REPORT

The State of Identity Security 2026

Insights from 5,000 IT and Cybersecurity Leaders Across 17 Countries

SOPHOS

Introduction

Identity is the perimeter of cybersecurity, and that perimeter is widening with the continued expansion of AI system access to business data through email, files, SaaS applications, and both human and non-human identities. The result is increased exposure, with sensitive information now easier to reach, and easier to move.

As organizations continue to accelerate cloud adoption, remote work, and the proliferation of applications and services that rely on machine-to-machine connections, the number of digital identities – both human and non-human – has exploded. Every user credential, API key, service account, and OAuth token represents a potential entry point for adversaries. This makes identity security one of the most critical and challenging domains in modern cyber defense.

Attackers have recognized this shift. Stolen credentials, compromised service accounts, and social engineering attacks targeting employees now rank among the most common initial access vectors in breaches worldwide. Adversaries are using AI and automation to move quicker, across more systems. The consequences range from data theft and extortion to full-scale ransomware incidents that can halt business operations for days or weeks.

To understand the true scale and impact of identity-related threats, Sophos commissioned an independent survey of 5,000 IT and cybersecurity leaders across 17 countries into experiences and impacts of identity threats in 2025. This report presents the findings, examining the frequency of identity attacks, organizations' ability to detect and stop them, the resulting consequences, the root causes of successful breaches, the financial toll, and the state of identity security hygiene.

The results paint a stark picture: identity threats are pervasive, consequential, and deeply intertwined with ransomware. Organizations that fail to invest in identity security do so at considerable risk to their operations, finances, and reputation.

5,000

IT and security leaders across 17 countries participated in a vendor-agnostic global survey

Key findings at a glance

- **71% of organizations experienced at least one identity-related security breach** in the past 12 months, with an average of 3 attacks per affected organization.
- **14% of organizations breached were not able to detect and stop** the most significant identity attack before damage was done.
- **The average (mean) cost to rectify an identity breach was $1.64 million**, with the median coming in at $750,000.
- **Data theft (49%) and ransomware (48%) were the most common consequences** of successful identity attacks.
- **Two thirds of ransomware victims (67%) reported the ransomware incident was also their most significant identity attack**, establishing a clear identity-to-ransomware pipeline.
- **Weak management of non-human identities (NHIs) was cited in 41% of identity breaches**, making it the second most common individual cause after human error (43%).
- **Organizations with weak non-human identity management are 22% more likely to experience financial theft, 24% more likely to experience extortion** and report overall recovery costs almost $150,000 higher than average.
- **Just 1 in 3 organizations (34%) regularly rotate or audit service accounts and non-human identities**, and only 11% do so continually – creating security gaps that attackers exploit.
- **Only 24% of organizations continually monitor for unusual login attempts**, and more than half check every three months or less.
- **Energy, oil/gas and utilities providers (80%) and central/federal government (78%) reported the highest identity breach rates**, while IT, technology and telecoms (63%) and healthcare (63%) had the lowest.
- **Smaller organizations (100–250 employees) were 72% less likely to detect an identity attack** compared to those with 1,001–3,000 employees (19% vs. 11%).

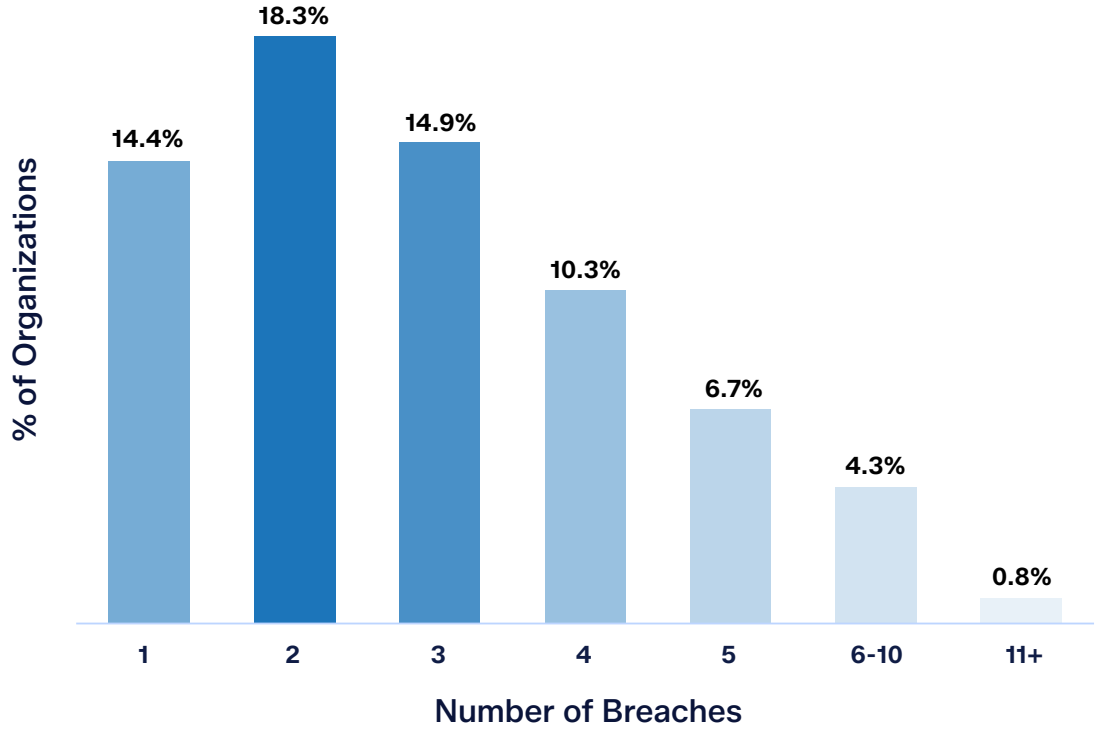
Detailed findings

Frequency of identity attacks

The survey reveals that identity-related breaches are not edge cases; they are the norm. More than seven in ten organizations (70.9%) experienced at least one identity-related security breach in the past 12 months. Only 22.6% said definitively that they had not experienced a breach, while 6.4% acknowledged that breaches may have occurred without their knowledge.

Among those breached, the mean number of incidents was 3.1, indicating that identity attacks are rarely one-off events. 5% of respondents reported six or more breaches in the past year.

Breach frequency distribution



Has your organization experienced any identity-related security breaches in the past 12 months? If so, how many? n=5,000

67%

of all incidents investigated by Sophos Incident Response and Sophos MDR in 2025 were rooted in identity-related attacks.

Sophos X-Ops Insight

Country insights

There is wide geographic variation in breach rates. Switzerland (88.7%) reported the highest rate, 18 percentage points above the global average, followed by Mexico (83.3%) and Italy (80.0%). Germany (62.6%), Colombia (62.7%), and Japan (64.7%) were the least affected, though even the lowest rates exceed 60%.

Country	Breach Rate	vs. Global (70.9%)
Switzerland	88.7%	+17.8 pp
Mexico	83.3%	+12.4 pp
Italy	80.0%	+9.1 pp
Australia	79.7%	+8.8 pp
India	76.8%	+5.9 pp
South Africa	75.0%	+4.1 pp
Brazil	74.0%	+3.1 pp
UAE	73.3%	+2.4 pp
Singapore	72.0%	+1.1 pp
Spain	70.0%	-0.9 pp
Chile	66.7%	-4.2 pp
USA	66.1%	-4.8 pp
France	66.0%	-4.9 pp
UK	65.3%	-5.6 pp
Japan	64.7%	-6.2 pp
Columbia	62.7%	-8.2 pp
Germany	62.6%	-8.3 pp

Has your organization experienced any identity-related security breaches in the past 12 months? If so, how many? n=5,000.

Industry insights

Looking at the data through an industry lens, energy, oil/gas, and utilities (80.3%) and central/federal government (78.4%) reported the highest breach rates. IT/technology/telecoms (63.1%) and healthcare (63.4%) were least affected, perhaps reflecting greater maturity in security investment in those sectors.

Industry	Breach Rate
Energy, oil/gas and utilities	**80.3%**
Central/Federal government	78.4%
Construction and property	76.1%
Manufacturing and production	73.6%
Retail	72.0%
Lower Education (K-12)	71.1%
Financial services	71.0%
Media, leisure & entertainment	70.9%
Local/State government	69.6%
Distribution and transport	67.6%
Higher education	65.9%
Business & professional services	64.5%
Healthcare	63.4%
IT, technology & telecoms	63.1%

Has your organization experienced any identity-related security breaches in the past 12 months? If so, how many? n=5,000.

Compliance as an indicator

Organizations that described keeping up with compliance requirements as "very challenging" had a breach rate of 82.4%, a full 14 percentage points higher than those who found compliance somewhat or not at all challenging (68.3%). This suggests that compliance difficulties are a leading indicator of broader security weaknesses.

Identity security basics

Four types of identity organizations must manage

Every organization grants access to different types of identities. Each carries its own risks.

Category 1 – Workforce identities

People inside the organization who need access to systems and data to do their jobs.

- Employees
- Contractors
- IT and infosec admins (people whose role requires elevated system access)
- Executives (people whose role makes them of particular value to an adversary)

Category 2 – External identities

People outside the organization who are granted access temporarily or on an ongoing basis to fulfill a specific and defined role or interaction.

- Partners
- Suppliers
- Customers

Category 3 – Non-human identities (NHIs)

Software, systems, and automated processes that are granted access to do tasks without a person being involved.

- Service accounts (e.g. scheduled backups)
- API keys (e.g. app integrations)
- AI agents (e.g. autonomous tasks)
- IoT devices (e.g. sensors, cameras)

Category 4 – Privileged identities (highest risk)

Any identity, human or non-human, with elevated permissions that give deep access to sensitive systems and data.

- Super admins (i.e. people with full system control)
- Root accounts (e.g. cloud admin access)
- Shared accounts (e.g. team logins)
- Emergency access (e.g. break-glass accounts)

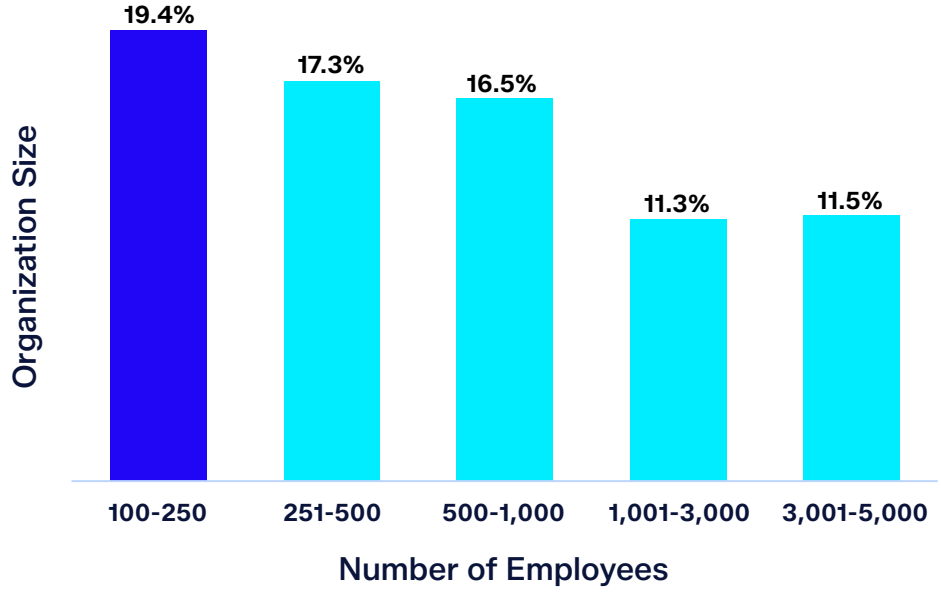
Every identity is a potential entry point. Managing who and what has access to your systems and ensuring that access is appropriate and monitored is one of the most important things an organization can do to stay secure.

Ability to detect and stop identity attacks

Of the 3,545 survey respondents that experienced an identity-related breach in 2025, 85.4% were able to detect and stop their most significant attack before damage was done. While this demonstrates that the majority have some detection capability, the 14.4% that could not stop the attack represents a substantial tail risk and, as subsequent findings reveal, the consequences for those organizations are severe.

Detection Failure by Organization Size

Smaller organizations were significantly less likely to detect attacks. Among the smallest companies surveyed (100–250 employees), 19.4% could not stop the attack, which is nearly double the rate of organizations with 1,001–3,000 employees (11.3%). This gap underscores the resource and capability challenges facing smaller businesses.



Thinking about the most significant identity attack your organization has experienced in the past 12 months, were you able to detect and stop the identity attack before any damage was done? Base: organization has experienced an identify-related security breach. n=3,545.

Detection Failure by Country

Brazil (21.6%) and Switzerland (21.1%) had the highest rates of detection failure, while the UK (7.1%) and Mexico (9.6%) performed best. Notably, Switzerland's high breach rate combined with high detection failure makes it a particularly exposed market.

Country	Failed to Detect
Brazil	**21.6%**
Switzerland	21.1%
Japan	19.6%
Spain	18.1%
Chile	18.0%
Singapore	17.6%
Germany	17.4%
France	14.6%
Italy	14.6%
Australia	13.8%
Columbia	13.8%
USA	12.8%
UAE	11.8%
India	11.2%
South Africa	10.7%
Mexico	9.8%
UK	7.1%

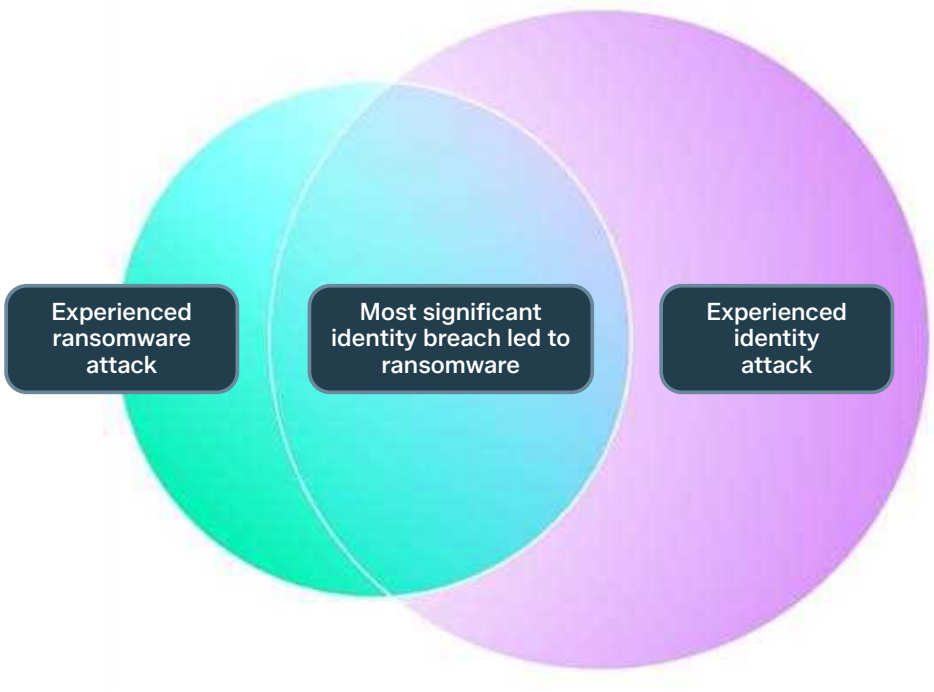
Thinking about the most significant identity attack your organization has experienced in the past 12 months, were you able to detect and stop the identity attack before any damage was done? Base: organization has experienced an identify-related security breach. n=3,545

Detection Failure by Industry

Media, leisure, and entertainment (22.4%) had the highest detection failure rate, followed by manufacturing (18.4%) and financial services (17.9%). Healthcare (8.1%) performed best at detection, possibly reflecting regulatory pressure to invest in threat monitoring.

The Identity-Ransomware Connection

One of the most striking findings in this survey is the direct link between identity attacks and ransomware. Among organizations that were hit by ransomware in 2025, two-thirds (66.5%) confirmed that the ransomware incident was the same event as their most significant identity attack. Although not all the attacks resulted in data encryption, this establishes identity compromise as a primary ransomware delivery mechanism.



In the last year, has your organization been hit by ransomware? (n=5,000). Has your organization experienced any identity-related security breaches in the past 12 months? If so, how many? n=5,000) [If yes to both] Was that ransomware incident the same event as your most significant identity-related attack?

Ransomware-Identity Link by Organization Size

The connection between identity and ransomware was strongest in organizations with 1,001-3,000 employees (71.6%) and weakest in those with 100-250 employees (62.4%). The variation may reflect the differing complexity of organization infrastructure, visibility levels, or ability to correlate attack vector with target outcome across the different segments.

Organizational Size	Ransomware = Identity Attack
100-250 employees	62.4%
251-500 employees	68.2%
501-1,000 employees	62.5%
1,001-3,000 employees	**71.6%**
3,001-5,000 employees	64.6%

In the last year, has your organization been hit by ransomware? (n=5,000). Has your organization experienced any identity-related security breaches in the past 12 months? If so, how many? n=5,000) [If yes to both] Was that ransomware incident the same event as your most significant identity-related attack?

Industry insights

Higher education (76.8%) and distribution/transport (75.0%) had the strongest ransomware-identity link, while financial services (57.6%) and IT, technology and telecoms (61.1%) were lower (although still well above the majority threshold).

Consequences of Undetected Identity Breaches

For the 510 organizations that could not stop their most significant identity attack, the impacts were severe and multifaceted, with victims reporting two consequences on average from the event.

Consequence	% of Breached Organizations
Data theft – attackers stole sensitive data	**48.8%**
Ransomware – stolen credentials used to help execute the ransomware attack	48.4%
Extortion – attackers demanded money with threats	43.9%
Sabotage – attackers used credentials to damage organization	30.0%
Financial theft – diverted payments	28.0%
Financial theft – stole money from accounts	25.5%
Summary: Financial theft (any form)	**46.7%**

What were the consequences of this identity breach for your organization? Base: organization could not stop the security breach. n=510.

Almost half of breached organizations suffered data theft (48.8%), and a near-identical proportion experienced ransomware (48.4%). Nearly half (46.7%) experienced some form of direct financial theft (diverted payments, stolen funds, or both). Taken together with extortion (43.9%), these findings illustrate that undetected identity attacks almost always lead to high-impact outcomes.

Why Organizations Fell Victim

Understanding why attacks succeed is essential for prevention. The survey revealed the mix of human, process, and technical failures that led organizations to fall victim to identity-based attacks. It also reveals that there is rarely a single reason, with respondents reporting two root causes, on average, that contributed to the incident.

Root Cause	% of Breached Organizations
Human error - employee tricked into providing credentials	**42.7%**
Weak non-human identity management (e.g., API keys stored in code, static credentials, orphaned service accounts that previously connected applications to systems, etc.)	40.6%
Weak human identity management for employees	38.6%
Lack of visibility into access and permissions granted to external applications	35.7%
Weak human identity management for suppliers/contractors	31.4%
Lack of control of access and permissions granted to external applications	30.8%
Malicious insider – employee deliberately enabled attack	26.7%
Summary: Weak human identity management (any form)	**60.2%**
Summary: Issues with access and permissions granted to external applications (any form)	**56.1%**

Why did your organization fall victim to the identity-related attack? Select all that apply. Base: organization could not stop the security breach. n=510.

Human error was the top individual contributor to identity breaches, cited by 42.7% of victims. In second position is weak non-human identity management (40.6%), which is particularly concerning because it covers API keys stored in code, static credentials, and orphaned service accounts that are harder to audit and monitor.

Malicious insider activity, where employees deliberately enabled the attack, was reported in over one quarter (26.7%) of attacks, highlighting the importance of maintaining strong internal controls and vigilance.

Collectively, weak human identity management (60.2%) is the most common reason organizations fell victim to identity-based attacks, while issues with access and permissions granted to external applications were a factor in 56.1% of incidents.

59.5%

MFA – a decades-old technology – was unavailable on the targeted system in 59.5% of MDR cases analyzed for the Sophos 2025 Active Adversary report.

Sophos X-Ops Insight

Organization Size Insights

Larger organizations struggle more than smaller ones in several areas of identity exposure, likely reflecting the greater size and complexity of environments that they need to see and secure.

Over half (55.6%) of those with 1,001-3,000 employees reported human error as a root cause compared to just 29.0% of those with 251-500 employees. Similarly, 68.6% of organizations with 3,001-5,000 employees said weak human identity management contributed to them falling victim to attacks compared to 58.5% of those with 100-250 employees.

Non-Human Identities Explained

A non-human identity (NHI) is a digital credential given to a piece of software, system, or automated process so it can access resources without human involvement. Rather than passwords, NHIs use non-human credentials to prove who they are, including:

- API keys connecting applications
- Service accounts running backups
- OAuth tokens for SaaS integrations
- AI agents accessing databases

NHI credentials can be stolen and misused in much the same way as human login details. This is even more problematic when organizations do not regularly audit NHI permissions, which very often are broad and significant.

NHIs significantly outnumber human identities with some organizations seeing ratios higher than 100:1. Agentic AI is a major driver of this increase in ratio in recent years.

96%

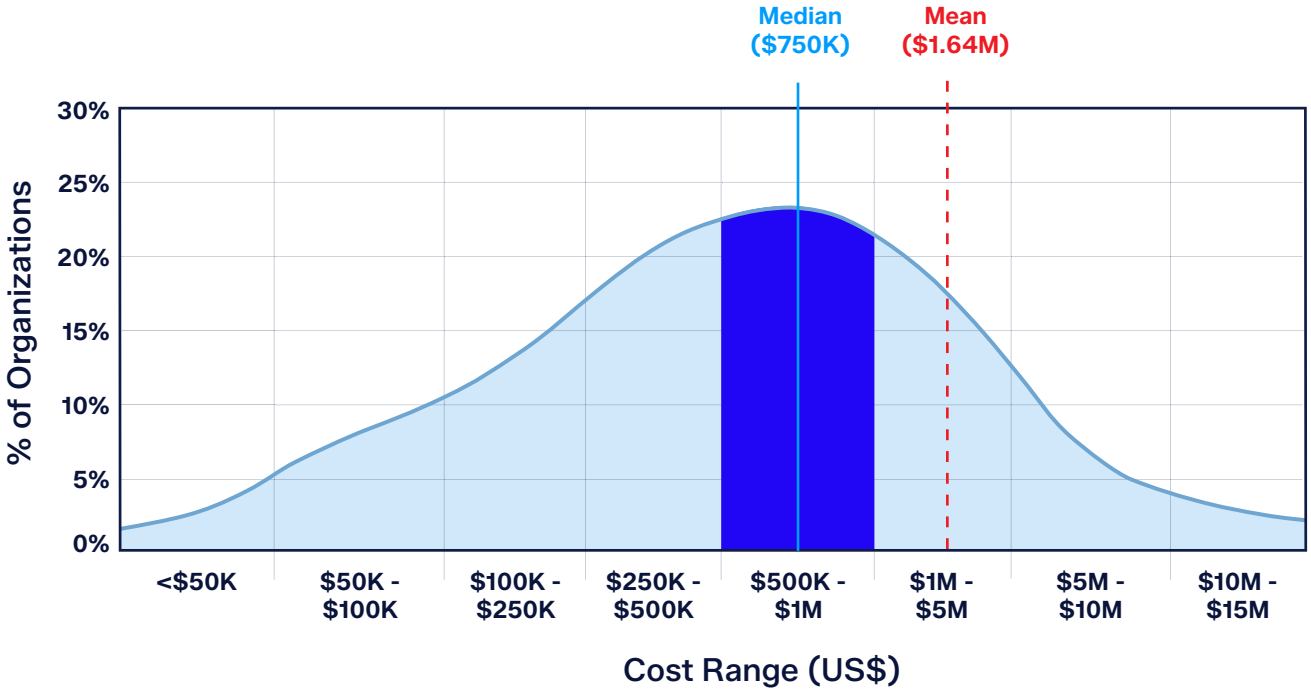
of Sophos ITDR customer environments have multi-tenant applications present. Auditing or even just enumerating the NHIs involved in those relationships can be difficult.

Sophos X-Ops Insight

The Financial Toll of Identity Breaches

Organizations that suffered a successful identity breach incurred significant remediation costs. The global mean recovery bill was $1,637,363 and the median was $750,000. 73% of breached organizations estimated costs of $250,000 or more, and almost a quarter (23.7%) fell in the $500,000-$1 million range.

Cost Distribution



What do you estimate to be the overall cost to your organization to rectify the identity breach? Base: organization could not stop the security breach. n=510.

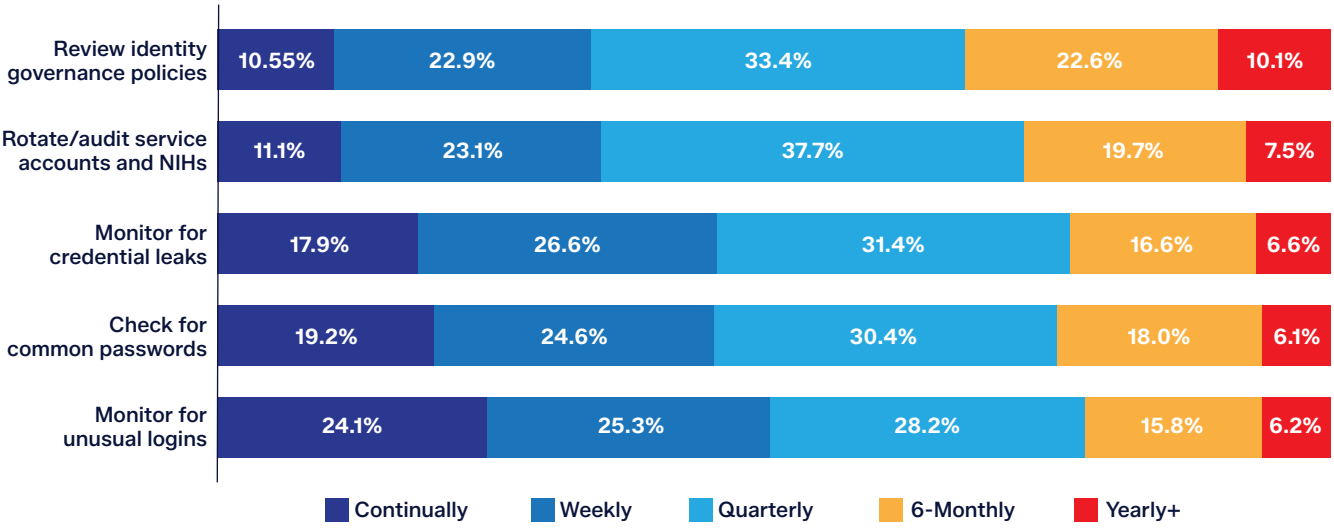
Cost by organization size

Organizational Size	Mean Cost	Median Cost
100-250 employees	$1,125,562	$375,000
251-500 employees	$1,978,043	$750,000
501-1,000 employees	$1,009,205	$375,000
1,001-3,000 employees	$1,907,594	$750,000
3,001-5,000 employees	$2,452,929	$750,000

What do you estimate to be the overall cost to your organization to rectify the identity breach? Base: organization could not stop the security breach. n=510.

Identity Security Hygiene

The survey examined five core identity management activities and how frequently organizations undertake them. The results reveal significant gaps between best practice and reality – gaps that increase exposure to identity attacks.



How frequently does your organization undertake the following identity management activities? n=5,000

Monitoring for unusual login attempts is the most commonly performed activity in real time (24.1% continual), yet even here, over half of organizations (50.6%) check no more frequently than every three months. For rotating or auditing non-human identities, a critical activity given that this is the #2 individual root cause of breaches, only 34.3% do so weekly or more often.

Review of identity governance policies is the least frequently performed activity at the continual level (10.5%), with a third of organizations (33.3%) reviewing policies no more than quarterly and 22.6% only every six months. Given that identity threats are evolving rapidly, annual, semi-annual, or even quarterly reviews leave dangerous gaps.

Agentic AI: Accelerating the NHI Problem

Agentic AI has made the NHI management challenge exponentially harder: more identities, created faster, with broader access and far less human oversight. Top challenges with NHIs include:

- **AI agents multiply NHIs automatically**
  Every AI agent needs it's own identity and credentials. Crucially, agents can autonomously spin up new agents to complete sub-tasks, each one creating more credentials without any human involvement or oversight.
- **AI agents demand broad, persistent access**
  To do their job, AI agents need to reach across many systems: calendars, databases, CRMs, file stores, and APIs. Unlike human accounts, these access rights rarely expire and are rarely audited.
- **AI agents are harder to monitor than traditional NHIs**
  A backup service account runs the same task at the same time every night, which is easy to monitor. AI agents, on the other hand, make autonomous decisions, act unpredictably, and operate 24/7, making it very difficult to spot when something has gone wrong.
- **Third party AI agents inherit unknown risks**
  When organizations use third-party AI agents capabilities, research indicates they inherit all the credentials and access permissions those agents carry, albeit with limited visibility into how securely they were built or what they can access.
- **Security rules weren't written for AI agents**
  Most identity security frameworks were built for human users and simple machine account. They don't account for agents that can autonomously create, delegate, and retire their own credentials mid-workflow, leaving a significant governance gap.

Agentic AI is a key reason NHI security has moved to the top of the CISO agenda.

Consequences of weak non-human identity management

As previously shared, weak non-human identity (NHI) management was a root cause in 40.6% of successful attacks. Diving deeper, the data reveals that compromised NHIs radically escalate the financial consequences of the breach.

Most notably, organizations with weak NHI management are considerably more susceptible to financial theft (where adversaries diverted payments from accounts) at +27.9 % above average, and extortion (where attackers demand money with threats) at +24.4% above average. The only categories where weak NHI management organizations fared slightly better than average were data theft and ransomware, although those differences are marginal.

Consequence	% of All Breached Organizations	% of Breached Organizations with Weak Non-Human Management	% Change with Weak Non-Human Identity Management
Data theft – attackers stole sensitive data	48.8%	47.8%	-2.1%
Ransomware – stolen credentials used to help execute the ransomware attack	48.4%	46.4%	-4.1%
Extortion – attackers demanded money with threats	43.9%	**54.6%**	**+24.4%**
Sabotage – attackers used credentials to damage organization	30.0%	33.8%	+12.7%
Financial theft – diverted payments	28.0%	**35.8%**	**+27.9%**
Financial theft – stole money from accounts	25.5%	29.9%	+15.7
Summary: Financial theft (any form)	**46.7%**	**57.0%**	**+22%**

What were the consequences of this identity breach for your organization? Base: organization could not stop the security breach. n=510 (all breaches), n=207 (breaches involving NHIs)

Given the increased financial impact of weak NHIs, it's unsurprising that organizations with weak NHI management report notably higher overall recovery costs from identity breaches, with the typical bill coming in almost $150,000 higher than average.

Mean cost to recover from identity breaches

There is clear correlation between poor NHI hygiene and propensity to experience an NHI-related breach. While one third (34%) of all organizations rotate or audit service accounts and NHIs continually or weekly, this drops to a quarter (24%) among those whose breach was due to compromised NHIs.

Conclusion

The findings of this survey leave no room for complacency. Identity-related breaches affected more than 7 in 10 organizations in the past year, with an average of more than three incidents per affected company. This is not a theoretical risk or a problem confined to specific industries or geographies. It is a universal, pervasive threat that touches organizations of every size, sector, and region. The data shows that identity attacks are the front door through which ransomware, data theft, and extortion enter an organization: 67% of ransomware victims traced the incident directly back to an identity compromise.

When identity attacks succeed, the impact is severe and multi-dimensional. Nearly half of breached organizations suffered data theft or ransomware, and the average remediation cost of $1.64 million makes each incident a material financial event.

The root causes point to systemic weaknesses: human error (42.7%), poor non-human identity management (40.6%), and insufficient visibility into third-party application permissions (35.7%) are all addressable, but only with sustained investment and attention. That smaller organizations are nearly twice as likely to fail to detect attacks as larger ones highlights a cybersecurity poverty gap that demands attention from the security community.

Perhaps most concerning is the state of identity security hygiene. Only around a quarter of organizations continually monitor for unusual login activity, and fewer than one in three regularly rotate non-human credentials, the very weaknesses attackers exploit.

Organizations must recognize that identity security is not a one-time project but a continuous operational discipline. Those that treat it as such will be far better positioned to defend against the threats that defined 2025 and will continue to escalate in 2026 and beyond.

Recommendations

As the survey has shown, strong identity security is an essential element of an effective cyber risk mitigation strategy. To reduce exposure to identity-related attacks, organizations should look to put in place a multi-layered defense for both human and non-human identities. Start with the Essential steps and work toward the Recommended actions as part of a continuous improvement program.

Essential steps

Human identities

- Enforce Multi-Factor Authentication (MFA) for all user accounts.
- Use distinct credentials for privileged and non-privileged operations.
- Implement account lockout and brute-force protection.
- Centralize identity management with Single Sign-On (SSO).
- Ensure your user awareness training reflects the latest phishing and credential theft techniques.

Non-human identities

- Periodically inventory and classify all non-human identities.
- Use short-lived credentials over long-lived secrets.

Human and non-human identities

- Apply least-privilege access.
- Secure and manage credentials properly.
- Disable or remove inactive identities promptly.
- Enforce a formal offboarding process that audits and decommissions access to employer resources.
- Log and monitor all authentication activity, and retain logs for at least 30 days.

Recommended steps

Human identities

- Implement conditional access and risk-based policies.
- Roll out passkeys (either hardware or software) as your primary authentication method.
- Federate identities using widely accepted identity protocols such as Security Assertion Markup Language (SAML) or the newer OpenID Connect (OIDC).

Non-human identities

- Use workload identity federation instead of static secrets.
- Adopt a secrets management platform for NHIs at scale.
- Enable scanning of secrets in supported platforms (GitHub, GitLab).

Human and non-human identities

- Deploy a Privileged Access Management (PAM) solution.
- Adopt a Zero Trust security model.
- Conduct periodic access reviews and entitlement recertification.
- Deploy Identity Threat Detection and Response (ITDR) capabilities.
- Segment network access by identity and role.
- Define and test one or more identity incident response playbooks addressing identity-related incidents such as those described in this report.

Learn More

Read our Identity Security Best Practices Guide

Methodology

This survey was conducted by Vanson Bourne on behalf of Sophos in Q1 2026. 5,000 IT and cybersecurity decision-makers were interviewed across 17 countries: USA, Brazil, Chile, Colombia, Mexico, UK, France, Germany, Italy, Spain, Switzerland, Australia, India, Japan, Singapore, South Africa, and UAE. Respondents came from organizations with 100 to 5,000 employees across 15 industry sectors.

SOPHOS

To discuss your identity security needs and how Sophos can help, visit our website or speak to an advisor.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2026-05-08 EN (TA) CRE-5312