Professional Services

NAICS 54 · Legal Services (5411), Accounting, Consulting, Architecture, Engineering & Technical Services

A SecurIT360 executive industry summary: our independent reading of what the latest publicly available breach data means for Professional Services firms.

At a glance. Professional Services recorded the second-highest number of confirmed breaches of any industry in the Verizon 2026 Data Breach Investigations Report (2,558), trailing only Manufacturing's 2,713.

Excluding the large "Unknown" category (2,998 of the 22,625 total breaches, some of which are likely unclassified Professional Services firms), the sector accounts for roughly 13% of all breaches with an identified industry (2,558 of 19,627).

Tellingly, the report devotes its own write-up to six industries (Educational Services, Financial and Insurance, Healthcare, Manufacturing, Public Administration, and Retail) but not to Professional Services. This SecurIT360 summary fills that gap.

The picture the data paints is consistent: attacks on this sector are overwhelmingly external, financially motivated, and aimed squarely at credentials and internal business data.

Frequency	3,578 incidents, **2,558** with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering, and Basic Web Application Attacks represent **91%** of breaches
Threat actors	External **97%**, Internal 3% (breaches)
Actor motives	Financial **96%**, Espionage 5% (breaches)
Data compromised	Internal **80%**, Credentials 31%, Personal 14% (breaches)

All figures are drawn from publicly available data published in the Verizon 2026 Data Breach Investigations Report (incident window Nov 1, 2024 – Oct 31, 2025). This is an independent SecurIT360 executive industry summary modeled on the report's published industry write-ups; it is not affiliated with or endorsed by Verizon.

WHY THIS MATTERS

Professional Services firms hold their clients' most sensitive material (legal strategy, financial records, intellectual property, deal terms) while typically running leaner security programs than the enterprises they advise. That makes the sector an efficient, high-yield target: compromise one firm and you often reach many of its clients at once.

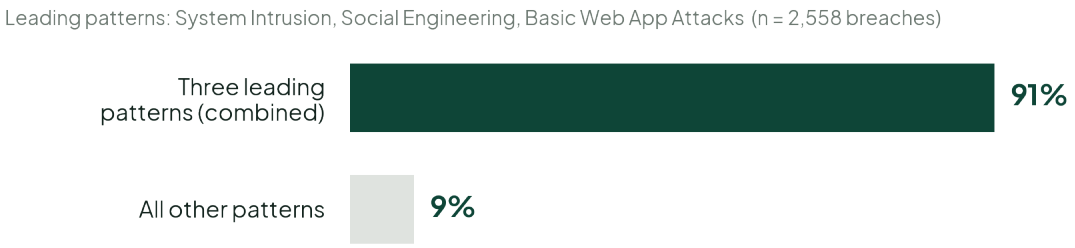
SecurIT360 publishes this summary so managing partners, general counsel, and firm leadership can turn sector-wide breach data into the handful of decisions that measurably reduce risk: identity, patching, third-party oversight, and tested recovery.

The state of Professional Services security

Three incident patterns do nearly all of the damage in this sector. System Intrusion, Social Engineering, and Basic Web Application Attacks together account for 91% of breaches with confirmed data disclosure. The shape mirrors the wider 2026 findings: intrusions increasingly begin with an exploited vulnerability rather than a guessed password, social engineering remains the reliable way through the human perimeter, and internet-facing applications continue to leak credentials and data when left exposed.

What sets Professional Services apart is not the methods used against it but the value of what those methods reach. A single mid-sized firm can hold privileged communications, financial data, and trade secrets for dozens of client organizations. Attackers understand the multiplier: breaching one firm can yield intelligence equivalent to breaching every client it serves. That is why the sector consistently draws external, profit-driven actors rather than the opportunistic noise seen elsewhere.

Patterns in Professional Services breaches



Who is behind the breaches, and why

The actor profile is stark. External actors are responsible for 97% of breaches in this sector, with internal actors involved in just 3%, a mix that points to organized, financially driven crime rather than insider misuse. Espionage and other motives are present but rare.

Threat actors in Professional Services breaches

Share of breaches by actor type (n = 2,558)

Motive follows the same line: 96% of breaches are financially motivated. For most firms that means ransomware, extortion, business email compromise, and the resale of stolen credentials and data, not nation-state espionage, even though high-profile firms do occasionally attract it. Defenses should therefore be tuned first to the economics of cybercrime: make compromise expensive and recovery fast, and the opportunistic majority moves on.

Actor motives in Professional Services breaches

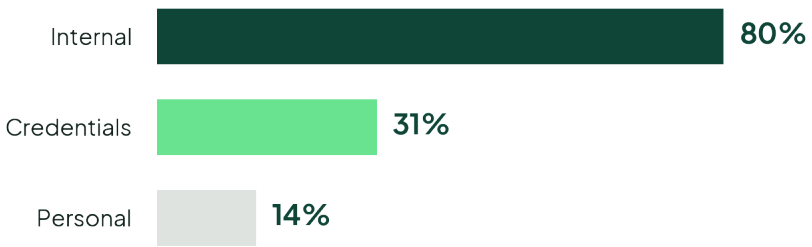
Share of breaches by motive; categories may overlap (n = 2,558)

What the attackers take

Internal business data is compromised in 80% of breaches: the contracts, memos, filings, and work product that are the sector's stock in trade. Credentials follow at 31%, valuable both as the entry point to the next system and as a saleable commodity. Personal data appears in 14% of breaches, reflecting the client and employee records these firms necessarily hold. Categories overlap, since a single breach often exposes more than one data type.

Data compromised in Professional Services breaches

Top data varieties (categories overlap; n = 2,558)



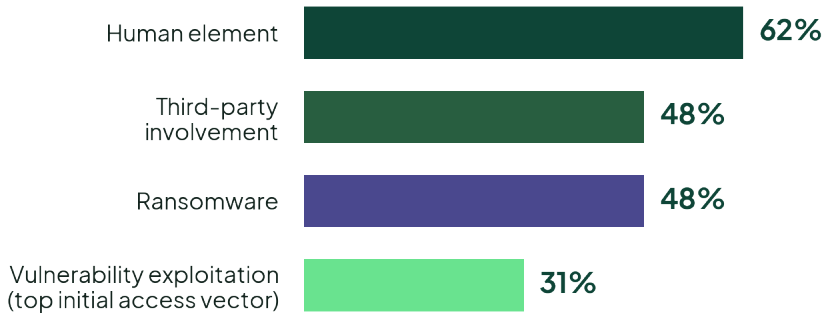
The credential loop is the part to watch. Stolen credentials are simultaneously a top target and a top entry method. Once a set of valid logins leaves a firm, it feeds the next intrusion — at that firm, at its clients, or at a vendor in the chain. Breaking this loop with phishing-resistant MFA and rapid credential rotation does more than protect one account; it disrupts the supply that fuels the broader market.

Cross-cutting 2026 themes that hit this sector hard

Several report-wide findings land with particular force on Professional Services firms, given their data sensitivity and typically modest security staffing.

2026 DBIR findings most relevant to this sector

Share of all breaches across the full 2026 dataset (context, not sector-specific)



Vulnerability exploitation is now the #1 way in (31%). For the first time in the report's history, exploiting an unpatched vulnerability overtook stolen credentials as the leading initial access vector. With AI compressing the gap between disclosure and exploitation from months to hours, the edge devices and document-management platforms common in legal and consulting environments need to be patched on a far tighter clock than most firms currently keep.

Ransomware is in 48% of all breaches, up from 44% the prior year. The encouraging counter-trend is that 69% of victims did not pay and the median ransom fell below $140,000, but encryption-plus-extortion against a firm's entire matter or client database remains an existential event, not merely an IT outage.

Third-party involvement reached 48% of breaches, up roughly 60% year over year. Professional Services firms sit on both sides of this risk: they are the trusted third party for their clients, and they depend on their own web of SaaS, cloud, and specialist vendors. A vendor's breach is now, statistically, the firm's breach.

The human element is in 62% of breaches. Phishing and pretexting still open most doors, and mobile-vector phishing click-through runs about 40% higher than email — a problem for a mobile, always-on professional workforce.

Shadow AI is the emerging exposure. Regular use of AI tools on corporate devices jumped to 45% from 15% in a single year, and roughly 67% of that access runs through non-corporate accounts. For firms handling privileged and confidential material, ungoverned AI use is a direct confidentiality and data-leakage risk that did not meaningfully register a year ago.

SPOTLIGHT

Law firms

Legal services fall within NAICS 5411, inside the Professional Services aggregate, so the sector profile above is the closest published proxy for the law-firm threat landscape. The fit is unusually good: like the sector at large, law firms face external, financially motivated actors after credentials and internal documents — except the internal documents in question are privileged.

Confidentiality and privilege raise the stakes. When the internal data compromised in 80% of sector breaches is attorney work product or privileged client communication, a breach is not only a security and regulatory event but a potential waiver of privilege and a bar-discipline exposure. The sector's own practitioners rank confidentiality as their top concern with emerging technology, and the 2026 data explains why.

The client-multiplier makes firms strategic targets. Because a law firm concentrates the secrets of many clients, it offers attackers leverage out of proportion to its size. Ransomware crews use this for pressure (publish-or-pay against named clients), and the rare espionage actor uses it for reach. It is the central reason a 40-attorney firm can face enterprise-grade adversaries on a small-business budget.

Shadow AI is a privilege problem, not just a data problem. The report-wide surge in ungoverned AI use is acute in legal work, where pasting a contract or case file into a consumer AI tool can expose privileged material to a third-party model. Firms need sanctioned tooling, clear policy, and monitoring before adoption outruns governance — which, on current numbers, it already is.

SPOTLIGHT

Small and medium-sized businesses

Most law firms, and a large share of Professional Services firms generally, fall within the small-and-medium-business (SMB) category, so the report's SMB findings are directly relevant to how these organizations actually experience risk.

96%

of ransomware victims in the 2026 DBIR

were small and medium-sized businesses

Ransomware appeared in 48% of all breaches · median ransom < $140K · only 31% of victims paid

Ransomware has become an SMB problem. 96% of ransomware victims in the 2026 dataset were small and medium-sized businesses. This is not because large enterprises have solved ransomware; it is because SMBs present the conditions attackers exploit: unpatched devices, reused or compromised credentials, and limited recovery capability. Attackers are opportunistic, and smaller firms are both abundant and softer.

The payment picture is shifting, slowly. Across all breaches, ransomware now appears in 48%, the median ransom has dropped below $140,000, and only about 31% of victims paid, evidence that better backups and a willingness to refuse are starting to change the economics. For an SMB, that willingness depends entirely on having tested, recoverable backups before the incident, not after.

SMB exposure tracks the same fundamentals. The report's guidance for smaller organizations is unglamorous and unchanged: patch internet-facing and edge systems quickly, enforce MFA everywhere (especially on remote access), govern which AI tools staff use, review third-party and vendor access at least annually, and practice — not merely document — a recovery plan. The difference in 2026 is that the cost of skipping these basics has never been higher.

Takeaways

1. **Patch on a threat-actor clock.** With exploitation the #1 entry vector and AI shrinking the patch window to hours, prioritize internet-facing and edge devices, VPNs, and document-management platforms.
2. **Make credentials hard to steal and useless when stolen.** Deploy phishing-resistant MFA, rotate exposed credentials fast, and monitor for credential reuse across the firm and its clients.
3. **Treat vendors as part of your attack surface.** Inventory third-party and SaaS access, require MFA and sound cloud configuration, and review access at least annually.
4. **Govern AI before adoption outruns policy.** Provide sanctioned tools, set clear confidentiality rules, and monitor for shadow AI, especially where privileged data is involved.
5. **Assume ransomware and rehearse recovery.** Maintain tested, offline backups and a practiced incident-response plan so refusing to pay remains a viable option.

Methodology and sources

Sector figures (incident and breach counts, patterns, actors, motives, and data varieties for NAICS 54) and all report-wide statistics are drawn from publicly available data published in the Verizon 2026 Data Breach Investigations Report, covering the period November 1, 2024 through October 31, 2025 (>31,000 incidents, >22,000 confirmed breaches, 145 countries). The three-pattern figure is reported as a combined share; the patterns chart reflects that combined value rather than an individual split. The overall-DBIR context chart shows full-dataset figures and is not sector-specific. SMB findings are drawn from the report's small-and-medium-business analysis. This document is an independent SecurIT360 executive industry summary structured to match the report's industry sections; it is not affiliated with or endorsed by Verizon.

The full 2026 DBIR is publicly available from Verizon.

About SecurIT360

SecurIT360 is an independent, vendor-agnostic cybersecurity and compliance consulting firm founded in 2009, with offices in Birmingham, Alabama and Kansas City. We work with organizations that handle sensitive, regulated information (including legal, financial, healthcare, and government) and have deep, long-standing experience securing law firms and Professional Services organizations like those profiled here.

Our professional services map directly to the risks in this summary: security program and risk assessments, penetration testing and offensive security, governance, risk, and compliance (GRC) advisory, virtual CISO (vCISO) leadership, security awareness training, and 24/7/365 U.S.-based managed detection, monitoring, and incident response. We translate findings like these into a prioritized, business-aligned security program, turning a sector-wide threat picture into the specific, defensible decisions your firm needs to make.

Learn more at **securit360.com** · explore our services at **securit360.com/services**.