Optery FOR BUSINESS

The Data Behind the Deception
Optery 2026 Enterprise Social Engineering Survey Report

Table of Contents

Foreword

In recent years there have been several documented examples of threat actors using commercial data brokers as part of their reconnaissance and targeting process against organizations.

Multiple cases illustrate the pattern. For example, leaked Black Basta communications showed members using data brokers[1] to identify targets and support social engineering. Federal guidance on Scattered Spider has also identified commercial intelligence tools as part of the group's reconnaissance inputs. In the 0ktapus campaign, which targeted more than 130 organizations and resulted in the theft of nearly 10,000 credentials, Okta reported that the attackers likely harvested mobile phone numbers from commercially available data aggregation services that link phone numbers to employees at specific organizations.

Some cybercriminal groups purchase access to these sites directly while others resell it as a lookup service. Either way, data broker profiles supply a major source of intelligence that drives social engineering attacks.

Despite this, the role of data brokers in enabling social engineering is still underrepresented in most threat reports and mitigation guidance.

This survey provides a new perspective, grounded in the experience of enterprise cybersecurity leaders on the front lines of social engineering defense.

The findings show that organizations are not only seeing an increase in targeted social engineering, but are also recognizing the role publicly accessible employee data plays in enabling those attacks. As AI makes reconnaissance, personalization, and impersonation easier to scale, that exposure becomes even more consequential. Respondents overwhelmingly report that attackers can easily obtain the information needed to target employees, and they rank data broker and people-search platforms as the most significant source of intelligence used in social engineering attacks.

At the same time, these organizations are taking action.

Many are looking beyond detection and response and are focusing earlier in the attack lifecycle, minimizing the information available to attackers in order to prevent attacks and reduce their volume. They recognize that effective defense requires addressing both how attacks are delivered and how they are enabled.

The findings in this report show that this shift towards prevention is already well underway and is poised to continue.

We hope this research helps bring greater attention to the role of publicly accessible data in enabling modern attacks against businesses, and that its findings encourage more organizations to shift protection upstream.

> Lawrence Gentilello, CEO & Founder, Optery

[1] https://www.optery.com/cisa-fbi-cnmf-confirm-data-broker-threat/

Introduction

Social engineering has for years been one of the most persistent and effective entry points into organizations.

Phishing campaigns are increasingly targeted, multi-channel operations shaped by sophisticated and data-driven reconnaissance.

Attackers are selecting specific employees, gathering detailed personal and professional information, and using that data to craft convincing impersonation attempts across email, voice, social media, and web channels.

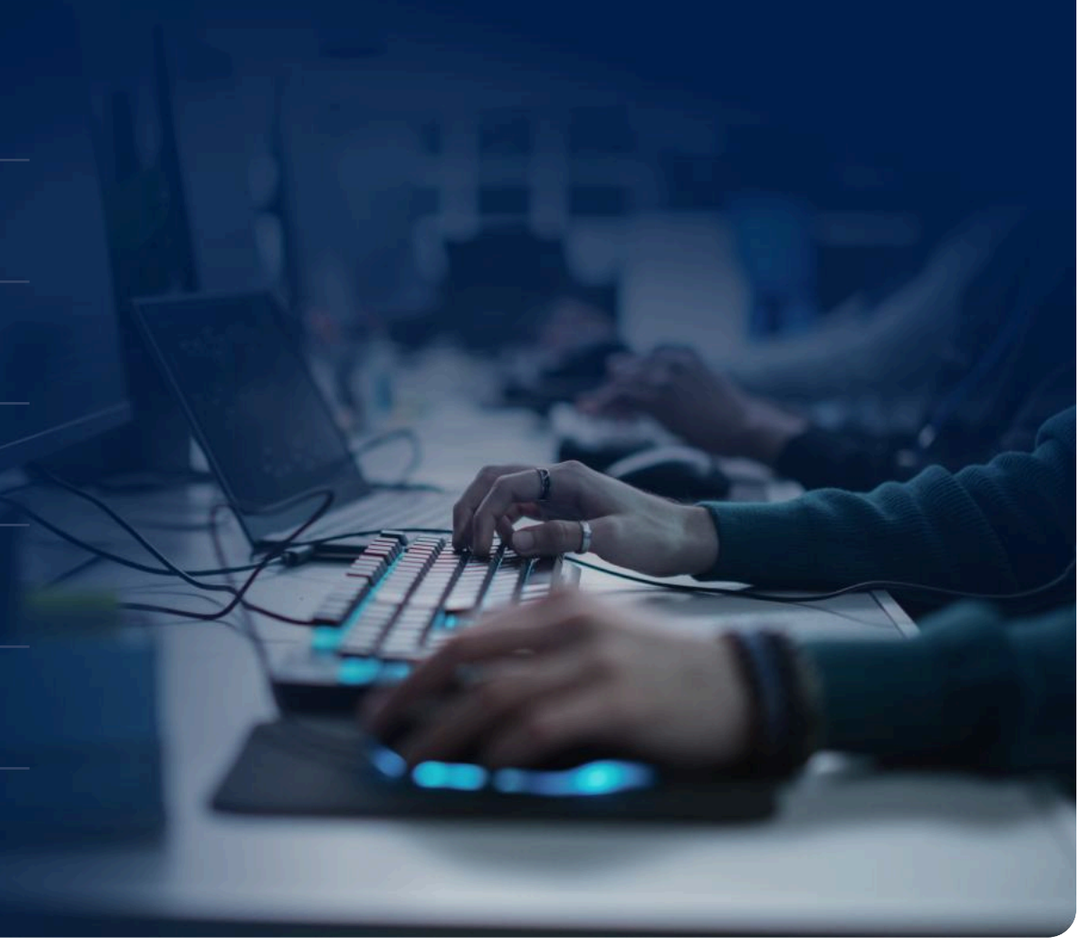
The scale of this activity is growing quickly.

In this study, 96% of cybersecurity leaders report an increase in targeted social engineering attempts over the past 12 months, and more than half say the volume is beginning to strain their defenses. Three-quarters of organizations report credential compromise resulting from targeted social engineering, highlighting the real operational impact.

Fueling these attacks is the availability of employee identity data.

Security leaders overwhelmingly report that attackers can easily obtain the information needed to target employees at their organization, including:

1. corporate email format patterns
2. personal mobile numbers
3. personal email addresses
4. breached credentials
5. job titles and reporting structures
6. family member or associate names
7. home addresses



At the same time, they identify data broker and people-search sites as the most significant source of intelligence used in these attacks, alongside social platforms and breach data.

More than three-quarters of respondents believe employees' personal data is very or somewhat exposed across data brokers and people-search websites.

As a result, many large-enterprise security teams are prioritizing and expanding their personal data removal efforts.

Methodology

This report is based on a survey of 421 cybersecurity professionals conducted by independent research agency TrendCandy on behalf of Optery.

All respondents identified as working in information technology or cybersecurity roles. The survey explores how large-enterprise cybersecurity leaders are experiencing and responding to social engineering.

The respondent pool is heavily weighted toward senior leadership, with approximately:

65%
Director-level

26%
Vice President

9%
Executive leadership

Organizations represented are predominantly large enterprises:

- **~68%** from companies with 5,001–10,000 employees
- **~29%** from companies with more than 10,000 employees
- **~2%** from companies with 1,001–5,000 employees
- **~1%** from companies with 100–1,000 employees

Industry representation is concentrated in:

~58%
Technology

~30%
Financial Services

~10%
Healthcare

~1%
Manufacturing

The findings in this report therefore reflect the perspectives of large-enterprise cybersecurity leaders, rather than the broader business population.

The margin of error for this sample size is approximately ±4.8% at a 95% confidence level.

Executive Summary

This survey of 421 cybersecurity leaders shows that targeted social engineering has become a high-pressure, multi-channel threat that is driving measurable credential compromise across large enterprises.

The findings point to a central enabler:

Attackers can easily obtain the personal and professional data needed to identify, profile, target, and impersonate employees.

Respondents rate data broker and people-search sites as the most significant source of targeting intelligence, ahead of social media platforms and breach data.

Reducing publicly exposed employee data ranked as both the most widely used defense and the largest investment priority in this sample, indicating that many large enterprises are prioritizing the prevention of social engineering attacks by minimizing the data that make those attacks possible.

Key Findings

96% report an increase in targeted social engineering attacks in the past 12 months

74.6% report credential compromise resulting from targeted social engineering (77.9% confirmed or suspected)

89.8% say recent attacks are highly or moderately personalized

97.6% rate data broker / people-search data as a significant source of attack intelligence

77.4% believe employees' personal data is very or somewhat exposed across data brokers and people-search websites

Reducing exposed employee data ranked:

#1 defense in use	**59.9%**
#1 investment priority	**33.7%**

85.3% agree that reducing exposed employee data lowers social engineering risk

76.5% say limiting employee personal data online is critical or very important as AI-generated attacks become more scalable

76.5% categorize reducing publicly exposed employee data as either a core security initiative or supporting security measure

Only 14.0% say personal data removal efforts currently cover the full workforce

82.2% plan to expand personal data removal coverage in the next 12 months

Rising Social Engineering Pressure Is Driving Real Impact

For most organizations, targeted social engineering is a growing and persistent operational challenge.

Nearly all respondents **(96%)** report that targeted social engineering attempts have increased over the past year, with about half describing the increase as significant.

At the same time, many security teams are feeling the impact of that growth. While some organizations report that the volume remains manageable, **52.7%** say social engineering volume is creating increasing strain, difficult to keep up with, or overwhelming existing defenses. This suggests that even well-resourced teams are beginning to encounter limits in how effectively they can respond to the volume of incoming attacks.

Approximately **75%** of organizations report that targeted social engineering attempts resulted in credential compromise within the last year, with additional respondents indicating suspected compromise.

This connects the increase in attack volume directly to tangible security impact, including unauthorized access and downstream risk.

At the same time, only **32.3%** say they are very confident in their ability to detect and block modern social engineering techniques before user interaction, while **61%** are somewhat confident.

Similarly, **29.9%** are very confident in their ability to detect and block AI-scaled personalized attacks, while **58%** are somewhat confident. That confidence, however, sits in tension with the high rate of reported credential compromise.

The pressure of social engineering activity is a key factor driving organizations to look beyond detection and response, and to reduce attacker opportunity earlier in the attack chain, limiting both the volume and effectiveness of these threats.

Attacker Reconnaissance Is Easy and Scalable

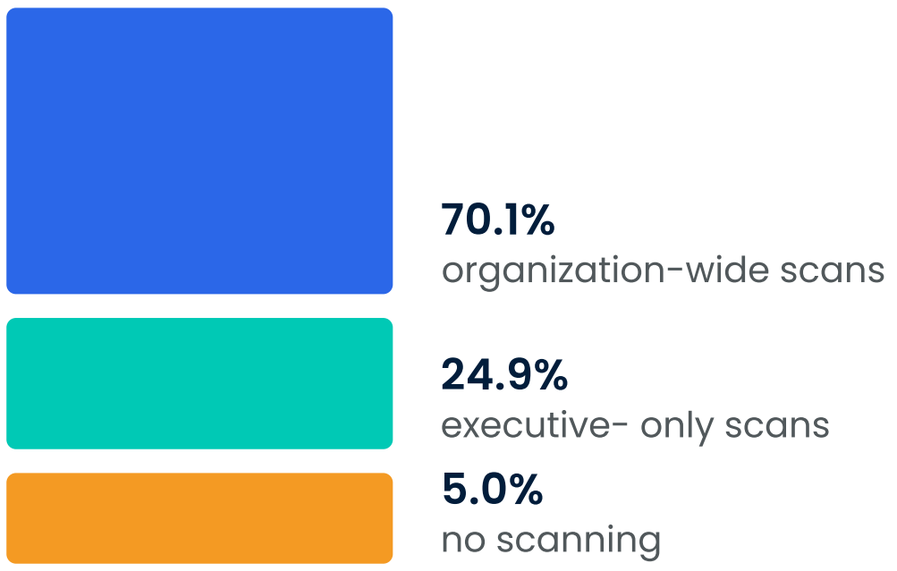
A consistent theme across the data is how easily attackers can obtain the information needed to target employees.

Large majorities of respondents report that key pieces of identity data are readily accessible online:

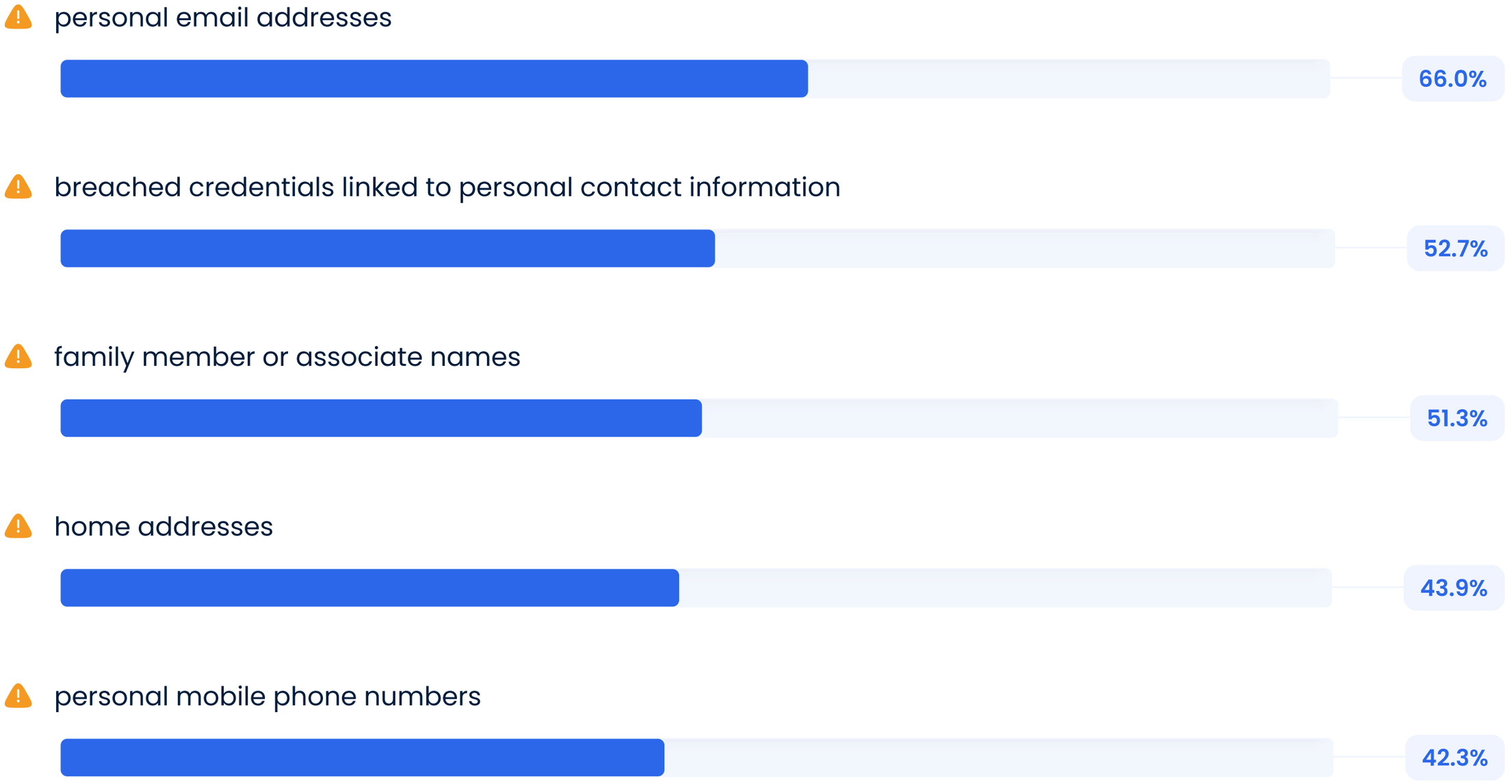
These findings point to a low-friction reconnaissance environment, where attackers can gather detailed targeting information quickly and at scale.

Rather than requiring sophisticated intrusion or privileged access, much of the data needed to initiate targeted attacks is already publicly or commercially available. This reduces the effort required to identify and profile potential victims.

A large majority of respondents report that their organizations have conducted scans for publicly exposed employee data. Specifically, **70.1%** say they have conducted organization-wide scans, while another **24.9%** say they have done so for executives only. **95.0%** of respondents thus report some level of exposure scanning.



When organizations assess exposed employee data, the most commonly evaluated categories are:



Visibility into exposed credentials is also relatively mature in this sample:

51.1%

say they actively monitor exposed credentials tied to both corporate email domains and personal accounts.

17.1%

monitor credentials tied to corporate email domains only.

Taken together, these findings show that large-enterprise security teams are not only aware of employee data exposure as a risk, but are already scanning for and assessing specific categories of exposed information that attackers can use.

This exposed employee data is fueling social engineering attacks:

89.8%

of respondents report that recent social engineering attacks were highly or moderately personalized, indicating that attackers are actively using this information to tailor their approach.

Multi-Channel Attacks Are Meeting Uneven Defenses

The data shows that targeted social engineering is not concentrated in a single channel.

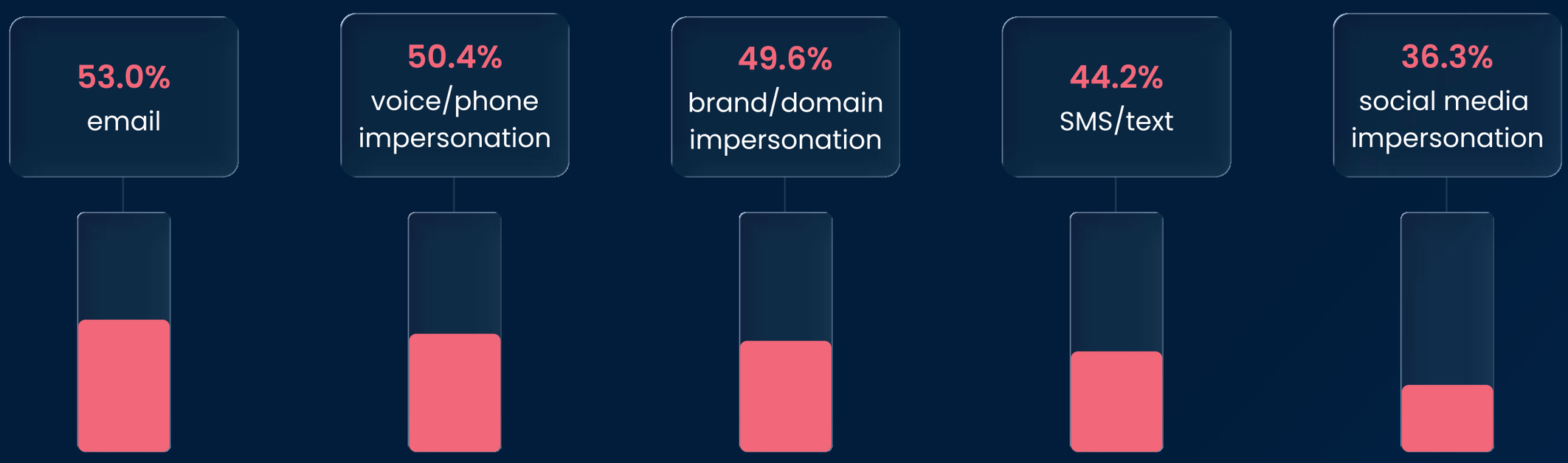
Organizations report confirmed incidents across a range of channels:

No single channel dominates. Attackers are reaching employees through voice, social media, SMS/text, spoofed domains, and email.

Attempted impersonation shows the same multi-channel pattern: 68.2% report email-based impersonation, 57.0% voice impersonation, 51.5% fake or cloned social media accounts, 50.8% spoofed domains or lookalike websites, and 49.4% SMS/text impersonation.

Defensive confidence also varies by channel.

While 53.0% rate their email defenses as strong, 50.4% say the same for voice / phone impersonation and 49.6% for brand / domain impersonation, compared with 44.2% for SMS / text messaging and 36.3% for social media impersonation.



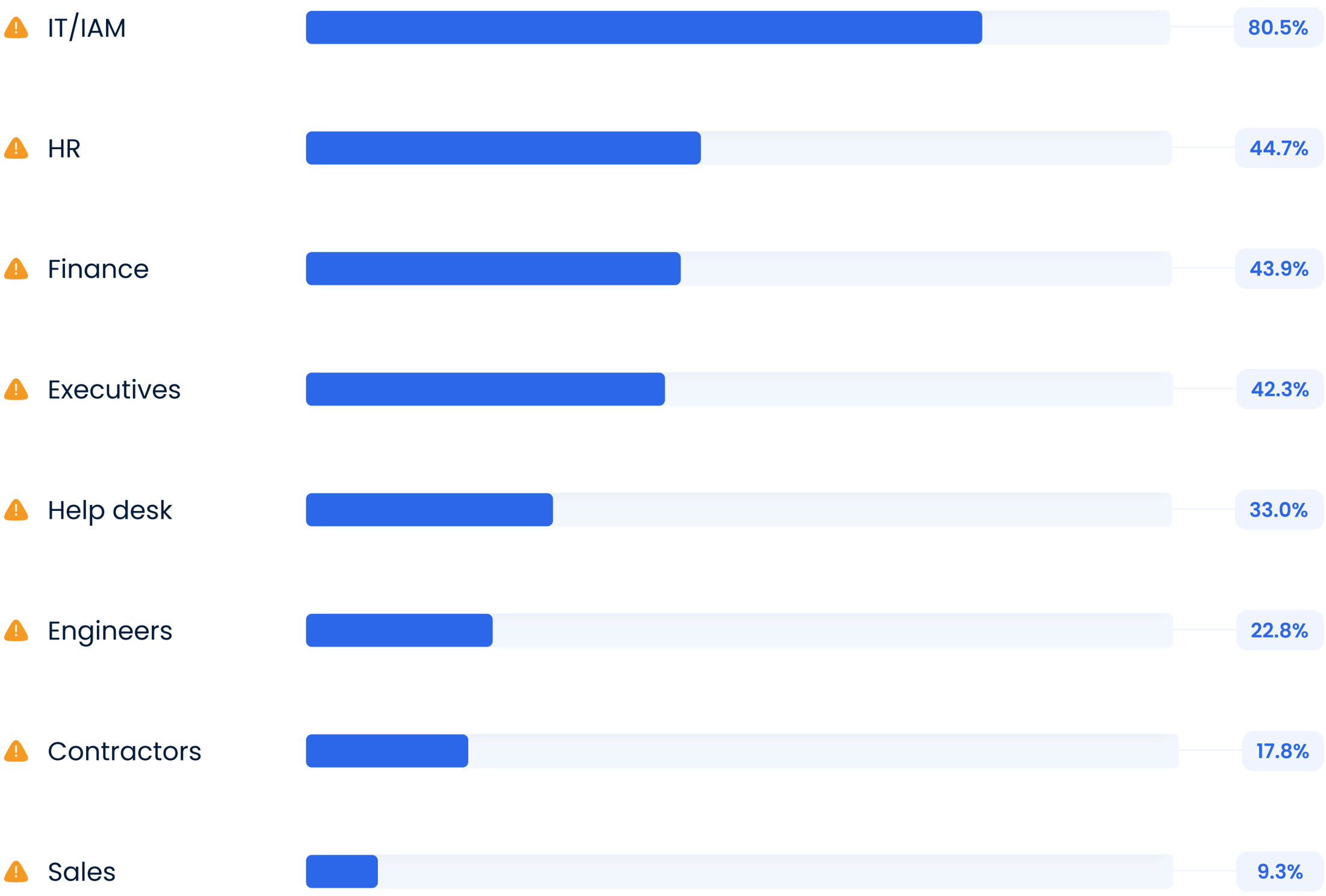
The result is a complex attack surface. Organizations are seeing incidents across a broad range of channels where defensive strength is not uniform.

Targeting Extends Well Beyond Executives

IT and identity-focused roles stand out as the most frequently targeted group, with **80.5%** of organizations reporting targeting of IT/IAM personnel. This is significantly higher than executives, who are reported as targets by **42.3%** of respondents.

Other frequently targeted groups include HR **(44.7%)**, finance **(43.9%)**, help desk **(33.0%)**, and engineers **(22.8%)**, showing that attackers are targeting employees based on access, relationships, and operational leverage rather than title alone.

Frequently targeted employees by role:



Employees with control over identity systems, authentication processes, and account provisioning represent high-value targets because of the access they can grant.

But the broader spread across HR, finance, and help desk roles shows that social engineering campaigns are also aimed at the people who can:

1. validate identities
2. approve payments or other sensitive requests
3. be used to lend legitimacy to an impersonation attempt

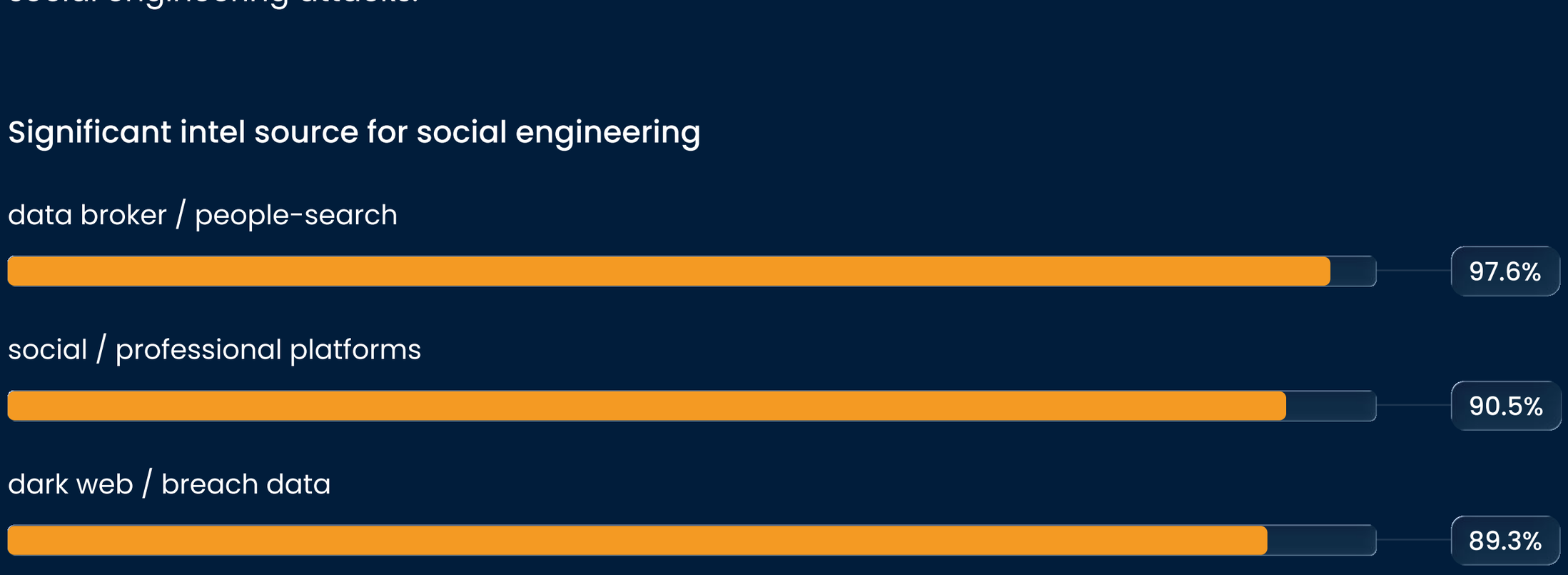
These findings indicate attackers are mapping exposed employee data to organizational roles in order to identify or impersonate the individuals most useful for compromise.

While executives are still being targeted and impersonated, they are only one important target set among several.

Data Brokers Are Considered the Primary Intelligence Source

Among all sources of information used for targeting, data broker and people-search sites are rated as the most significant.

Respondents rank these platforms above social media and breach data as contributors to targeted social engineering attacks.



Data broker and people-search platforms were rated as significant by **97.6%** of respondents, compared to **90.5%** for social/professional platforms and **89.3%** for dark web/breach data.

The gap is even clearer at the highest severity level: 64.4% rate data broker and people-search sites as very significant, compared with 48.9% for social/professional platforms and 46.6% for breach repositories or dark web sources.

While social platforms and breach datasets are often discussed in the context of reconnaissance, respondents rated commercially aggregated identity data as the most significant source of intelligence enabling targeting.

Data brokers provide structured, searchable, and often highly detailed information about individuals, including contact details, employment context, and personal relationships.

Their accessibility and scale make them particularly effective for reconnaissance, allowing attackers to quickly identify targets and assemble the information needed to target or impersonate them convincingly.

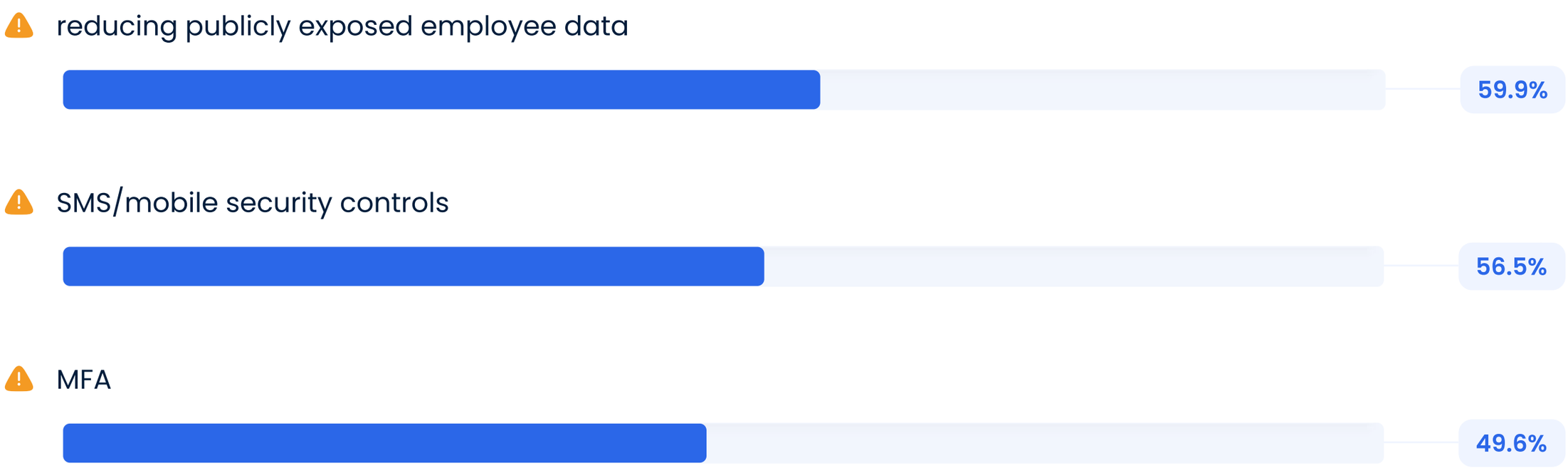
The Defensive Shift Is Already Underway

Organizations are not only recognizing the role of exposed data in enabling attacks, they're acting on it.

Reducing publicly exposed employee data ranks as the most widely used security measure for addressing social engineering, with **59.9%** of organizations reporting it is already in use.

Other commonly used measures include SMS/mobile security controls **(56.5%)**, multi-factor authentication **(49.6%)**, email filtering and blocking **(46.3%)**, social media monitoring for impersonation **(41.8%)**, user training and phishing simulations **(34.2%)**, and brand/domain monitoring and takedown **(28.5%)**.

Security measures currently in use:



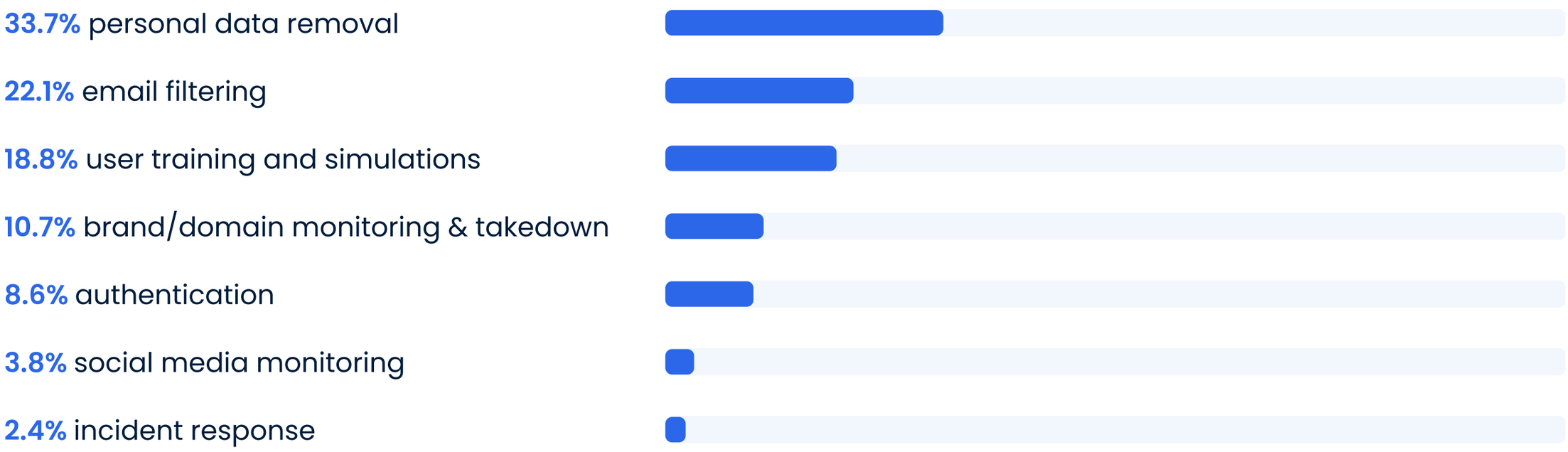
Personal data removal also receives the largest share of investment, with **33.7%** of respondents identifying it as the primary area of spend, ahead of email filtering **(22.1%)**, user training and simulations **(18.8%)**, brand/domain monitoring and takedown **(10.7%)**, authentication **(8.6%)**, social media monitoring **(3.8%)**, and incident response **(2.4%)**.

As AI-generated social engineering attacks become more scalable, organizations also see limiting employee personal data online as important to disrupting reconnaissance and preventing targeting. More than three-quarters of respondents **(76.5%)** say limiting this data is critical or very important in the age of AI, while another **20.6%** say it is moderately important.

A strong majority **(85.3%)** also agree that limiting exposed data reduces social engineering risk, and most organizations classify these efforts as part of their security strategy. Overall, **76.5%** categorize reducing publicly exposed employee data as either a core security initiative or a supporting security measure.

Budget support is also broad: **64.6%** say funding for reducing publicly exposed employee data is already included in their 2026 budget, while another **34.0%** say it is under consideration.

Personal Data Removal Ranked as the Top Investment Priority:



This indicates that exposure reduction is already being operationalized within large enterprises as a formal part of how they manage social engineering risk.

PII Removal Programs Exist, But Are Not Yet Scaled

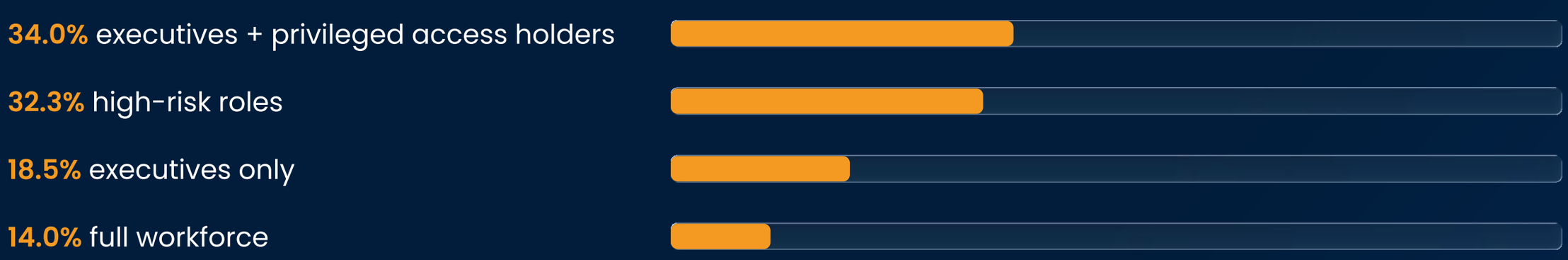
While many organizations report having formal programs to reduce exposed employee data, coverage across the workforce remains limited.

Responsibility for these efforts most often sits within IT **(62%)**, which shows organizations are treating exposed employee data as an operational security issue. Budget ownership points in the same direction: **43.5%** say these efforts are funded through Information Technology, **26.8%** through Cybersecurity, and **21.1%** through Privacy or Compliance. Combined, **70.3%** place the budget in IT or Cybersecurity.

More than half of respondents **(53.9%)** report having a broad program to reduce exposed employee data, with an additional **38.7%** reporting programs focused on specific roles. However, only **14.0%** say personal data removal efforts currently cover the full workforce.

When coverage is provided, it's concentrated among high-risk groups: **34.0%** cover executives plus privileged access holders, **32.3%** cover high-risk roles, while **18.5%** cover executives only

Most personal data removal programs are still focused on high-risk groups:



This gap is also reflected in how respondents assess overall employee exposure.

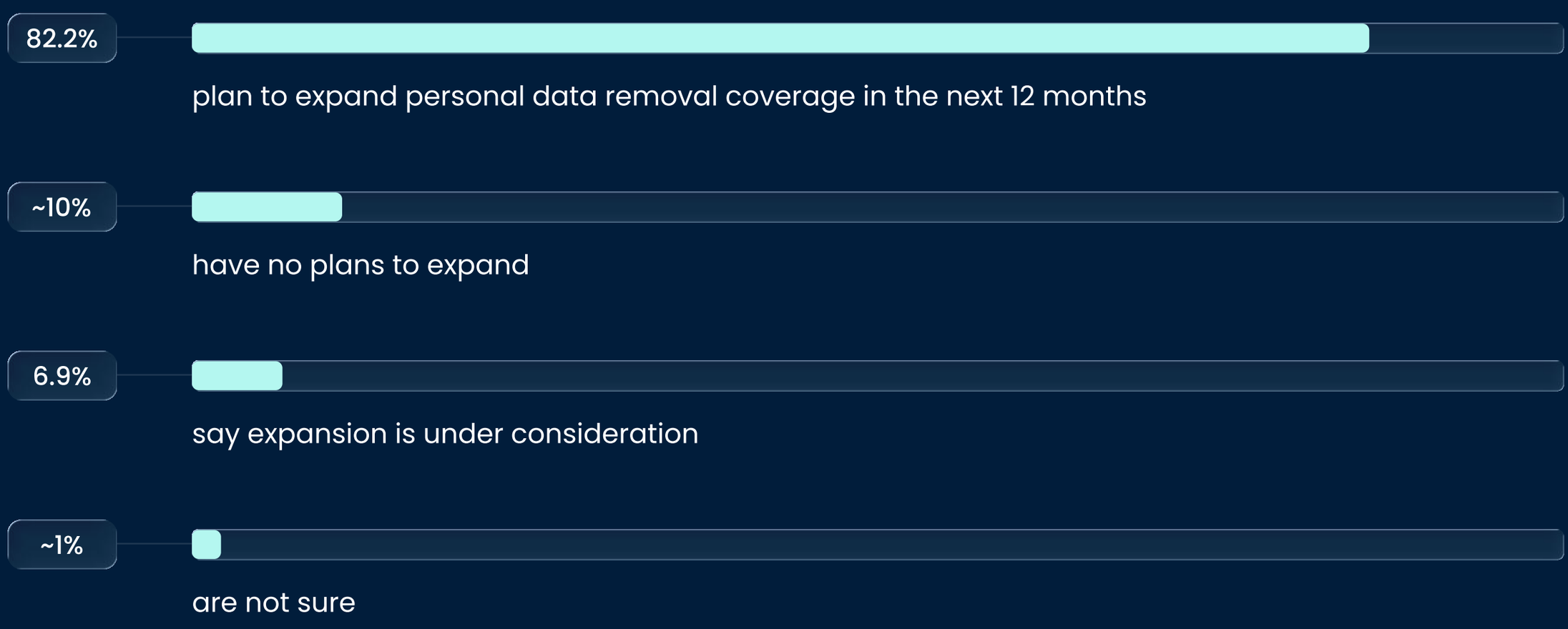
Only **19.0%** say employees' personal data is minimally exposed across data broker and people-search sites, and just **3.6%** say it is not exposed.

Taken together, these findings point to a pattern of risk-based prioritization combined with early-stage scaling. Organizations are focusing first on the employees most likely to be targeted or exploited, but most have not yet extended these controls across the full workforce.

This is a growing area:

82.2% say they plan to expand personal data removal coverage in the next 12 months, and another **6.9%** say expansion is under consideration.

Most organizations plan to expand personal data removal coverage:



Conclusion: Moving Upstream

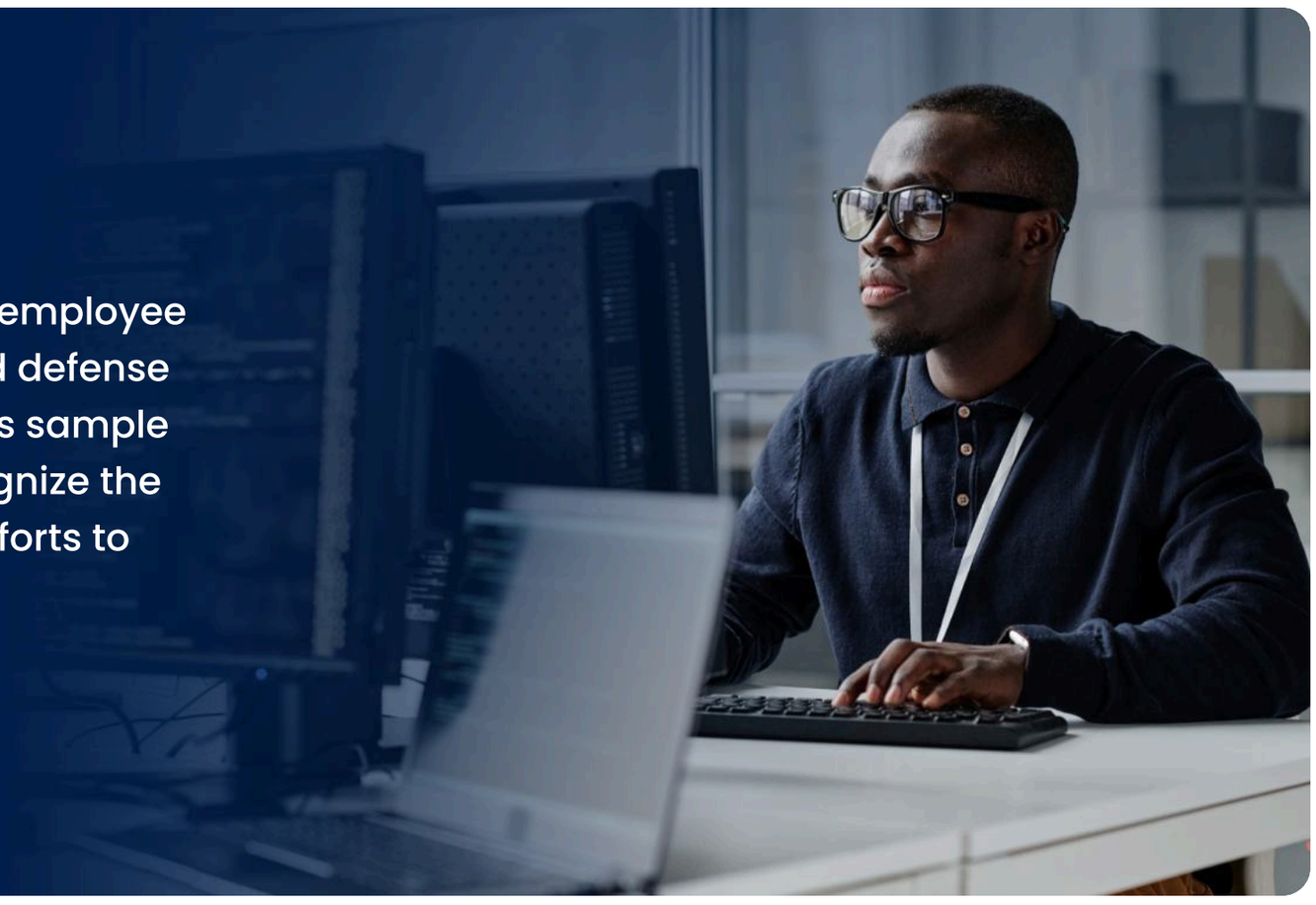
The findings in this survey point to a shift in how organizations are approaching social engineering risk.

Attackers are operating in an environment where reconnaissance is easy, data is widely available, and targeting can be executed across multiple channels. This has contributed to increased attack volume, greater operational strain, and measurable compromise.

In response, organizations are beginning to move earlier in the attack lifecycle.

Unlike channel-specific controls, the protective benefit of reducing publicly exposed employee data is not limited to a single channel. Personal data removal helps address targeted social engineering across all of the channels identified in this report because it reduces the data attackers need regardless of delivery method.

The fact that reducing publicly exposed employee data ranks as both the most widely used defense and the largest investment priority in this sample shows that many large enterprises recognize the exposure risk and are expanding their efforts to address it.



Optery FOR BUSINESS

How Optery Helps Security Teams Move Upstream

The findings in this report show that many large enterprises are already prioritizing the reduction of exposed employee data as part of their social engineering defense strategy. Optery helps organizations operationalize that approach at scale.

Optery for Business finds and **removes exposed employee and executive personal information** from data broker and people-search sites, helping organizations reduce the personal data attackers use for reconnaissance, targeting, social engineering, account takeover, doxxing, and physical threats.

Optery combines **patented search technology** with sophisticated opt-out automation to discover and remove dozens more exposed data broker profiles per person on average than competing services. Its recursive search technology expands discovery using data found in exposed profiles, helping organizations identify and remove more of the information attackers can use to select and target employees.

Optery currently supports automated removals across more than 640 data broker sites and broader coverage across more than 1,000 sites overall, with coverage continually expanding.

It is also the only service to provide screenshot-based Exposure and Removals Reports to prove its effectiveness. For security teams, leadership, insurers, and other stakeholders, Optery also provides measurable visibility into organizational exposure reduction over time through its reporting and administrative dashboard.

Independent evaluations and media testing have highlighted the breadth of Optery's search capabilities, the speed of its removals, and the transparency of its reporting.

TechCrunch reported that Optery identified nearly 50 additional exposed profiles for one of its journalists beyond what had been removed by a competing service.

In testing by a writer for The Wall Street Journal, Optery removed personal information from more than 100 sites within two days.

PCMag has repeatedly recognized Optery as "Editors' Choice" for personal data removal (2022-2026).

Optery's technology and growth have also been widely recognized across the cybersecurity and technology industries, including awards from PCMag, Inc., Fast Company, Cybersecurity Excellence Awards, Cyber Defense Magazine, Fortress Cybersecurity Awards, SiliconANGLE, and Globee.

Built for enterprise deployment, Optery for Business supports SOC 2 Type II attestation, SSO, SCIM, an enterprise admin dashboard, and API options for platform integration.

As organizations face increasing volumes of targeted social engineering and account takeover attempts, Optery provides a measurable way to reduce PII exposure and limit the data attackers rely on to identify and target individuals.