cowbell®

Cyber Threats Targeting Software and IT Organizations

Notable incidents, threat actors, and mitigations for IT and software SMEs

Executive Summary

Small and Medium-sized businesses or Enterprises (SMEs) within the software and Information Technology (IT) sectors are experiencing highly sophisticated, escalating cyber threats. Financially motivated cybercriminals and nation-state actors target these organizations due to the valuable intellectual property (IP), access credentials, and personally identifiable information (PII) they hold.

More critically, IT and software organizations provide high-leverage entry points for broader supply chain compromises. Modern software relies heavily on third-party integrations and open-source packages, creating a “transitive dependency” model. Threat actors increasingly exploit these pipelines to insert malware into legitimate software updates, simultaneously compromising downstream customers. This white paper outlines the regional threat landscapes across the US, UK, and Australia, profiling notable incidents and offering a sound approach to digital resilience.

Matthieu Chan Tsin
SVP & General Manager, Cowbell Resiliency Services

Strengthening cyber resilience alongside tailored cyber insurance is crucial to avoiding catastrophic losses. Cowbell Resiliency Services equips policyholders with the tools and expertise to proactively detect and mitigate vulnerabilities, fortify infrastructure, and counter evolving threats.

Additional questions? Request a consultation.

Our experts are happy to explain the process in more detail and address any issues you may have.

Notable Cyber Incidents: United States

US software providers are squarely in the crosshairs of both aggressive ransomware syndicates and nation-state actors. The intelligence below highlights a critical reality: a breach of a single technology vendor can cascade across dozens of downstream financial, municipal, and healthcare clients. As brokers, it is crucial we help our technology policyholders understand that their digital risks extend far beyond their own perimeter. By properly structuring Technology E&O and Cyber Liability coverage, we can ensure these organizations have the financial backing to navigate zero-day exploits, secure their codebases, and maintain the trust of their enterprise customers.

Marquis Software Solutions

In August 2025, the Akira ransomware collective breached this Texas-based fintech software provider, exposing names, Social Security numbers, and financial account information. The incident impacted over 672,000 individuals across approximately 74 to 80 downstream financial institutions.

Smarter Tools

In January 2026, the Warlock ransomware gang (also tracked as China-nexus Storm-2603) exploited an unpatched vulnerability in this software company's infrastructure. The attack compromised 12 Windows servers and led to the potential exfiltration of over 1 million documents.

ConnectWise

In May 2025, a nation-state cyberattack targeted ConnectWise's ScreenConnect remote desktop software, exploiting a high-severity code injection flaw (CVE-2025-3935). The breach forced emergency environment-wide hardening and intensified legal pressures stemming from previous class-action lawsuits.

Notable Cyber Incidents: United Kingdom

Software and IT firms in the UK reported more cyber incidents than any other sector last year. The incidents below underscore the severe disruption caused when critical codebases and production databases are compromised. Furthermore, with the UK's Business and Trade Committee actively proposing reforms to introduce strict legal liability for software developers, the regulatory landscape is shifting dramatically. Our role within the UK Market is to provide these tech firms with the clarity and specialized coverage they need to confidently weather ransomware extortion, regulatory scrutiny, and supply chain disruptions.

Claud Bilbao
VP, Underwriting & Distribution UK & Australia

Adaptavist Group

In April 2026, ransomware collective 'The Gentlemen' attacked this UK software developer. Using stolen credentials, attackers claimed a complete infrastructure compromise, exposing source code, legal contacts, and production databases, while actively impersonating Adaptavist communications to phish downstream clients.

DXS International

In December 2025, the DevMan ransomware group launched a double-extortion attack against this clinical decision support software provider, exfiltrating 300 GB of internal data. Given the firm's integration with the NHS, the breach placed DXS under active regulatory scrutiny.

Distinctive Systems

In January 2026, INC Ransom breached this software provider for global transport operators. Attackers published pricing documents, R&D data, and employee passports on their dark web leak site, posing severe supply-chain risks to global clients.

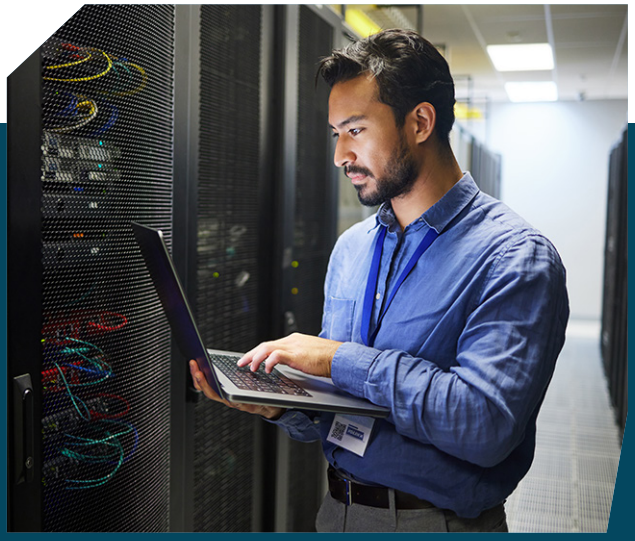
Threat Actor Profiles & The Nation-State Overlap

Threat actors targeting this sector rely on RaaS models, internet-facing vulnerabilities, and double-extortion tactics. Alarmingly, cybercriminals are increasingly collaborating with nation-state actors.

- **The Gentlemen:** A rapidly rising ransomware group offering a 90/10 affiliate revenue split to attract experienced hackers.
- **Warlock (Storm-2603):** A China-based threat actor group that actively deploys Warlock ransomware, targeting software providers like Smarter Tools to conduct espionage and steal IP.
- **Medusa:** A traditional Russian-speaking RaaS collective that researchers indicate has collaborated with North Korea's Lazarus Group (APT38), demonstrating that ransomware actors are renting their infrastructure for nation-state espionage.

The Sound Approach to Risk: Recommendations

- **Enforce MFA and Basic Access Controls:** Implement strong Multi-Factor Authentication and Role-Based Access Control (RBAC) across all code repositories, cloud platforms, and administrative systems.
- **Adopt Secure Software Development Practices:** Implement supply chain security measures to prevent vulnerabilities during the development process. Use tools like OWASP Dependency-Track to track open-source components.
- **Strengthen Vulnerability Management:** Regularly apply security updates to prevent attackers from exploiting known vulnerabilities in internet-facing assets.



Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today's threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.

cowbell®

US0076 0726