

LIYATECH EXECUTIVE READINESS SERIES

TECHNOLOGY, DIGITAL & COMMERCIAL BUSINESSES CYBER READINESS CHECKLIST

IT Companies, Software Firms, Marketing Agencies, Media, Retail, E-commerce & Digital Enterprises

"If your digital platforms went offline today, how quickly would your business and customers be affected?"

Introduction

Digital and commercially driven organisations operate in environments where technology is not support infrastructure – it is the business.

Platforms, cloud systems, customer portals, digital assets, and online services directly impact revenue, customer experience, and brand reputation.

Even short disruptions or security incidents can lead to:

- Revenue loss
- Customer churn
- Brand damage
- Operational delays
- Data exposure

This checklist is designed to help leadership teams assess whether their digital environment is truly resilient, secure, and scalable.

Tick what applies to your organisation.

1. Cloud & Platform Security

- ☐ We know exactly which cloud platforms and digital systems our business depends on.
- ☐ Access to cloud environments is strictly controlled and regularly reviewed.

- ☐ We are confident our cloud infrastructure is protected against unauthorised access or misconfiguration risks.
 - ☐ We have visibility into security risks across all digital platforms we use.
-

2. Customer Data & Digital Trust

- ☐ We are confident customer data is protected across all digital platforms and applications.
 - ☐ Customer accounts and profiles are secured against unauthorised access or takeover.
 - ☐ We can detect unusual activity involving customer data or accounts.
 - ☐ We understand the business impact if customer data were exposed.
-

3. Platform Availability & Business Continuity

- ☐ We are confident our digital services and platforms can remain available during disruptions.
 - ☐ We understand how quickly downtime would affect revenue and customer retention.
 - ☐ We have tested recovery processes for critical digital systems.
 - ☐ We know which systems are essential for continued business operations.
-

4. Identity, Access & Remote Workforce Security

- ☐ Staff access to systems is based strictly on role and responsibility.
 - ☐ Multi-Factor Authentication is used across all critical systems and platforms.
 - ☐ Access is immediately removed or updated when employees leave or change roles.
 - ☐ Remote access to systems is fully secured and monitored.
-

5. Application, Website & Digital Asset Protection

- ☐ Websites, applications, and APIs are regularly monitored for vulnerabilities.

- ☐ We can detect unauthorized changes to digital content or platforms.
 - ☐ Digital assets (designs, campaigns, code, media files) are securely stored and controlled.
 - ☐ We understand the risks associated with third-party integrations and plugins.
-

6. Incident Response & Recovery Readiness

- ☐ We have a clear response plan for cyber incidents affecting digital platforms.
 - ☐ Technical and business teams know how to respond during downtime or breaches.
 - ☐ Recovery procedures are documented and tested.
 - ☐ We are confident we can restore services quickly without significant customer impact.
-

Leadership Reflection

This checklist is designed to highlight digital and operational exposure — not to provide a score.

If several responses were **“No” or “Not Sure”**, it may indicate risk in areas affecting:

- Customer trust
 - Revenue continuity
 - Platform stability
 - Data security
 - Brand reputation
 - Business scalability
-

Optional Executive Conversation

If this checklist raised concerns or uncertainty, it may be useful to review your organisation's digital resilience and cybersecurity posture in a structured discussion.

The aim is to identify practical improvements that strengthen stability, trust, and performance.

Contact

Nomfundo Makapela

 nomfundo.makapela@liyatech.co.za

 073 582 4195

Terence Moabi

 terence.moabi@liyatech.co.za

 078 710 4180

 www.liyatech.co.za