P U L S E

MONTHLY SECURITY POSTURE REPORT

PREPARED FOR	Maple Crest Accounting LLP (fictional demonstration client)
ENVIRONMENT	Microsoft 365 Business Premium · 28 users · 31 devices
REPORTING PERIOD	Monthly — trailing 30 days
REVIEWED BY	Senior Incident Responder, Cyber Elixir Inc.
CLASSIFICATION	Confidential — prepared exclusively for the client

READ-ONLY ACCESS · NOTHING INSTALLED · FIRST MONTH FREE — CYBERELIXIR.CA

// SECTION 01

Executive Summary

B

POSTURE GRADE

↑ FROM B– LAST MONTH

THE WIN

MFA enforcement reached 25 of 28 staff this month — the single biggest risk reducer available to a firm your size, and it's nearly closed.

THE RISK

Three accounts — including one partner — still sign in without MFA, and attackers targeted your firm with 41 phishing emails this month, several impersonating the CRA.

THE ACTION

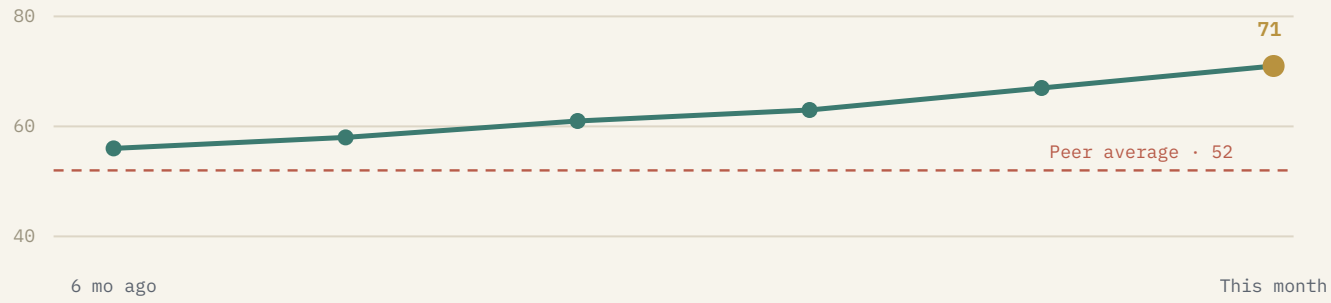
Enable MFA for the final three accounts and disable legacy IMAP authentication. Both fit inside one hour of IT effort and would lift next month's grade to A–.

F EXPOSED	D	C TYPICAL SMB	**B HARDER THAN AVERAGE**	A HOSTILE TERRITORY

// SECTION 02

Posture Score & Trend

Your Microsoft Secure Score measures how well the security features you already own are configured. This month it rose to **71%** — your sixth consecutive month of improvement, and now well above the average for organizations of similar size (52%).



TRAILING SIX MONTHS · SOURCE: MICROSOFT SECURE SCORE, GRAPH SECURITY API · PEER AVERAGE: ORGANIZATIONS OF 25–50 SEATS

// SECTION 03

Threats We Saw This Month

4	4	219	0
ALERTS RAISED	RESOLVED / CONTAINED	THREATS AUTO-BLOCKED	ACTIVE INCIDENTS

SEVERITY	WHAT DEFENDER CALLED IT	WHAT ACTUALLY HAPPENED	OUTCOME
MEDIUM	Suspicious inbox forwarding rule	A rule was created on a staff mailbox forwarding invoices to an external Gmail address — a classic precursor to invoice fraud. Created by the user themselves for a legitimate reason, but risky practice.	Rule removed; staff briefed
MEDIUM	Atypical travel sign-in	A partner's account signed in from Calgary 40 minutes after a Toronto sign-in. Verified legitimate — the partner was travelling and used hotel Wi-Fi plus a phone hotspot.	Verified legitimate
LOW	Malware detected & quarantined	A trojan downloader arrived inside a fake "court notice" PDF. Defender quarantined it on arrival; the user never opened it.	Quarantined automatically
LOW	Password spray attempt	An external IP tried common passwords against five of your mailboxes overnight. All attempts failed; the source was blocked.	Blocked; no access

PLAIN-ENGLISH TAKEAWAY

Nothing got through this month. The forwarding-rule finding is the one to remember: invoice-redirect fraud is the most common way accounting firms actually lose money, and the controls that stop it are configuration, not luck.

// SECTION 04

Identity Risk

25/28	3	1	2
USERS WITH MFA	USERS WITHOUT MFA	LEGACY PROTOCOL OPEN	RISKY SIGN-INS REVIEWED

ACCOUNT	GAP	WHY IT MATTERS
j.kowalski@ (Partner)	No MFA enrolled	Partner mailboxes are the #1 target for CRA-impersonation and invoice fraud.
reception@ (Shared)	No MFA enrolled	Shared mailboxes with passwords are routinely sprayed; this one was targeted this month.
d.tremblay@	No MFA enrolled	Seasonal staff account left enabled after contract end — disable or protect.
IMAP (tenant-wide)	Legacy auth enabled	IMAP ignores MFA entirely — it's the side door that makes the front-door lock irrelevant.

PLAIN-ENGLISH TAKEAWAY

Every gap on this page is closable in a single afternoon, and one of them was actively probed this month. These three accounts are your entire remaining identity exposure — after them, an attacker needs to beat MFA, not just guess a password.

// SECTION 05

Device Health

27/31	3	1	0
DEVICES FULLY PATCHED	MISSING CRITICAL UPDATES	NOT REPORTING (DARK)	UNSUPPORTED OS

DEVICE	EXPOSURE	PLAIN ENGLISH
MC-LT-014	Chrome — 2 critical CVEs	Browser is 6 weeks out of date; these flaws are actively exploited via malicious websites. A restart completes the fix.
MC-LT-007	Windows — latest cumulative missing	Laptop has dodged its update window twice. Schedule a forced restart.
MC-DT-003	Adobe Reader outdated	For a firm that opens client PDFs all day, PDF-reader flaws are a direct path in.
MC-LT-019	Offline 23 days	Device hasn't checked in for 23 days — likely a drawer laptop. Locate it or wipe and retire it; lost devices holding client files are a privacy-breach risk.

PLAIN-ENGLISH TAKEAWAY

Patching is the quiet hero of your posture — 27 of 31 machines are current without anyone thinking about it. The four above are named, specific, and fixable this week; the dark laptop is the only one that needs a decision rather than a restart.

// SECTION 06

Email Threat Picture

41	7	3	0
PHISHING BLOCKED	MALWARE ATTACHMENTS	CRA IMPERSONATIONS	REPORTED CLICKS

Attackers aimed most heavily at the people who handle money and client onboarding — a pattern, not a coincidence:

MOST-TARGETED PEOPLE	ATTEMPTS	DOMINANT LURE
Accounts payable clerk	14	Fake supplier "updated banking details" requests
Managing partner	11	CRA notice-of-assessment impersonations
Reception / intake	8	Malicious "new client documents" attachments

SEASONAL CONTEXT

CRA impersonation tracks the tax calendar — phishing against Ontario accounting firms spikes around filing deadlines and stays elevated for months afterward, as attackers exploit clients expecting CRA correspondence. Your three most-targeted staff would benefit from a 15-minute briefing — we include one in your monthly review.

// SECTION 07

The Fix-First Five

Ranked by risk reduced per hour of effort. Items 1–2 close the gaps attackers actually probed this month.

1. **Enrol the final three accounts in MFA**
   j.kowalski, reception, d.tremblay. One of these was password-sprayed this month — the attacker is already knocking.
   RISK REDUCED: HIGH EFFORT: 30 MIN

2. **Disable legacy IMAP authentication tenant-wide**
   Closes the protocol that bypasses MFA entirely. We verified no legitimate application in your environment still uses it.
   RISK REDUCED: HIGH EFFORT: 15 MIN

3. **Disable the seasonal-staff account**
   d.tremblay's contract ended months ago; dormant enabled accounts are how attackers persist unnoticed.
   RISK REDUCED: MEDIUM EFFORT: 5 MIN

4. **Patch the three exposed devices and resolve MC-LT-019**
   Forced restart window for the laptops; locate-or-wipe decision for the device that's been dark for 23 days.
   RISK REDUCED: MEDIUM EFFORT: 1–2 HRS

5. **Add an external-sender warning banner**
   A one-line banner on outside email measurably blunts the supplier-banking-change fraud your AP clerk is being targeted with.
   RISK REDUCED: MEDIUM EFFORT: 20 MIN

// LAST MONTH'S ITEMS

Enable Defender attack-surface reduction rules in block mode	DONE
Remove two stale global-administrator accounts	DONE
Enrol remaining staff in MFA (3 of 6 completed)	CARRIED → ITEM 1

// SECTION 08 — ANALYST'S NOTE

Where You Stand

Your trend line is the story this month: six straight months of improvement, and the remaining gaps are small, named, and cheap to close. What I want on your radar for next month is the CRA-impersonation wave — your partners' inboxes are where that fight happens, which is exactly why item 1 leads the list. Close items 1 and 2 and your firm moves from "harder than average to breach" to "genuinely hostile territory for an attacker." That's a real place to be, and you're an hour of IT work away from it.

— SENIOR INCIDENT RESPONDER · CYBER ELIXIR INC.

Your monthly review

We walk this report with you every month — this time we'll also brief your three most-targeted staff and set next month's priorities. Your coordinator will propose times this week.