

EXECUTIVE PAPER · INFRASTRUCTURE

Patch Debt and Shared Passwords Are Balance-Sheet Risk

The breaches that cost the most still begin with an unpatched system or a password nobody protected. CFOs and CEOs should carry these gaps as liabilities and fund their retirement on a schedule.

AUTHOR

Chris Watkins

SERVICE

Infrastructure

FOR

CFO, CEO · 11 min read

AT A GLANCE

The problem. Attackers now get in through known, already-exploited software flaws more often than any other way, and stolen passwords remain close behind. A single remote access portal without multifactor authentication cost one US company $3.09 billion in 2024. In both of the largest US breaches that year, the missing piece was a standard control.

Why it persists. Patching and access cleanup compete with feature work and look like overhead. Nobody puts a price on an unpatched server or a shared admin password, so the debt never appears in a budget review. Security reports describe activity, such as scans run and tickets closed, instead of exposure.

The recommendation. Carry five hygiene gaps as liabilities on a ledger the CFO reviews: known exploited vulnerabilities past deadline, external logins without MFA, shared or unrotated credentials, standing administrator access, and systems without audit logs. Give each an owner and a deadline, and report the balance every month until it reaches zero.

The Decision in Front of You

Every company carries security debt. Some servers run software with published flaws. Some vendor portals and admin consoles still accept a password alone. Some service accounts share one password that has not changed in years. The decision is whether that debt stays an engineering backlog item or becomes a liability with a value, an owner, and a payoff schedule.

The cost of leaving it alone is now well measured. IBM's 2026 Cost of a Data Breach study put the average breach at $4.99 million globally and $11.5 million in the United States, both records [1][2]. Breaches that took longer than 200 days to contain averaged $5.65 million, against $4.32 million for those contained sooner [2].

The two largest US breaches of 2024 did not require novel attacks. One entered through a remote access portal that lacked multifactor authentication, or MFA, the second check beyond a password. The other used passwords stolen years earlier from customers' own computers. Both were preventable with controls the victims already knew about.

What's Happening

Known flaws are now the most common way in

Verizon's 2026 Data Breach Investigations Report found that exploitation of software vulnerabilities was the initial access route in 31% of breaches, overtaking stolen credentials for the first time in the report's 19-year history [3]. A year earlier, the 2025 edition had put exploitation at 20%, a 34% jump

over the prior report, across 12,195 confirmed breaches [4]. Edge devices and VPNs, the gateways that connect a company to the internet, accounted for 22% of exploitation actions in the 2025 data, up from 3% the year before [4].

Patching is falling behind. In the 2025 report, only about 54% of edge device and VPN vulnerabilities were fully fixed during the year, with a median of 32 days to do so [4]. Coverage of the 2026 report says organizations patched roughly a quarter of their critical vulnerabilities, down from 38%, and the average time to patch grew from 32 to 43 days [5]. Even the best performers fixed only 30% to 40% of actively exploited flaws within the first week of detection [5].

The list of flaws known to be in active use is public. CISA, the US Cybersecurity and Infrastructure Security Agency, maintains the Known Exploited Vulnerabilities catalog, usually called KEV. It grew by 245 entries in 2025, up from 185 added in 2024, and closed the year at 1,484 [6]. At that size, matching every internet-facing system against it is a routine weekly task.

The federal government already set the standard

CISA issued Binding Operational Directive 22-01 on November 3, 2021 [7]. It requires federal agencies to fix KEV entries within two weeks, or within six months for older flaws assigned identifiers before 2021 [8]. The directive explains why: many flaws rated critical on paper are never exploited, so a list of flaws attackers actually use is a better guide to priority than severity scores [8]. The directive binds only federal agencies, but CISA encourages every organization to use the catalog to set patching priorities [8].

Stolen passwords and weak sign-in fill the rest

Third parties are now in the path of half of all breaches. Verizon's 2026 report found a third party involved in 48% of breaches, up 60% from the prior period [3]. The 2025 report had already doubled that figure, from 15% to 30% [4].

Credential theft has become industrial. Infostealers, malware that copies saved passwords from a browser, are a major supply. In Verizon's 2025 data, 46% of infected systems holding corporate logins were unmanaged personal devices, and 54% of ransomware victims studied had their domains appear in credential dumps [4].

MFA is the standard defense against stolen passwords. A Microsoft study of Azure Active Directory accounts found MFA cut the risk of compromise by 99.22% overall and by 98.56% for accounts whose credentials had already leaked [9].

Two Cases from 2024

Change Healthcare. On February 12, 2024, attackers used stolen credentials to log in to a Change Healthcare Citrix remote access portal. The portal did not require MFA [10]. Nine days later they deployed ransomware [10]. UnitedHealth Group, the parent, paid a $22 million ransom [10]. Its CEO,

Andrew Witty, told the House Energy and Commerce Committee on May 1, 2024, that "this particular server did not have MFA installed" [11].

The cost was historic. UnitedHealth reported a total 2024 impact of $3.09 billion and advanced $9.03 billion in loans to affected providers [12]. In August 2025 the company confirmed that about 192.7 million people had data exposed [13]. Senator Ron Wyden told Witty the attack could have been stopped with basic security measures [11].

Snowflake customers. Starting no later than April 14, 2024, a group Mandiant tracks as UNC5537 logged in to customer accounts on the Snowflake cloud data platform. Mandiant and Snowflake notified about 165 potentially exposed organizations [14]. At least 79.7% of the accounts the attackers used had credentials exposed earlier, most through infostealer infections on computers Snowflake did not own, some dating back to 2020 [14]. The affected accounts did not require MFA, many credentials had gone unrotated for up to four years, and customers had not limited logins to trusted networks [14].

AT&T was among those hit. Its July 2024 SEC filing disclosed that call and text records for nearly all of its mobile customers, about 110 million people, were taken from its workspace on a third-party cloud platform between April 14 and April 25, 2024 [15].

Exhibit 1. Both 2024 breaches turned on a basic control that was missing

Case	Way in	Missing control	Known cost or scale
Change Healthcare, February 2024	Stolen credentials on a remote access portal	MFA on an internet-facing login	$3.09B 2024 impact; $22M ransom; about 192.7M people affected
Snowflake customers, April 2024	Infostealer-harvested passwords, some years old	MFA; credential rotation; network allow lists	About 165 organizations notified; AT&T records for about 110M customers

Source: The Register [10], HC Innovation Group [11], Becker's [12], Business Insurance [13], Mandiant via TechTarget [14], Security Affairs coverage of AT&T SEC filing [15].

Why the Usual Approach Fails

Security hygiene is usually funded as operating expense and measured as activity. A monthly report says how many scans ran and how many patches shipped. It rarely says how many internet-facing systems still carry a flaw on the KEV list, or how many logins still accept a password alone. Leadership sees effort and cannot see exposure.

Patching competes with revenue work. Every patch needs testing, a maintenance window, and someone to apply it. Teams defer the ones that look risky to deploy, which often means the edge devices and legacy servers attackers target most. The 2026 Verizon data shows that backlog growing [5].

Exceptions outlive their reasons. Change Healthcare's breach turned on one server without MFA [11]. Most large organizations have a similar list: a vendor portal, a legacy app that cannot take MFA, a break-glass account. Each exception was approved once and never reviewed.

Shared and standing credentials hide in automation. Service accounts, API keys, and database passwords often live in scripts and configuration files, shared by several people and never rotated. The Snowflake victims were compromised with passwords up to four years old [14]. Standing administrator rights compound the damage, because any stolen admin login reaches everything at once.

Audit trails are left off to save money or effort. Without logs of who signed in and what they touched, a company cannot say what was taken, which lengthens containment and raises the bill. IBM's data ties longer breach lifecycles to higher cost [2].

The Framework: The Hygiene Ledger

Finance already knows how to manage a liability: measure it, assign it, schedule its retirement, and review the balance. The Hygiene Ledger applies that discipline to the five gaps behind most costly breaches.

Exhibit 2. The Hygiene Ledger: five liabilities, each with a balance and a target

Liability	How to count the balance	Target	Evidence for the board
Known exploited vulnerabilities past deadline	Systems with a KEV entry unpatched beyond 14 days, internet-facing first	Zero past deadline	Weekly scan matched against the KEV catalog [6][8]
Logins without MFA	Internet-facing applications, remote access, vendor portals, and cloud consoles that accept a password alone	Zero, with phishing-resistant MFA for administrators	Identity provider report; list of approved exceptions with expiry dates
Shared or unrotated credentials	Passwords and keys used by more than one person, or older than policy allows	All secrets in a vault, rotated on schedule	Vault inventory; age report for every secret
Standing administrator access	Accounts with permanent admin rights	Admin rights granted per task, with expiry	Monthly access review signed by system owners
Systems without audit trails	Critical systems not sending sign-in and data-access logs to central storage	Every critical system logging, retained at least one year	Log coverage report

Source: author's framework. Targets draw on CISA BOD 22-01 timelines [8] and the controls missing in the 2024 cases [10][14].

Each row produces a single count, and that count is the liability balance. The CFO reviews the five balances monthly, the same way finance reviews aged receivables, and asks why any balance grew.

Exceptions are allowed and priced. A system that cannot take MFA gets a named owner, a compensating control such as a network restriction, and an expiry date. An exception without an expiry counts as an open liability.

What the ledger is worth

The following is the author's illustrative estimate for a hypothetical mid-size US company. Assume a hygiene program costs $500,000 a year in staff time and tooling, and use IBM's 2026 US average breach cost of $11.5 million [1]. The program pays for itself if it lowers the annual probability of a breach by about 4.3 percentage points ($500,000 divided by $11.5 million). Given that MFA alone cut account compromise risk by more than 99% in Microsoft's data [9], and that the two largest 2024 breaches each turned on a single missing control, that threshold is modest. Real breach costs vary widely by industry and size, and the probability reduction cannot be measured precisely.

Costs, Risks, and Tradeoffs

Exhibit 3. The ledger has real costs and does not fit every company

Area	Cost or risk	Mitigation
Patch disruption	Fast patching occasionally breaks an application or forces an outage	Test KEV patches on a small group first; keep a short, documented emergency window
Legacy systems	Some older systems cannot be patched or cannot take MFA	Isolate them behind a gateway that enforces MFA; set a retirement date
User friction	MFA prompts and per-task admin rights slow people down	Use phishing-resistant methods with fewer prompts; grant admin access quickly through an approval workflow
Tool spend	Vaults, identity tools, and log storage add licensing and storage cost	Start with internet-facing systems and administrators; size log retention to legal need
Vendor dependence	Third parties involved in about half of breaches sit outside your direct control [3]	Require MFA, logging, and patch timelines in contracts; review vendor access quarterly
False comfort	A ledger at zero can miss new systems nobody inventoried	Reconcile the ledger against the asset inventory monthly
When this is wrong	A small firm with no servers of its own, running entirely on SaaS, has little to patch and few secrets to vault	Enforce MFA on every SaaS account, use a password manager, and rely on vendor patching and contracts

Source: author's analysis, with references as cited.

How to Act

Exhibit 4. A one-year roadmap to retire hygiene debt

Window	Actions	Owner	Milestone
First 30 days	Match every internet-facing system against the KEV catalog. List every login that accepts a password alone.	CISO or security lead	Opening balances for all five ledger lines reported to the CFO
First 30 days	Turn on MFA for remote access, cloud consoles, and every administrator account.	IT operations lead	Zero internet-facing remote access without MFA
First 90 days	Patch all internet-facing KEV entries and adopt a 14-day KEV deadline. Move shared passwords and keys into a vault and rotate them.	Infrastructure lead with application owners	Zero internet-facing KEV entries past deadline; shared secrets in the vault
First 90 days	Add MFA, logging, and patch timeline clauses to contracts with vendors who hold access.	General counsel with procurement	Top 20 vendors reviewed; renewal terms drafted
First 365 days	Replace standing admin rights with time-limited access. Send sign-in and data-access logs from every critical system to central storage.	CISO with CTO	Under 5% of admins hold standing rights; 100% of critical systems logging
First 365 days	Report all five balances to the board audit or risk committee each quarter.	CFO with CISO	Four quarterly reports delivered; every exception carries an expiry date

Source: author's recommendation. The 14-day deadline follows CISA BOD 22-01 [8].

Questions to Ask Your Team

1. How many of our internet-facing systems have a flaw on CISA's KEV list right now, and for how long?
2. Which logins still accept a password alone, including vendor portals and remote access?
3. How many credentials are shared between people or service accounts, and when were they last changed?
4. Who holds permanent administrator rights, and why?
5. If we were breached tonight, could we tell from logs what was accessed?
6. Which approved security exceptions have no expiry date?

7. What do our contracts require of vendors who can reach our data?

Closing

Change Healthcare and the Snowflake victims had the controls they needed within reach, and the gap cost billions [12][15]. Unpatched known flaws and unprotected passwords are liabilities with a measurable balance. Put the five on a ledger the CFO reviews, give each an owner and a deadline, and fund their retirement before an attacker collects on them.

Sources

[1] IBM. "IBM Study: One in Four Malicious Breaches are AI-Enabled, Costing Companies $6 Million on Average." Press release, Cost of a Data Breach Report 2026. 2026. https://www.placera.se/telegram/avanza/39_5f4ce762-b6a2-495d-b2cc-d9d94dc4560d.html.

[2] Baker Donelson. "Ten Takeaways from IBM's 2026 Cost of a Data Breach Report." 2026. https://www.bakerdonelson.com/ten-takeaways-from-ibms-2026-cost-of-a-data-breach-report.

[3] Health Care Innovation (HC Innovation Group). "AI-Driven Vulnerability Exploitation Now Leading Cause of Data Breaches, Verizon Report Finds." Coverage of the Verizon 2026 Data Breach Investigations Report. 2026. https://www.hcinnovationgroup.com/cybersecurity/news/55379376/ai-driven-vulnerability-exploitation-now-leading-cause-of-data-breaches-verizon-report-finds.

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

[5] BankInfoSecurity. "Verizon Breach Report: Vulnerability Exploitation Surges." Coverage of the Verizon 2026 Data Breach Investigations Report. 2026. https://www.bankinfosecurity.net/verizon-breach-report-vulnerability-exploitation-surges-a-31719.

[6] SecurityWeek. "CISA KEV Catalog Expanded 20% in 2025, Topping 1,480 Entries." 2025. https://www.securityweek.com/cisa-kev-catalog-expanded-20-in-2025-topping-1480-entries/.

[7] Cybersecurity and Infrastructure Security Agency. "CISA Issues BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities." Alert. 2021. https://cisa.gov/news-events/alerts/2021/11/03/cisa-issues-bod-22-01-reducing-significant-risk-known-exploited.

[8] Cybersecurity and Infrastructure Security Agency. "BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities." Binding Operational Directive 22-01. 2021. https://cisa.gov/binding-operational-directive-22-01.

[9] Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., and Lavista Ferres, J. "How effective is multifactor authentication at deterring cyberattacks?" Microsoft. arXiv:2305.00945. 2023. https://arxiv.org/abs/2305.00945.

[10] The Register. Coverage of UnitedHealth CEO testimony on the Change Healthcare ransomware attack. 2024. https://www.theregister.com/2024/04/30/unitedhealth_ceo_ransom/.

[11] Health Care Innovation (HC Innovation Group). "UnitedHealth CEO Testifies on Cyberattack Before Senate." Report on the May 1, 2024 House Energy and Commerce hearing. 2024. https://www.hcinnovationgroup.com/cybersecurity/news/55036427/unitedhealth-ceo-testifies-on-cyberattack-before-senate.

[12] Becker's Hospital Review. "The financial toll of the Change Healthcare hack: 7 numbers." 2025. https://www.beckershospitalreview.com/cybersecurity/the-financial-toll-of-the-change-healthcare-hack-7-numbers.html.

[13] Business Insurance. "Hack at UnitedHealth's tech unit impacted 192.7 million, US website shows." 2025. https://www.businessinsurance.com/hack-at-unitedhealths-tech-unit-impacted-192-7-million-us-website-shows/.

[14] TechTarget. "Mandiant: 'Exposed credentials' led to Snowflake attacks." Coverage of Mandiant's UNC5537 investigation. 2024. https://www.techtarget.com/cybersecurity/news/366588655/Mandiant-Exposed-credentials-led-to-Snowflake-attacks.

[15] Security Affairs. "AT&T disclosed a new data breach." Coverage of AT&T Form 8-K. 2024. https://securityaffairs.com/165658/uncategorized/att-disclosed-a-new-data-breach.html.

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.