Data Breach Financial Exposure Assessment Checklist

Use this checklist to evaluate whether your organisation is financially exposed to a preventable high-cost cyber recovery event.

Prevention Controls

☐ Multi-factor authentication is fully implemented on critical platforms.
☐ Employees receive recurring phishing/security awareness training.
☐ Password management practices are standardised.
☐ Critical backups are documented and tested.
☐ Access permissions are reviewed regularly.

Detection and Response Readiness

☐ We have a defined cyber incident reporting process.
☐ Employees know how to report suspicious events immediately.
☐ External cybersecurity support contacts are pre-identified.
☐ Internal leadership knows who owns incident decisions.
☐ Cyber insurance policy details are understood.

Vendor and Operational Continuity

☐ Key third-party vendors have been reviewed for cyber reliability.
☐ Critical SaaS platform dependencies are mapped.
☐ Customer communication procedures exist for service disruption.
☐ Manual continuity procedures exist for major system downtime.

Financial Exposure Awareness

☐ Leadership has estimated potential downtime payroll waste.
☐ Leadership has estimated likely revenue interruption impact.
☐ Legal/notification obligations have been discussed internally.
☐ We understand what cyber insurance may not cover.
☐ Customer trust impact has been considered in incident planning.

Governance Maturity

☐ Cybersecurity spending is budgeted proactively, not only reactively.
☐ Policies are reviewed annually.

☐ Vendor access is reviewed periodically.
☐ Recovery testing occurs on a scheduled basis.
☐ Executive leadership reviews cyber risk as a financial issue.
☐ We have compared annual prevention spend to probable breach loss.

SCORING YOUR RESULTS

20–24 boxes checked = STRONG MATURITY

Your organisation is thinking about cybersecurity as a continuity and financial safeguard, not merely a technical task.

12–19 boxes checked = MODERATE EXPOSURE

Some meaningful protections exist, but there are still major cost-amplifying gaps that could make breach recovery far more expensive than necessary.

0–11 boxes checked = HIGH VULNERABILITY

Your organisation is likely underestimating both cyber likelihood and cyber financial consequence, creating substantial preventable recovery exposure.