LOTUS SECURITY

EXECUTIVE CYBER RISK & THREAT INTELLIGENCE AUDIT

Report ID: LS-2026-0813-SAMPLE
Date: August 13, 2026
Contact: lotusaidrop@gmail.com

Target Domain: example.com (Fictional Sample)

Company Name: Apex Legal Partners LLP (Fictional)

Service Tier: Basic Executive Audit ($295)

Mail Provider: Google Workspace

Scope: Passive External OSINT Scan

Staff Emails Checked: 10 Addresses

54/100
GRADE D
HIGH EXPOSURE

Executive Risk Overview

Apex Legal Partners LLP demonstrates critical email domain spoofing vulnerabilities and staff dark-web password leaks. Immediate remediation is required to prevent wire fraud and account takeover.

Critical Finding: Missing DMARC enforcement allows cybercriminals to impersonate attorneys via @example.com emails. 3 staff emails were also identified in historical public breach databases.

CORE EXPOSURE METRIC BREAKDOWN

1. Email Authentication & Spoofing Defense

30/100 — CRITICAL RISK

- **DMARC Record:** **INACTIVE / WEAK (p=none)** — Domain monitoring mode only. Offers ZERO protection against domain spoofing or wire fraud impersonation.
- **SPF Record:** **SOFTFAIL (v=spf1 include:_spf.google.com ~all)** — Unauthorized sending servers are permitted to attempt delivery.
- **DKIM Configuration:** **VERIFIED** — Active 1024-bit Google cryptographic key present.
- **Business Impact:** Attackers can send fake invoices or settlement wire instructions directly from @example.com to firm clients.

2. Employee Dark Web Credential Exposure

55/100 — MODERATE RISK

- **Staff Accounts Scanned:** 10 Primary Addresses | **Exposed Accounts:** 3 Flagged (30% Compromise Rate)
- **Exposed Accounts & Sources:**
  - `j.apex@example.com` (Managing Partner) — 4 Breaches (Historic Third-Party Vendor Dumps) [Passwords Leaked]
  - `billing@example.com` — 2 Breaches (Historic Third-Party Marketing Leaks)
  - `paralegal@example.com` — 1 Breach (Historic Cloud Storage Leak)
- **Business Impact:** Credential stuffing risk. If employees reuse passwords across work and personal accounts, firm email is vulnerable to account takeover.

3. Infrastructure & Domain Security Integrity

80/100 — LOW RISK

- **Domain Age & Health:** Established domain history. Excellent domain reputation score.
- **DNS & Mail Routing:** Properly routed Google Workspace MX records. No unauthorized DNS modifications detected.
- **Public Information Leakage:** WHOIS privacy shield enabled; no sensitive administrative contact phone numbers exposed publicly.

3-STEP IT REMEDIATION CHECKLIST

STEP 1: IMMEDIATE PRIORITY (Execute within 24–48 Hours) — BLOCK SPOOFING

Task: Upgrade DMARC DNS Record Policy from p=none to p=quarantine or p=reject.

Current TXT Record at `_dmarc.example.com`:

```
v=DMARC1; p=none; rua=mailto:dmarc@example.com
```

Recommended Updated DNS TXT Record:

```
v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@example.com;
```

Expected Business Impact: Instructs Gmail and Outlook to quarantine or reject spoofed emails claiming to be from @example.com, instantly eliminating domain wire fraud risk.

STEP 2: HIGH PRIORITY (Execute within 7 Days) — CREDENTIAL HARDENING

Task: Mandatory Password Reset & Multi-Factor Authentication (MFA) Audit for Compromised Accounts.

- Force immediate password reset for `j.apex@`, `billing@`, and `paralegal@` email accounts.
- Enforce mandatory Google Workspace 2-Step Verification (MFA) for all firm users.
- Deploy a firm-wide password manager (e.g., 1Password / Bitwarden) to prevent personal browser password saving.

Expected Business Impact: Neutralizes leaked breach credentials and blocks automated account takeover attempts.

STEP 3: MEDIUM PRIORITY (Execute within 14 Days) — SPF POLISHING

Task: Harden SPF Record from Softfail (`~all`) to Strict Fail (`-all`).

Recommended Updated SPF Record at `example.com`:

```
v=spf1 include:_spf.google.com -all
```

Expected Business Impact: Guarantees that only authorized Google Workspace servers can transmit emails for your practice.

EXECUTIVE SUMMARY & ACTIONABLE TAKEAWAY

Addressing the DMARC record gap (Step 1) requires less than 15 minutes of DNS configuration by your webmaster and immediately eliminates domain spoofing risks. Combined with MFA enforcement for compromised emails (Step 2), firm external cyber risk drops by over 85%.

Lotus Security | B2B Cyber Risk & Threat Intelligence Audits | Contact: lotusaidrop@gmail.com