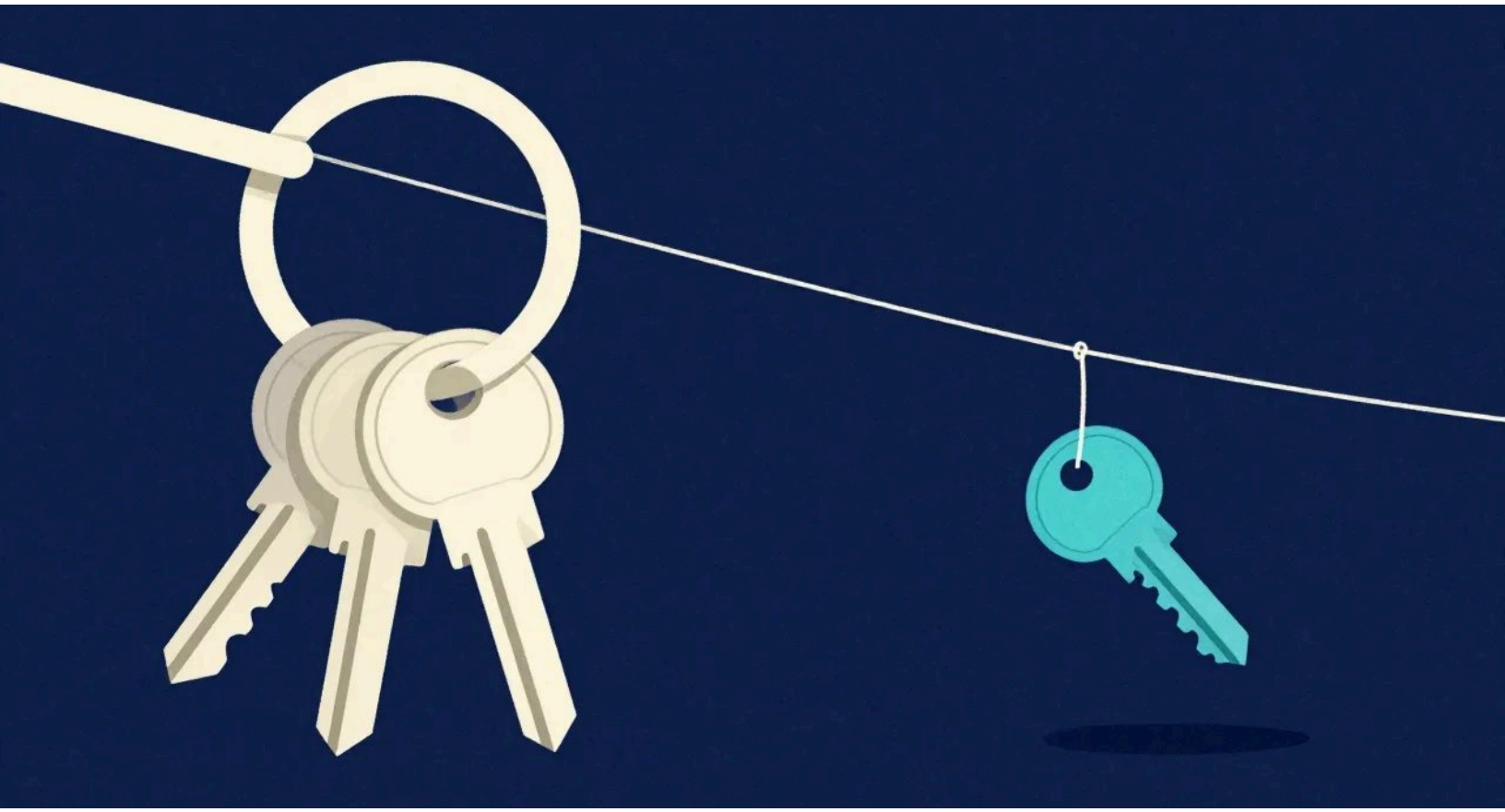


EXECUTIVE PAPER · INFRASTRUCTURE

Identity Is Where Attackers Get In

Most breaches now begin with a login that works, through a stolen password, a talked-into reset, or a forgotten token. Executives should fund identity as the control that matters most and measure it like one.

AUTHOR

Chris Watkins

SERVICE

Infrastructure

FOR

CEO, CFO, CISO, Board · 12 min read

AT A GLANCE

The problem. Credential abuse was the most common way into a network in Verizon's 2025 breach data, ahead of software exploits. Microsoft found that more than half of intrusions using a valid account went on to steal more credentials. The costliest retail attacks of 2025 began with a phone call to a help desk, and M&S put its direct costs at about £136 million.

Why it persists. Identity is spread across HR, IT, the help desk, application owners and developers, and nobody owns the whole of it. MFA is counted as done when the weakest methods are enabled. Service accounts, API keys and integration tokens far outnumber people and sit outside most reviews.

The recommendation. Name one executive owner for identity. Move administrators first, then all staff, to phishing-resistant sign-in. Remove standing administrator rights, inventory and rotate every machine credential, rebuild help desk resets around verification the caller cannot fake, and close access the day someone leaves. Report these numbers to the board each quarter.

The Decision in Front of You

Security budgets still go mostly to stopping malicious software and patching servers. The evidence now says most attackers skip both. They sign in.

Verizon's 2025 Data Breach Investigations Report, built from more than 22,000 incidents and 12,195 confirmed breaches, found credential abuse was the leading initial access vector at 22%, ahead of exploited vulnerabilities at 20% [1]. Microsoft's Digital Defense Report 2025 calls identity "the primary control plane" for defense and found that 52.2% of intrusions through valid accounts went on to steal further credentials, so one stolen login tends to become many [3].

The decision is whether to run identity as one program with an owner, a budget and board metrics, or leave it as settings spread across a dozen teams. This paper covers the accounts themselves, for people and machines. Patching and shared passwords, VPN appliances, and payment fraud by email have their own papers in this series.

What's Happening

Attackers log in instead of breaking in

Coverage of Microsoft's 2025 report says identity-based attacks rose 32% in the first half of 2025, and 97% of them were password spraying or brute force, guessing common passwords across many accounts [4]. These are cheap attacks. They fail against any account that requires a second factor attackers cannot replay.

Infostealer malware supplies the rest. Verizon's analysis of infostealer logs found that 46% of compromised systems holding corporate logins were unmanaged devices, most likely personal computers used for work [2]. When Verizon matched those logs against the victims named by ransomware groups in 2024, 54% of the victims had their domains in the credential dumps and 40% had corporate email addresses among the stolen credentials [2].

Third parties widen the exposure. Breaches involving a third party doubled to 30% in the 2025 report, and the median time to fix secrets leaked in a public GitHub repository was 94 days [1][2].

Machine identities outnumber people

Every integration, script, pipeline and AI agent signs in with something: a service account password, an API key, a certificate, an OAuth token granted to a connected app. A 2025 survey of 2,600 security decision makers in 20 countries, sponsored by the identity vendor CyberArk, estimated 82 machine identities for every person, and found that 42% of machine identities had privileged or sensitive access [18]. In the same survey, 88% of respondents said their definition of a privileged user covered humans only [18].

These credentials cannot use MFA and rarely expire. Microsoft's 2025 report adds AI agents to the same problem and recommends scoped credentials and least privilege for them [3].

The standards have moved

CISA calls phishing-resistant MFA, meaning FIDO security keys, passkeys and smart cards, "the gold standard" [5]. App codes can be relayed through a fake login page, and text messages can be stolen through SIM swaps [5]. CISA asks administrators and other high-value targets to move first [5].

NIST finalized SP 800-63-4, its Digital Identity Guidelines, in July 2025 [7]. Its authentication volume, SP 800-63B-4, requires services at the second assurance level to offer a phishing-resistant option, accepts synced passkeys there, and restricts text and voice codes [6][7]. It drops forced password changes and complexity rules in favor of length and a check against known compromised passwords [6]. Every account recovery must trigger a notification to the account holder [6].

Four Cases, 2024 to 2025

M&S, April 2025. On April 17, 2025, attackers impersonated an M&S employee and persuaded a third party to reset that employee's password [9]. Chairman Archie Norman told a UK parliamentary sub-committee the entry came through "sophisticated impersonation" involving a third party, reported to be its outsourced help desk [9]. The attackers then encrypted servers with DragonForce ransomware [9]. Online orders stopped for weeks [10]. M&S had warned in May the attack could cost £300 million; in November it put direct costs at about £136 million, against an insurance claim of up to £100 million [10]. The lesson: a password reset over the phone is an authentication event, and it was the weakest one M&S had.

Co-op, April 2025. Sources told BleepingComputer that attackers used social engineering to reset an employee's password at the Co-op, then stole the Active Directory database that holds every user's password hash [11]. The chief executive confirmed that data on all 6.5 million members was taken [11]. Co-op estimated £206 million in lost sales and an £80 million hit to operating profit in the six months to July 5, 2025, and it had no dedicated cyber insurance [12]. CISA's July 2025 update on Scattered Spider, the group reported to be behind both attacks [9][11], describes the same method: callers pose as employees, ask the help desk to reset passwords and move MFA to a device the attacker holds [8].

Microsoft, January 2024. The Russian intelligence group Microsoft tracks as Midnight Blizzard used a low-volume password spray to take over a legacy, non-production test tenant account that had no MFA [13]. From there it found a legacy test OAuth application with elevated access to Microsoft's corporate environment and used it to grant itself access to corporate mailboxes [13]. No cost has been published. Forgotten test accounts and test applications carried real permissions.

Salesloft Drift, August 2025. Between August 8 and at least August 18, 2025, a group Google tracks as UNC6395 used stolen OAuth tokens from the Salesloft Drift chat integration to export large volumes of data from customers' Salesforce instances [14]. The attackers then searched the stolen records for AWS keys, passwords and Snowflake tokens to reach further systems [14]. No password was stolen and no MFA prompt was bypassed, because the connected app already had access. Google advised treating every Drift-connected token as compromised [14].

SIDEBAR: THE TOKEN NOBODY ROTATED

In October 2024 an attacker found an authentication token in an exposed GitLab configuration file on an Internet Archive development server, reportedly exposed since December 2022 [15]. It led to more credentials in source code, a database of about 31 million user accounts, and a Zendesk token reaching more than 800,000 support tickets [15]. Later that month the attacker used the Zendesk access again, and coverage faulted the failure to rotate exposed tokens [15].

The best-known 2024 cases, covered in this series' paper on patch debt and shared passwords, fit the pattern: Snowflake customer accounts entered with old infostealer passwords and no MFA [16], and a Change Healthcare remote access portal that "did not have multifactor authentication" [17].

Why the Usual Approach Fails

Identity has no single owner. HR creates the person, IT creates the account, application owners grant access, developers create service accounts and API keys, and the help desk resets everything. Nobody sees the whole account. At M&S and the Co-op the gap was the reset process [9][11], and at Microsoft a test tenant outside production controls [13].

MFA gets reported as a percentage of accounts enrolled. That number counts text messages and push prompts as equal to security keys, though CISA ranks them far apart [5]. It also excludes the accounts that matter most: break-glass administrator accounts, legacy protocols that bypass MFA, and the machine credentials that cannot use it.

Administrator rights are standing, so one stolen admin login reaches everything at once. Microsoft's 2025 report says attackers commonly exploit excess privileges and standing access [3].

Machine identities sit outside the review cycle. Access reviews ask managers to confirm what their people can reach. Service accounts and OAuth grants have no manager, so they are skipped [14][15].

Offboarding is a ticket. IT disables the main directory account, while local application accounts, SaaS logins outside single sign-on and API keys the person created survive.

The Framework: Five Doors

Every account in the business enters through one of five doors. Each door needs an owner, a control and a number the board can read. The model treats people and machines as the same problem: anything that can sign in is an identity.

Exhibit 1. One stolen login becomes many: the chain each door is meant to break



Source: author's model, drawn from the cases in this paper [9][11][13][14] and Microsoft's finding on follow-on credential theft [3].

Exhibit 2. The Five Doors: owner, control and board measure for each

Door	What it covers	Control	Board measure
1. Sign-in	Every staff and contractor login	Phishing-resistant MFA (security keys, passkeys, smart cards); block legacy sign-in protocols; ban text codes for staff [5][6]	Share of staff sign-ins using phishing-resistant methods
2. Privilege	Domain, cloud, SaaS and finance administrators	Separate admin accounts; time-limited elevation on approval; hardware keys only; break-glass accounts sealed and alarmed [3] [5]	Number of standing admin accounts; share of elevations that expired automatically
3. Machines	Service accounts, API keys, certificates, OAuth grants, AI agents	Inventory with a named owner each; a secrets vault; rotation schedules; least-privilege scopes; revoke unused grants [3] [14]	Machine identities with no owner; secrets older than the rotation limit
4. Recovery	Password resets, MFA re-enrollment, lost devices	No reset on caller-supplied facts alone; callback to the number on file plus manager approval; video check against the ID photo for admins; alert the user after every reset [6][8]	Resets per month; share verified by a second channel; reset-to-alert time
5. Lifecycle	Joiners, movers, leavers, contractors, test and legacy accounts	HR system triggers creation and removal; all apps behind single sign-on; leaver revocation includes tokens and keys; test tenants under production rules [13]	Median hours from leaving to full revocation; accounts with no sign-in in 90 days

Source: author's framework, built on CISA [5], NIST SP 800-63B-4 [6], CISA AA23-320A [8] and Microsoft [3].

Start sign-in work with administrators and the finance staff who release payments. Synced passkeys satisfy NIST's second assurance level, so most staff can use a phone or laptop they already have [6][7].

For machines, the first job is a list: what each credential reaches, who owns it, when it was last rotated and last used. Anything without an owner is disabled after notice. Anything holding "full" access to a SaaS platform is cut back to what it uses, as Google recommended after Drift [14].

For recovery, the help desk should never reset a password or move MFA on facts an attacker can research, such as an employee number or a manager's name. The notification NIST requires after every recovery gives a real employee the chance to report a reset they did not request [6]. Outsourced desks get the same procedure written into the contract, with call recordings and audit rights.

Costs, Risks, and Tradeoffs

Consider an illustration, the author's estimate. At an assumed $50 per hardware key and two keys per person, keys for 50 administrators cost $5,000, and for all 1,000 staff of a mid-size company $100,000. Most staff can use built-in passkeys instead. The larger costs are an identity governance tool, a secrets vault, help desk time per verified reset, and engineering time to move service accounts into the vault. Set those against the M&S direct costs of about £136 million and the Co-op's £80 million half-year profit hit [10][12].

Exhibit 3. Tradeoffs of making identity the primary control

Area	Cost or risk	Mitigation
Staff friction	New sign-in methods and slower resets annoy people; the help desk takes complaints	Roll out by risk tier; offer passkeys on existing devices; publish reset times
Help desk cost	Callbacks and manager approval add minutes to each reset	Self-service recovery with saved recovery codes, which NIST lists as an acceptable method [6]
Lockout	Strict recovery can lock out a real executive while traveling	Pre-registered backup keys; an emergency path that needs two people
Legacy systems	Old applications cannot use modern sign-in or single sign-on	Put them behind an identity-aware proxy, or isolate them with a dated retirement plan
Machine rotation	Rotating a key breaks an integration nobody documented	Rotate in a test window first; the inventory shows dependencies
Vendors	Outsourced help desks and SaaS integrations follow their own rules	Contract terms for reset procedures, token scopes and breach notice; review connected apps quarterly
When this is wrong	A small firm on a few SaaS tools with no internal admins, no developers and no help desk has little to inventory	Turn on phishing-resistant MFA everywhere, review connected apps twice a year, and spend the rest on backups and payment controls

Source: author's analysis; costs are the author's illustrative estimate.

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	Name one executive owner for identity. List every administrator account across directory, cloud, SaaS and finance systems. Issue hardware keys to administrators. Rewrite the help desk reset script, including the outsourced desk.	CEO names owner; CISO; head of IT service	Owner named; 100% of administrators on hardware keys; no reset or MFA change without a second-channel check
First 90 days	Block legacy sign-in protocols. Remove text-message MFA for staff. Inventory service accounts, API keys and OAuth grants with an owner for each. Disable test and legacy tenants or bring them under production policy.	CISO with IAM lead; CTO for machine identities	Zero accounts able to sign in without MFA; machine identity inventory complete with owners for 90%
First 90 days	Connect the HR system to account creation and removal. Revoke all access for leavers, including tokens and keys.	CHRO with head of IT	Median leaver revocation under 24 hours, measured weekly
First 365 days	Phishing-resistant sign-in for all staff. Time-limited administrator elevation. All secrets in a vault on rotation schedules. Quarterly review of connected apps and their scopes. Identity metrics in the board pack.	CISO, CTO, CFO for funding	95% of staff sign-ins phishing-resistant; zero standing domain administrators; no secret older than its rotation limit; quarterly board report

Source: author's recommendation, aligned to CISA [5] and NIST SP 800-63B-4 [6].

Questions to Ask Your Team

1. Who owns identity across HR, IT, the help desk and developers, and who reports on it to us?
2. What share of staff sign-ins use security keys or passkeys, and how many accounts can still sign in with a password alone?
3. How many people hold administrator rights right now, and how many of them are using those rights today?
4. If someone calls the help desk claiming to be our CFO with a new phone, what exactly happens, and does our outsourced desk follow the same script?
5. How many service accounts, API keys and connected apps do we have, and how many have no named owner?
6. Which third-party apps hold tokens into our email, CRM or file storage, and with what scope?
7. When someone left last month, how long did it take to remove every account and key they held?

8. Do any test, legacy or acquired environments sit outside our normal sign-in rules?

Closing

Attackers now get in by signing in, with a stolen password, a reset talked out of a help desk, or a token nobody remembered issuing. The 2025 retail attacks began that way. Make identity one program with one executive owner. Fund phishing-resistant sign-in, time-limited administrator access, an owned and rotated inventory of machine credentials, help desk resets that a caller cannot talk past, and same-day removal for leavers. Then put the five measures in front of the board every quarter.

Sources

[1] Verizon. "Verizon's 2025 Data Breach Investigations Report: Alarming surge in cyberattacks through third-parties." News release. 2025. https://www.verizon.com/about/news/2025-data-breach-investigations-report.

[2] Verizon. "2025 Data Breach Investigations Report: Executive Summary." 2025. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf.

[3] Microsoft. "Microsoft Digital Defense Report 2025." 2025. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/.

[4] Expert Insights. "97% Of Identity Attacks Involve Passwords, Says Microsoft." Coverage of the Microsoft Digital Defense Report 2025. 2025. https://expertinsights.com/news/97-of-identity-attacks-involve-passwords-says-microsoft.

[5] Cybersecurity and Infrastructure Security Agency. "Implementing Phishing-Resistant MFA." Fact sheet. 2022. https://cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[6] National Institute of Standards and Technology. "Digital Identity Guidelines: Authentication and Authenticator Management." NIST SP 800-63B-4. 2025. https://pages.nist.gov/800-63-4/sp800-63b.html.

[7] National Institute of Standards and Technology. "NIST SP 800-63 Digital Identity Guidelines." SP 800-63-4 overview. 2025. https://pages.nist.gov/800-63-4.

[8] Cybersecurity and Infrastructure Security Agency, FBI, and partners. "Scattered Spider." Cybersecurity Advisory AA23-320A, updated July 29, 2025. 2023, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a.

[9] BleepingComputer. "M&S confirms social engineering led to massive ransomware attack." Report on M&S evidence to the UK Business and Trade Sub-Committee. 2025. https://bleepingcomputer.com/news/security/mands-confirms-social-engineering-led-to-massive-ransomware-attack.

[10] The Register. "M&S pegs cyberattack cleanup costs at £136M as profits slump." Coverage of M&S half-year results. 2025. https://theregister.com/2025/11/05/ms_pegs_cyberattack_cleanup_costs/.

[11] BleepingComputer. "Co-op confirms data of 6.5 million members stolen in cyberattack." 2025. https://www.bleepingcomputer.com/news/security/co-op-confirms-data-of-65-million-members-stolen-in-cyberattack/.

[12] Retail Gazette. "Co-op reports £80m profit loss after April cyber-attack." Coverage of Co-op interim results. 2025. https://www.retailgazette.co.uk/blog/2025/09/co-op-interim-results/.

[13] Microsoft Threat Intelligence. "Midnight Blizzard: Guidance for responders on nation-state attack." Microsoft Security Blog. 2024. https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/.

[14] Google Threat Intelligence Group. "Widespread Data Theft Targets Salesforce Instances via Salesloft Drift." Google Cloud Blog. 2025. https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift.

[15] Security Affairs. "Internet Archive was breached twice in a month." 2024. https://securityaffairs.com/170068/data-breach/internet-archive-second-data-breach.html.

[16] Mandiant, Google Cloud. "UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion." Google Cloud Blog. 2024. https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion.

[17] TechCrunch. "Change Healthcare hackers broke in using stolen credentials and no MFA, says UHG CEO." Coverage of written testimony by UnitedHealth Group CEO Andrew Witty. 2024. https://techcrunch.com/2024/04/30/uhg-change-healthcare-ransomware-compromised-credentials-mfa.

[18] CyberArk. "Machine Identities Outnumber Humans by More Than 80 to 1: New Report Exposes the Exponential Threats of Fragmented Identity Security." Press release on the 2025 Identity Security Landscape, survey by Vanson Bourne. 2025. https://www.silicon.co.uk/press-release/machine-identities-outnumber-humans-by-more-than-80-to-1-new-report-exposes-the-exponential-threats-of-fragmented-identity-security.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.