

Threat	Likelihood	Impact	Risk Level	Recommended Controls
Phishing Emails	High	High	High	Security awareness training; email filtering; phishing simulations
Weak Passwords / No MFA	High	High	High	Enforce strong passwords; implement MFA; use password managers
Cloud Misconfiguration	Medium	Critical	Critical	Regular cloud audits; least privilege access; automated config monitoring
Unpatched Software	High	High	High	Automated patch management; vulnerability scans
Third-Party Vendor Breach	Medium	High	High	Vendor risk assessments; contracts requiring security standards; continuous monitoring
Insider Threat (Employee Mistakes)	Medium	Medium	Medium	Access monitoring; role-based permissions; ongoing training

Risk Assessment Summary

This risk matrix highlights some of the most common and damaging cybersecurity threats faced by both small and large businesses, with an emphasis on cloud security and governance, risk, and compliance (GRC). Phishing and weak authentication practices remain leading attack vectors because they exploit human error and poor credential management. Without strong controls like MFA and training, attackers can easily bypass defenses and compromise accounts.

Cloud misconfiguration stands out as a critical risk because it directly impacts data security in hosted environments. Many organizations move to the cloud for scalability and cost savings but fail to properly secure storage buckets, databases, and access permissions. For small businesses, this often comes from lack of expertise; for large enterprises, the issue is complexity across teams and accounts. Automated configuration monitoring and least-privilege policies are essential safeguards.

Third-party vendor risk and insider threats reinforce the importance of GRC. A business can have strong technical defenses, but if vendor contracts don't enforce security requirements or employees aren't monitored and trained, gaps will remain. GRC frameworks ensure that responsibilities are documented, vendors are vetted, and policies are enforceable. For both small and large businesses, applying GRC alongside cloud security best practices turns ad hoc security into structured, repeatable protection.

This assessment also shows why I'm focusing my portfolio on Cloud Security and GRC: they're where technical controls and business policies meet to reduce real-world risk.