

Lumen Courier Inc.: where you stand, and what to fix first

A fixed-scope review of the five areas attackers try first. Read-only, non-intrusive, completed in two weeks.

Organization	Size	Review period	Prepared by
Lumen Courier Inc. (fictional)	38 staff · 41 accounts	Oct 5–16, 2026	Mikhaël Esterez

OVERALL

Needs attention

Four high-risk issues give an attacker a realistic way in today. **All four can be fixed within a month, and three of them in under a day.** Nothing suggests an active intrusion.

4 High: fix this month

4 Medium: fix this quarter

2 Low: good practice

THE FIVE CHECKS

CHECK	RESULT	IN ONE LINE
Internet exposure	HIGH	Remote Desktop and an outdated VPN are reachable from the internet
Email and domain	MEDIUM	Anyone can send email that looks like it comes from your domain
Microsoft 365	HIGH	6 accounts, including an administrator, have no second factor
Leaked passwords	HIGH	3 staff passwords were captured by password-stealing malware
The basics	MEDIUM	3 of 13 national baseline controls fully met; backups never restore-tested

TOP THREE RISKS, PLAINLY

- 1 Your office server answers anyone on the internet.**
Exposed Remote Desktop is a common way ransomware gets in.
- 2 A stolen password is enough** for 6 Microsoft 365 accounts, one of them an administrator.
- 3 Three employees' passwords are already in criminal hands.** Treat those accounts and their computers as compromised.

DO THIS MONTH

- ☐ Close Remote Desktop to the internet; reach it through the VPN with a second factor
- ☐ Update the VPN firmware
- ☐ Turn on multi-factor authentication for every account
- ☐ Reset the three exposed passwords and check those computers

Full ranked list of fixes on page 5.

WORKING WELL Microsoft Defender runs on every laptop, laptops update automatically, nightly backups run, USB storage is blocked, and the website uses HTTPS with a current certificate. These are good foundations to build on.

Scope and how we worked

LUMEN COURIER INC.

WHAT WAS IN SCOPE

AREA	SCOPE
Domain	lumen-courier.example and its subdomains
Internet-facing addresses	203.0.113.10 to 203.0.113.24 (15 addresses, confirmed by the client)
Microsoft 365	One tenant, 41 accounts (36 users, 5 shared mailboxes), read-only access granted for the review
Interview	One hour with the office manager and the external IT provider
Authorization	Signed by the president on Oct 3, 2026: non-intrusive checks only, no exploitation

THE FIVE CHECKS

CHECK	WHAT WE DID
01 Internet exposure	Found everything reachable from the internet (subdomains, addresses, open services), then checked versions, encryption and known vulnerabilities. Each result was confirmed by hand.
02 Email and domain	Checked the records that stop others sending email in your name (SPF, DKIM, DMARC) and encryption of mail in transit (MTA-STS).
03 Microsoft 365	Compared the tenant to recognized baselines (CISA SCuBA, Microsoft Secure Score), then reviewed MFA coverage, admin roles, forwarding rules and sharing settings.
04 Leaked passwords	Searched breach data and infostealer intelligence for accounts on your domain. We report accounts and dates only; we never retrieve or use passwords.
05 The basics	Interview against the Canadian Centre for Cyber Security's baseline controls for small and medium organizations.

HOW TO READ THE RESULTS

RATING	MEANING	FIX BY
HIGH	Realistic way in for an attacker, with serious impact	This month
MEDIUM	Raises the chance or the damage of an incident	This quarter
LOW	Good practice; limited risk on its own	When convenient

LIMITS This is a point-in-time review, not a penetration test: nothing was exploited, the internal network was not scanned, and web applications were not tested. A clean result in one area does not guarantee that area is secure. Findings reflect what was visible between Oct 5 and Oct 16, 2026.

Findings (1 of 2)

RANKED BY RISK

HC-01 Remote Desktop is reachable from the internet

HIGH

WHAT WE FOUND

Remote Desktop (RDP) answers on the office file server from anywhere on the internet.

203.0.113.14:3389 open · Windows Server 2012 R2

WHY IT MATTERS

Attackers scan the whole internet for open RDP and try stolen or guessed passwords. It is a common entry point for ransomware.

HOW TO FIX

Block port 3389 at the firewall. Staff who need the server connect through the VPN with a second factor.

Effort: ~1 hour · IT provider

HC-02 VPN firmware has an actively exploited vulnerability

HIGH

WHAT WE FOUND

The VPN login page reports a FortiOS version affected by CVE-2024-21762, listed by CISA as exploited in the wild.

vpn.lumen-courier.example · FortiOS 7.0.x

WHY IT MATTERS

The flaw can let an attacker run code on the VPN device without a password, giving a foothold inside the network.

HOW TO FIX

Update to the vendor's fixed version, then review VPN logs since the issue was published for unknown logins.

Effort: ~2 hours · IT provider

HC-03 6 of 41 Microsoft 365 accounts have no second factor

HIGH

WHAT WE FOUND

Multi-factor authentication is not enforced. Six accounts never registered a second factor, including one Global Administrator.

6/41 without MFA · 1 of 3 Global Admins

WHY IT MATTERS

For these accounts a phished or leaked password is all an attacker needs, and the admin account controls the whole tenant.

HOW TO FIX

Enforce MFA for everyone (Security Defaults or Conditional Access). Give admins a separate account used only for admin work.

Effort: ~2 hours · IT provider

HC-04 3 staff passwords captured by password-stealing malware

HIGH

WHAT WE FOUND

Three company accounts appear in infostealer logs collected between June and September 2026. Usernames are listed in the confidential appendix given to the president.

3 accounts · source: infostealer intelligence

WHY IT MATTERS

Infostealers also copy browser sessions, so attackers may get in even without the password. The infected computers may still be compromised.

HOW TO FIX

Reset the three passwords, sign out all sessions, and check or reinstall the computers they were used on. MFA (HC-03) limits the damage.

Effort: ~3 hours · IT provider + staff

HC-05 Your domain can be spoofed in email

MEDIUM

WHAT WE FOUND

DMARC is set to monitor only and SPF ends in a soft fail, so receiving servers deliver forged email.

_dmarc: p=none · SPF: ~all · no MTA-STS

WHY IT MATTERS

Fake invoices or payment-change requests that look like they come from your team are the start of most invoice fraud.

HOW TO FIX

Review DMARC reports for two weeks, move to p=quarantine, then p=reject. Change SPF to ~all.

Effort: ~1 hour over 4 weeks · IT provider

Findings (2 of 2)

RANKED BY RISK

HC-06 Two mailboxes forward all email to outside addresses

MEDIUM

WHAT WE FOUND

Two mailboxes have rules forwarding every message to personal webmail accounts. External forwarding is allowed for the whole tenant.

2 rules · tenant setting: external forwarding on

WHY IT MATTERS

Client and payment information leaves the company unprotected. Attackers also create forwarding rules to watch for invoices.

HOW TO FIX

Confirm with the two users, remove the rules, and block automatic external forwarding for everyone.

Effort: ~30 minutes · IT provider

HC-07 File server runs an unsupported Windows version

MEDIUM

WHAT WE FOUND

The file server runs Windows Server 2012 R2, which stopped receiving security updates in October 2023.

FS01 · Windows Server 2012 R2

WHY IT MATTERS

New vulnerabilities in it will never be fixed, and it holds the company's shared files.

HOW TO FIX

Plan a replacement (newer server or SharePoint). Until then, keep it off the internet (HC-01) and limit who can reach it.

Effort: project · owner + IT provider

HC-08 Backups have never been restore-tested and have no offline copy

MEDIUM

WHAT WE FOUND

Nightly backups go to a storage device on the same network. Nobody remembers a restore test.

Interview · NAS on office network

WHY IT MATTERS

Ransomware usually encrypts or deletes reachable backups first. An untested backup may not work when it's needed.

HOW TO FIX

Add an offline or immutable cloud copy. Test a restore every quarter and write down how long it took.

Effort: ~1 day · IT provider

HC-09 Files are shared with "anyone with the link", without expiry

LOW

WHAT WE FOUND

27 active links to SharePoint and OneDrive files work for anyone who has them, and never expire.

27 anonymous links · no expiry policy

WHY IT MATTERS

A forwarded or leaked link exposes the file to anyone, with no record of who opened it.

HOW TO FIX

Default sharing to people in the organization; require expiry (e.g. 30 days) for external links; review the 27.

Effort: ~1 hour · IT provider

HC-10 No written plan for a cyber incident

LOW

WHAT WE FOUND

No incident plan exists, and staff weren't sure who to call or what to do first.

Interview

WHY IT MATTERS

The first hour decides how much an incident costs. Insurers also ask for a plan.

HOW TO FIX

Write a one-page plan: who decides, who to call (IT, insurer, lawyer), what not to touch. Privateer's free first-hour card is a starting point.

Effort: ~2 hours · owner

Your top 10 fixes, in order

IMPACT FIRST, THEN EFFORT

THE PLAN

	FIX	FINDING	EFFORT	WHO	WHEN
01	Block Remote Desktop from the internet	HC-01	1 h	IT provider	Week 1
02	Reset the 3 exposed accounts, sign out sessions, check their computers	HC-04	3 h	IT + staff	Week 1
03	Enforce MFA for every account; separate admin accounts	HC-03	2 h	IT provider	Week 1
04	Update the VPN firmware and review its logs	HC-02	2 h	IT provider	Week 1
05	Remove the 2 forwarding rules; block external forwarding	HC-06	30 min	IT provider	Week 2
06	Move DMARC to quarantine, then reject; SPF to -all	HC-05	1 h	IT provider	Month 1
07	Add an offline backup copy and test a restore	HC-08	1 day	IT provider	Month 1
08	Limit "anyone" links and require expiry	HC-09	1 h	IT provider	Month 1
09	Write a one-page incident plan	HC-10	2 h	Owner	Month 1
10	Plan the file server replacement	HC-07	Project	Owner + IT	Quarter

WEEK 1 Fixes 1 to 4 take about **8 hours of IT work** in total and close all four high-risk issues. Most small IT providers can do them in a single visit.

AFTER THE FIXES

Re-check (optional). Once the week-1 fixes are done, a short re-check confirms they work as intended and updates this report.

Your insurer and clients. Page 1 can be shared with your insurer or a client asking about your security. Pages 3–5 are best kept internal.

Going further. If you want to know what an attacker could actually do with what we found, a penetration test is the next step. Health Check clients get 10% off it when it's booked within 60 days.

The basics: national baseline controls

CANADIAN CENTRE FOR CYBER SECURITY

SCORECARD · 3 MET · 7 PARTLY MET · 3 NOT MET

	CONTROL	STATUS	WHAT WE SAW
01	Incident response plan	NOT MET	No written plan (HC-10)
02	Automatic patching	PARTLY	Laptops update automatically; VPN and server do not (HC-02, HC-07)
03	Security software	MET	Microsoft Defender active on all laptops
04	Secure configuration	PARTLY	Defaults mostly hardened; RDP exposed (HC-01)
05	Strong authentication	NOT MET	MFA not enforced (HC-03)
06	Awareness training	PARTLY	Covered at onboarding only
07	Backup and encryption	PARTLY	Backups exist; no offline copy, never tested (HC-08)
08	Secure mobility	PARTLY	Company phones have a PIN; not centrally managed
09	Perimeter defences	NOT MET	RDP and a vulnerable VPN reachable (HC-01, HC-02)
10	Cloud and outsourced IT	PARTLY	IT provider contract has no security clauses
11	Secure websites	MET	Website on HTTPS with a current certificate
12	Access control	PARTLY	Admin account used for daily work
13	Portable media	MET	USB storage blocked by policy

APPENDIX · TOOLS AND TERMS

Tools used: certificate transparency logs, subfinder, httpx, nmap (authorized addresses only), nuclei, testssl.sh, checkdmarc, CISA ScubaGear, Microsoft Secure Score, breach and infostealer intelligence. All results were confirmed by hand.

MFA: a second proof of identity after the password. **DMARC:** tells mail servers what to do with forged email. **RDP:** remote access to a Windows computer.

Infostealer: malware that copies saved passwords and browser sessions.

Want this for your organization?

Fixed price, read-only, report in two weeks. English or French.