Sample report — fictional business and example data

FLINTLATCH

Monthly security report

Example Property Co.

example.com · All figures below are example data for this sample.

BUSINESS PLAN (SAMPLE)

Period: October 1–31, 2026

Prepared by Davis · Sample date: November 3, 2026

STATUS THIS MONTH

Needs attention

2 High · 3 Medium · 1 Low

I did not see signs that the site is already compromised. The items below are gaps I recommend fixing, starting with the High ones. This is a point-in-time check, not a compliance certification, and it is not a promise that the business cannot be breached.

What I checked

- **Website security check** (monthly, passive only) of https://www.example.com: certificate, security headers, SPF/DKIM/DMARC, visible software versions and public exposure. No logins, attacks or load testing.
- **Breach monitoring** for the example.com email domain, using known-breach data from Have I Been Pwned.
- **Phishing training and one simulated test** for the approved list of 12 people. No real malware, and I do not collect real passwords.
- **Quarterly vulnerability assessment** (included this month) of www.example.com, mail.example.com and remote.example.com. Authorized scan only; no exploitation.
- **Policy checklist**, reviewed this quarter against the starter checklist.

Findings (example data)

Severity	What I found	What it means	Plain fix
HIGH	**Website certificate expires in 21 days** The HTTPS certificate for www.example.com is set to expire on November 24, 2026.	After that date, browsers will warn visitors that the site is not secure. People may hesitate to use a form or pay a bill.	Renew the certificate with your website host or domain registrar, and turn on auto-renew if they offer it. This is the first thing I would do. I'll recheck as soon as you tell me it's renewed.
HIGH	**Two staff emails appeared in a known data breach** leasing@example.com and books@example.com appeared in a publicly catalogued credential leak (Have I Been Pwned). Example data only — not a named real breach or company.	Those passwords may already be in circulation. If either one was reused on a business email, website admin, bank or property-software account, someone could try it.	Change those two passwords now, and any other account that shared them. Turn on multi-factor authentication. I cannot remove leaked data from the internet — no one can.
MEDIUM	**No SPF or DMARC on example.com** I did not find SPF or DMARC records. DKIM was also not published.	Anyone can send email that looks like it came from your domain. For a property business, that can look like a fake rent invoice or a fake wiring instruction.	Add an SPF record that lists only your real mail service, then a DMARC record starting with p=none. I can send the exact records once I know your mail provider.
MEDIUM	**The site is running an outdated plugin** The site appears to use an older "Example Booking Form" plugin, version 3.2. Generic example only; not a real product or vulnerability ID.	Outdated plugins are a common way websites get defaced or used to send spam. This does not mean the site has already been broken into.	Update the plugin in your site admin, or ask the person who maintains the site to do it, then tell me and I'll recheck next month.
MEDIUM	**Unused remote-management port was reachable** Found on the quarterly vulnerability assessment of remote.example.com. I did not try to exploit it.	That gives strangers a door to knock on, even if a login is still required.	Close that port at the firewall, or restrict it to a short list of known IP addresses. I'll recheck on the next quarterly scan, or sooner if you want.
LOW	**Common security headers are missing** www.example.com did not send a Content-Security-Policy, a click-jacking protection header (frame-ancestors or X-Frame-Options), or HSTS.	These headers help browsers block some types of attacks. Missing them is a hardening gap, not a sign of an active incident.	Add the headers in your host or CDN settings. I can send the exact lines to paste.

Phishing practice test

I sent one safe practice email to the approved list of 12 people. **3 of 12** opened the test link, and **1** entered a made-up password on the practice page. I do not collect real passwords.

This is for coaching, not punishment. I'll share a short refresher with everyone. Next month's test will use a different scenario.

Policy checklist

Quarterly review: **8 of 12** starter items are already in place. Two I'd work on next: there is no short written rule yet for passwords and multi-factor authentication, and backups are being made but I did not see a restore test in the last 90 days.

This is a practical aid based on free public guidance (CISA, NIST Cybersecurity Framework, FTC small business guidance). It is not legal advice, an audit or a certification.

What's next month

I'll recheck the certificate, email records, plugin, headers and that open port after you've had time to fix them. Breach monitoring stays on. I'll run the next monthly phishing test with a new scenario. The next quarterly vulnerability assessment is due in January 2027 (example date).

If I see something urgent before then, I'll email you right away.

A few important limits. This sample uses a fictional business and made-up data. On a real report, findings reflect only what I could see at a point in time, inside the signed scope. Results are not a compliance certification, and no check can find every issue or make a business "unhackable." I do not promise that.

All testing requires your written authorization and a signed scope first. © 2026 Flintlatch. This page is a fictional sample for review and is not published.