CyberSecure

THE CYBER RISK CHECKLIST

Practical steps to understand and strengthen your digital risk structure

Most cyber incidents do not begin with a hacker. They begin with blind spots in the way your business connects. This checklist helps you see those blind spots clearly so you can take the right next step with confidence.

This is not a technical exercise. It is a structural one.

---

1. Know how your business actually runs

Cyber risk grows when the structure of the business is unclear.

Check the following:

☐ You know the core workflows that keep the business moving

☐ You know which systems and vendors support those workflows

☐ You know where your critical data lives

If you cannot answer these, your exposure is higher than you think.

---

2. Identify your critical systems and connections

Risk lives in the connections between tools, not the tools themselves.

Review the following:

☐ You can list the systems your operation depends on

☐ You understand how those systems integrate or connect

☐ You know which failures would create the biggest disruption

A failure in any one of these often causes multiple downstream impacts.

---

3. Review your vendor and third party exposure

Most incidents originate through vendors, not your internal systems.

Check the following:

☐ You know your top three mission critical vendors

☐ You know whether they carry cyber insurance

☐ You understand what happens if one of them goes down

If you are unsure about any of these, your vendor risk is not under control.

---

4. Confirm your basic controls are in place

You do need fundamentals.

Verify the following:

☐ Multi factor authentication is enabled for critical accounts

☐ Backups are tested on a recurring schedule

☐ Software updates and security patches are consistently applied

These are the controls that prevent most claims.

5. Understand the limits of your current cyber coverage
Many businesses are covered on paper but exposed in practice.
Review these questions:
☐ Does your coverage reflect how your business actually operates
☐ Do you understand what is excluded in a cyber incident
☐ Do you know how a vendor related breach would be handled
If you cannot answer these, your policy may not perform when it matters.

---

6. Assess your readiness during an incident
Clarity reduces stress and speeds recovery.
Consider the following:
☐ You know who to call first during an incident
☐ You know how long systems can be down before impact becomes critical
☐ You know who is responsible for internal communication
Preparedness is structural, not reactive.

---

7. Identify your top three priorities
Cyber risk becomes manageable when you focus on what matters most.
Choose your three highest impact actions:
☐ Strengthen MFA and reduce access
☐ Validate backups and test recovery
☐ Review policy alignment and vendor exposure
Small steps create meaningful protection.

Your next step
If this checklist surfaced blind spots, you are exactly where most businesses find themselves. The goal is not perfection. The goal is clarity. Once you have clarity, the path forward becomes simple.
When you are ready, schedule a Cyber Clarity Call and we will walk through your structure together.

CyberSecure
Your Business. Protected.
www.cybersecure.insure