CYBERSECURITY AND AI THREAT LANDSCAPE: AN ORGANIZATIONAL AND ROLE-SPECIFIC ANALYSIS

SL API
BY SOCIAL LINKS

SOCIAL LINKS

TABLE OF CONTENTS

INTRODUCTION

The contemporary cybersecurity landscape is undergoing a profound transformation, driven significantly by the rapid integration of Artificial Intelligence (AI) into business operations and the parallel evolution of AI-powered cyber threats.

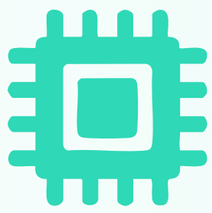
This report presents a fresh analysis of cybersecurity questionnaire data, offering an in-depth examination of general trends, role-based perceptions, and industry-specific vulnerabilities. This research was conducted by Social Links, a leading provider of open-source intelligence solutions. The study was carried out through a survey among 237 respondents from CEO and Technical C-level to Cybersecurity Specialists and Product Managers representing various industries,including Financial Services, Technology, Manufacturing, Retail, Healthcare, Logistics, Government.

PROFESSIONALS SURVEYED

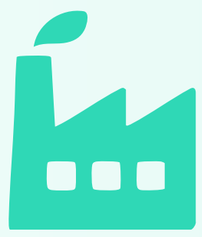
237

INDUSTRIES COVERED

FINANCIAL SERVICES



TECHNOLOGY



MANUFACTURING

RETAIL

HEALTHCARE

LOGISTICS

GOVERNMENT

AND MORE

GENERAL CYBERSECURITY AND AI LANDSCAPE OVERVIEW

SOCIAL LINKS

The survey data provides a panoramic view of the current cybersecurity environment, highlighting prevalent employee behaviors, existing organizational policies, and the perceived effectiveness of protective measures, especially in the context of AI.

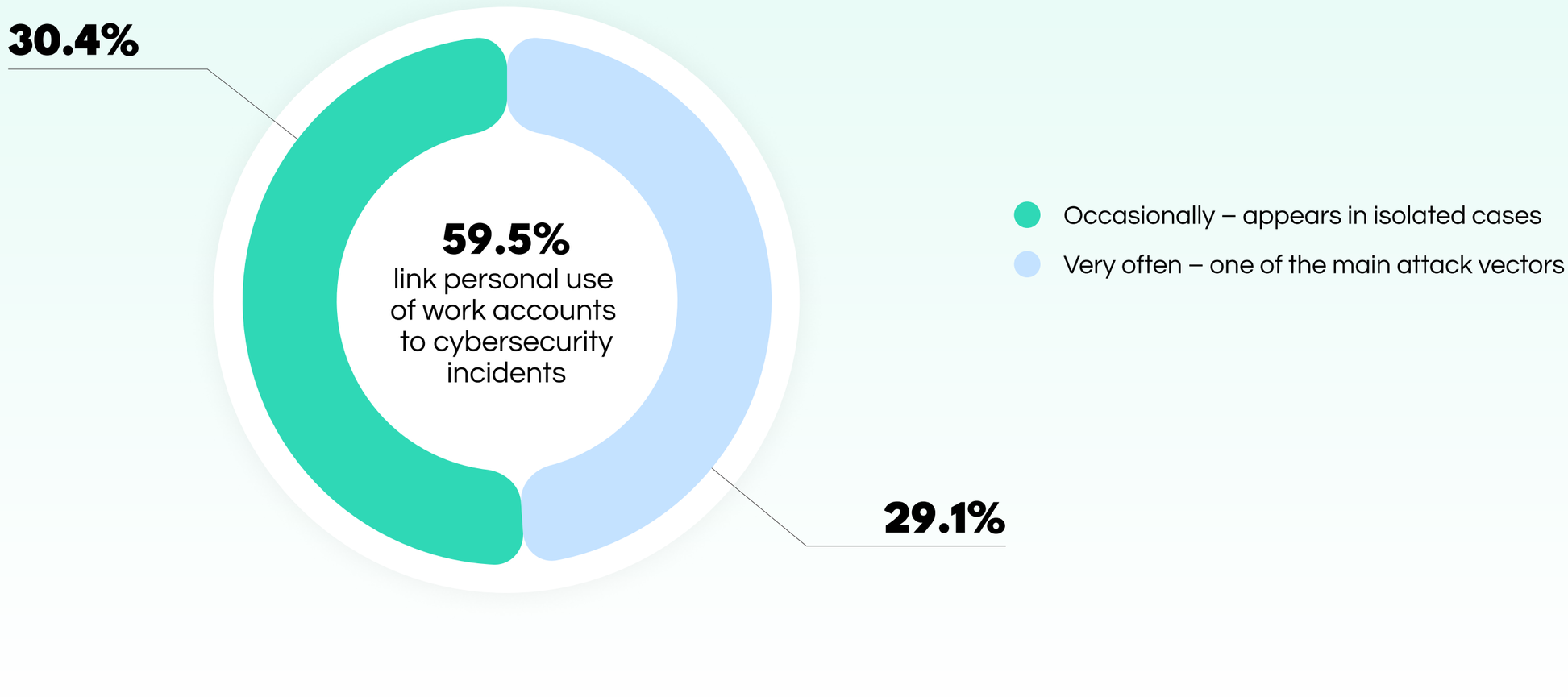
EMPLOYEE ONLINE BEHAVIOR AND DATA EXPOSURE RISKS

Employee online behavior presents a significant human-factor vulnerability within organizations. The data indicates that a substantial proportion of respondents observe their employees using work accounts for personal activities (such as using a company email for personal sign-ups, storing personal files on corporate cloud storage, or using work devices for personal social media and shopping etc). Specifically, 34.2% (81 out of 237 respondents) reported that such activity occurs ". Often – it's noticeable and discussed within the team," while an additional 26.6% (63 out of 237) noted it "Occasionally – I've heard of such cases". Only a small minority, 7.6% (18 out of 237), stated they had "Not observed" this behavior.

The personal use of work accounts is directly linked to perceived cybersecurity incidents. Nearly three out of ten respondents (29.1%, 69 out of 237) consider the use of publicly available employee data (e.g., social media profiles, public biographies) as "Very often – one of the main attack vectors" for cybersecurity incidents in their industry. Another 30.4% (72 out of 237) believe it "Occasionally – appears in isolated cases". The collective observation of frequent personal use of work accounts, combined with the significant perception of publicly available employee data as a primary attack vector, suggests a pervasive human-factor vulnerability. This pattern indicates that despite a general awareness of the risks associated with employee online presence, the actual behavior of employees remains a critical, often unaddressed, vulnerability.

6 OUT OF 10

RESPONDENTS OBSERVE THEIR EMPLOYEES USING WORK ACCOUNTS FOR PERSONAL ACTIVITIES



GENERAL CYBERSECURITY AND AI LANDSCAPE OVERVIEW

SOCIAL LINKS

ORGANIZATIONAL POLICIES AND MONITORING PRACTICES

Organizations are actively attempting to manage employee online conduct through policies and monitoring. The survey shows that a majority of companies, 58.2% (138 out of 237), have "formal policies" that restrict what employees can share online as representatives of the company. However, a notable 25.3% (60 out of 237) rely on "recommendations, but they are not mandatory," and 8.9% (21 out of 237) allow employees "free to decide".

Many companies are actively looking at what's being said or shared online about their brand, and also what their employees are doing on public platforms (like social media profiles or forums). This is done to catch potential risks, protect the company's image, or see if any sensitive company information is accidentally getting out there.

Nearly four out of ten respondents (39.2%, 93 out of 237) consider this practice "Very common – part of standard processes," and another 25.3% (60 out of 237) describe it as "Fairly common – used by many companies".

While formal policies are prevalent, the continued reliance on non-mandatory recommendations and the fact that digital presence monitoring is common but not universally integrated into standard processes point to inconsistencies in proactive risk management. This scenario can create a false sense of security, as formal policies are only truly effective when they are rigorously implemented, communicated, and consistently monitored.

> You can’t really stop people from using work accounts or data when they’re active online. The same goes for AI tools: people will use them to save time or get help with tasks, whether there’s a policy or not. But all this activity leaves digital traces. And those traces can make it easier for scammers to find and target employees. What actually helps is teaching people how to spot the risks and giving them the right tools to stay safe, instead of just saying ‘don’t do it.

Ivan Shkvarun, CEO of Social Links

PREVALENCE OF DATA LEAK INCIDENTS

Despite existing policies and monitoring efforts, data leaks remain a significant and common occurrence. The survey data indicates that a considerable majority of organizations have come across data leaks in the past two years. Specifically, 39.2% (93 out of 237) of respondents reported encountering data leaks "involving personal or sensitive data," while an additional 26.6% (63 out of 237) had seen leaks where the data involved was "limited in nature". Only 27.8% (66 out of 237) reported they haven’t heard about such incidents.

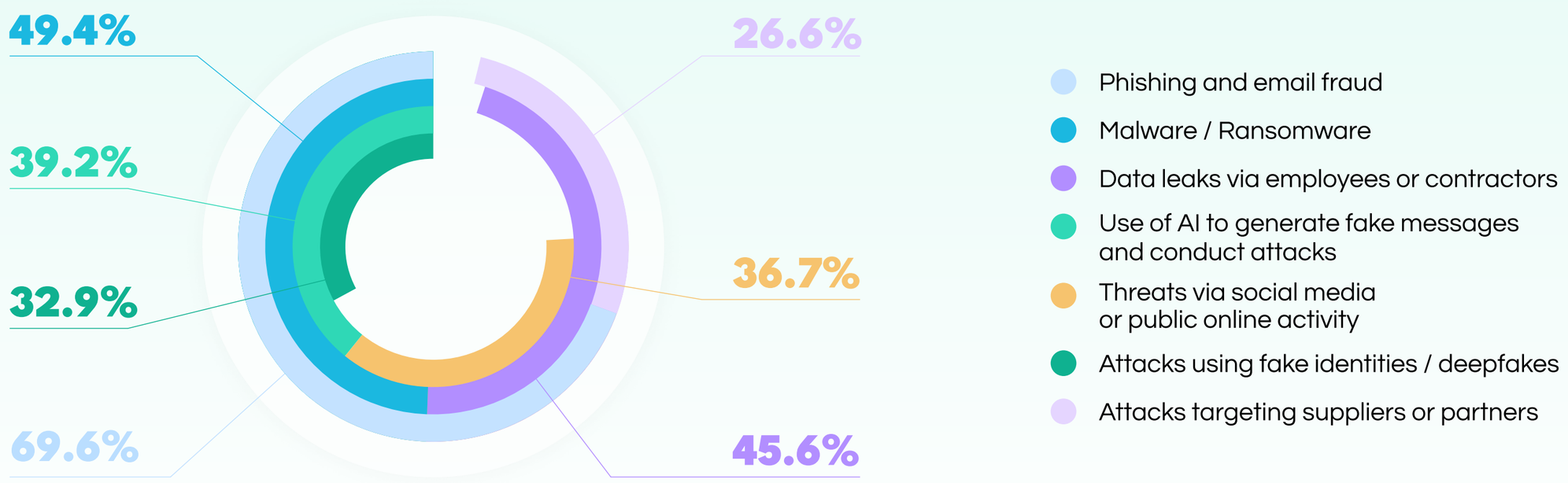
GENERAL CYBERSECURITY AND AI LANDSCAPE OVERVIEW

MOST RELEVANT CYBER THREATS IN 2024-2025 (OVERALL PERSPECTIVE)

When asked about the most relevant cyber threats for 2024-2025, respondents highlighted a combination of persistent traditional threats and rapidly emerging AI-driven attack vectors. Phishing and email fraud remains the most pressing concern, cited by 165 respondents, representing 69.6% of the total. Malware/Ransomware follows closely, identified by 49.4% (117 respondents), and data leaks via employees or contractors are a concern for 45.6% (108 respondents).

Crucially, AI-driven threats are also highly prominent. The "Use of AI to generate fake messages and conduct attacks" was identified by 39.2% (93 respondents), and "Attacks using fake identities / deepfakes" by 32.9% (78 respondents). The following table summarizes these top perceived threats:

OVERALL PERCEIVED CYBER THREATS



The high ranking of traditional threats like phishing and malware indicates their continued prevalence and effectiveness, requiring ongoing vigilance and defense. However, the significant presence of AI-driven threats, such as fake messages and deepfakes, among the top concerns signifies a growing recognition of sophisticated, technologically advanced attack vectors. This indicates a dual challenge for organizations: they must continue to defend against established attack methods while simultaneously preparing for and mitigating emerging AI-powered threats.

> Traditional threats like phishing and malware still dominate the charts. But what we're seeing now is that AI isn't replacing these threats, it's supercharging them, turning generic scams into tailored operations - fast, cheap, and more convincing. That's the real shift: automation and personalization at scale.
>
> Ivan Shkvarun, CEO of Social Links

OVERALL PERCEIVED DATA PROTECTION AGAINST AI-RELATED THREATS

Organizations express a mixed, but generally cautious, outlook on their ability to protect sensitive data from AI-related threats. Only a combined 43.1% of respondents feel "Very well protected" (20.3%, 48 out of 237) or "Rather well protected" (22.8%, 54 out of 237) against AI-driven threats such as phishing, fake request generation, and data leakage through AI tools.

A significant portion, 25.3% (60 out of 237), reported an "Average level of protection," while 13.9% (33 out of 237) feel "Rather poorly" and 8.9% (21 out of 237) "Very poorly protected".

The fact that almost half of organizations (48.1%) perceive their data protection against AI threats as average or below average points to a collective vulnerability and a lag in adapting security measures to the rapidly evolving AI-driven attack vectors.

GENERAL CYBERSECURITY AND AI LANDSCAPE OVERVIEW

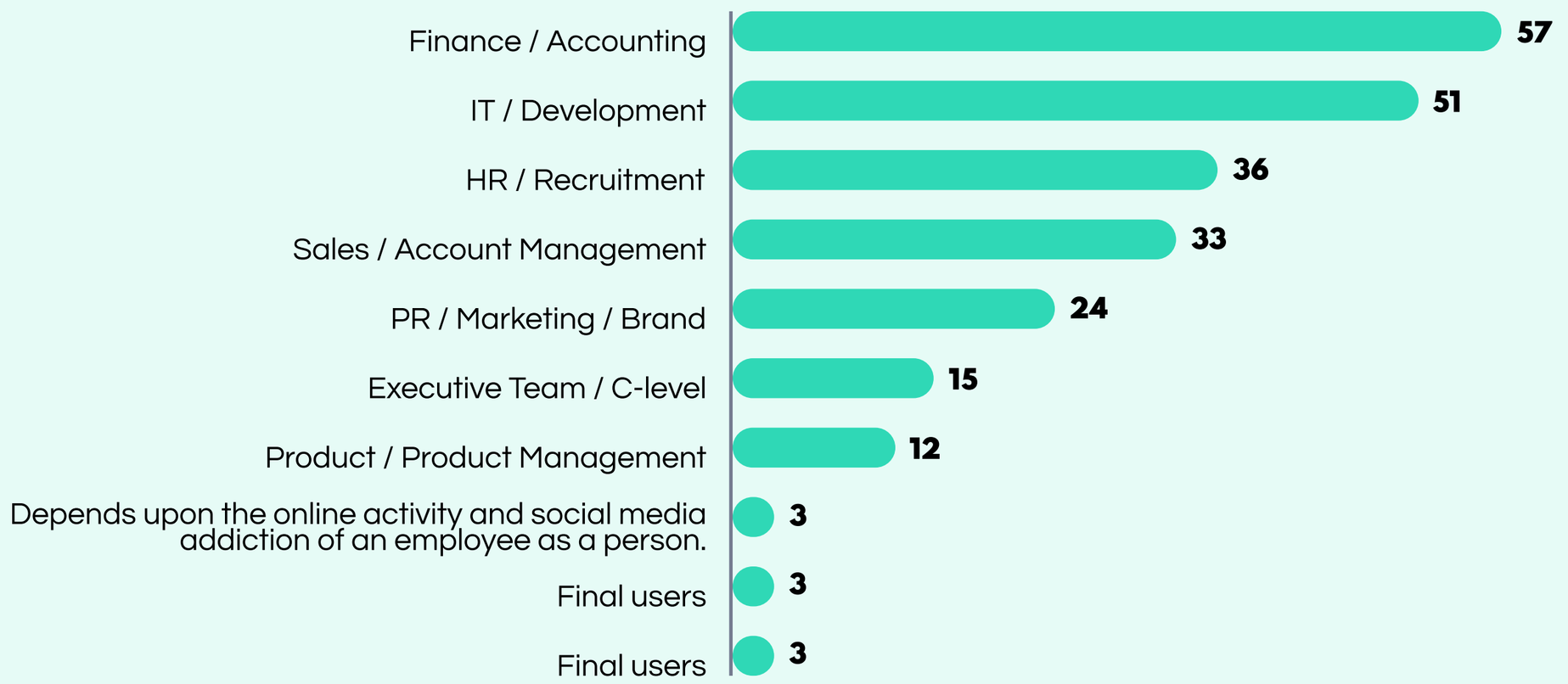
OVERALL MOST VULNERABLE DEPARTMENTS

Across all surveyed organizations, regardless of industry or specific role, certain departments are consistently identified as being most vulnerable to cyber threats. This overall perspective highlights common areas of risk that organizations should prioritize in their security strategies.

Based on the responses from 237 participants, Finance / Accounting is perceived as the most vulnerable department, cited by 24.1% (57 out of 237) of respondents. Closely following is IT / Development, identified by 21.5% (51 out of 237) of respondents. These two departments collectively account for nearly half of all perceived vulnerabilities.

Other departments also show significant levels of perceived vulnerability:

OVERALL MOST VULNERABLE DEPARTMENTS



CURRENT STATE OF AI TOOL USAGE AND GOVERNANCE IN COMPANIES

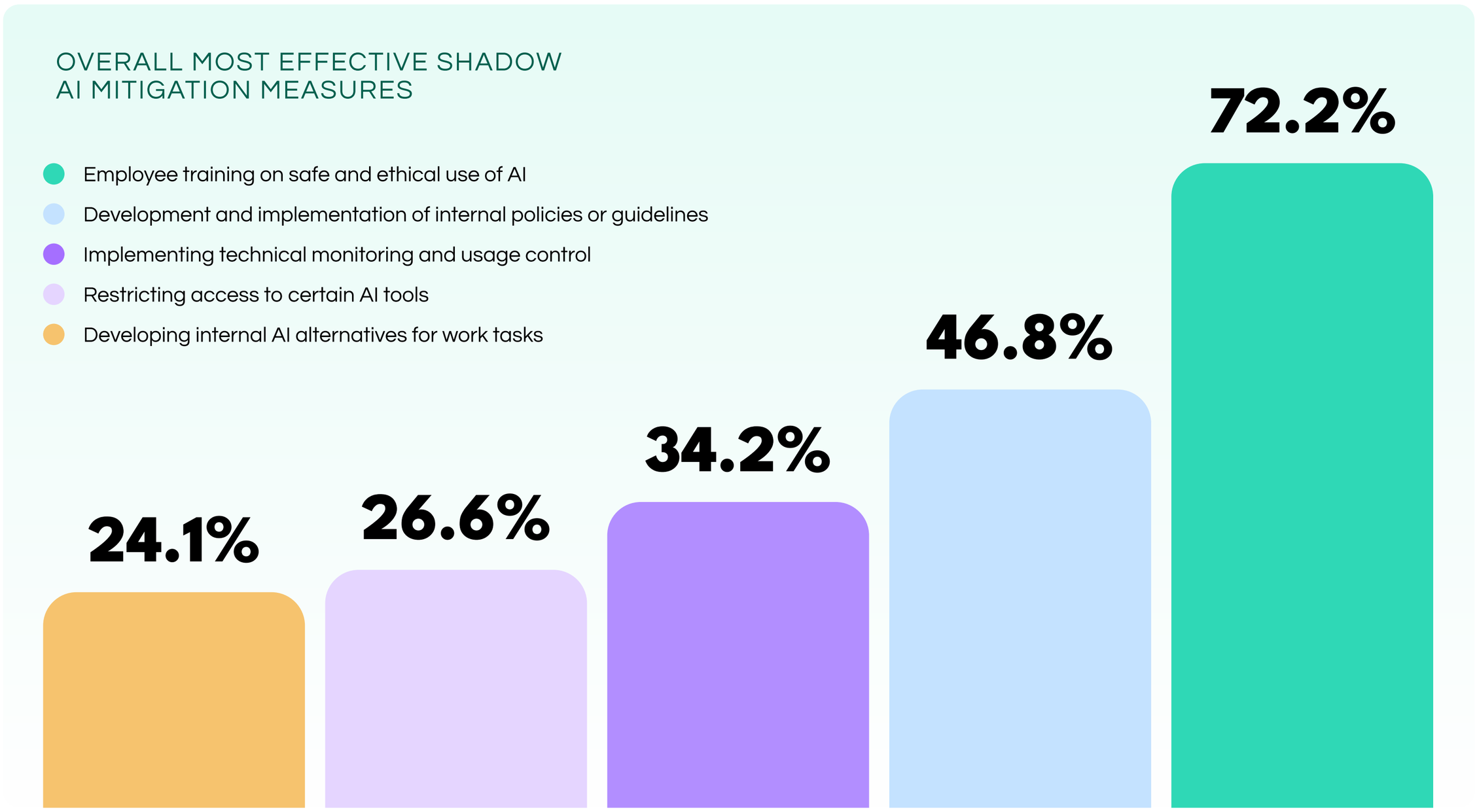
The adoption of AI tools within organizations for work-related tasks is widespread. A significant majority of companies allow AI tool usage: 51.9% (123 out of 237) permit it and it is "partially regulated," 30.4% (72 out of 237) allow it "without formal guidelines," and 12.7% (30 out of 237) allow it "with limitations" for specific teams. Only a small fraction, 5.1% (12 out of 237), prohibit AI tool usage entirely.

Despite this broad adoption, the development of internal policies or regulations governing AI tools is not keeping pace. Only 36.7% (87 out of 237) of companies have an "official policy or regulation." Alarmingly, 25.3% (60 out of 237) have "No" policy at all, and 17.7% (42 out of 237) rely merely on "informal guidelines". This significant disconnect between the widespread allowance of AI tools and the severe lack of formal governance creates a fertile ground for "Shadow AI" risks, like inadvertent data leaks, exposure of sensitive company information to unauthorized external AI models, intellectual property theft, compliance violations due to data residency or privacy concerns with third-party AI services, and the introduction of new security vulnerabilities through unvetted AI applications.

GENERAL CYBERSECURITY AND AI LANDSCAPE OVERVIEW

PERCEIVED EFFECTIVENESS OF SHADOW AI MITIGATION MEASURES

When considering measures to reduce the risks associated with unauthorized AI tool usage by employees, often referred to as "Shadow AI," organizations overwhelmingly favor human-centric approaches. "Employee training on safe and ethical use of AI" is perceived as the most effective measure, cited by 72.2% of respondents. Following this, "Development and implementation of internal policies or guidelines" is deemed highly effective by 46.8%. While less favored than training and policies, technical measures also play a role. "Implementing technical monitoring and usage control" was identified by 34.2%, and "Restricting access to certain AI tools" by 26.6%. The following table illustrates these perceptions:



The strong emphasis on employee training and policy development as primary mitigation strategies for Shadow AI, rather than purely technical restrictions, highlights a growing understanding that human factors are central to effective AI security. This indicates a maturing perspective within organizations, recognizing that AI tools are powerful enablers of productivity and that outright prohibition or strict technical blocking may be impractical or counterproductive. Instead, empowering employees through comprehensive education and clear guidelines is increasingly seen as a more sustainable and effective approach to managing these risks. This suggests a strategic shift towards a "human-centric security" model for AI, where trust, education, and responsible usage complement, rather than are superseded by, technical safeguards.

ROLE-BASED PERCEPTIONS AND VULNERABILITIES

Understanding how different organizational roles perceive cybersecurity risks and vulnerabilities is crucial for developing targeted and effective security strategies.

Significant disparities emerge when comparing the perspectives of Top Management and Technical roles, as well as Technical and broader Business functions.

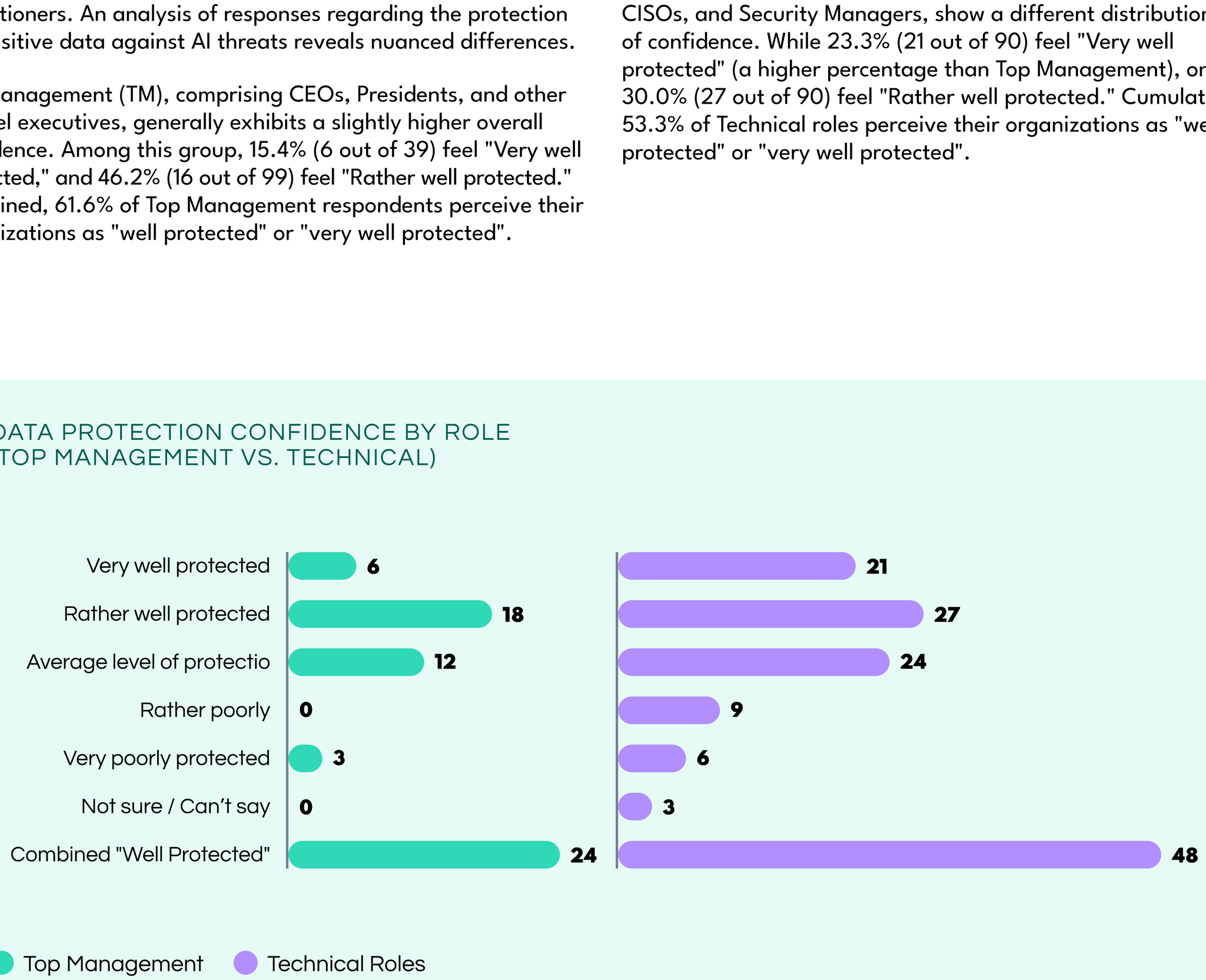
DATA PROTECTION CONFIDENCE: TOP MANAGEMENT VS. TECHNICAL ROLES

The perceived level of data protection against AI-related threats varies between strategic leaders and frontline cybersecurity practitioners. An analysis of responses regarding the protection of sensitive data against AI threats reveals nuanced differences.

Top Management (TM), comprising CEOs, Presidents, and other C-level executives, generally exhibits a slightly higher overall confidence. Among this group, 15.4% (6 out of 39) feel "Very well protected," and 46.2% (16 out of 99) feel "Rather well protected." Combined, 61.6% of Top Management respondents perceive their organizations as "well protected" or "very well protected".

In contrast, Technical Roles (Tech), including Cyber Threat Intelligence Analysts, Information Security Specialists, IT Directors, CISOs, and Security Managers, show a different distribution of confidence. While 23.3% (21 out of 90) feel "Very well protected" (a higher percentage than Top Management), only 30.0% (27 out of 90) feel "Rather well protected." Cumulatively, 53.3% of Technical roles perceive their organizations as "well protected" or "very well protected".

DATA PROTECTION CONFIDENCE BY ROLE (TOP MANAGEMENT VS. TECHNICAL)



ROLE-BASED PERCEPTIONS AND VULNERABILITIES

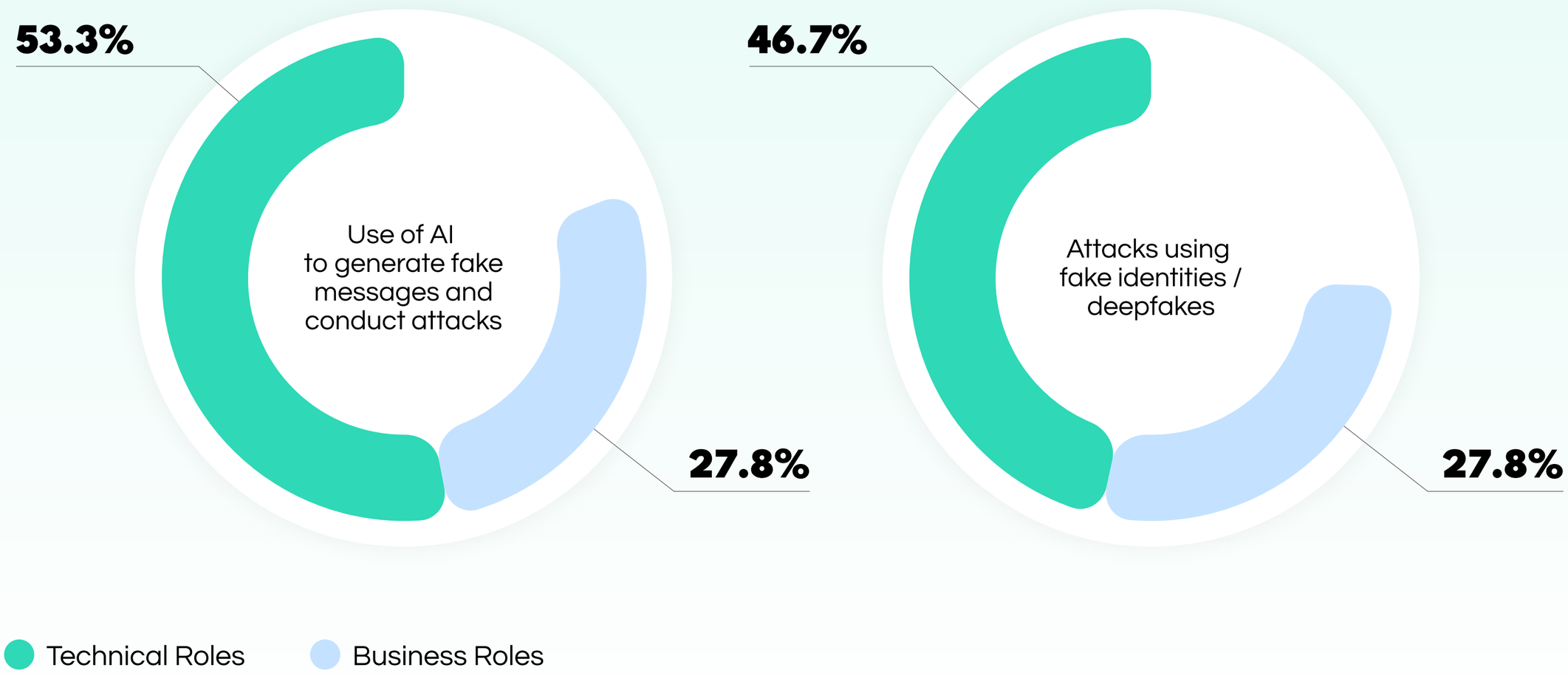
AI-DRIVEN INCIDENT AWARENESS: TECHNICAL VS. BUSINESS ROLES

The perception of AI-driven threats differs significantly between technical and broader business functions, highlighting a critical awareness gap. This analysis focuses on the perceived relevance of "Use of AI to generate fake messages and conduct attacks" and "Attacks using fake identities / deepfakes."

Among Technical Roles, a substantial proportion recognize these threats. 53.3% (48 out of 90) identified "Use of AI to generate fake messages and conduct attacks" as relevant, and 46.7% (42 out of 90) cited "Attacks using fake identities / deepfakes".

In contrast, Business Roles, encompassing various non-technical functions, show considerably lower awareness. Only 27.8% (30 out of 108) of business respondents identified "Use of AI to generate fake messages and conduct attacks," and an identical 27.8% (30 out of 108) cited "Attacks using fake identities / deepfakes".

AI-DRIVEN INCIDENT AWARENESS BY ROLE (TECHNICAL VS. BUSINESS)



Technical roles are significantly more attuned to AI-driven threats compared to business roles. This substantial awareness gap suggests a critical organizational vulnerability, particularly because business personnel are frequently the primary targets for AI-enhanced social engineering attacks. AI-driven attacks, such as sophisticated phishing campaigns leveraging AI-generated text or deepfake voice/video impersonations, are specifically designed to exploit human trust and decision-making.

> This is no longer a question of ‘if’ — AI-powered threats are already here and evolving quickly. We’re seeing a clear gap between those building defenses and those most likely to be targeted. Bridging that gap requires not just better technical tools, but broader awareness and education across all levels of an organization.

Ivan Shkvarun, CEO of Social Links

ABOUT SOCIAL LINKS

SOCIAL LINKS

Since the company's foundation in 2015, Social Links has been empowering LEAs, governmental bodies, businesses, and commercial enterprises to harness OSINT in accomplishing core objectives, saving vast resources, and making the modern digital world a safer place.

With many clients from among the S&P 500 as well as organizations operating at the highest levels of state, we have established ourselves as a key company within the OSINT industry and continue to develop products that operate at the forefront of a range of sectors including law enforcement, national security, cybersecurity, insurance, banking, due diligence, and more.

OUR PRODUCT LINE

SL API

A SUITE OF DATA EXTRACTION AND ANALYSIS METHODS ACROSS SOCIAL MEDIA, BLOCKCHAINS, MESSENGERS, AND THE DARK WEB CONNECTED DIRECTLY TO YOUR IN-HOUSE PLATFORM VIA OUR API

SL CRIMEWALL

A full-cycle OSINT investigation platform

SL PROFESSIONAL

MALTEGO AND i2

OSINT Tool for conducting in-depth investigations across social media, blockchains, messengers, and the Dark Web in Maltego and i2 platforms.

SL PRIVATE PLATFORM

An enterprise-grade on-premise OSINT platform with customization options, private data storage, and our widest range of search methods.

SOLUTIONS YOU CAN TRUST

Companies from the S&P 500 and leading law enforcement agencies from more than 80 countries around the globe rely on Social Links

Gartner peer insights™
4.8/5

4.7/5
Review us on G2

ABOUT SOCIAL LINKS

FOUNDED IN 2015

HQ THE UNITED STATES

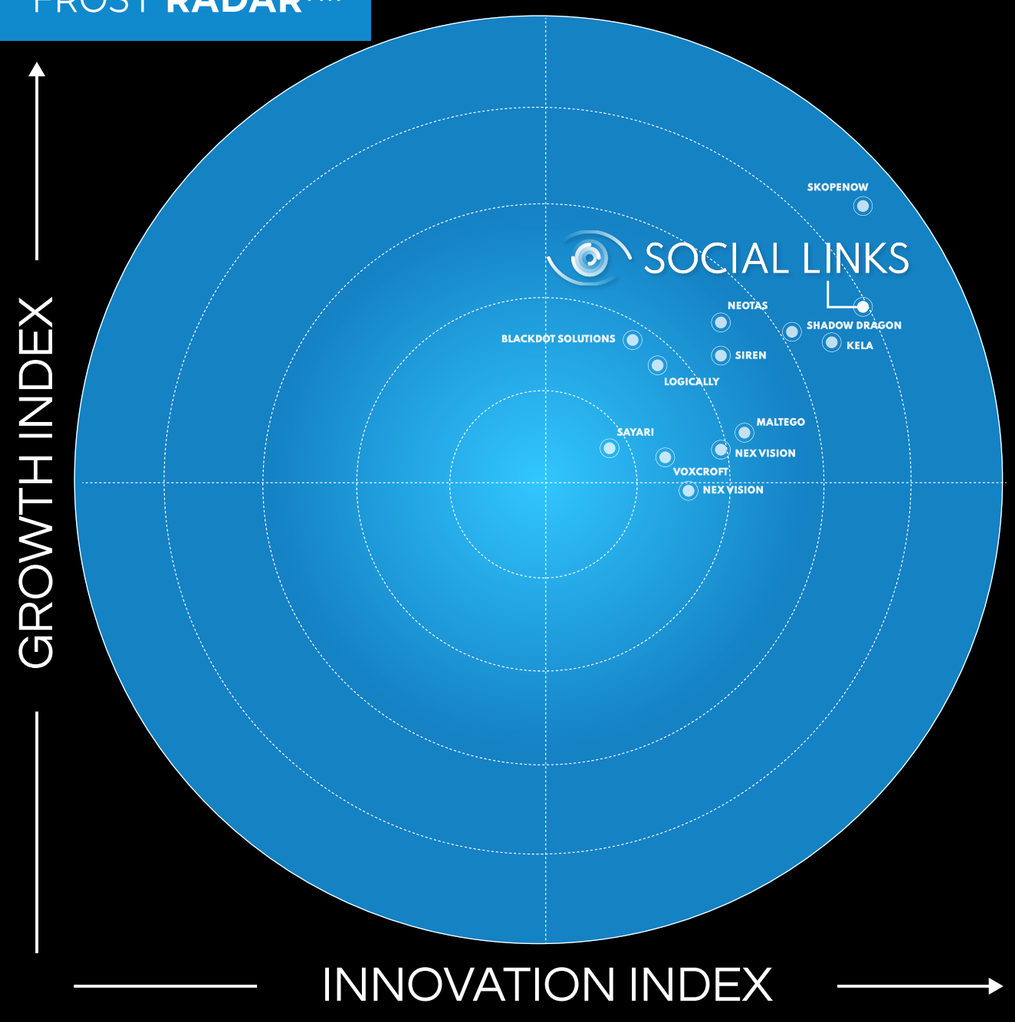
500+ CLIENTS

80+ COUNTRIES

BOOK A DEMO

OSINT INDUSTRY LEADER, 2025

FROST **RADAR**™



Contact us at:
sales@sociallinks.io

More information at sociallinks.io