QBE Insurance

Supplementary May 2026 Update

Cyber Threats

Legal and Professional Services Sector

In April 2025, we published the original report on cyber threats to the legal and professional services (LPS) sector. This is a supplementary report that draws on some of the latest statistics, trends and case studies since that report was published.

It assesses what has changed with regards to the threat from ransomware actors, as well as other types of actors such as state sponsored groups. It covers 'global' threat trends before digging into the LPS sector and what recent incidents tell us about how the threat has changed.

Executive Summary

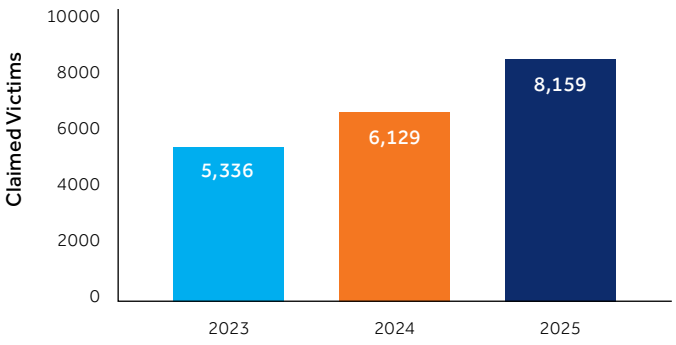
- The cyber threat to the LPS sector has remained a key risk as we progress through 2026.
- It remains one of the most targeted sectors by highly active and sophisticated ransomware actors, as well as some state sponsored groups.
- The legal and professional services sector should remain aware of broader threat trends including how social engineering and the exploitation of critical vulnerabilities has increasingly enabled threat actors to launch highly impactful attacks in 2025.
- While ransom payment rates have generally decreased, the legal sector remains one of the most heavily targeted sectors by ransomware actors.*
- So far in 2026, the sector remains one of the most targeted globally, with high numbers of known victims across the US, UK, Australia and Asia.*

Ransomware and Extortion: Global Picture

Since we published our last report, ransomware attacks have continued to increase. New groups have emerged, existing groups have ramped up their operations, while others have disappeared.

What is clear is that ransomware and data extortion continues to be the most significant threat to almost every industry vertical, especially the LPS sector. The table below shows the number of publicly listed victims by ransomware groups was at an all time high in 2025.[1]

Claimed Ransomware Victims 2023–2025



*https://www.chainalysis.com/blog/crypto-ransomware-2026/ 1. This data is taken from Ransomware.live, which actively scrapes known data leak sites and presents the data on the site. The data is unlikely to be completely accurate as incorrect sector classification and other factors may skew the figures. Important note: the data is also not reflective of the number of actual ransomware attacks, as those companies that paid a ransom will not have appeared on the leak site.

Ransomware and Extortion

Key Trends Update

In the previous report, we covered how threat actors were focusing on virtual supply chain targets, the development of defence evasion techniques, and blurring of lines between criminal and state groups. There is no doubt that threat actors have continued to exploit the supply chain and have continued to improve their techniques, but the second half of 2025 also demonstrated other key trends:

Social engineering is often the root cause of high-profile ransomware attacks.

Groups like the Scattered Spider collective have demonstrated how social engineering tactics, such as using phone calls to IT helpdesk staff to obtain employee credentials, can provide information to bypass access controls and multifactor authentication, and give them a foothold from which to launch highly disruptive ransomware attacks.

These high-profile attacks in 2025 reportedly involved third party service providers, presenting issues for organisations looking to control and ensure good security practises. Some prominent ransomware groups have also made it clear that they are open to recruiting insiders at large enterprises, paying them for access.[2] This will be a key trend to monitor throughout 2026.

Some threat actors have focused heavily on data theft only attacks.

Attackers have adopted highly effective techniques to access mass amounts of business data from enterprise assets that store it.

Expansive campaigns like Scattered Spider/ShinyHunters' gaining access to CRM systems, either by socially engineering IT staff[3] or targeting third-party applications[4] is a key example from 2025.

The exploitation of various enterprise software by the CL0P group also demonstrates the threat when zero-day exploitation enables widespread data theft.[5]

Critical vulnerabilities are jumped on quickly by ransomware groups.

Threat actors, and in particular, ransomware actors, are becoming even quicker at exploiting newly discovered vulnerabilities.

QBE has observed numerous public cases where waves of organisations have all been affected by the same vulnerability, many of which suffered ransomware attacks, or incidents which were contained shortly before ransomware could be deployed.

Vulnerabilities in widely used enterprise software, including VPNs, firewalls, file-transfer platforms and, more recently, AI tools, were heavily exploited by malicious actors in 2025. In addition to this, there has been a staggering 42% rise in the exploitation of zero-day vulnerabilities in 2025, posing a significant challenge for all organizations.[6]

Ransom payments are reportedly continuing to fall.

In our April 2025 report, we referenced research that showed the rate of ransom payments had slowed, despite the volume of attacks remaining high. Reporting in 2026 has shown that while the rate in which organisations are paying has decreased, the average ransom amount paid has gone up.[7]

This challenge for ransomware actors will likely force them to be less opportunistic and more targeted, going after sectors and market segments, where operational disruption is highly damaging or where the confidentiality of data is paramount. These actors are also developing their technical capabilities to compromise back-ups, which are often what organisations lean on when they refuse to pay. Given the sensitivity of data held by LPS firms, this high threat from ransomware actors is likely to continue.

2. picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup 3. cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion 4. cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift 5. crowdstrike.com/en-us/blog/crowdstrike-identifies-campaign-targeting-oracle-e-business-suite-zero-day-CVE-2025-61882/ 6. M-Trends 2026 Report 7. chainalysis.com/blog/crypto-ransomware-2026/

Legal and Professional Services Threat Landscape

By the end of 2025, the numbers showed that globally, the LPS sector remains one of the most affected by ransomware.[8]

While groups like RansomHub and Black Basta, who plagued LPS firms in 2024, seem to have disappeared from the landscape, several other groups have escalated their operations. Based on public ransomware data, groups like Qilin and Akira are now the forerunners in the landscape, with others like INC and Lynx also filling the gap left by others, and who are demonstrating a consistently high intent towards LPS firms.

Key threat trends in the legal and professional services sector[8]

In 2025: Professional Services was the top 3 most affected sector by ransomware and remains in the top 5 most affected sectors in 2026

54% increase from 2024-2025 in ransomware attacks in the legal sector

Average ransomware demands in the legal sector rise from $383,000 in 2024 to $611,000 in 2025 (up 60 %)

The legal sector was 8th most affected by ransomware according to Microsoft[9]

Prominent groups like Qilin, Lynx, INC, and Dragonforce continually named firms in the sector on ransom leak sites

The legal sectors in the US, Canada, UK, Germany, Italy, Australia, India, and South Korea have been most affected in 2025

8. comparitech.com/news/worldwide-ransomware-roundup-2025-end-of-year-report/ 9. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

Recent case studies in the LPS sector

- **Lynx ransomware poses a high threat to law firms, especially those in Australia.** This group have publicly listed two Australian law firms, one in New South Wales and one in Adeleide (April and August 2025) respectively.[10] The Lynx ransomware operation is highly capable, offering a robust and flexible encryption and data leak platform for affiliates.[11]
- **Large US law firm targeted by Chinese state actors.** In September 2025, Mandiant reported on a widespread campaign by Chinese advanced persistent threat (APT) group Silk Typhoon using the BRICKSTORM malware against law firms and the IT sector. They were reportedly using a zero-day vulnerability to compromise organisations before deploying BRICKSTORM as a backdoor for persistent access to these networks.[12] At the same time, a major law firm in the US, Williams & Connolly, said they suspected that Chinese state actors had compromised their network through a zero-day vulnerability.[13]
- **Emerging ransomware group uses initial access broker to compromise law firms.** A ransomware operation called GLOBAL GROUP, which emerged in July 2025, has been reportedly targeting various sectors primarily in the UK, US and Australia. In one case, it appears as though a member of GLOBAL GROUP acquired access to a law firm from an initial access broker who had advertised access on a cybercriminal forum. The IAB was asking for 1,000 USD and return, would provide remote desktop access (RDP) into the law firm's network.[14]
- **INC Ransom group heavily targeting the legal sector**. In 2026, this group listed 20 firms, with 10 victims listed in only 2 days. Given this unusually high number, it's possible that a common third party has been exploited by the group that granted them access to at least some of these firms.[15]

Threat actor snapshot

Silent Ransom Group

Overview: Silent Ransom Group (aka Luna Moth, Chatty Spider) are an extortion group that almost exclusively target law firms. They emerged in Spring 2023 and have primarily targeted US firms, though their geographic scope is likely to be wider.

Initial access techniques: Their go-to technique is callback phishing. This involves sending spam emails to their targets, which are historically related to unwanted subscriptions. The emails then prompt the victim to resolve the unwanted subscription by calling a number operated by the threat actors, who pretend to be IT support personnel.

The threat actors then guide the victim through installing a remote access tool (such as Atera, AnyDesk, Splashtop) on their machines, which gives them control.

Actions on objectives: The group then use this access to identify sensitive information, which they then steal from the network using tools like WinSCP or Rclone. They then threaten to leak the stolen data if they are not paid.[16]

10. Information from Ransomware Live Tracker - https://www.ransomware.live/ 11. group-ib.com/blog/cat-s-out-of-the-bag-lynx-ransomware/ 12. cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign 13. therecord.media/us-law-firm-hackers-breached-email 14. blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service 15. halcyon.ai/ransomware-alerts/inc-ransom-group-mounts-rapid-campaign-against-law-firms 16. ic3.gov/CSA/2025/250523.pdf

Guidance for organisations

Below are high-level recommendations for organisations to consider when taking steps to mitigate threats.

It is not an exhaustive list, and the suitability and applicability of the recommendations will differ depending on the organisational context. More detail on these points are included in the original report.

Ransomware

- Implement and test secure and robust back-ups.
- Perform regular exercises and technical assessments to test recovery processes and systems.
- Ensure you have incident response playbooks and plans that are regularly tested, reviewed, and communicated to staff, with a focus on technical response and recovery, as well as clear documentation for escalation procedures and communications.
- Ransomware attacks start with initial access, so focus on controls that reduce the chances of remote access into the network through phishing, credential theft, and exploitation of vulnerabilities (see below).
- Ensure training is carried across the organisation that aligns with the current threat landscape.

Cloud

- Establish consistency in user, administrative, and service account access within cloud environments dependent on roles and responsibilities.
- Review cloud logging strategy and ensuring that suspicious activity, such as suspicious logins or data exfiltration, in the cloud is being appropriately monitored.
- Refer to public guidance on securing cloud environments.

Vulnerabilities

- Create and follow a patch management process so that high severity vulnerabilities are remediated (patched or closed) quickly.
- This should be underpinned by a vulnerability prioritisation process that considers several factors such as whether the system is internet facing, the nature of the vulnerability (e.g. privilege escalation, or remote code execution), whether it is being exploited in the wild, etc.
- Disable unnecessary devices, ports and services for internet facing systems.

Supply Chain

- Rate the criticality of each supplier with respect to the data they hold and the extent they underpin critical business services, i.e. assess what the likely organisational impact would be of a cyberattack against the supplier.
- Ensure appropriate due diligence is conducted for each supplier according to criticality, mapping minimum security requirements and formally embedding them into contractual arrangements.
- Communicate expectations, requirements and intelligence to suppliers.

Contact us

For further assistance on QBE's cyber insurance solutions, your local cyber Underwriter is available to assist.

Contact information can be found at **qbe.com/cyber**

QBE Insurance