FREE RESOURCE / XBITIUM SECURITY

Security Risk Assessment Worksheet

Find your real risks in an afternoon, without a consultant.

You cannot protect against everything, so the job is to spend your limited time and money on the risks that are both **likely** and **damaging**. This worksheet walks you through it the same way a professional would: list what could go wrong, rate how likely and how bad, multiply, and work from the top of the list down.

How the scoring works

For each risk, rate two things from 1 to 5, then multiply them for a **risk score** from 1 to 25. Higher means deal with it sooner.

LIKELIHOOD — how probable?	IMPACT — how bad if it happens?
1 Rare — hard to imagine	**1** Trivial — minor annoyance
2 Unlikely	**2** Minor — a bad day
3 Possible — could happen this year	**3** Moderate — real cost, recoverable
4 Likely	**4** Major — serious money or reputation
5 Almost certain — happening already	**5** Severe — could end the business

READING YOUR SCORES

15–25 (act now): your top priority, address immediately. **8–14 (plan it):** schedule a fix this quarter. **1–7 (monitor):** be aware, but do not lose sleep. Work strictly from the top of the list down — that is the whole discipline.

Worked example (so you can see how it is done)

Risk	L	I	Score	What you will do about it
Ransomware via exposed remote desktop	4	5	20	Close RDP, put behind VPN, verify backups. This week.
Staff falls for invoice-fraud email	4	4	16	Phone-verify all bank changes; train staff on the tactic.
Laptop lost or stolen	3	3	9	Turn on full-disk encryption everywhere.
Website defaced	2	2	4	Keep platform patched and monitor. Lower priority.

Your worksheet

Start with the common risks below, then add your own. Rate L and I, multiply, and sort by score. Delete any that do not apply to you.

Risk	L	I	Score	Action / owner / date
Ransomware / malware infection				
Phishing / stolen credentials				
Invoice or wire fraud				
Lost or stolen device				
Insider mistake or misuse				
Cloud data exposed publicly				
Key vendor is breached				
Website or system outage				

Revisit this worksheet at least once a year, and any time the business changes significantly — new systems, new staff, new data, new clients.