resilience

CYBERSECURITY AND THE PUBLIC SECTOR

Third-party risk in the public sector

How claims in the public sector create pockets of loss around shared vendors.

resilience

Third-party risk in the public sector

Public entities file fewer claims per account than our other clients, according to Resilience claims data from 2022 through 2026. Their claims come in clusters, each around an incident at a vendor many of them share.

Executive summary

According to Resilience claims data, public entities in our portfolio filed fewer claims per account than our other clients, but they filed them in clusters, and each cluster we identified traces to a single vendor incident. From February 2022 through September 2026, third-party vendors were the leading source of these clients' claims. According to the Resilience Risk Operations Center (ROC), three compromises at widely used vendors account for nearly nine in 10 of the portfolio's claims with an identified threat actor: MOVEit in 2023,[1] Change Healthcare in 2024,[2] and Canvas in 2026.[3]

Vendor incidents and insider error together make up more than half of these claims (58%). Both involve access the public entity grants, to a vendor or to its own staff, and the entity can limit that access through contracts and account settings it already controls.

Key findings

41%	of public entity claims began at a third-party vendor, the leading cause of loss
About half	of claims with an identified entry point started in a vendor's systems
Nearly 9 in 10	claims with an identified threat actor trace to three vendor compromises: MOVEit, Change Healthcare, and Canvas
4 in 10	public entity claims in 2023 came from the MOVEit campaign alone

Source: Resilience internal claims data for public entity clients, dates of loss February 2022 through September 2026; threat actor figures from the Resilience Risk Operations Center.

Scope note

These findings reflect public entity clients in the Resilience portfolio: government entities, school districts, universities, special districts, and similar public-sector organizations, which we identified by matching organization names and web domains against public-sector naming conventions. The figures come from Resilience's internal, unpublished claims and account records. The data covers dates of loss from February 2022 through September 2026, and we pulled it October 5, 2026. These findings describe this population only.

Public entity claims come in clusters

Four incidents relating to discreet vendors each produced a cluster of public entity claims in our data. MOVEit claims made up four in ten public entity claims in 2023.[1] In 2024 the Change Healthcare attack and the CrowdStrike outage together account for 23% of the year's claims.[2,4] So far in 2026, the Canvas compromise, an attack on the learning management system from Instructure used by schools, accounts for nearly one in five.[3]

Three of those four incidents were attacks by known threat groups. According to the ROC, about one in five public entity claims in our portfolio (21%) have an identified threat actor, and nearly nine in ten of those come from the three groups behind these incidents. Cl0p, the group behind the MOVEit campaign that the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI documented in June 2023,[1] appears on 40% of them. BlackCat appears on 19%. UnitedHealth Group's then-CEO told the Senate Finance Committee in May 2024 that a group calling itself ALPHV or BlackCat carried out the ransomware attack inside Change Healthcare.[2] ShinyHunters appears on 30%. The FBI says ShinyHunters claimed the spring 2026 attack on a learning management system that interrupted service to schools across the country,[5] and we match those claims to the Canvas incident by event code and claim narrative; neither the FBI notice nor Instructure's incident page names the other.[3] The fourth incident, the CrowdStrike outage, came from a faulty software update CrowdStrike released, so those claims have no threat actor.

Three vendor attacks account for nearly nine in 10 claims with an identified threat actor

Share of claims with an identified threat actor, by incident and the group behind it



Source: Resilience internal claims data for public entity clients, dates of loss February 2022 through September 2026; threat actor figures from the Resilience Risk Operations Center.

The clusters stand out because public entities otherwise file claims less often than the rest of our portfolio. Pooled across 2022 through 2025, they filed 24 claims per 100 accounts a year against 32 for everyone else, and they matched the rest of the portfolio only in 2023, the MOVEit year. We can't tie their low 2025 rate (15 against 31) to any single event.

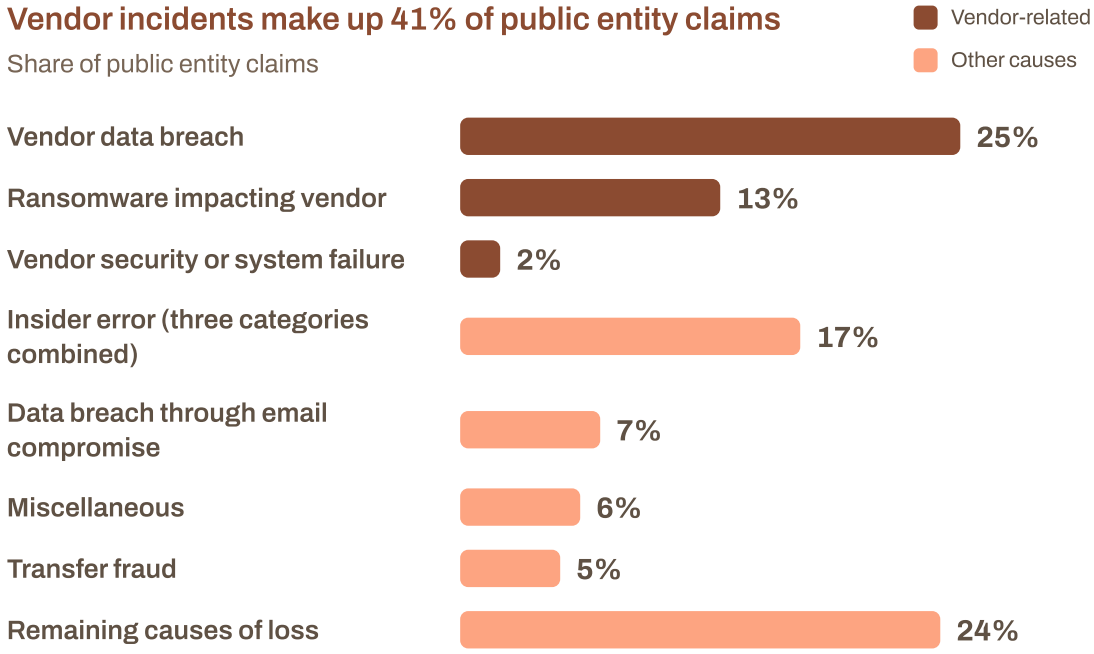
The spikes coincide with compromises at vendors many public entities share. The Information Technology and Innovation Foundation's 2026 report Improving State and Local Government Cybersecurity found that state and local governments are short on security staff and run aging systems, and that they compensate by outsourcing work like cloud hosting and threat monitoring to vendors.[6] It separately names concentration risk, meaning many organizations depend on the same software and one flaw affects many of them at once, and uses MOVEit as the example.[6]

Vendors are the leading cause of claims

Vendor incidents make up 41% of public entity claims, 24 points more than insider error, the next largest cause. Vendor incidents combine four claim categories: vendor data breach, ransomware impacting vendor, vendor security failure, and vendor system failure. Each share is of public entity claims with dates of loss from February 2022 through September 2026. Investigators identified the entry point in 85% of public entity claims, and in about half of those (49%) the entry point was a vendor's systems. Phishing came second at 13%.

Vendor incidents make up 41% of public entity claims

Share of public entity claims



Shares of the public entity claims with dates of loss from February 2022 through September 2026, rounded to whole numbers. Totals are computed from unrounded shares: the vendor rows total 41% and the column 100%, while the rounded figures shown sum to 40% and 99%.

The vendor share splits into two different exposures. A quarter of all public entity claims (25%) began with a breach at a vendor holding the entity's data, which leaves the entity answering for records it no longer controlled. Another 15% began when attackers deployed ransomware on a vendor's systems or those systems failed, which can take down a service the entity depends on.

Insider error is the second-largest cause, at 17%, about one in six claims. We count three claim categories as insider error: insider error data breach and its intentional and mismailing variants. So the 17% combines employees' honest mistakes with deliberate misuse of access, and it measures how often a claim started with one of the entity's own people, whatever they intended. The next largest causes are data breaches through email compromise (7%), miscellaneous causes (6%), and transfer fraud (5%).

Resilience recommends two changes

Each of the two largest causes maps to a moment a public entity already schedules: contract renewal for vendors, and role changes for staff. The recommendations that follow are Resilience's, based on the patterns in our public entity claims data.

Recheck vendors at renewal

Start by listing which vendors hold your residents' or students' data and which connect directly into your network, since those are the two kinds of vendor exposure in our claims data. Ask each of them at renewal what you asked at procurement: how quickly they patch internet-facing software, and how soon they'll tell you about a breach. The same ITIF report found that many public-sector technology contracts lack enforceable security requirements and carry few consequences for undisclosed vulnerabilities or slow patching, and that smaller agencies can't easily demand better terms on their own. It recommends joint procurement agreements to give them more bargaining power.[6]

Plan separately for shared platforms, since compromises at those vendors produced the clusters in our data. Write down now what you'd do the day a platform vendor announces a breach: who decides whether to cut the connection, and who notifies the people whose records it held.

> Write down now what you'd do the day a platform vendor announces a breach: who decides whether to cut the connection, and who notifies the people whose records it held.

Remove staff access when roles change

Two controls apply to each of the three insider error categories in our data: give each account only the access its role needs, and remove access the same day someone changes roles or leaves. Mismailing also calls for a second review before records go out in bulk.

Methodology

Population. This analysis covers claims from public entity clients in the Resilience portfolio. Public entities were identified by matching organization names and web domains against public-sector naming conventions, such as city, county, school district, authority, and .gov or .k12 domains. Name and domain matching is an imperfect filter. It can miss public entities whose names follow none of these conventions, and it can include a small number of private organizations whose names match one. No matched organizations were removed from the population. The population includes public hospital and health care systems whose names or domains match these conventions.

The analysis covers claims with dates of loss from January 2022 through September 2026, drawn from Resilience internal claims and account records on October 5, 2026, using a date-of-loss cutoff of that day. Claims were included only where the associated account record shows bound or issued status. Each claim is counted once.

Categories and shares. Cause-of-loss shares are each category's share of the public entity claims in the population. Vendor incidents combine four claim categories: vendor data breach, ransomware impacting vendor, vendor security failure, and vendor system failure. We count three claim categories as insider error: insider error data breach and its intentional and mismailing variants. Two rows in the cause-of-loss table were derived by subtraction: vendor security or system failure (the vendor total minus vendor data breach and ransomware impacting vendor) and remaining causes of loss (the full population minus each listed category). The 58% figure for vendor incidents and insider error together adds those two categories. Shares of a year's claims tied to a specific incident identify those claims by their event code and claim narrative.

Entry-point shares are shares of the 85% of claims whose files record a point of failure. Claims with that field blank or holding a placeholder value were excluded from that base. Threat actor shares are shares of the 21% of claims with an identified threat actor, and the attribution percentages come from the Resilience Risk Operations Center. Records that spell ShinyHunters as one word or as two were merged.

Claim rate. Claims per 100 accounts for each year from 2022 through 2025 equals the claims with a date of loss in that year, divided by the number of distinct accounts whose records show bound status for any part of that year, multiplied by 100. Each account counts once per year regardless of how many months its record shows that status, and an account's bound status is assumed to persist after the record's end date. The multi-year figure divides total claims across 2022 through 2025 by the sum of the four annual account counts. 2026 is excluded from rate calculations because the year is incomplete.

Precision and confidence. Shares and rates are rounded to whole numbers, and differences between shares are expressed as percentage-point gaps, because the public entity populations in this analysis are small enough that finer precision would overstate it. Shares for individual causes of loss other than vendor data breach, for individual threat actors, and for phishing as an entry point, along with the 2022 public entity claim rate, rest on small numbers of claims and should be read as directional. Combined figures, such as the vendor total, are computed from unrounded shares and can differ from the sum of the rounded rows. Counts can shift slightly between data pulls as claims with earlier dates of loss are entered or recategorized; two pulls against the same cutoff differed by less than 2%.

Exclusions. Loss severity was not analyzed for this population. Claims from account records without bound or issued status and claims with dates of loss after October 5, 2026, were excluded.

Endnotes

1. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability," Joint Cybersecurity Advisory AA23-158A, June 7, 2023, updated June 16, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

2. Andrew Witty, then Chief Executive Officer, UnitedHealth Group, testimony before the U.S. Senate Committee on Finance, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," May 1, 2024, https://www.finance.senate.gov/imo/media/doc/0501_witty_testimony.pdf.

3. Instructure, "Security Incident Update & FAQs," last updated September 29, 2026, https://www.instructure.com/incident_update.

4. CrowdStrike, "Channel File 291 Incident: Root Cause Analysis Is Available," August 6, 2024, https://www.crowdstrike.com/blog/channel-file-291-rca-available/.

5. Federal Bureau of Investigation, Internet Crime Complaint Center, "ShinyHunters: Cyber Criminal Group Attacks Learning Management System," Public Service Announcement I-051526-PSA, May 15, 2026, https://www.ic3.gov/PSA/2026/PSA260515.

6. David Kertai, "Improving State and Local Government Cybersecurity," Information Technology and Innovation Foundation, May 2026 (web release April 27, 2026), https://www2.itif.org/2026-state-local-cybersecurity.pdf.

This material is provided for informational purposes only. Accordingly, this material should not be viewed as a substitute for guidance and recommendations of a trained professional. Additionally, Arceo Labs, Inc. d/b/a Resilience does not endorse any coverage, systems, processes, or protocols addressed herein. Any references to non-Resilience websites are provided solely for convenience, and Resilience disclaims any responsibility with respect to such websites. To the extent that this material contains any examples, please note that they are for illustrative purposes only. Additionally, examples are not intended to establish any standard of care, to serve as legal advice appropriate for any factual situation, or to provide an acknowledgment that any factual situation is covered by Resilience products. This material is not intended as a solicitation of insurance coverage. Arceo Labs, Inc. d/b/a Resilience, 55 2nd St Suite 1950, San Francisco, CA 94105. All Rights Reserved.

The purchase of insurance coverage is in no way tied to the purchase of security services. Resilience's software solutions, including Arc and Edge, are offered separately from any insurance product and their use does not imply or guarantee insurance coverage, terms, or eligibility.

In the United States, insurance products are distributed by Ocrea Risk Services, LLC (NPN 19169260) d/b/a Resilience Cyber Insurance Solutions. Resilience products are underwritten by Homeland Insurance Company of New York or Homeland Insurance Company of Delaware. Both are subsidiaries of Intact Insurance Group USA LLC. Their principal place of business is at 605 Highway 169 N, Plymouth, Minnesota 55441. Arceo Labs, Inc. d/b/a Resilience provides security services through its expert security team. [LEGAL: confirm the current underwriter, since section 9.1 names Accredited and the approved US disclaimers name Homeland; add the California NAIC number.]