SAMPLE. Fictional firm, fictional answers and illustrative costs, to show what a RestoreMark report looks like. Not a real client.

Example Ltd (fictional)

Prepared by RestoreMark (sample report) on 25 November 2026, from evidence supplied by Example Ltd (fictional) on 12 November 2026. This is an evidence review, not a test of your systems, a certification or a guarantee.

Bottom line

Based on the evidence supplied: Some accounts are not protected by MFA, so a stolen password alone could open them. If that happened, there is no written incident plan, or the only copy is on the network that would be down.

How an attacker could get in

Five steps, from your own answers. Each is the most important gap we found for that step.

1. **Entry** No gap found in the evidence supplied for this step.
2. **Why it works** Some accounts are not protected by MFA, so a stolen password alone could open them.
3. **Spread** Too many accounts have admin rights, or admins use their admin account every day. *(2 related findings)*
4. **Unnoticed** Nobody is watching security alerts around the clock. *(2 related findings)*
5. **Hard to recover** There is no written incident plan, or the only copy is on the network that would be down. *(5 related findings)*

This is a document-based hypothesis about the most plausible route, built from the evidence you supplied. It is not a penetration test and does not confirm that any weakness can be exploited.

Witnessed restore

A timed restore of the shared file server (client files) was run by the IT supplier on 19 November 2026 and watched by RestoreMark by video call. It was only partly restored, after 3 hours 40 minutes. Not restored: the practice-management database, which needed the software vendor's help and was still not working when the call ended. This shows what happened for this one system on that day. It does not show that every system, or a full rebuild after an attack, would succeed. The supplier had not run a restore of this server before and worked out the steps during the call.

Your IT team or provider ran the restore; RestoreMark watched and recorded it and did not operate your systems.

Readiness by area

Exposure	Green	**Patching**	Green	**Identity**	Amber
Alerting	Amber	**Response**	Red	**Recovery**	Red

3 red and 7 amber findings, 46 green, out of 56 questions rated.

SAMPLE

What a serious incident could cost you

Using your own figures (5 days down at about £4,000 a day), lost trading alone would be about £20,000. This is an estimate and excludes recovery fees, regulator or client costs.

What fixing the top five costs

About 5.5 days of effort in total, plus spend of **about £500 a month, all illustrative figures for this fictional firm**. Effort figures are our estimates for a firm your size.

SAMPLE

Your ranked 90-day plan

Ranked by how many steps of the attack route each fix helps close, then by effort. Maximum ten fixes.

#	Fix	Closes	Owner	Effort	Cost	Due
1	**Written incident plan** Write a one-page first-hour plan and keep a printed copy off the network.	Hard to recover	Managing director	1 day	£0 (internal)	25 December 2026
2	**Backups out of reach of admin accounts** Keep an immutable or offline copy that admin accounts cannot delete.	Hard to recover	IT supplier	2 days	about £40 a month (illustrative)	25 December 2026
3	**Rehearsal in the last 12 months** Run a tabletop exercise this quarter.	Hard to recover	Managing director	0.5 days	£0 (internal)	25 December 2026
4	**MFA everywhere** Require MFA for every account, including admins, shared mailboxes and remote access, and remove exceptions.	Why it works	IT supplier	1 day	£0 (licence already held)	24 January 2027
5	**Out-of-hours alerts** Set a named out-of-hours alert route, or buy monitoring.	Unnoticed	Managing director	1 day	about £150 a month (illustrative)	24 January 2027
6	**Timed restore test** Fix what stopped the restore, then repeat it and record the time.	Hard to recover	IT supplier	1 day	£0 (internal)	24 January 2027
7	**Admin rights** Cut admin accounts to the minimum and use separate accounts for daily work.	Spread	IT supplier	1.5 days	£0 (internal)	24 January 2027
8	**Round-the-clock monitoring** Add monitoring, or agree an out-of-hours alert route with a named person.	Unnoticed	Managing director	3 days	about £300 a month (illustrative)	23 February 2027
9	**Downtime targets** Set a downtime target for each top-five system and compare it with the timed restore.	Hard to recover	Managing director	0.5 days	£0 (internal)	23 February 2027
10	**AI assistants and agents register** List every AI tool, agent, connector and built-in AI feature with an owner and the data it can read.	Spread	IT supplier	1 day	[£ to confirm]	23 February 2027

SAMPLE

Insurance evidence map

Your answers lined up against questions insurers commonly ask. We do not advise on policy cover.

Common insurer question	Your answer	Evidence attached	Status
MFA on email, remote access and admins	Some accounts are not protected by MFA, so a stolen password alone could open them.	Entra sign-in report, 12 Nov	Can confirm, with exceptions
Endpoint protection on all devices	No gap found in the evidence supplied.	[evidence to attach]	Can confirm, with evidence
Immutable or offline, tested backups	Backups can be deleted or encrypted by the same accounts an attacker would reach. A witnessed restore only partly worked, so full recovery has not been shown.	Backup console settings; Witnessed restore, 19 November 2026	Can't confirm yet
Patching of internet-facing systems	No gap found in the evidence supplied.	[evidence to attach]	Can confirm, with evidence
Incident response plan tested	There is no written incident plan, or the only copy is on the network that would be down. The plan has not been rehearsed in the last 12 months.	Plan, undated	Can't confirm yet
Staff awareness training	No gap found in the evidence supplied.	[evidence to attach]	Can confirm, with evidence

SAMPLE

Status: **Can confirm, with evidence** (green); **Can confirm, with exceptions** (amber; each exception is listed); **Can't confirm yet** (red: evidence missing or unverified, never assumed). Anything we could not see is marked unverified.

Evidence types (Appendix A): **Documented** (a record or screenshot was supplied and reviewed); **Customer-confirmed** (you told us the control exists); **Third-party evidence** (a supplier or insurer document); **Not verified** (the material cannot establish the position).

Appendix A: every question

#	Question	Rating	Evidence type	Reviewer note
1.1	Security ownership	Green	Customer-confirmed	
1.2	Owner agreed to act	Green	Customer-confirmed	
2.1	List of internet-facing systems	Green	Customer-confirmed	
2.2	Remote desktop and admin consoles	Green	Customer-confirmed	
2.3	Login pages: MFA and lockout	Green	Customer-confirmed	
2.4	Staff credentials in known breaches	Green	Customer-confirmed	
2.5	Patch speed on internet-facing systems	Green	Customer-confirmed	
2.6	Custom-built web apps	Green	Customer-confirmed	
2.7	Website hosting and software versions	Green	Customer-confirmed	
2.8	APIs and bulk exports	Green	Customer-confirmed	
3.1	Licence features switched on	Green	Customer-confirmed	
3.2	Endpoint protection coverage	Green	Customer-confirmed	
3.3	Automatic containment	Green	Customer-confirmed	
3.4	Supplier tools with access	Green	Customer-confirmed	
3.5	Round-the-clock monitoring	Amber	Documented	Alerts go to the IT supplier's inbox, in office hours only.
3.6	Email spoofing protection	Green	Customer-confirmed	
3.7	Remote-managed equipment	Green	Customer-confirmed	
3.8	Equipment firmware and alerts	Green	Customer-confirmed	
3.9	Suppliers holding client data	Green	Customer-confirmed	

SAMPLE

4.1	MFA everywhere	Amber	Documented	MFA required for staff, but one group (reception, 6 people) is excluded.
4.2	Strength of admin MFA	Green	Customer-confirmed	
4.3	Conditional access rules	Green	Customer-confirmed	
4.4	Admin rights	Amber	Documented	Two admin accounts are shared by the IT supplier and a partner.
4.5	Third-party app access	Green	Customer-confirmed	
4.6	Who approves new apps	Green	Customer-confirmed	
4.7	Service accounts and API keys	Green	Customer-confirmed	
4.8	Help-desk identity checks	Green	Customer-confirmed	
4.9	Enrolling new devices and MFA methods	Green	Customer-confirmed	
4.10	Platforms holding or messaging client data	Green	Customer-confirmed	
4.11	Who can message all clients	Green	Customer-confirmed	
4.12	Call-back rule for requests	Green	Customer-confirmed	
4.13	Leaver access	Green	Customer-confirmed	
4.14	AI assistants and agents register	Amber	Documented	Copilot Chat and a meeting note-taker are in use; no register of AI tools or what they can read.
4.15	AI agents that can act alone	Green	Customer-confirmed	No agent can send, share or pay unattended.
4.16	AI apps connected to mail and files	Green	Customer-confirmed	User consent is off; AI app grants approved by IT.
4.17	Copilot and oversharing	Green	Customer-confirmed	Microsoft 365 Copilot not licensed; Copilot Chat only.
4.18	Assistants reading outside content	Green	Customer-confirmed	
4.19	Switching off an AI agent fast	Green	Customer-confirmed	
5.1	Out-of-hours alerts	Amber	Documented	Nobody is on call at night or weekends.
5.2	Sign-in logs	Green	Customer-confirmed	

SAMPLE

5.3	Alerts for sign-in bursts and new app access	Green	Customer-confirmed	
5.4	Written incident plan	Red	Documented	A plan exists, but only on the shared drive, and it has never been tried.
5.5	Plan starts with the insurer	Green	Customer-confirmed	
5.6	Rehearsal in the last 12 months	Red	Customer-confirmed	No tabletop exercise has ever been run.
5.7	First-hour authority	Green	Customer-confirmed	
5.8	Outage or attack?	Green	Customer-confirmed	
6.1	Backup map	Green	Customer-confirmed	
6.2	Backups out of reach of admin accounts	Red	Documented	The domain admin account can delete the nightly backups.
6.3	Timed restore test	Amber	Documented	One witnessed restore (the file server) took 3 hours 40 minutes and only partly worked: the practice-management database did not come back. No restore of other systems has been tried.
6.4	Downtime targets	Amber	Customer-confirmed	Targets not set for the top five systems.
6.5	Decision if data is stolen	Green	Customer-confirmed	
6.6	Build documents and clean images	Green	Customer-confirmed	
6.7	Working without the main platform	Green	Customer-confirmed	
7.1	Insurance questionnaire matches reality	Green	Customer-confirmed	
7.2	Dated evidence folder	Green	Customer-confirmed	
7.3	Staff awareness training	Green	Customer-confirmed	

SAMPLE

Appendix B: first-hour response plan (print this and keep a copy off your network)

1. **Is it an outage or an attack?** Check the supplier's status page (Microsoft 365 and others) and a second device before shutting anything down. Who checks: IT supplier.
2. **Call your insurer first:** [insurer] (fictional), [number], policy [policy no.].
3. **Then** [legal adviser], then [response firm named by the insurer].
4. **Actions you may take without waiting:** disable the affected account ([who]), isolate the device ([who]), cut supplier access ([who]).
5. **Keep a printed copy** of this page at the office safe.

Appendix C: 90-day re-check

Open routes in now: **10** (3 red, 7 amber). After 90 days we recount the open routes, not the tickets closed: start 10, now [n].

RestoreMark is a trading name of Christian Perry, a sole trader. RestoreMark provides an independent readiness review. It is not a certification, an accredited audit, legal advice, insurance advice or a guarantee of protection.

SAMPLE