Tech-to-Business Risk Translator

Technical Risk	Business Impact
Zero-day exploit in Apache server	Our customer-facing services could be taken offline without warning, affecting revenue.
MFA is not enabled on email accounts	An attacker could impersonate an employee, gaining access to confidential information.
Phishing simulation click rate is 30%	1 in 3 staff could expose the company to malware or ransomware attacks.
S3 bucket misconfigured as public	Sensitive company documents are publicly accessible — potential data breach.
No logging enabled on critical systems	If we're hacked, we won't know when or how — or be able to prove it legally.
Unpatched vulnerabilities in production systems	Known weaknesses could be exploited at any time, leading to service outages or theft.
Outdated antivirus signatures	New malware can bypass our current protection, increasing breach risk.
Insecure Wi-Fi in branch offices	Anyone nearby could access internal systems — including competitors or attackers.
BYOD devices aren't encrypted	If a device is lost or stolen, client or financial data could be leaked.
No role-based access control (RBAC)	Staff may be able to access data they shouldn't — increasing risk of insider misuse.
Legacy software running on unsupported OS	We can't patch known security holes, leaving us open to ransomware.
Open RDP ports on external-facing servers	Attackers could directly access internal systems and take control remotely.
No formal incident response process	In a cyberattack, we'd waste valuable time — increasing recovery costs and downtime.
Third-party vendors not assessed for risk	A supplier could be the weak link that lets attackers into our network.
Backups are not tested regularly	If we're hit by ransomware, our backups might not work — and recovery could fail.

LAB CYBER