REXON
CYBER SECURITY

10-Point Cybersecurity Checklist: A Rapid Risk Scan for Modern Businesses

Let's go

Why should you use this cybersecurity checklist?

A cyber incident is no longer an "IT problem" - it's a balance-sheet event. IBM's 2024 Cost of a Data Breach report pegs the average hit at US $4.88 million, up 10% in a single year, with lost revenue and regulatory penalties driving most of the bill.

For mid-market and smaller firms, the stakes turn existential: 75% say they would struggle to survive if struck by a ransomware attack, as cash flow evaporates and customers head for the exits. At the same time, boards, insurers and regulators increasingly expect clear evidence that basic safeguards are in place before they approve budgets, renew policies or green-light new projects. In short, sound cyber hygiene has become a prerequisite for growth, trust and day-to-day business continuity - not a technical nice-to-have.

This checklist will help you ensure you have the right controls in place to make your business a harder target to crack.

How to use the cybersecurity checklist

Read each question on the next two pages, and score one point for every **"Yes"** we have this under control.

Total up the **"Yes"** answers to get your total (**between 0 and 10**).

Go to the chart on page 5 to see how secure your business scores.

We've included some **"next best move"** suggestions to help you on your way to making your business a harder target to crack.

QUESTION

Ask the business a question to quickly diagnose and addresses a cybersecurity concern.

RED FLAG

This is a telltale sign that something is awry with your cybersecurity controls and mitigations and should be addressed.

QUICK WIN

This represents an action your business can take to quickly get the right security control or mitigation in place.

1 Asset Visibility & Inventory

	"Do we have a real-time register of all devices and SaaS apps?"
	Shadow IT and spreadsheets used as CMDB
	Deploy automated discovery tool

2 Identity & Access Management

	"Have we enforced MFA on every privileged account?"
	Shared admin passwords and default credentials in use
	Turn on enforced MFA on all accounts

3 Endpoint Security

	"Are laptops/servers covered by EDR with 24/7 alerting?"
	AV only with no central view of alerting
	Pilot an Endpoint Detection & Response (EDR) tool trial on critical hosts

4 Network & Perimeter Controls

	"Are inbound ports limited to documented business need?"
	Open ports (RDP/SHH for example) to internet
	Run weekly external port scans

5 Data Protection & Encryption

	"Is all sensitive data encrypted at rest and in transit?"
	S3 buckets left publicly available
	Force encryption defaults and enable object-lock

6 Vulnerability & Patch Management

	"Is critical patch SLA more than 14 days?"
	Quarterly patch cycles
	Weekly vulnerability scans and automate patch rollout on tier-1 assets

7 Incident Response & Continuity

	"Have we tested our IR plan in the past 12 months?"
	Dusty PDF with no tabletop exercises
	Schedule a cyber tabletop exercise with execs

8 Third-Party & Supply-Chain Risk

	"Do we risk-rank vendors and track their security attestations?"
	No contract language on cyber
	Add security clauses into new Master Service Agreements (MSAs).

9 Security Awareness & Culture

	"Is phishing training measured with click-rates less than 5%?"
	One-off training with no metrics being tracked
	Launch monthly micro-learning nuggets to keep on top of cyber awareness

10 Governance, Compliance & Metrics

	"Does senior management see a cyber KPI dashboard quarterly?"
	Cybersecurity is buried under the IT ops banner
	Develop and present a cyber heat-map to business execs.

Unsure where you land?

Book a free 30-minute cybersecurity health consultation with a Rexon Cyber analyst.

We'll translate your score into a cyber roadmap and outline how you can close the gaps you've identified, before an attacker (or investor) finds them. **Click the link below to book your free consultation.**

Free consultation

info@rexoncyber.com
+44 203 355 5492

Scoring and Interpretation

Total "Yes"	Risk Posture	What It Means	Next Best Move
0 to 3	Critical	Major safeguards are missing; exposure is high and incident impact could be existential.	Prioritise quick wins—multifactor login, backed-up data, and an incident response playbook.
4 to 6	Vulnerable	Foundations exist but are inconsistent; one weak link could still trigger serious disruption.	Map out a 90-day remediation plan, focusing on patching gaps and formalising responsibilities.
7 to 8	Managed	Controls are largely in place and monitored; resilience is acceptable but not yet optimised.	Move to continuous improvement—regular testing, vendor oversight, and board-level metrics.
9 to 10	Resilient	Best-practice controls are embedded and reviewed; you're positioned to resist and recover quickly.	Maintain momentum with periodic external reviews and scenario based stress-tests.