Rezliant

2025 Software Company Breach Scenarios Cheat Sheet

Tech companies face unique cyber risks due to open-source dependencies, rapid release cycles, and cloud-first architectures. This cheat sheet outlines common breach scenarios, outcomes, and insurance impacts.

Attack Vector	Typical Breach Scenario	Common Outcome	Insurance Impact
🔑 GitHub secrets leak	Stolen API keys/tokens used for privilege escalation	Ransomware deployment, cloud resource hijacking	Ransom/extortion payouts, forensic costs, regulatory penalties
🗄️ Misconfigured S3 bucket	Public exposure of sensitive data	PII/PHI/data leaks, reputational harm	Privacy breach notifications, legal defense, class-action suits
🐞 Unpatched open-source dependency	CVE exploited in library for remote code execution	Service downtime, unauthorized system access	SLA payouts, customer churn, business interruption claims
🛠️ CI/CD pipeline compromise	Malicious code injected into builds	Supply chain breach, downstream client impact	Third-party liability, massive claim exposure
🔌 Third-party SaaS breach	Vendor compromise → backdoor into insured	Data theft, lateral access	Contingent business interruption, vendor liability disputes
🌐 Flat internal network	Lateral movement after phishing or initial access	Ransomware propagation, system-wide outages	Large-scale BI, ransom payments, forensic investigations
📉 Weak monitoring & alerting	Breach persists undetected for weeks	Long attacker dwell time, data exfiltration	Increased loss severity, prolonged claim costs
💾 No tested backups	Ransomware destroys data, recovery fails	Complete business interruption	Ransom + business interruption payouts

"... a world where every software company can confidently release secure code knowing they protect not just data or IP, but the livelihoods of all stakeholders"