resilience

WHITEPAPER

The Vendor Problem in Public Sector Cyber

The Vendor Problem in Public Sector Cyber

What Resilience claims data reveals about where government entities are getting hit — and why it keeps happening

Executive summary

Among public entity policyholders in the Resilience portfolio, third-party vendors are both the leading cause of claims and the most common documented point of entry. Vendor-related incidents — data breaches and ransomware attacks originating from third-party systems — account for roughly four in ten claims. Among claims where the entry method is known, vendor systems account for more than half of all documented failure points. Two of the three most prevalent named threat actors in this dataset — Cl0p and ShinyHunters — achieved their reach by exploiting shared platforms used widely across the public sector, including by educational institutions.

That double signal runs through everything that follows. Insider error adds a second structural layer, appearing in roughly one in six claims.

2024 was a full calendar year and the cleanest single-year baseline — claim volume grew 26% from 2023. The underlying trend has not reverted. 2025 figures are preliminary and will rise as claims are reported and adjudicated.

The data points to two places where the risk is manageable: vendor relationships and internal access controls. Neither is a perimeter problem. Both require decisions that get made before the incident response team picks up the phone.

SCOPE NOTE

All findings in this report reflect public entity policyholders in the Resilience cyber insurance portfolio — government entities, school districts, universities, special districts, and similar public-sector organizations identified through name and domain pattern matching. Findings should not be generalized to private-sector organizations or the broader cyber market. The dataset covers loss dates from January 2022 through May 2026.

The public sector's unusual exposure

Public entities are not typical cyber insurance policyholders. A county government, a transit authority, a school district, and a public university share a common challenge: they carry significant digital infrastructure and often sensitive personal data, but they operate under budget constraints, procurement rules, and staffing realities that most private-sector organizations don't face.

Dedicated security personnel in the public sector are scarce. Procurement decisions prioritize cost and compliance over security posture. And shared vendor platforms — the same payroll system, the same student information system, the same file transfer tool — run across hundreds of entities at once, which means a single vulnerability can become a portfolio-wide event overnight.

The Resilience public entity portfolio spans counties, cities and municipalities, transit and water and housing authorities, school districts, public colleges and universities, and government agencies. Counties represent the largest single category by claims volume, followed by cities and municipalities, special district authorities, and school districts.

Cause of loss and point of entry data are strong across this population, providing a clear picture of how cyber claims develop in the public sector. This report focuses on that pattern data rather than financial severity figures, which are not reported consistently enough across this population to analyze.

Where the claims come from

Vendor data breaches account for roughly one in four claims — the single largest cause of loss in the dataset. Ransomware attacks originating from vendor systems add another one in seven, bringing the combined vendor share to roughly four in ten claims overall.

THE VENDOR HEADLINE

Vendor-related incidents — including data breaches and ransomware attacks originating from third-party systems — account for roughly four in ten claims among public entity policyholders in the Resilience portfolio.

Insider error appears in approximately one in six claims — spanning accidental data disclosure, unauthorized access, and similar events. Whether the driver is process gaps, access control failures, or deliberate wrongdoing, the control response is the same: limit what any account can reach, and revoke access promptly when someone leaves. Whether training deficits contribute is a question the pattern data alone can't fully resolve, though it's a reasonable inference given the staffing environment described above.

Other cleared causes of loss — data breach via email compromise and transfer fraud — each account for a small but meaningful share of claims. Both carry appropriate sample-size caveats and are addressed in the methodology note.

Cause of loss	Share of Claims
Vendor data breach	~24% (roughly 1:4)
Ransomware impacting vendor	~15% (more than 1:7)
Insider error (combined variants)	~16% (approximately 1:6)
Data breach — email compromise	~8%*
Transfer fraud	~6%*
Miscellaneous	~7%

** Small sample — interpret with caution. See methodology note.*

How attackers get in

The vendor signal doesn't stop at cause of loss. It runs straight through to entry point as well.

Among claims where the point of entry is documented — approximately four in five claims in this dataset — vendor systems account for more than half of all documented failure points. That's nearly four times the next most common entry method.

THE DOUBLE SIGNAL

In the Resilience public entity portfolio, third-party vendors are both the leading cause of claims and the most common point of entry — appearing in more than half of all documented failure points.

Phishing accounts for roughly one in seven documented entry points, noted with appropriate sample-size context.

The practical implication is that traditional perimeter defenses don't address the primary failure mode here. The risk runs through contractual relationships, shared platforms, and vendor security posture — not just the public entity's own internal controls. You can patch your own systems and still be fully exposed through a vendor that has not patched theirs.

REQUIRED FRAMING

Point of failure figures are scoped to claims where the entry method is documented. The entry method is known for approximately four in five claims in this dataset. All POF percentages are shares of that documented subset.

Who's behind the attributed claims

Named threat actor attribution requires forensic investigation, and it isn't available for most incidents in this dataset. Roughly one in four claims carries named attribution. All percentages in this section are shares of that attributed subset — not of all public entity claims.

Among claims with named threat actor attribution, Cl0p accounts for roughly four in ten. That share is driven almost entirely by the 2023 MOVEit campaign. MOVEit is a file transfer tool used widely across public sector organizations; the Cl0p group exploited a vulnerability in it and hit dozens of public entities at once. It was a coordinated mass-exploitation event, not an indicator of sustained Cl0p activity targeting the public sector.

ShinyHunters accounts for roughly three in ten attributed claims. The pattern is similarly event-driven, linked to the Canvas breach — a credential exposure campaign that affected educational institutions relying on the platform. ShinyHunters is known for large-scale credential theft and data extortion, including a May 2026 attack targeting education and government databases.

BlackCat accounts for roughly two in ten attributed claims, noted with appropriate sample-size context.

HOW TO READ THE ACTOR DATA

Both Cl0p and ShinyHunters appear at high concentrations because each exploited a single widely used platform — MOVEit and Canvas respectively — that many public entities relied on simultaneously. These are event-driven spikes. They are not indicators of ongoing threat prevalence from either group.

Both dominant named actors in this dataset achieved their reach by exploiting shared platforms — MOVEit across government and higher education, Canvas specifically within educational public entities. Neither campaign required targeting individual organizations. The sector's reliance on common platforms means a single exploit can generate a wave of claims across unrelated entities simultaneously.

Where the leverage is

Both primary failure modes in the public entity portfolio run through relationships and access decisions rather than perimeter defenses.

Third-party vendor risk

Vendor relationships are the dominant risk surface in this dataset — roughly four in ten claims by cause, more than half of documented entry points. The practical response goes beyond vendor contracts. It means treating vendor security posture as an ongoing operational question: which vendors have access to sensitive systems, what their security practices look like, and whether that posture is reviewed at renewal rather than just at procurement.

For public entities, that's harder than it sounds. Procurement rules constrain vendor selection. Budget constraints limit the resources available for vendor audits. Shared platforms are often mandated at the state or district level. None of that changes the risk profile, but it does shape what a realistic mitigation program looks like for this population — and it's why the sector's vendor exposure persists even as awareness of third-party risk has grown across the broader market.

Insider error and access controls

Insider error spans a wide range — accidental data disclosure, unauthorized access, off-boarding failures, over-permissioned accounts — and the right response depends on which variant is driving it. Process and access control gaps call for different fixes than deliberate wrongdoing does. The data doesn't break out that distinction, but both are addressed by the same foundational control: limit what any account can reach, and revoke access promptly when someone leaves.

Methodology

All findings in this report reflect public entity policyholders in the Resilience cyber insurance portfolio. Public entities were identified through name and domain pattern matching — not industry classification tags. The population includes municipalities, counties, school districts, public colleges and universities, transit and water and housing authorities, and similar government and quasi-government organizations.

The dataset covers loss dates from January 2022 through May 2026. 2025 data is partial through the May 2026 run date and will increase as incidents are reported and adjudicated — 2025 figures in this report are noted accordingly.

Cause of loss percentages are each category's share of the full deduplicated claims population in this dataset. Point of failure percentages are shares of the subset of claims where entry method is documented — approximately four in five claims carry this information. Threat actor attribution percentages are shares of the subset of claims with named forensic attribution — approximately one in four claims in this dataset.

All findings are scoped to this population. They should not be generalized to private-sector organizations or read as representative of the broader cyber insurance market.

Notes

1. Resilience public entity claims data, January 2022–May 2026. Data sourced from Resilience's internal claims and policyholder records. Public entities identified by name and domain pattern matching.

2. Cause of loss and point of failure categorizations follow Resilience internal taxonomy. The 'vendor' cause-of-loss figure combines four vendor-related categories: vendor data breach, ransomware impacting vendor, vendor security failure, and vendor system failure.

3. The 2023 Cl0p/MOVEit campaign: Progress Software disclosed a critical vulnerability in MOVEit Transfer in May 2023. The Cl0p ransomware group exploited the vulnerability in a coordinated campaign targeting organizations across multiple sectors including government and education.

4. ShinyHunters is a threat actor group known for large-scale credential theft and data extortion. The Canvas breach referenced in this report refers to a credential exposure event affecting institutions using the Canvas learning management platform.