

2025 SPYCLOUD
IDENTITY THREAT REPORT

➤ TRENDS, BENCHMARKS, AND STRATEGIES TO STRENGTHEN IDENTITY THREAT PROTECTION ◀



LOCATION: EDX 26.26 / FRT 785.12

SPEED

325.7 KM/H.

DURATION

00:45:23²⁶

GPS

AVC0135LJASBPB4FHE
BKA0352LJASBPB4FHE
QPS0453LJUNASBPB4FHE

LOAD

AP+063
AP+063
AP+063


INCOMING TRANSMISSION

CRACKLING

...SECURITY TEAMS, THIS IS GROUND CONTROL, DO YOU READ?...

...THE PERIMETER HAS SHIFTED, **I REPEAT, DO YOU READ?...**

...TEAMS, YOU **MUST** REPOSITION YOUR DEFENSES...

...THIS HAS TO HAPPEN NOW, **DO YOU COPY? **

CRACKLING

ZUL3N
SC
A02LJAN3
UM4033
RK
BAK0351
ZPLJBRX
A03246
Z53
QW39
TH45
AS

BAK0351
ZPLJBRX
A03246
UM4033
RK
A02LJAN3
Z53
QW39
TH45
AS

BX-26.13

31.26 XE4

W06-23.3

26.06

423.14

BAK0351
ZPLJBRX
A03246
ZUL3N
RK
A02LJAN3
UM4033
Z53
QW39
TH45
AS

+3000 +4000 +5000 +6000 +7000 +8000 +9000 0 +1000 +2000

WE'VE ALL FELT THE PERIMETER SHIFT...

Today, **identity** is the gravitational center of modern cybercrime – and the critical point around which the majority of attacks now orbit.

Teams are aware that identity attacks have broadened the boundaries of traditional perimeter defense. But there's a growing gap between perceived control and actual preparedness.

This year's **SpyCloud Identity Threat Report**, which surveyed more than 500 cybersecurity professionals, uncovers a troubling pattern: 86% of security leaders express confidence in their ability to prevent major identity-based attacks. Yet 85% of organizations were affected by a ransomware incident at least once in the past year, and over one-third affected between six and ten times.

This confidence gap extends beyond ransomware, to incidents rooted in infostealer malware infections, phishing attacks, supply chain exposures, and more – reflecting a broader disconnect between how secure organizations feel and how vulnerable they truly are to identity-based threats like account takeover, session hijacking, insider threats, and fraud. Security teams' confidence, it turns out, may be grounded more in perception than in operational readiness.



Damon Fleury

DAMON FLEURY | CHIEF PRODUCT OFFICER, SPYCLOUD

HOUSTON, WE HAVE AN IDENTITY THREAT PROBLEM.

TABLE OF CONTENTS

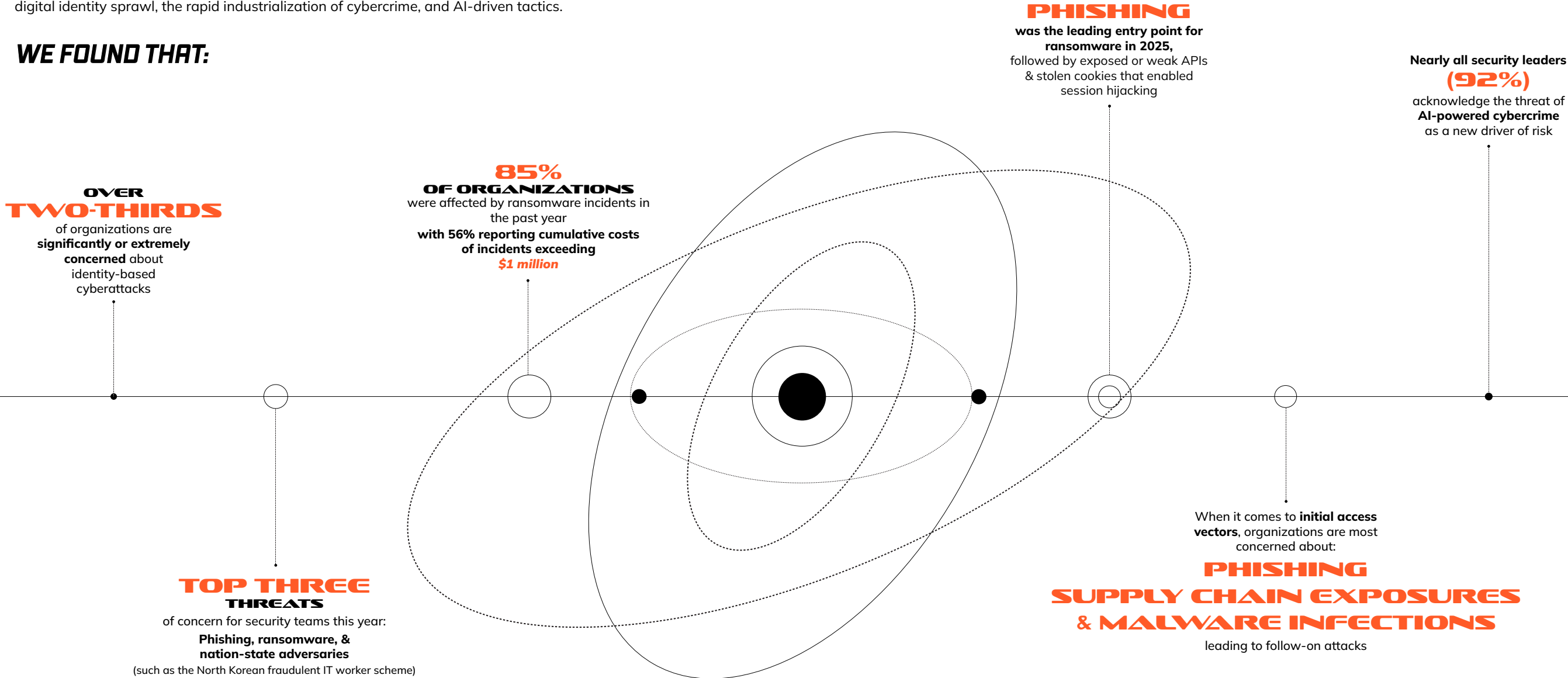
- 5** *Key Takeaways from This Year's Report*
- 7** *The Threat Resurgence: Modern Attack Realities*
- 12** *Top Phishing Threats of 2025*
- 15** *The Confidence Trap: Perception vs. Reality*
- 17** *Identity Black Holes: The Remediation Lag*
- 19** *Crash Landing: The Fallout of Malware and Ransomware*
- 21** *AI: The Force Accelerating Threats*
- 23** *Recalibrating Fundamentals and Expanding Your Mission Scope*
- 25** *Beyond Confidence: Building Operational Maturity*
- 26** *Methodology*



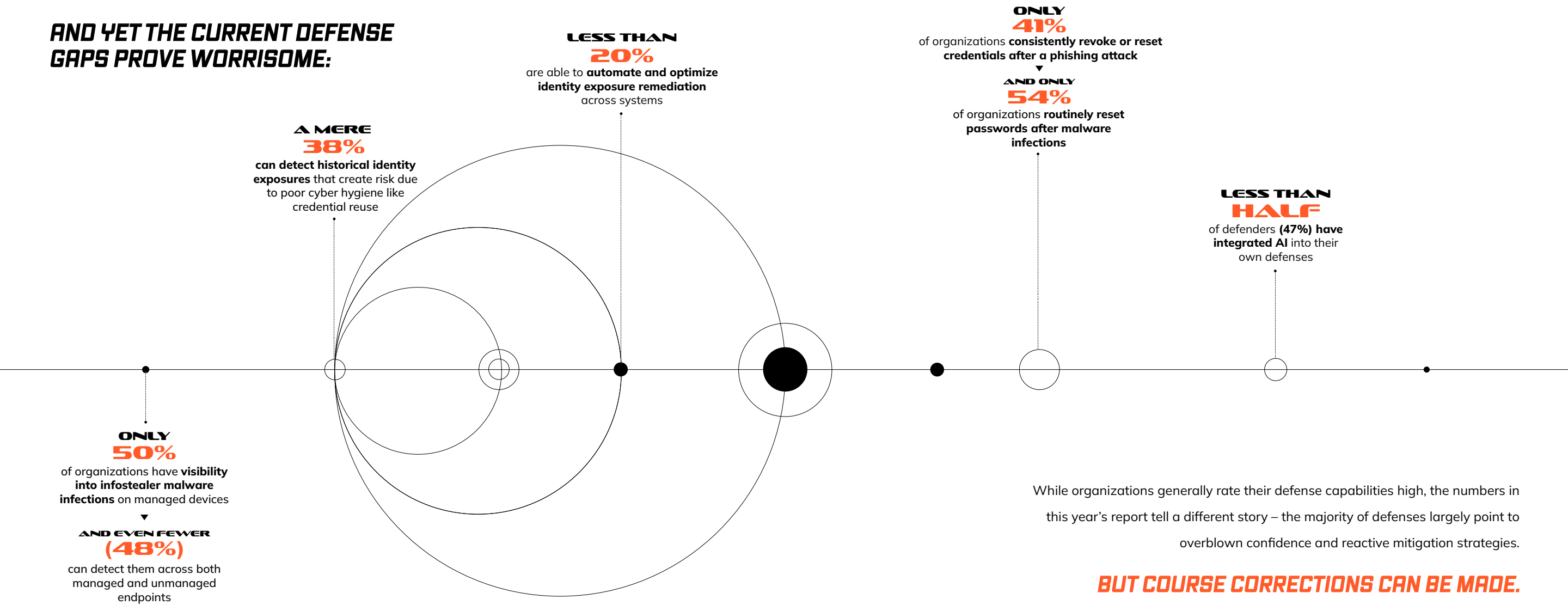
KEY TAKEAWAYS FROM THIS YEAR'S REPORT

We asked security teams to share their perceptions and preparedness as threat actors take advantage of a perfect storm of opportunities: the ever-present occurrence of human error, combined with vast digital identity sprawl, the rapid industrialization of cybercrime, and AI-driven tactics.

WE FOUND THAT:



AND YET THE CURRENT DEFENSE GAPS PROVE WORRISOME:



While organizations generally rate their defense capabilities high, the numbers in this year’s report tell a different story – the majority of defenses largely point to overblown confidence and reactive mitigation strategies.

BUT COURSE CORRECTIONS CAN BE MADE.

The data also shows that organizations that invest in identity-centric strategies, focus on security fundamentals like credential resets and session invalidation, and build automated, cross-team workflows are not only detecting threats earlier, they’re more likely to recover data after ransomware incidents, reduce attacker dwell time, and avoid financial fallout like ransom payments or customer churn.

In this report, we chart the coordinates for operational maturity. Not just a defense against today’s threats, but a proactive course correction toward long-term security sustainability.

THE THREAT RESURGENCE: MODERN ATTACK REALITIES

IDENTITY SPRAWL AND THE EXPANDING ATTACK SURFACE ---

An individual's digital identity now spans hundreds of touchpoints: personal and corporate credentials, session tokens, financial data, and personally identifiable information (PII) sprawling across SaaS tools, corporate and unmanaged devices, and more. These elements – when exposed on the darknet – form a vast, connected, and increasingly vulnerable attack surface.

This fragmentation is exactly why identity has become the gravitational center of cybercrime. Rather than battering down fortified perimeters, attackers exploit the exposed threads of identity, slipping through overlooked gaps and escalating access from within.

If teams fail to seal the gaps, attackers will seize the path of least resistance and exploit it repeatedly.

SpyCloud has recaptured more than 850 billion exposed identity assets, demonstrating the vast scale of exposed data in circulation on the dark web. With so many stolen identity fragments available, bad actors have plenty of access opportunities at their disposal.

Recent industry research confirms the breadth and urgency of this threat:

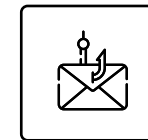
- » **91% OF ORGANIZATIONS EXPERIENCED AN IDENTITY-RELATED INCIDENT IN THE PAST YEAR – NEARLY DOUBLE THE PREVIOUS YEAR'S TOTAL**
- » **SPYCLOUD HAS RECAPTURED 63.8 BILLION DISTINCT IDENTITY RECORDS FROM THE DARK WEB, A 24% INCREASE YEAR-OVER-YEAR**

To stop this cycle, defenders need more than visibility. They need the ability to close the door and change the locks – fast. That means remediating compromised identities, invalidating stolen sessions, and making sure what bad actors have can't be used against them in a follow-on attack.

THE GRAVITY OF MODERN CYBER THREATS ---

Today's adversaries are orchestrating hybrid attacks that blend technical exploits with human deception. Rather than relying solely on software vulnerabilities, which have long been standard fare, attackers now increasingly weaponize identity sprawl – and organizations are taking notice.

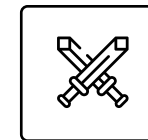
According to our findings, over **three-quarters of organizations** report significant or extreme concern across these threat categories:



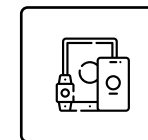
PHISHING
40% EXTREMELY CONCERNED



RANSOMWARE
37% EXTREMELY CONCERNED



NATION-STATE ADVERSARIES
36% EXTREMELY CONCERNED



UNMANAGED OR UNAUTHORIZED DEVICES
36% EXTREMELY CONCERNED

And as shown to the right, nearly 40% of survey respondents flagged four or more of these threats as “extreme,” underscoring the pressure security teams face to prioritize an ever-expanding attack surface.

Certain groups show even greater concern. Security leaders in the healthcare (52%) and IT (47%) industries are more likely to be extremely concerned about phishing. Energy and utility sectors express elevated worry around malware (48%).

Lived experience also appears to drive heightened vigilance. Organizations that were affected by ransomware six or more times in the past year are significantly more likely to be extremely concerned about insider risk (43%) and phishing (48%). And those who haven’t been attacked? They’re markedly less concerned about these issues, highlighting just how much direct exposure shapes cybersecurity priorities.



**A DANGEROUS COMBINATION:
NATION-STATE ADVERSARIES AND INSIDER THREATS**

Security teams at Fortune 500 and other US companies are showing increasing awareness of threats from Democratic People’s Republic of Korea (DPRK) nationals infiltrating their workplaces. **Fraudulent IT workers** are impersonating contractors and job candidates, obtaining remote work positions in software engineering and IT under synthetic or stolen identities. Their paychecks then presumably go towards funding the North Korean regime. The **FBI has also warned** that these individuals are increasingly engaging in data theft and extortion against the companies that have inadvertently hired them.

A recent SpyCloud study shows that over a third of security professionals are extremely concerned about insider threats, and more than half of enterprises report experiencing an insider threat incident within this last year. Investigative tooling and mitigation strategies should be top priorities for enterprises in the year ahead.

**TOP SECURITY THREATS
BY AREA OF CONCERN**



STOLEN IDENTITY DATA AND DANGEROUS FOLLOW-ON ATTACKS ---

When it comes to threats survey respondents are most worried about leading to follow-on attacks, phishing again tops the list, followed by supply chain exposures, malware infections, and insider threats.



MONITORING THE IDENTITY SOLAR SYSTEM:
SUPPLY CHAIN IDENTITY THREAT INDEX* BY INDUSTRY

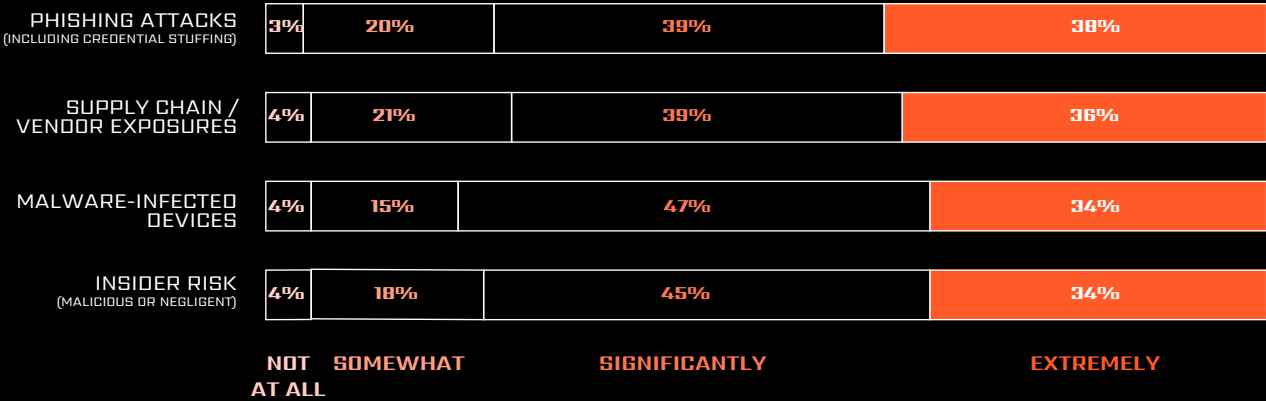
Vendors and supply chain partners with privileged access are prime targets to become entry points for attackers. SpyCloud's Identity Threat Index can be applied across industries to reveal which segments face a higher frequency of identity threats based on the severity of darknet exposures and domain targeting. Threats stemming from malware, phishing attacks, third-party breaches, and circulated combolists were considered and included in this analysis.

Based upon active threats seen through recent darknet exposures, SpyCloud analysis indicates the IT, telecom, and software industries are experiencing the highest levels of threats facing their organizations in 2025. We recommend enterprises confirm they are prepared to respond to active supply chain threats by prioritizing the following steps:

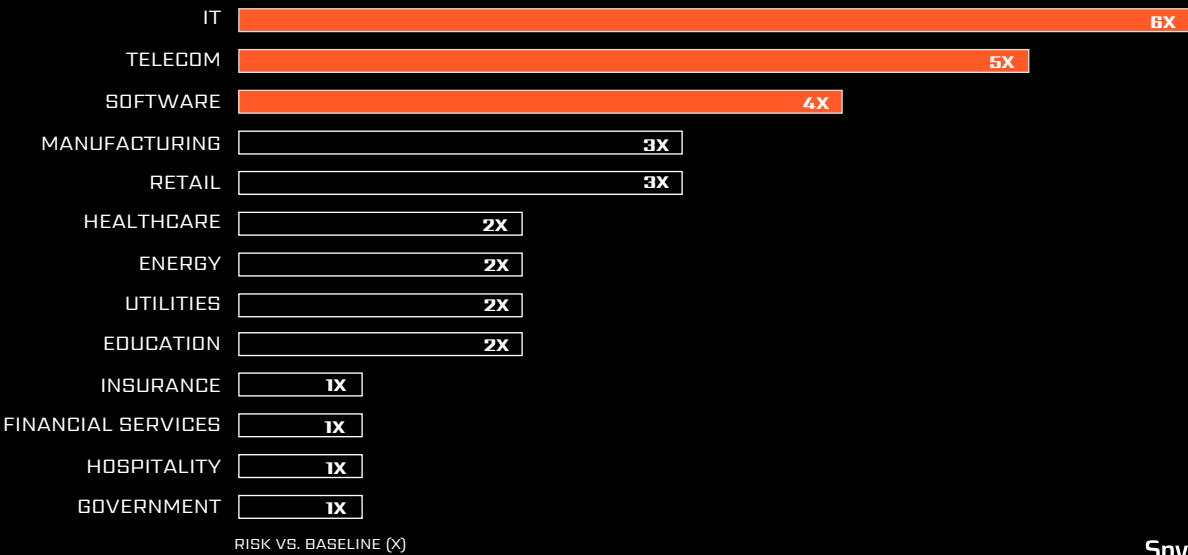
- » Continuous monitoring of active identity threats facing your vendors
- » Open and transparent lines of communication about active threats
- » Implementation of controls to limit the access and impact of vendor security issues
- » Incident response (IR) planning that includes security issues of key vendors

*SpyCloud calculates its Supply Chain Identity Threat Index using darknet exposure data. Data analyzed is from the first six months of 2025.

TOP THREATS
TEAMS FEAR WILL TRIGGER MORE
DAMAGING ATTACKS



SUPPLY CHAIN
THREAT GRAVITY
BY INDUSTRY



ENTRY INTO A PERPETUAL ATTACK ORBIT ---

The defense mission has changed. We know that attackers can piece together identity data from multiple sources, leveraging phished cookies, malware-exfiltrated API keys, and recycled user credentials to find various entry points. Their approach is opportunistic, aimed at creating maximum disruption through whatever access they can find. Organizations are rightfully concerned about related risks:

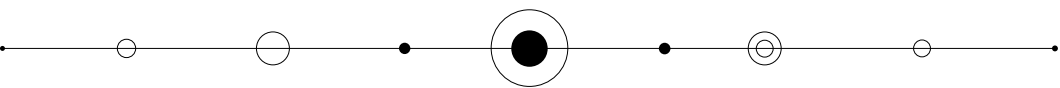
1 | PHISHING / SOCIAL ENGINEERING (39%)

2 | AI-GENERATED THREATS (35%)

3 | EXPOSED OR WEAK CREDENTIALS (35%)

4 | THIRD-PARTY OR SUPPLY CHAIN COMPROMISE (33%)

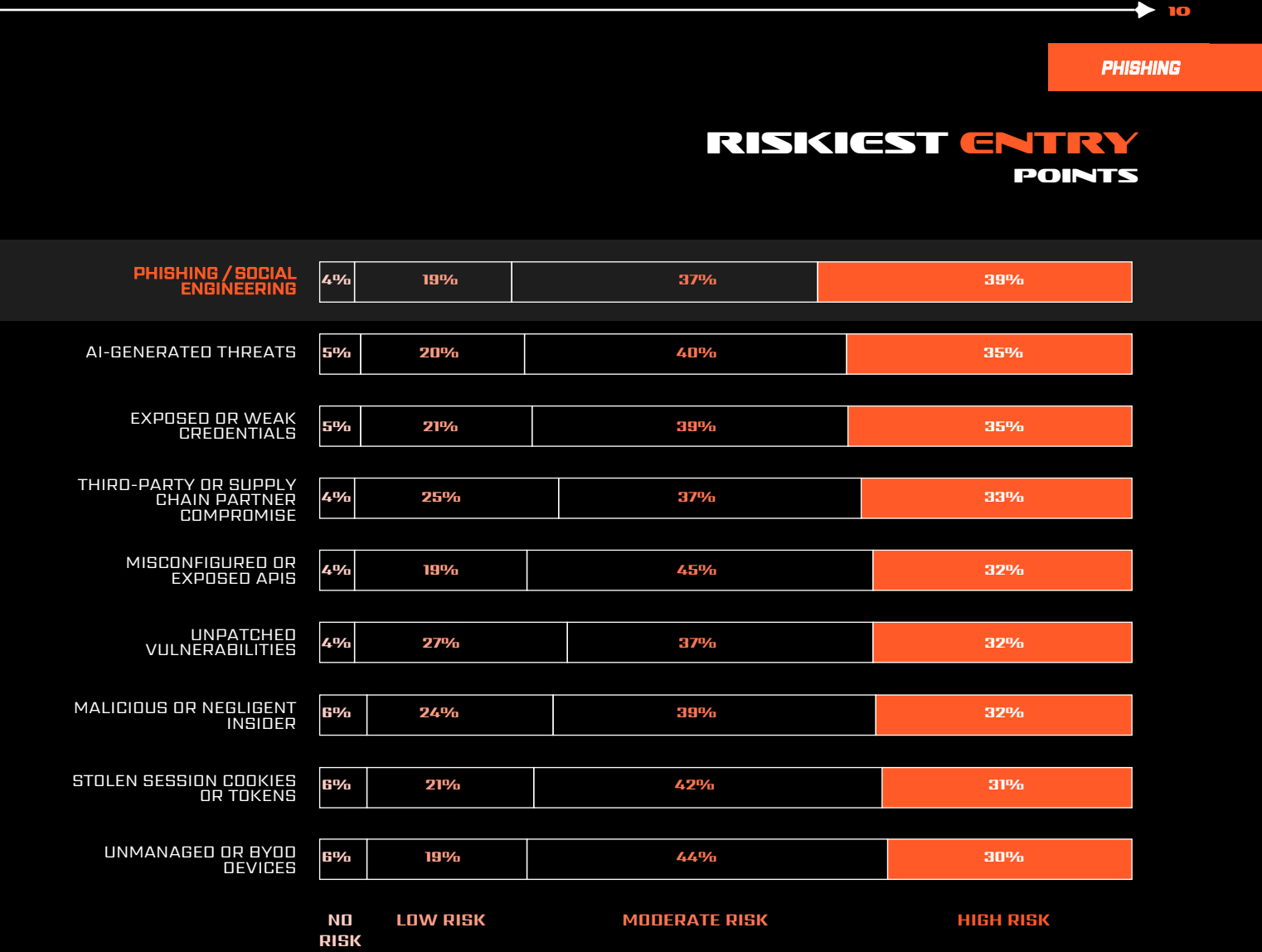
WERE RATED THE RISKIEST ENTRY POINTS TO AN ORGANIZATION
BY SURVEY RESPONDENTS



Phishing blazes the ransomware trail – and evolves

Phishing remains one of the most pervasive cyber threats to businesses because the data collected in a successful phish is so useful for the more malicious follow-on attack. **Case in point: Phishing was cited by 35% of respondents as the leading entry point by organizations that experienced at least one ransomware attack in 2025, up from 25% last year, a significant 10-point increase that underscores both its growth in popularity and its evolution.**

This rise may also reflect the increased sophistication of phishing campaigns, many of which now leverage capabilities like 2FA theft or AI functionality to create hyper-targeted lures tuned to individual employees or business units.



***PHISHING WAS RATED BOTH THE PERCEIVED RISKIEST ENTRY POINT AND THE MOST-USED ACTUAL ENTRY POINT IN SUCCESSFUL RANSOMWARE ATTACKS THIS YEAR.**

MOST COMMON ENTRY POINTS USED BY ATTACKERS IN REPORTED **RANSOMWARE ATTACKS** ---



TOP PHISHING THREATS OF 2025 ---

SpyCloud recaptures data from phishing-as-a-service (PhaaS) platforms and kits, including both phishing targeting lists and successfully phished user data. Analyzing these tools and their capabilities is helpful for understanding how bad actors are quickly evolving their phishing tactics to extract valuable user information.

TYCOON
2FA PHAAS

Tycoon 2FA is a sophisticated PhaaS platform that has been active since August 2023. It specializes in bypassing multi-factor authentication (MFA) protections, particularly targeting Microsoft 365 and Gmail accounts. The platform employs an Adversary-in-the-Middle (AitM) technique, capturing session cookies during the authentication process to grant unauthorized access to user accounts.

FLOWERSTORM
PHAAS

FlowerStorm is a PhaaS platform that emerged in mid-2024, rapidly gaining prominence following the November 2024 disruption of Rockstar 2FA. Both platforms share striking similarities in their design and operation, suggesting a possible shared origin or operational overlap. FlowerStorm is also known as Storm-1167, or ODx, and is designed to steal Microsoft 365 credentials and MFA tokens, using AitM attacks to bypass authentication.

EVILGINX
FRAMEWORK

Evilginx is a sophisticated AitM phishing framework designed to intercept login credentials and session cookies, effectively bypassing MFA protections. Initially developed as an open-source tool for penetration testing, it has evolved into a modular platform capable of targeting various services, including Microsoft 365, Google, and LinkedIn.

THE REVOLVING STEALTH THREAT: INFOSTEALER MALWARE ---

We can't talk about the most pressing threats today without talking about infostealer malware. Security professionals – including our researchers here at SpyCloud – have been raising concerns about infostealers for years, but only recently has the broader security community recognized the scale of damage they are capable of causing. Stealers are finally getting the attention they unfortunately deserve.



SPYCLOUD INSIGHT

An analysis of SpyCloud data shows that about **1 in 2 corporate users*** have been the victim of an infostealer infection in their digital history, whether that be on a managed or unmanaged device. Additionally, and worthy to note, our data shows that **66% of malware infections** occur on devices with endpoint security or antivirus solutions installed.

*Calculated using a sample of all-time recaptured corporate identity data using SpyCloud's **holistic identity matching analytics**.

Infostealer malware operates quietly in the background, collecting swaths of identity information like credentials, financial information, session tokens, and much more – without setting off antivirus or EDR alarms. Once attackers exfiltrate data, they can use it in a myriad of illicit tactics to take over accounts with stolen credentials or hijack active sessions and bypass MFA controls in the case of stolen session cookies, which can allow ongoing access until the session expires or is invalidated.

- » **ONLY 54% OF ORGANIZATIONS ROUTINELY RESET PASSWORDS AFTER MALWARE INFECTIONS**
- » **JUST 33% INVALIDATE EXPOSED USER SESSIONS AFTER MALWARE INFECTIONS**

STEALERS ON THE RADAR ---

Based on our collection of recaptured infostealer malware data from more than 80 different malware families, **LummaC2** – which targets Windows devices and can exfiltrate PII, financial information, crypto wallets, password vaults, 2FA secrets, and more – has consistently been the top infostealer malware in terms of daily numbers of infections since the fall of 2024.

In May, the FBI, Europol, and Microsoft announced **a coordinated takedown** of infrastructure related to LummaC2. We saw a slight decrease in the number of new LummaC2 infections on the day of the takedown, but after only a few days, the infection numbers rebounded, returning to similar levels as the days leading up to the disruption, and there has been no slowing down since. As shown in the numbers on the following page, Lumma still dominates the infostealer world in 2025.



As the single most prevalent infostealer threat globally, LummaC2 clocked over 23.3 million detections in our recaptured data lake so far in 2025. To put this in perspective:

LUMMAC2

- » **Peak activity: 204,045 detections in a single day in February 2025**
- » **Monthly volume: Peaked at 4.2 million detections in February 2025**
- » **Current trend: While showing a 31% decline from January to August, it maintains massive volume with 1.9 million monthly detections by SpyCloud**

And while Windows is overwhelmingly the target of commodity malware, devices running macOS have seen notable increases in targeting this year as well, largely thanks to highly-available macOS stealers like **Atomic Stealer**.

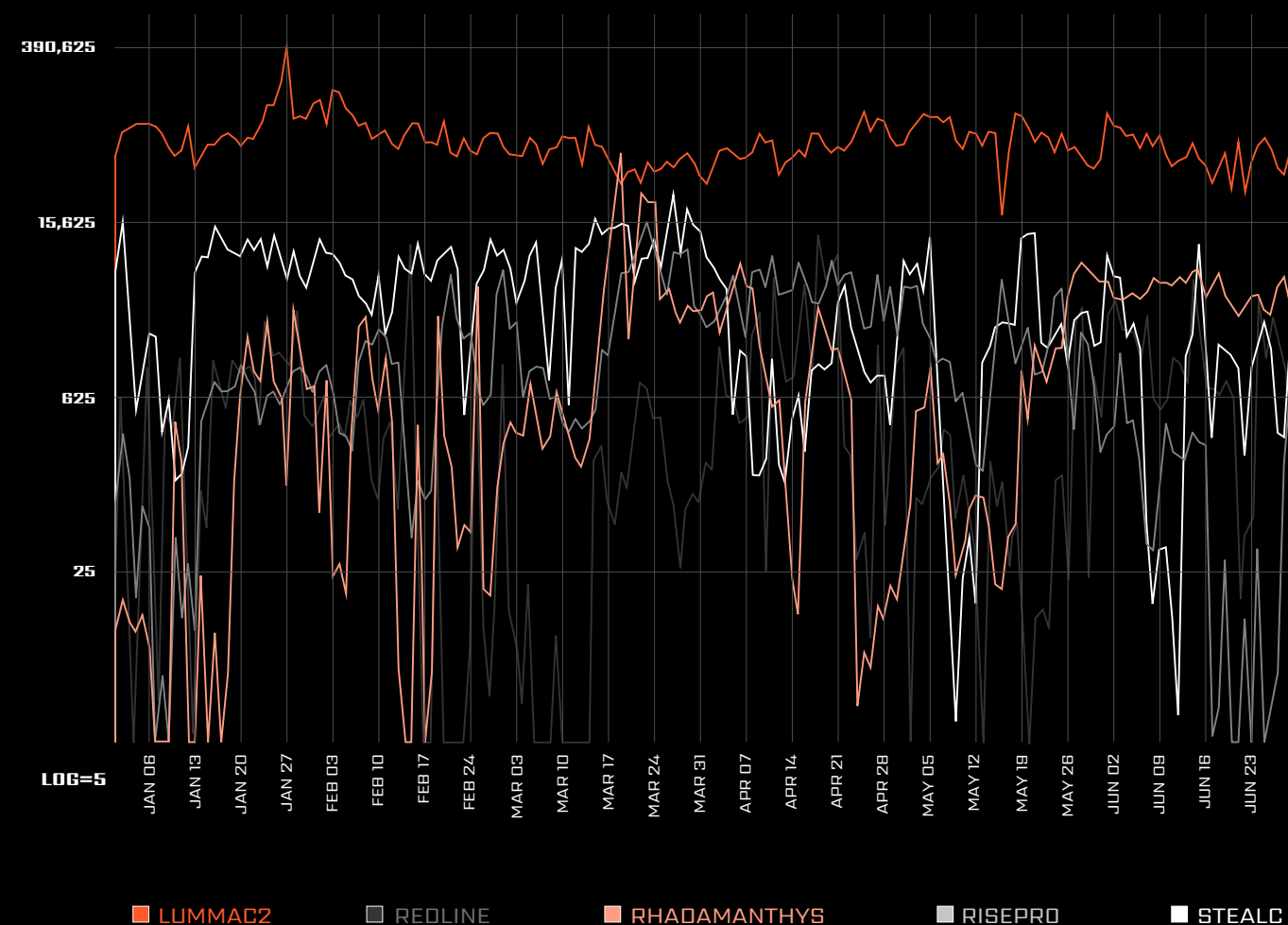
While showing significantly lower volume than Lumma infections (118,436 total detections), Atomic's behavior patterns suggest targeted campaigns rather than mass distribution:

ATOMIC

- » **Highly volatile activity with dramatic spikes and drops**
- » **Peak detection of 10,689 on a single day in August 2025**
- » **Monthly detections ranging from just 154 to over 33,000**

What does this mean for defenders? Without question, macOS is being targeted as threat actors have successfully industrialized attacks against Apple's ecosystem. The data clearly shows we're witnessing a leveling in the infostealer ecosystem – one where platform diversity no longer provides protection, and where identity-based threats have truly become platform-agnostic.

TOP 5 STEALER VARIANTS DAILY INFECTION COUNTS



THE CONFIDENCE TRAP: PERCEPTION VS. REALITY

From a distance, many organizations appear to be on course – fortified by dashboards, workflows, and modern tooling. But beneath that polished exterior lies a disconnect between perceived readiness and operational reality.

While 86% of organizations report feeling somewhat or very confident in their ability to prevent a ransomware attack, 85% actually experienced an attempt or successful attack in the past year. Even more concerning, 31% endured 6 to 10 separate incidents. The confidence is there, but the course is far less stable than it seems.

85% OF ORGANIZATIONS WERE AFFECTED BY RANSOMWARE IN THE PAST YEAR, AND 31% WERE AFFECTED 6-10 TIMES ➤➤

The confidence divide: Executives vs. Operators

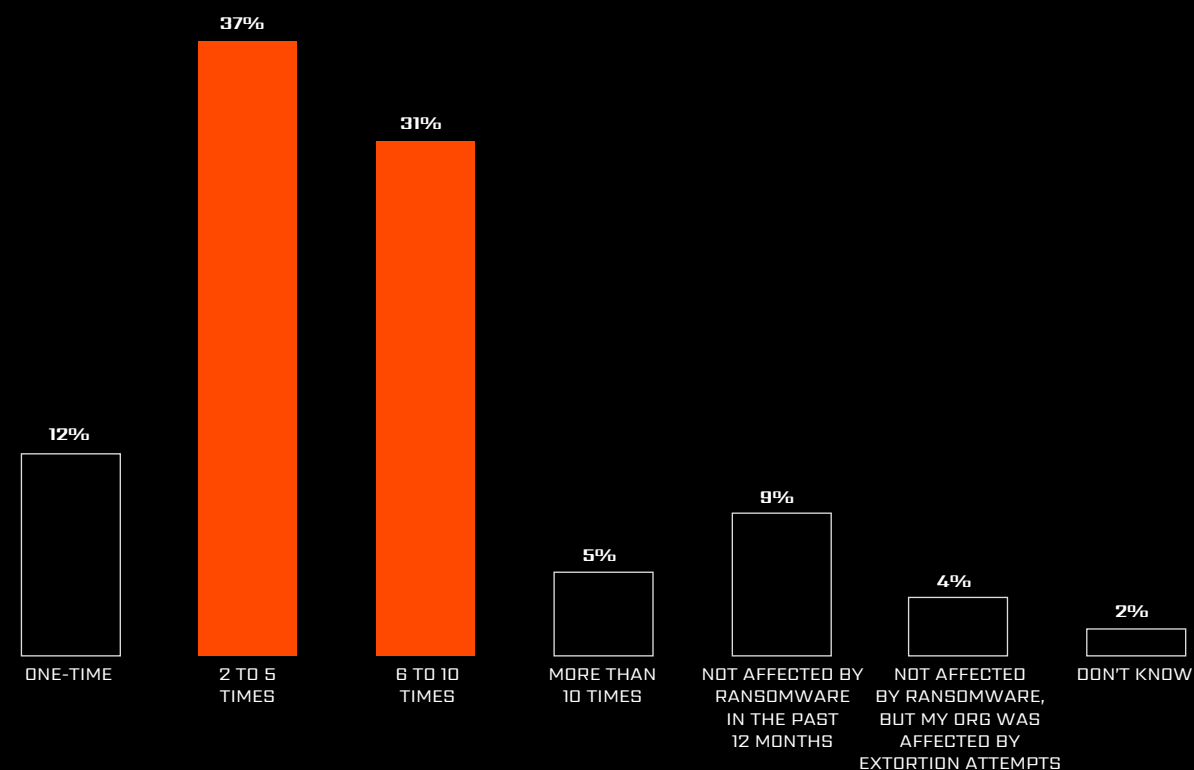
The confidence paradox becomes sharper when you zoom in by role:

- › **45% of CIOs and CISOs** report feeling very confident in their ransomware defense capabilities
- › **But only 28% of security directors and team leads** say the same

Practitioners – those in the trenches with alert fatigue, limited automation, manual workflows, and inconsistent follow-through – see the cracks up close. They're more likely to recognize where friction, fatigue, and blind spots persist.

By contrast, executives often rely on reporting dashboards and compliance milestones. These optics can obscure the deeper operational risks hiding in identity sprawl.

FREQUENCY OF RANSOMWARE INCIDENTS IN THE PAST YEAR



False assurance

Many teams treat successful audits or new tech investments as proof of readiness. But without the supporting operational procedures, these become check-the-box exercises rather than pillars of real security.

- » **Nearly two-thirds of organizations** lack repeatable workflows for identity exposure remediation.
- » **About two-thirds** have no formal investigation protocols for identity-related incidents.

These gaps mean even advanced tools struggle to prevent identity threats from spreading. They simply generate alerts faster in an uncoordinated response environment.

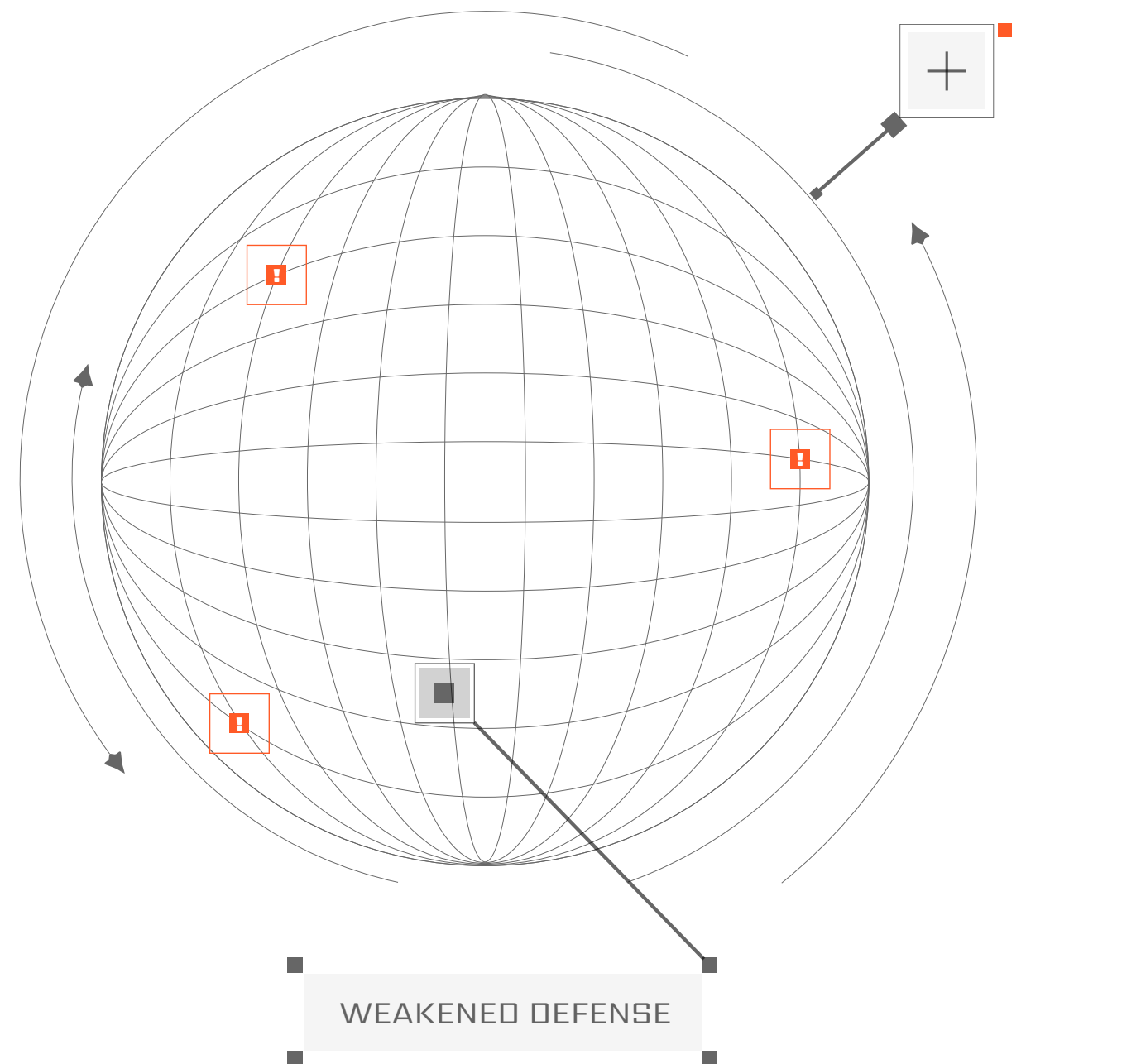
Overestimating malware and phishing defenses

Phishing and malware remain among the most common initial access vectors, yet detection and response practices are often incomplete or inconsistent.

- » **Only 41% of organizations** consistently revoke or reset credentials after a phishing attack
- » **Just 54%** routinely reset user passwords, and **only 33%** terminate active sessions

In both cases, basic security procedures – like resetting credentials after an infection – is often skipped. These oversights create long-lived risks that threat actors are eager to exploit.

Ultimately, confidence without rigor creates complacency. It may feel stable until telemetry says otherwise. And by then, it may be too late.



IDENTITY BLACK HOLES: THE REMEDIATION LAG

What makes identity exposure uniquely dangerous is its ability to penetrate an organization from nearly any angle. And identity artifacts – harvested via phishing, malware, and credential stuffing – require continuous monitoring and remediation to prevent abuse. It only takes one exposure to bring down the ship.

Without full remediation, attackers can return or sell access to the same systems again and again, escalating access, exfiltrating data, or planting malware with each visit. And yet, organizations are still playing catch-up:

- » **ONLY 35% HAVE REPEATABLE WORKFLOWS TO REMEDIATE IDENTITY EXPOSURES**
- » **JUST 33% HAVE PROTOCOLS TO INVESTIGATE IDENTITY-RELATED INCIDENTS**
- » **A MERE 38% CAN DETECT HISTORICAL EXPOSURES THAT CREATE RISK DUE TO BEHAVIORS LIKE CREDENTIAL REUSE**

Remediation gaps that keep the doors open

Despite the scale of exposure, less than 20% are able to automate and optimize remediation across systems. Workflows tend to break down at three key points:

1 | DISCOVERY

Alert fatigue and limited visibility delay the identification of exposed data.

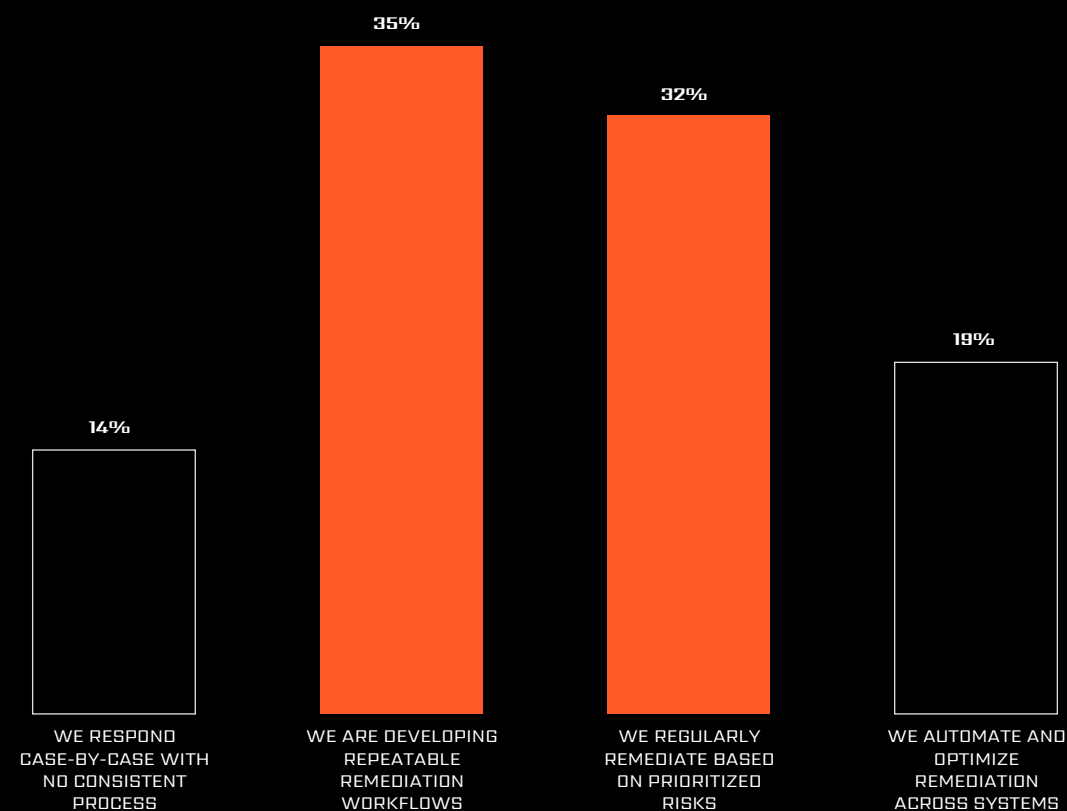
2 | OWNERSHIP

Teams are often unsure who is responsible for what, especially when third-party accounts or unmanaged devices are involved.

3 | CONSISTENCY

Without playbooks, some exposures are fully remediated while others are partially addressed or missed entirely.

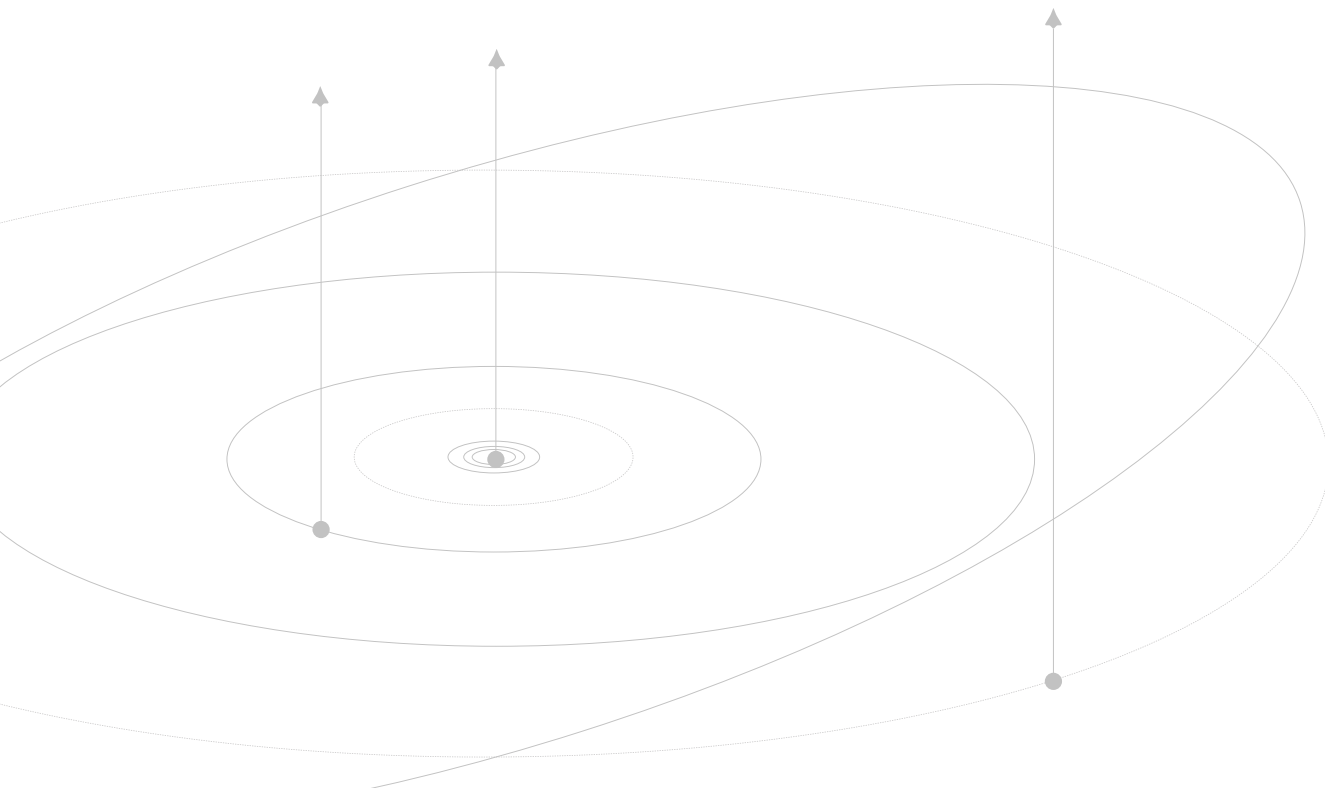
ORGANIZATION'S ABILITY TO REMEDIATE IDENTITY EXPOSURES



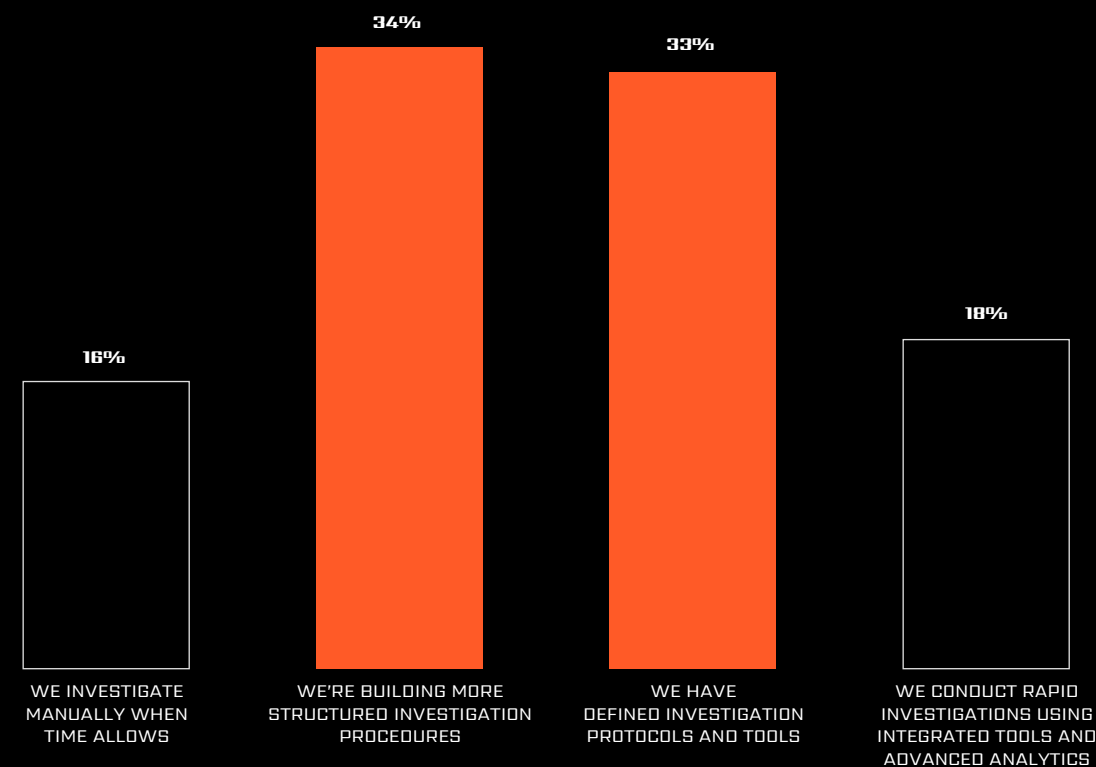
Detection lags: Investigation without a manual

Beyond remediation, detection and investigation processes are also severely underdeveloped. Less than **20%** can conduct rapid investigations using integrated tools and analytics. That means most responses are improvised, reactive, and siloed, leading to prolonged dwell times and a higher risk of follow-on attacks.

This lack of structure is especially problematic for large or hybrid organizations, where exposures may cross multiple systems, teams, or geographies. In these environments, a stolen credential or phished token can quietly enable a campaign of lateral movement, surveillance, and data collection before anyone notices.



ORGANIZATION'S ABILITY TO INVESTIGATE IDENTITY-RELATED INCIDENTS



CRASH LANDING: THE FALLOUT OF MALWARE AND RANSOMWARE

Ransomware and identity-driven attacks don't just inflict damage during the incident – they trigger a cascade of operational and reputational fallout that lasts long after the event is contained. The true cost isn't just the ransom. It's the ripple effects.

Last year, **56% of organizations we surveyed reported ransomware-related costs exceeding \$1 million.** Even when no ransom is paid, expenses from system restoration, forensic investigations, and compliance reporting can quickly spiral.

But the toll extends beyond the balance sheet. **Fifty-five percent of organizations experienced significant operational downtime**, grinding business operations to a halt and disrupting critical services. For industries like finance, healthcare, and critical infrastructure, that disruption can be more than just costly – it can be dangerous.

At the same time, brand trust takes a hit. **Fifty percent of organizations cited significant reputational damage after an attack.** Lost customer confidence, delayed sales cycles, and investor skepticism become silent taxations on future growth. And unlike system recovery, rebuilding trust isn't governed by SLAs.

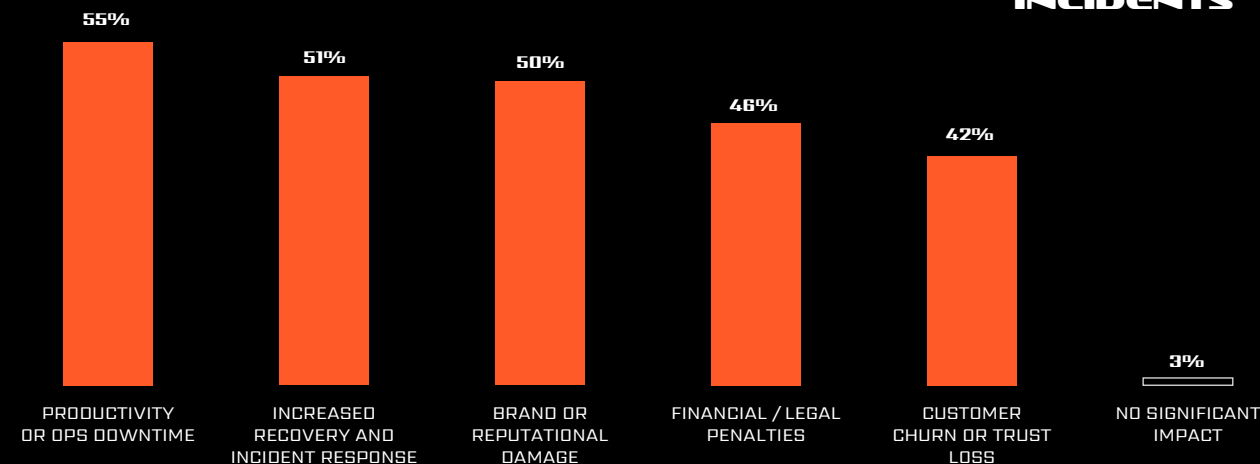
Similar impacts were experienced for malware incidents. **Ninety-three percent** of organizations suffered some significant impact, with over half of organizations experiencing increased recovery and incident response costs.

These outcomes aren't limited to catastrophic events – they increasingly reflect the everyday cost of incomplete identity hygiene and delayed remediation. Without robust credential reset processes, session invalidation, and automated workflows, organizations stay stuck in reactive mode. And that's a mode attackers are counting on.

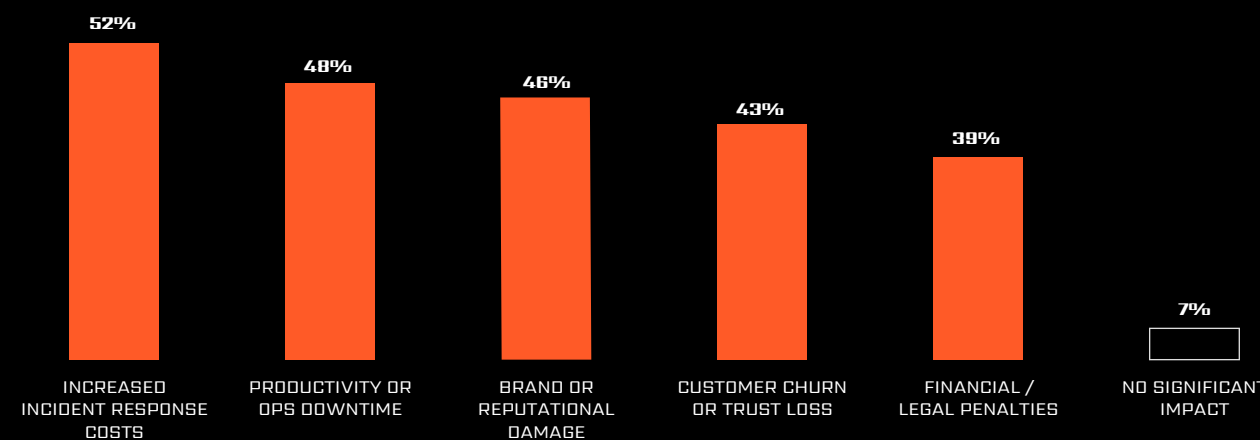
⇒ **BETTER SECURITY STARTS WITH SHUTTING DOWN ACCESS BEFORE ATTACKERS HAVE A CHANCE TO DO DAMAGE.**

IMPACTS

IMPACTS EXPERIENCED DUE TO RANSOMWARE INCIDENTS

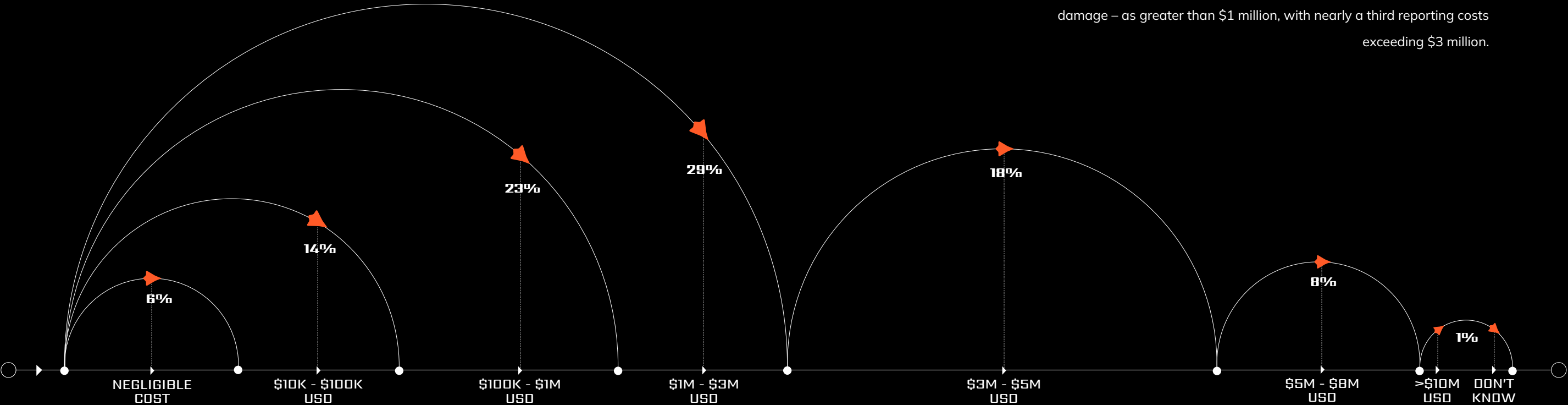


IMPACTS EXPERIENCED DUE TO MALWARE INCIDENTS



AVERAGE CUMULATIVE COST
PER RANSOMWARE INCIDENT
OVER THE PAST 12 MONTHS

More than half of organizations affected by ransomware this year report cumulative costs – whether from actual ransom payments, general disruption, loss of business and opportunities, productivity decreases, and/or reputational damage – as greater than \$1 million, with nearly a third reporting costs exceeding \$3 million.



AI: THE FORCE ACCELERATING THREATS

To make the threat landscape more complex, artificial intelligence is rapidly transforming the dynamics of cyber conflict, empowering both defenders and attackers. For security teams, it offers the ability to accelerate detection, streamline investigations, and scale remediation efforts. Meanwhile, adversaries are already using AI to generate highly convincing phishing lures, automate malware development, and expand their operations with unprecedented efficiency. As both sides race to adapt, the question becomes which will leverage this technology more effectively.

It's a high-speed arms race playing out in real time. Yet, without the right data and frameworks, defenders risk being left on the losing end.

Adversary Boosters: AI-Powered Threat Acceleration

Almost all of the organizations we surveyed this year agree that AI-powered cybercrime has intensified risk. Adversaries are already using generative AI to:

- » Create highly personalized phishing lures in seconds
- » Generate high-quality phishing pages with the click of a button
- » Write or modify malware that evades signature-based detection
- » Launch adaptive social engineering campaigns with voice synthesis and deepfakes

This is not a far-off risk – it's happening now, accelerating the speed, volume, and sophistication of cyberattacks. What once took days or weeks of human effort now takes seconds, pushing defenders to rethink their strategies.

92% OF ORGANIZATIONS AGREE THAT AI-POWERED CYBERCRIME HAS INTENSIFIED RISK.



AI-POWERED PHISHING AND CYBERCRIME ENABLEMENT: DARCULA

Darcula is a phishing kit created by Chinese-speaking cybercriminals that allows less technical users to set up sophisticated phishing pages and launch smishing campaigns. The V3 version of Darcula, released in early 2025, has a particularly novel new feature: phishing kit generation.

Cybercriminal users of Darcula can create their own phishing kit to impersonate any brand simply by inserting the URL of the brand's legitimate website into the Darcula suite. The platform then appears to use a browser automation tool to export the webpage and associated assets like logos and fonts. Darcula users can then choose a scam template based on the specific types of data they want to phish, make any stylistic changes to make sure the phishing page(s) look legitimate and match the impersonated brand's website, and finally export the new custom phish kit.

The takeaway? PhaaS platforms like Darcula are making phishing drastically more accessible to actors of any skill level, greatly reducing the technical expertise required to participate in cybercrime operations. SpyCloud categorizes the broader network of tools and services that allow novice threat actors to execute advanced cyber attacks as 'cybercrime enablement services'. Darcula V3 exemplifies this trend by enabling users to generate and launch professional-grade, customized phishing campaigns that authentically replicate any target brand without demanding specialized technical or web development knowledge.

Thrust Imbalance Causes Defenders to Lag

Despite widespread awareness, only 47% of organizations currently leverage AI tools in their security stack.



This gap represents a dangerous asymmetry. While criminals use AI to scale precision attacks, many defenders are still hampered by manual workflows and overwhelmed by alert fatigue. The result is a growing mismatch: AI-enhanced adversaries are outpacing traditional security models, leaving organizations effectively flying blind against machine-speed threats.

Harnessing AI for Defense

Early adopters show that the right implementation of AI can be transformative:

- » Organizations using AI tools report **higher rates of automated identity remediation**
- » They also experience **faster, deeper investigations**, cutting attacker dwell time and strengthening containment

In effect, these teams are shifting from reactive alerts to proactive, continuous response, navigating the threat landscape with real-time telemetry and system-wide context. They're not just using AI to detect; they're using it to decide and act, augmenting human expertise with machine precision.

Fueling the System: AI's Data Dependency

AI is not a silver bullet. Its value depends entirely on the quality of the information it is given.

Without well-structured identity data, even the most advanced systems can produce false positives, miss real threats, or create a misleading sense of security. Effective AI-driven defense begins with strong foundations. That means supplying models with accurate, relevant, and contextualized data that reflects the real tactics criminals use.

When AI is trained on meaningful signals from the criminal underground, such as breach data, infostealer malware logs, and phishing records, it becomes far more capable of helping teams:

- » Pinpoint compromised identities and threat signals with greater speed
- » Automate remediation processes at scale
- » Focus on threats based on actual adversary behavior

AI can amplify what works, but it can just as easily amplify what's broken. Organizations that succeed with AI are the ones that pair it with robust processes, comprehensive data visibility, and a disciplined approach to identity hygiene.

Copilots of Defense

Ultimately, AI isn't meant to replace security teams; it's designed to *augment them*. The most successful organizations will use AI to:

1 | ENRICH THREAT CONTEXT

2 | SCALE TASKS AND WORKFLOWS

3 | FREE UP HUMAN ANALYSTS FOR HIGH-IMPACT DECISIONS

With the right data, tools, and integration strategy, thoughtful use of AI becomes an important teammate. As defenders chart a course through the turbulent AI era, their trajectory depends on this balance: strategic human judgment, fueled by clean data, and enhanced by intelligent automation.



SPYCLOUD PRODUCT: INVESTIGATIONS WITH AI INSIGHTS

At SpyCloud, we harness this philosophy by using AI to power solutions like **SpyCloud Investigations with AI Insights**, which spots threats by correlating patterns in identity misuse that would slip past human analysis. Built on investigative tradecraft, it automatically analyzes connected exposure data and produces a comprehensive report in seconds – work that would otherwise take hours. By turning identity relationships, digital behavior patterns, and categorized domains of digital activity into clear, actionable summaries, AI Insights helps teams catch more threats, faster.



LESS THAN 1/2 OF RESPONDENTS STRONGLY AGREE THAT IDENTITY PROTECTION ROLES AND RESPONSIBILITIES ARE CLEARLY DEFINED

RECALIBRATING FUNDAMENTALS AND EXPANDING YOUR MISSION SCOPE

The threat landscape has irrevocably changed. Defending the perimeter and monitoring the inside is insufficient when credentials, tokens, PII, and dozens of other data types drift untethered through the criminal underground, and criminals move at lightspeed to take advantage. Now is a critical time for teams to take a hard look under the hatch, confront any confidence biases, and set identity-centric priorities for the year ahead.

BACK TO OPERATIONAL BASICS ---

Despite growing awareness of identity threats, basic yet critical prevention techniques remain widely underused. Among the most overlooked:

- » **ROUTINE CREDENTIAL RESETS AFTER PHISHING OR MALWARE EXPOSURES**
- » **SESSION INVALIDATION TO DISABLE STOLEN TOKENS**
- » **PROACTIVE AUDITS OF EXPOSED APPS FOR INDICATORS OF COMPROMISE**
- » **MONITORING SUPPLY CHAIN VENDORS AND PARTNERS FOR EXPOSURES**

Even modest improvements in these areas can seal off key entry points attackers repeatedly exploit, helping reduce dwell time and downstream risk.

AUTOPILOT ACTIVATION: AUTOMATING IDENTITY RESPONSE ---

Only **19% of organizations automate the remediation of identity exposures**. Of the rest, 14% handle identity exposures on a case-by-case basis, 32% remediate based on prioritized risks, and 35% are still developing repeatable remediation processes. Manual approaches are not only slow, but they're also inconsistent, error-prone, and difficult to scale.

Automation is mission critical for:

- » **MOVING QUICKLY TO SHUT DOWN POTENTIAL ENTRY POINTS BEFORE ATTACKERS**
- » **FULLY REMEDIATING COMPROMISED EMPLOYEE AND CONSUMER CREDENTIALS**
- » **REDUCING HUMAN FATIGUE IN THE FACE OF RECURRING ALERTS**

Organizations that prioritize identity remediation automation are able to shift from reaction to readiness, transforming their response process into a strategic strength.

CREW COORDINATION: CLARIFYING ROLES ---

Identity protection is not the domain of one team – it's a multi-departmental mission. Success hinges on coordination between:

- » **IT AND IAM TEAMS**
WHO MANAGE AND ACCESS CONTROLS
- » **SECURITY AND CTI TEAMS**
WHO MONITOR FOR COMPROMISE AND ARE RESPONSIBLE FOR INVESTIGATION
- » **EXECUTIVE LEADERSHIP**
WHO ALIGN PRIORITIES AND RESOURCES

Yet today, less than half of respondents (42%) strongly agree that roles and responsibilities for identity protection are clearly defined.

MISSION PRIORITIES: ANCHORING IN IDENTITY FIRST ---

The shift to identity-centric security is already underway. Moreover, it's showing up in the top strategic priorities organizations are setting for the next 12 to 18 months:

- » **IMPROVED COLLABORATION TO BREAK DOWN SILOS AND BUILD NEW WORKFLOWS**
- » **STRONGER RANSOMWARE DEFENSES**
- » **INVESTMENT IN AI-POWERED TOOLS**
- » **BETTER VISIBILITY AND CONTROL OVER MALWARE AND PHISHING THREATS**

These are operational blueprints for navigating a threat landscape where threats may be inevitable, but damage does not have to be.

RECOMMENDATIONS

TOP SECURITY PRIORITIES FOR THE NEXT 12 TO 18 MONTHS



BEYOND CONFIDENCE: BUILDING OPERATIONAL MATURITY

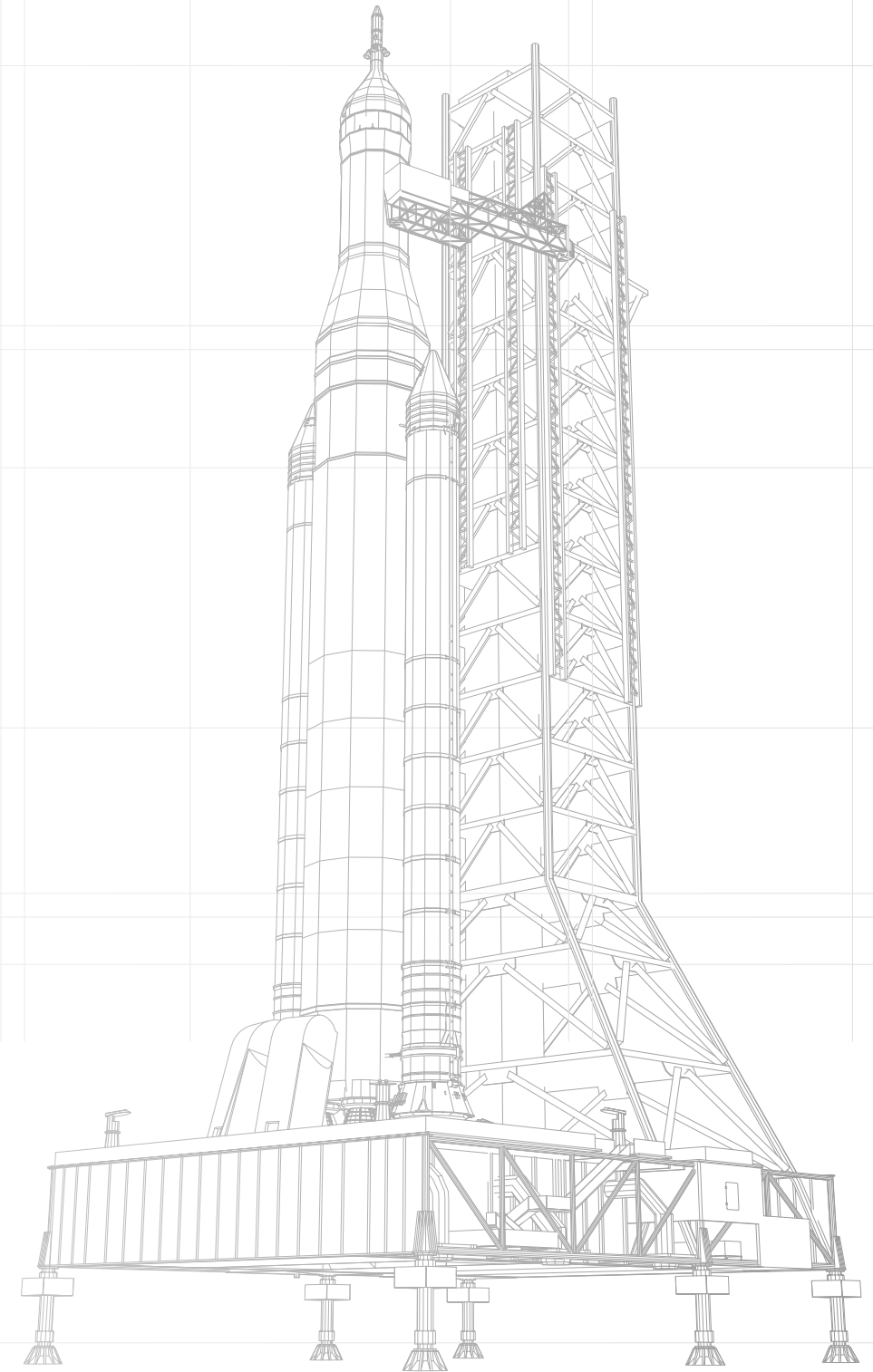
The organizations best positioned to repel, recover from, and outpace identity-driven attacks are those that adopt an identity-centric mindset – one built on continuous exposure monitoring, automated response, and cross-functional alignment.

The question is no longer whether your defenses are strong enough, but whether they are broad enough – and represent the adaptive, unified, and identity-driven qualities needed for modern defense.

Teams that excel in identity security know exactly where exposures exist, can address them at scale, operate with clearly defined responsibilities, and continually adapt rather than simply react.

THE COURSE AHEAD ---

THE FUTURE BELONGS TO THOSE WHO TREAT IDENTITY AS MISSION-CRITICAL ... BUILDING SYSTEMS THAT DETECT COMPROMISE EARLY, RESPOND DECISIVELY, AND NEUTRALIZE THREATS BEFORE LAUNCH.



METHODOLOGY



The study surveyed **507 security professionals** across a wide spectrum of organizational roles, sizes, and industries. All respondents had direct or indirect responsibility for identity security within their organizations.

Roles Represented

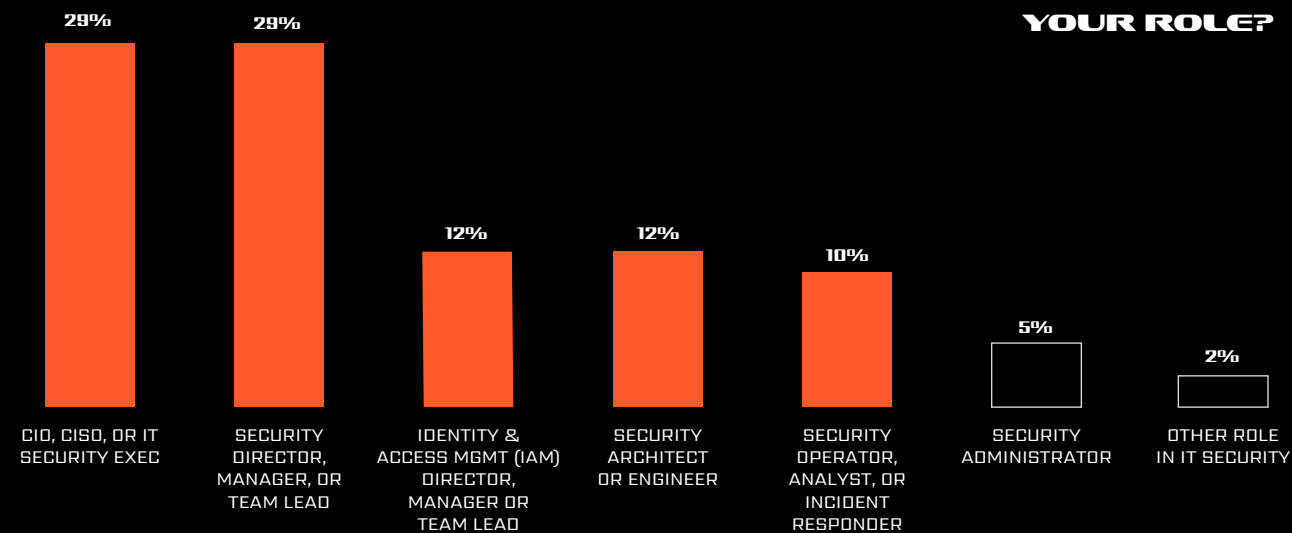
- » **EXECUTIVE LEADERSHIP**
CIOs, CISOs, VPs OF SECURITY
- » **MID-LEVEL MANAGEMENT**
IT DIRECTORS, SECURITY MANAGERS
- » **TECHNICAL PRACTITIONERS**
IAM SPECIALISTS, SECURITY ENGINEERS, SOC ANALYSTS

Geographic Distribution ---

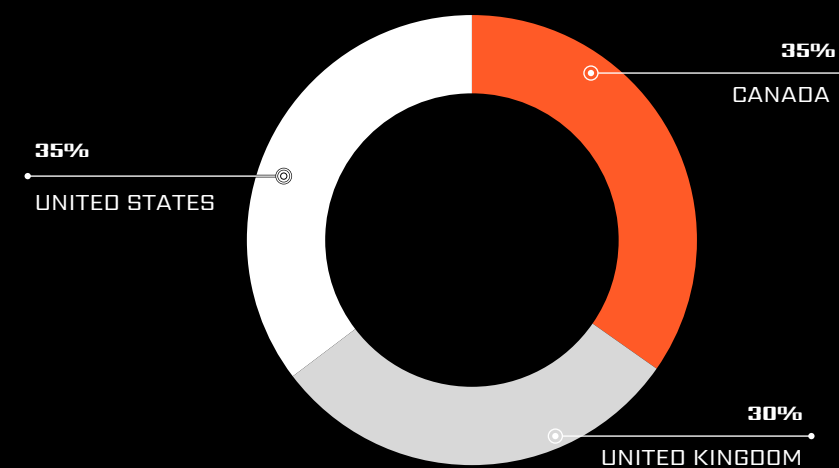
The research captured perspectives from key regions with advanced digital ecosystems and regulatory landscapes:

- » **NORTH AMERICA**
UNITED STATES & CANADA
- » **UNITED KINGDOM**

WHICH BEST DESCRIBES YOUR ROLE?



COUNTRY OF RESPONDENT



COMPANY SIZE ---

Respondents represented organizations of all sizes, reflecting the reality that identity threats are not confined to large enterprises:

- » **SMALL TO MID-SIZE BUSINESSES (SMBs)**
<500 EMPLOYEES
- » **MID-MARKET ORGANIZATIONS**
500 - 5,000 EMPLOYEES
- » **LARGE ENTERPRISES**
>5,000 EMPLOYEES

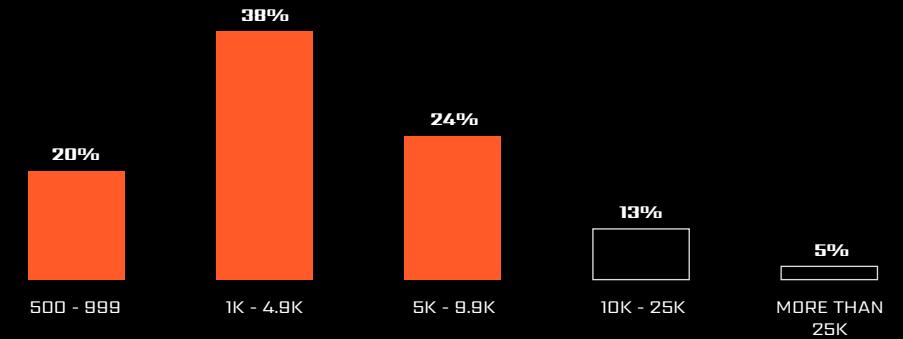
INDUSTRY REPRESENTATION ---

To reflect the wide-ranging impact of identity-driven attacks, the sample included organizations from high-risk and high-regulation sectors, such as:

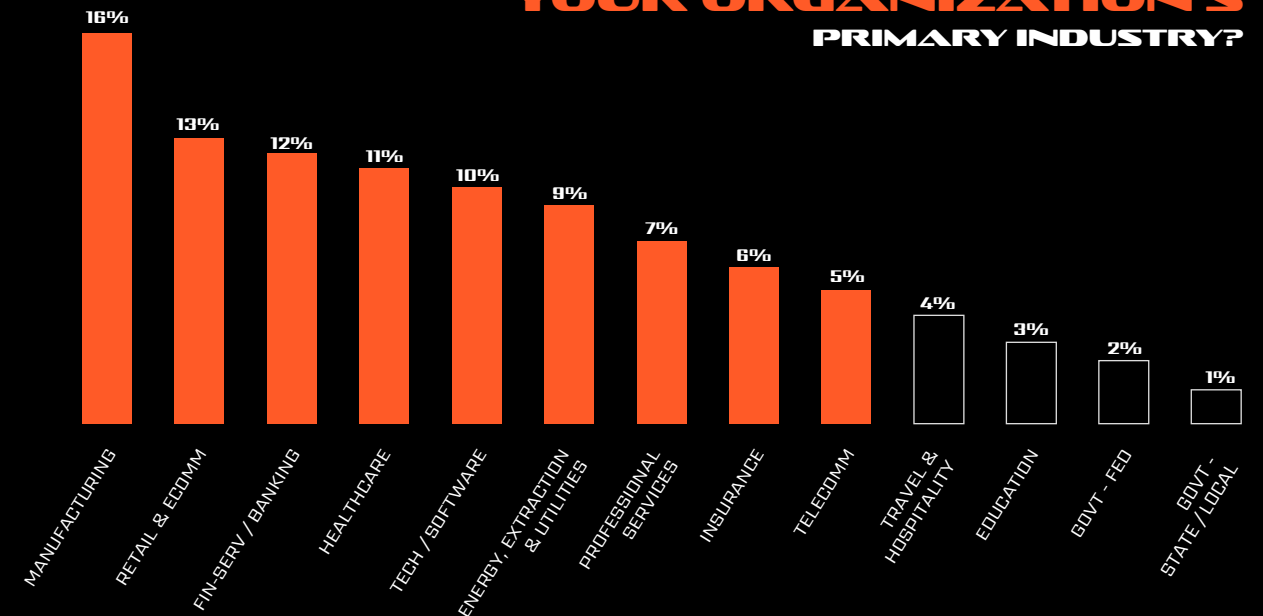
- » **FINANCE**
- » **HEALTHCARE**
- » **TECHNOLOGY**
- » **RETAIL**
- » **ENERGY AND CRITICAL INFRASTRUCTURE**
- » **EDUCATION, GOVERNMENT, AND OTHER SECTORS**

Together, this methodology forms a statistically sound, industry-relevant foundation for the report's findings, combining the strategic perspective of leadership with the hands-on insights of those responsible for protecting identity on the front lines. The result is a comprehensive view of where identity security stands today and what must change for defenders to succeed in the next phase of this mission.

HOW MANY EMPLOYEES ARE IN YOUR ORG WORLDWIDE?



WHICH BEST DESCRIBES YOUR ORGANIZATION'S PRIMARY INDUSTRY?



ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics and AI to proactively prevent ransomware and account takeover, detect insider threats, safeguard employee and consumer identities, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include seven of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

To learn more and see insights on your company's exposed data, visit spycloud.com.