











The Cyber Insurer's Playbook for Software Companies

Top 10 Red Flags in a Tech Company's Security Posture

Software companies face unique risks — from vulnerable code to misconfigured cloud services. This playbook highlights the most common red flags insurers should watch for, and the underwriting questions that reveal them.

Red Flag	Why It Matters	What to Ask
 No MFA	Credentials are the #1 breach vector	Do you enforce MFA on all employees, admins, and production?
 No SSDLC practices	Shipping insecure code raises breach chance	"Do you run code scanning in your build pipelines?"
 Unscanned open-source	Vulnerable libraries fuel supply chain	Do you use software composition analysis (SCA) tools?
 No logging/monitoring	Breaches go undetected for months	Do you enable centralized logging and alerting in AWS/Azure/GCP?
 Unmanaged CI/CD secrets	Keys in GitHub/GitLab can be stolen	How do you manage and rotate CI/CD secrets?
 Weak patch management	Exploits often target known CVEs	What's your SLA for patching critical vulnerabilities?
 No incident response	Increases claim size/duration	Do you have a tested IR plan and playbook?
 Flat network access	Lateral movement risk	Do you use network segmentation or Zero Trust?
 No vendor risk oversight	Third parties introduce hidden risk	Do you assess third-party software and service providers?
 Lack of backups	Shipping insecure code raises breach risk	Do you maintain immutable, tested backups?

"... 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"