.

Helping businesses navigate shifting economic conditions has always been central to Tri Counties Bank's mission. As *California's Local Bank*, we are committed to delivering exceptional service, innovative digital tools, and trusted partnerships to support businesses at every stage of their journey.

Richard P. Smith
Tri Counties Bank
President, CEO, and Chairman of the Board

About Tri Counties Bank

Established in 1975, Tri Counties Bank is a wholly-owned subsidiary of TriCo Bancshares (NASDAQ: TCBK) headquartered in Chico, California with corporate offices in Roseville, South San Francisco, and Bakersfield, with assets of nearly $10 billion and 50 years of financial stability.

Tri Counties Bank is dedicated to providing exceptional service for individuals and businesses throughout California with more than 75 locations, advanced mobile and online banking, and access to approximately 40,000 surcharge-free ATMs nationwide.

As *California's Local Bank,* Tri Counties Bank prioritizes serving clients with local bankers and local decision-making, backed by corporate philanthropy, community engagement, employee volunteerism, and investments. Recognized by various publications as among the Top Workplaces and Best Banks, Tri Counties Bank recruits and retains diverse and talented team members.

Summary

Cyberattacks pose a significant threat to U.S. small businesses.

Small businesses are concerned that a cyberattack could have substantial adverse impacts on their business.	Eighty-seven percent (87%) of U.S. small business owners (SBOs) believe a cyberattack could have severe financial consequences (59% strongly agree, 28% somewhat agree), while 84% agree it could damage customer relationships. Four in five SBOs (81%) agree that small businesses are prime targets for cyberattacks. Roughly one in seven SBOs (15%) say they experienced a cyberattack during the past three years.
Malware is the most concerning type of cyberattack for SBOs.	More than seven in ten SBOs (72%) consider malware or malicious software to be the cyber risk of greatest concern for their business.
Small businesses are prepared for a cyberattack to some extent and have cybersecurity measures in place.	Nearly three in four SBOs (73%) have a plan in place to respond to a cyberattack if they were to experience one. The majority of SBOs report using cybersecurity measures in their business that include regular software updates (59%), the required use of strong passwords (59%), and technical network security protocols, such as firewalls, VPNs, etc. (52%).
Small businesses believe they share cybersecurity responsibility mainly with their tech providers.	Responsibility for the cybersecurity of small businesses lies mainly with the businesses themselves (63%), technology vendors (56%), and internet providers (55%) according to SBOs.
Tech vendors and providers, along with staff at the business, have a key role in preventing cyberattacks.	SBOs consider technology vendors (87%), the business's internet providers (81%), and their staff (80%) to be highly effective in preventing or protecting their business from a cyberattack.
Private cybersecurity firms are considered effective in protecting small businesses from cyberattacks.	Private cybersecurity firms are viewed by nine in ten SBOs (91%) as very or somewhat effective in preventing or protecting small businesses from a cyberattack, while 73% believe the banking industry is very or somewhat effective.

Methodology

This survey was conducted online within the United States by The Harris Poll on behalf of Tri Counties Bank from May 5–11, 2026 among 306 small business owners (defined as CEO, CFO, Owner, Partner, or President). The sampling precision of Harris online polls is measured by using a Bayesian credible interval. For this study, the sample data is accurate to within +/- 5.6 percentage points using a 95% confidence level.

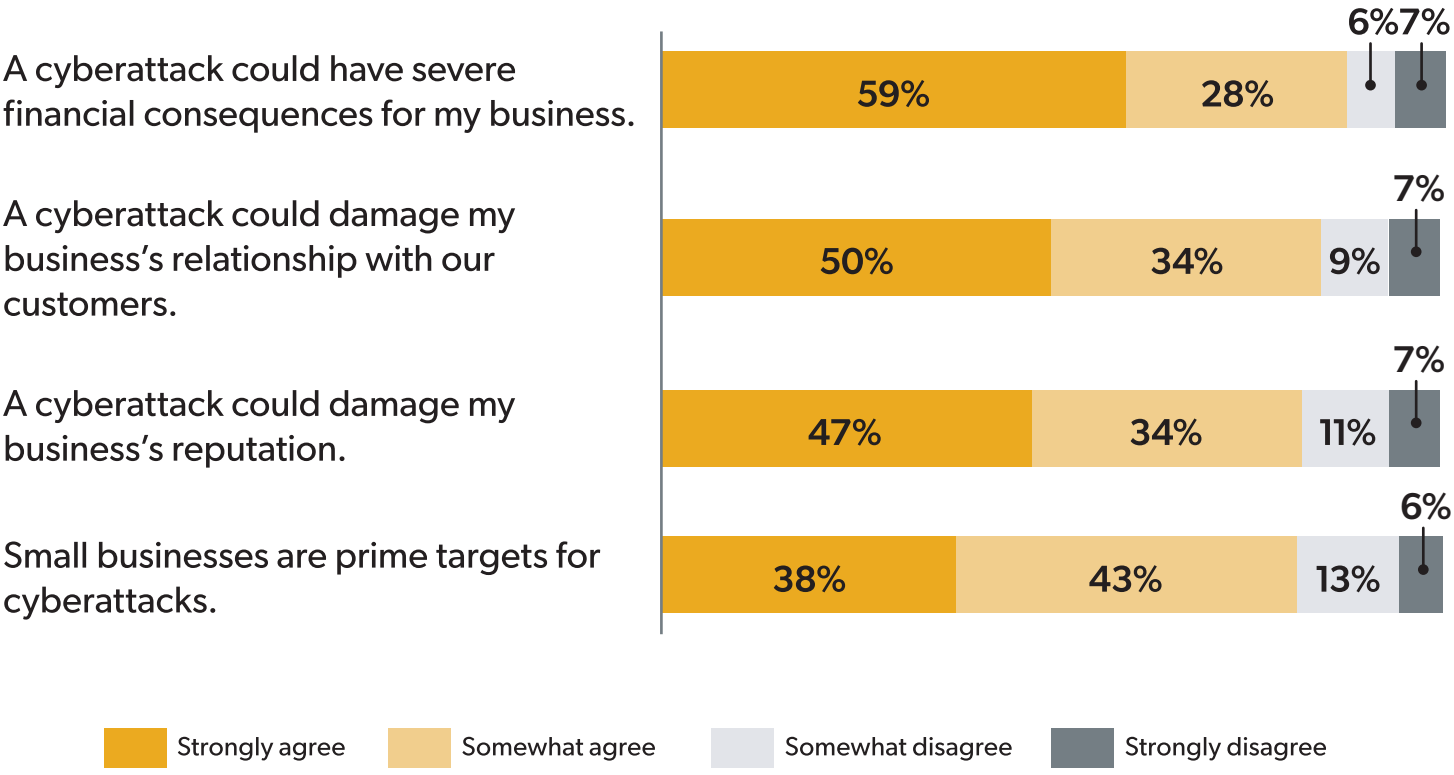
Key Findings

CYBERATTACKS AND SMALL BUSINESSES

U.S. small business owners (SBOs) have concerns that a cyberattack could have substantial adverse impacts on their business. Nearly nine in ten agree that a cyberattack could have severe financial consequences (59% strongly agree, 28% somewhat agree), while nearly as many believe it could damage the relationship with their customers (84% agree) or damage their business reputation (81% agree). Four in five SBOs (81%) agree that small businesses are prime targets for cyberattacks.

Perceptions of cyberattacks and small businesses

Base: SBOs (n=306)



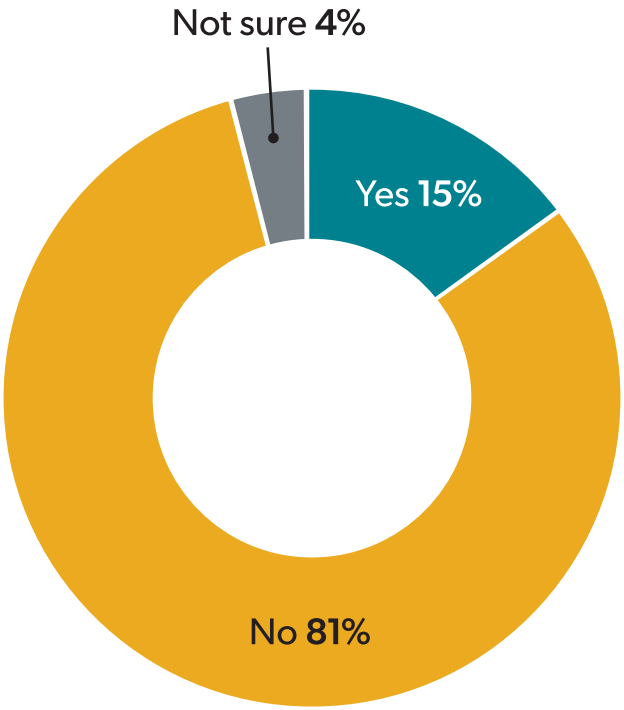
Survey Question | A cyberattack is an attempt by cybercriminals, hackers, or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying or exposing information. Please share your thoughts about cyberattacks by indicating your level of agreement with the statements below.

CYBERATTACK EXPERIENCE

Roughly one in seven U.S. small business owners (SBOs) (15%) say they have experienced a cyberattack during the past three years, although the majority of SBOs (81%) did not.

Experienced a cyberattack in past three years

Base: SBOs (n=306)



Survey Question | Has your business experienced a cyberattack within the past three years?

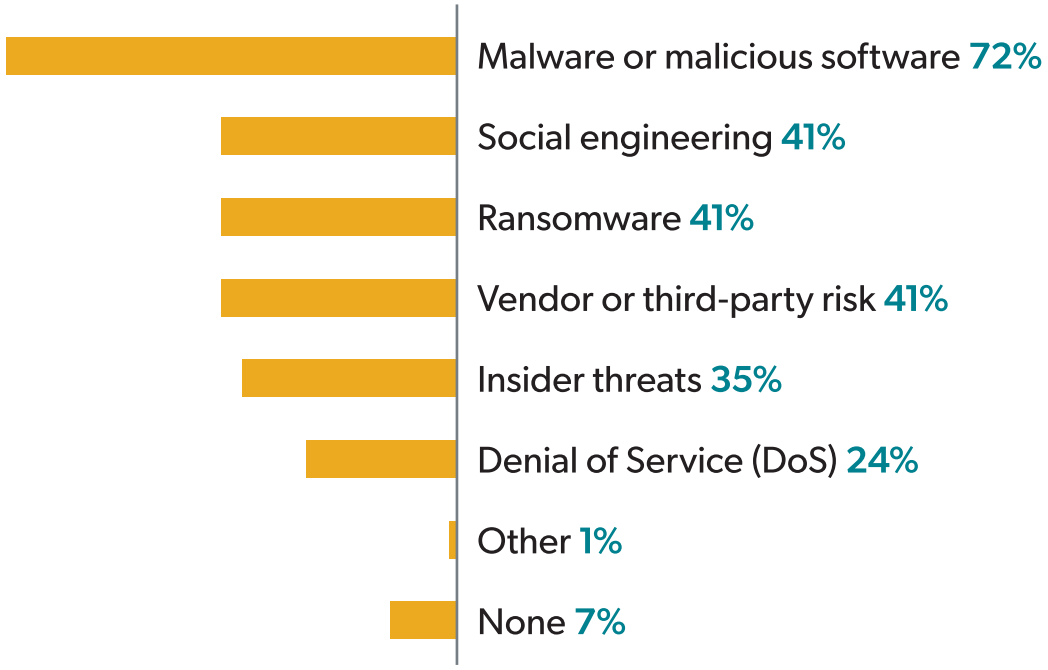
MOST CONCERNING TYPES OF CYBERATTACKS

Malware or malicious software is the most concerning type of cyberattack for U.S. small business owners (SBOs). More than seven in ten (72%) consider malware to be of greatest concern for their business.

Other potential types of cyberattacks are of concern, but to a far lesser extent. These include social engineering (41%), ransomware (41%), vendor or third-party risk (41%), and insider threats (35%).

Types of cyberattacks of greatest concern

Base: SBOs (n=306). Total exceeds 100% (multiple responses allowed)



Malware or malicious software	Any computer program designed to damage, spy on, or steal from your computer, phone, or network.
Social engineering	Phishing, spoofing, spear, etc., that trick or manipulate people into revealing information or taking a desired action.
Ransomware	Type of malware used to extort money.
Vendor or third-party risk	Breach, supply chain, etc.
Insider threats	Misuse of access to sensitive information from within an organization by current or former employees, contractors, etc.
Denial of service (DoS)	Network server disruption by overwhelming it with excessive traffic.

Survey Question | Which of the following types of cyberattacks, if any, are of greatest concern for your business? Please select all that apply.

RESPONSE TO CYBERATTACKS

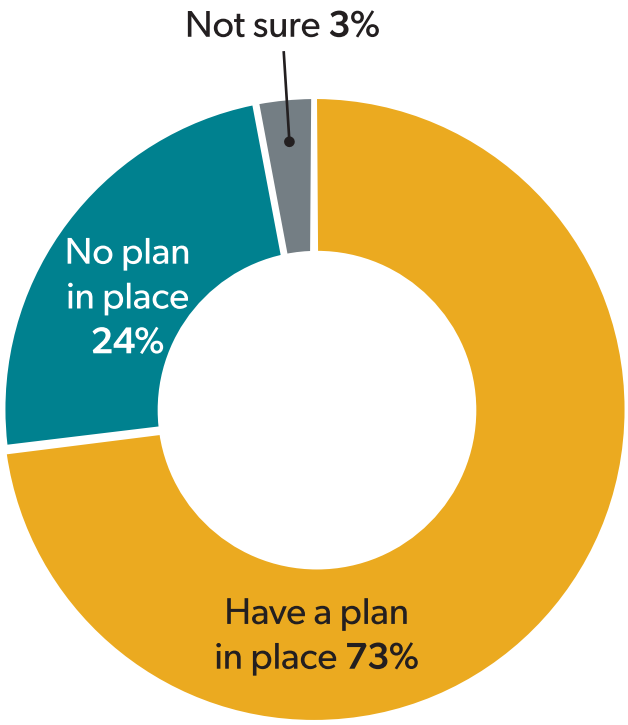
Nearly three in four U.S. small business owners (SBOs) (73%) have a plan in place to respond to a cyberattack if they were to experience one, while nearly one in four (24%) do not have a plan.

The most frequently noted components of the plan are focused on data, systems, and recovery:

- Regular data backup and recovery procedures (46%)
- Steps for restoring systems and data (38%)
- A plan for notifying affected individuals in case of a data breach (30%)
- Employee training on how to respond to a cyber incident (29%)
- Procedures for identifying and containing a cyberattack (28%)
- A process for reporting incidents to authorities or regulators (26%)

Business has plan to respond to cyberattacks

Base: SBOs (n=306)



Survey Question | Which of the following, if any, are part of your business's plan to respond to a cyberattack if you experienced one? Please select all that apply.

Components of business's plan to respond to a cyberattack

Base: SBOs (n=306). Total exceeds 100% (multiple responses allowed).

Have a formal plan in place (Net)		**73%**
Regular data backup and recovery procedures	46%	
Steps for restoring systems and data (e.g., backups, recovery plans)	38%	
A plan for notifying affected individuals in case of a data breach	30%	
Employee training on how to respond to a cyber incident	29%	
Procedures for identifying and containing a cyberattack	28%	
Process for reporting incidents to authorities or regulators	26%	
Coordination with external partners (e.g., IT providers, cybersecurity firms, legal counsel)	25%	
Communication plan for employees	25%	
Business continuity or contingency plans to keep operations running	24%	
Communication plan for customers or clients	24%	
Cyber insurance coverage as part of response planning	21%	
Regular testing or simulation of the response plan	20%	
Defined roles and responsibilities for responding to an incident	19%	
Documentation of past incidents and lessons learned	14%	
Other	1%	
Not sure	3%	
Not applicable – we don't have a formal plan in place		**24%**

CYBERSECURITY MEASURES USED

A majority of U.S. small business owners (SBOs) report using cybersecurity measures in their business, such as regular software updates (59%), required use of strong passwords (59%), and technical network security protocols like firewalls, Virtual Private Networks (VPN), etc. (52%).

About half of SBOs use required secure data backups (50%), multi-factor authentication (49%), and email security (47%) in their business.

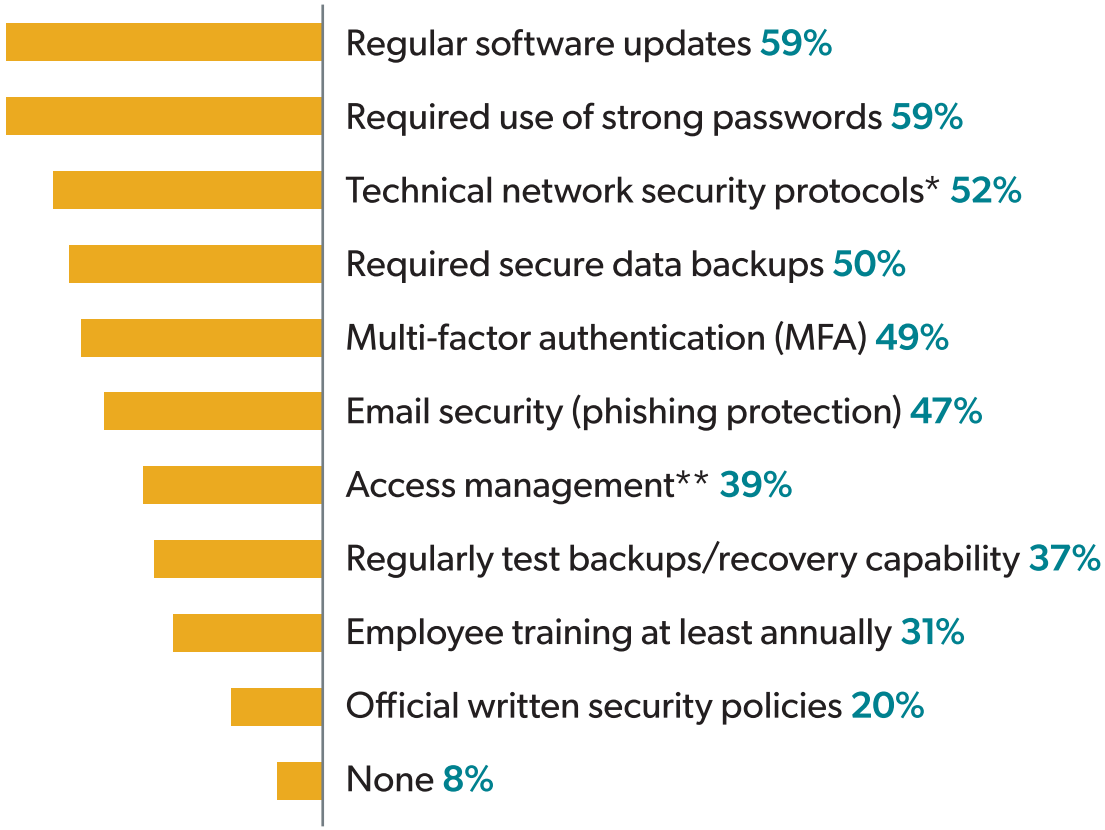
Less frequently used cybersecurity measures include access management (39%), regular testing of backup or recovery capability (37%), employee training at least annually (31%), and official written security policies (20%).

9 in 10

U.S. small businesses (92%) have some type of cybersecurity measure(s) in place.

Cybersecurity measures used in business

Base: SBOs (n=306). Total exceeds 100% (multiple responses allowed).



* e.g., firewalls, VPNs, secure Wi-Fi

** Controlling who can get into which systems, data, and applications, and what they are allowed to do once they are in

Survey Question | Which cybersecurity measures, if any, are currently used in your business? Please select all that apply.

RESPONSIBILITY FOR CYBERSECURITY

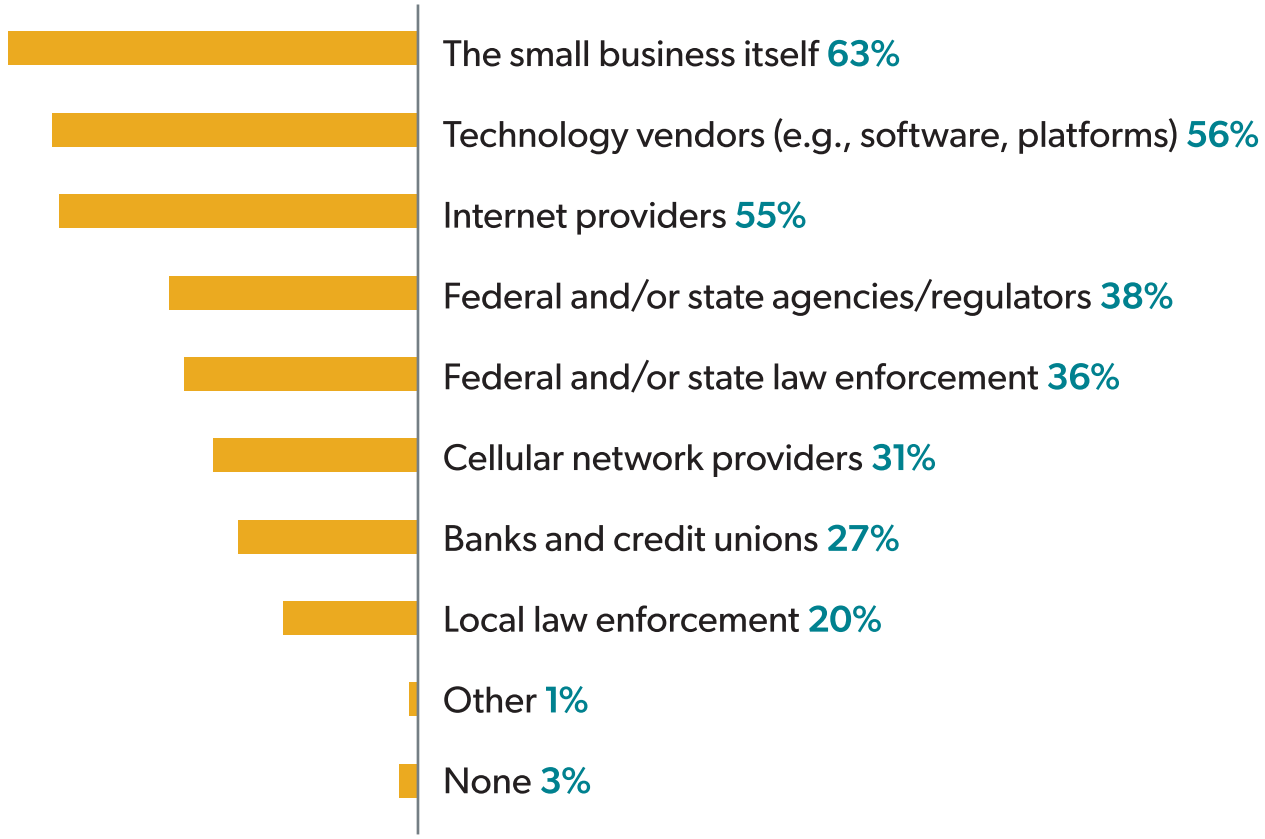
Nearly two in three U.S. small business owners (SBOs) (63%) believe the small business itself has responsibility for the cybersecurity of the business. However, over half think that technology vendors (56%) and internet providers (55%) also share in the responsibility.

Fewer believe that federal and/or state agencies/regulators (38%) and federal and/or state law enforcement (36%) have a level of responsibility for the cybersecurity of small businesses.

Less than a third of SBOs feel cellular network providers (31%), banks and credit unions (27%), and local law enforcement (20%) have responsibility for cybersecurity.

Who should be responsible for the cybersecurity of small businesses?

Base: SBOs (n=306). Total exceeds 100% (multiple responses allowed).



Survey Question | Which of the following do you believe should be responsible, at least to some extent, for the cybersecurity of small businesses? Select all that apply.

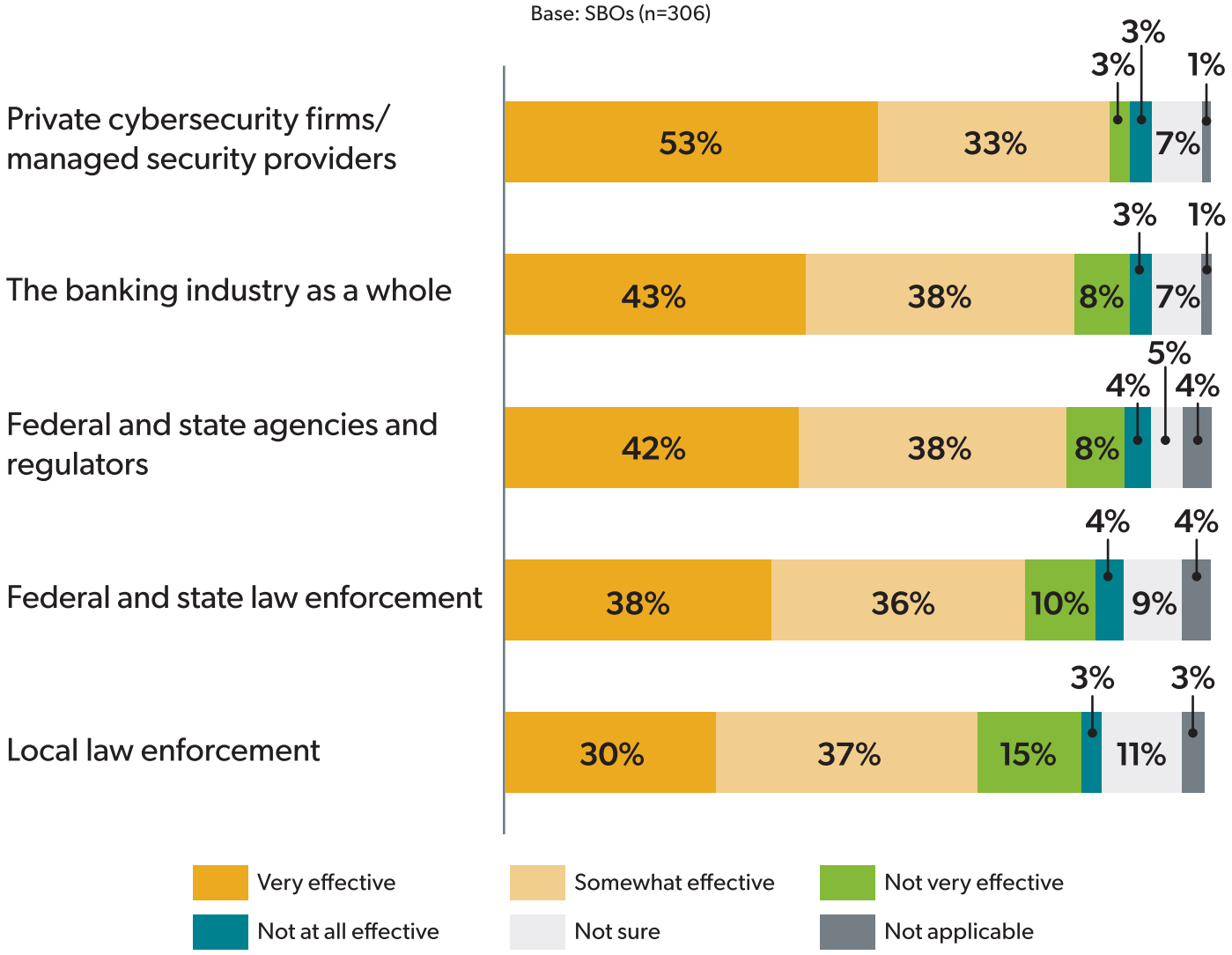
CYBERATTACK PREVENTION AND PROTECTION | MY BUSINESS

Most U.S. small business owners (SBOs) believe that technology vendors are or would be effective in preventing or protecting their business from a cyberattack (53% very effective, 33% somewhat effective).

Four in five SBOs consider the business's internet providers (81%) and the staff at their business (80%) as effective in preventing or protecting the business from a cyberattack, while fewer believe their bank or credit union (74%) and their cellular network provider (67%) would be effective in cyberattack prevention or protection efforts.

Effectiveness in preventing/protecting my business from cyberattacks

Base: SBOs (n=306)



Survey Question | How effective do you believe each of the following are/would be at preventing or protecting your business from a cyberattack?

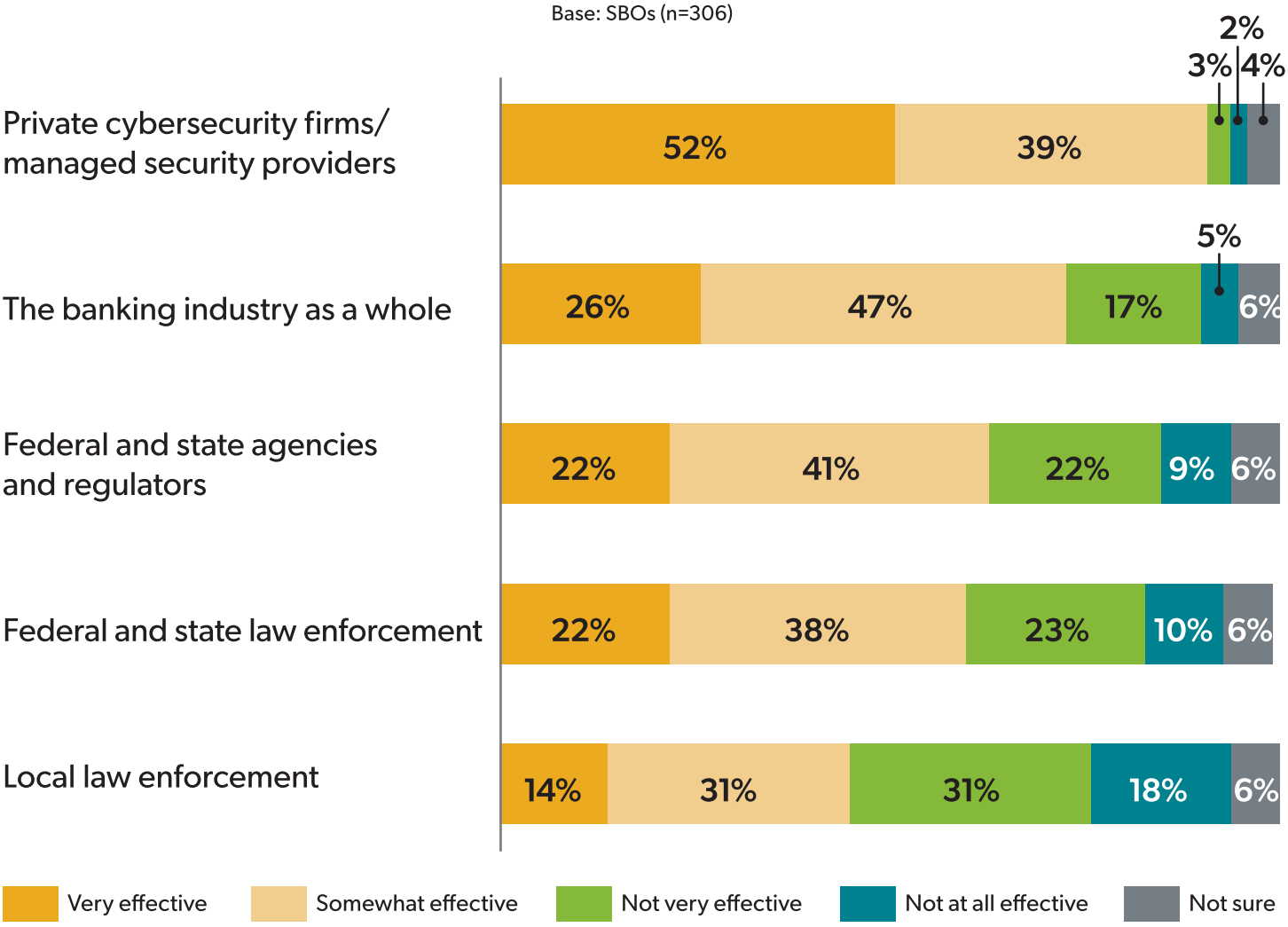
CYBERATTACK PREVENTION AND PROTECTION | SMALL BUSINESSES

Not surprisingly, private cybersecurity firms or managed security providers are viewed by nine in ten U.S. small business owners (SBOs) as effective in preventing or protecting small businesses from a cyberattack (52% consider them very effective, 39% somewhat effective). In comparison, nearly three in four SBOs (73%) believe the banking industry is effective, to some extent, in preventing or protecting small businesses from a cyberattack.

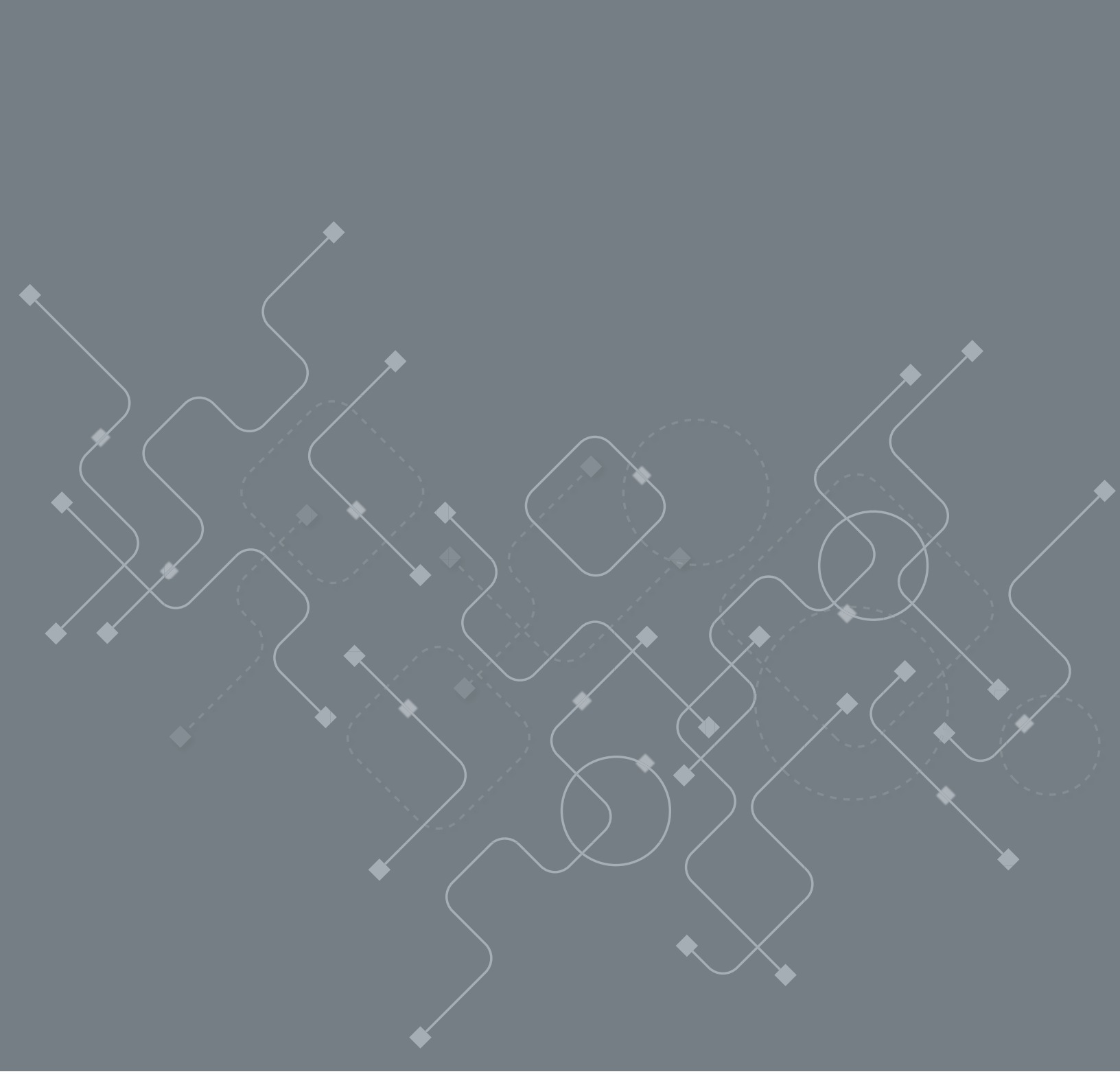
Fewer SBOs have confidence in the effectiveness of federal and state agencies and regulators (63%), federal and state law enforcement (61%), or local law enforcement (45%).

Effectiveness in preventing/protecting small businesses from a cyberattack

Base: SBOs (n=306)



Survey Question | How effective do you believe each of the following are/would be in preventing or protecting small businesses in general from a cyberattack?



tri counties bank

California's *local* bank

1-800-922-8742 | TriCountiesBank.com

EQUAL HOUSING LENDER

Bank NMLS #458732

Member FDIC

(07/26)