SAMPLE DELIVERABLE · PRE-SALES SECURITY ASSESSMENT

You are already exposed.

A public-signal review of ridgewaydistribution.ca revealed 7 critical, 4 high, and 3 medium findings within 30 minutes of the intake form being submitted. No credentials were used. No systems were touched. This is what an attacker sees before deciding you are worth targeting.

7	4	3	1
CRITICAL	HIGH	MEDIUM	CONTROLS OK

PREPARED FOR	SCOPE	STATUS
Ridgeway Distribution Co.	External + stated internal	HIGH RISK
(fictional prospect · sample)	Preliminary, no intrusive testing	Composite posture 2.1 / 5.0

PREPARED BY

North Star IT Services Ltd.

Keegan Martin, Owner · keegan@northstarit.ca

SAMPLE NOTICE. This document is a sanitized illustration of the pre-sales security assessment North Star prepares for prospects. The organization (Ridgeway Distribution Co.), domain (ridgewaydistribution.ca), findings, and dollar figures shown are constructed for demonstration. A real assessment reflects the requester's actual environment and observed technical signals.

01

Executive summary

The headline read for leadership. What we found, how bad it is, what it would cost you, and what the engagement to fix it looks like.

EXECUTIVE SUMMARY

Ridgeway is one email away from a bad week.

Ridgeway Distribution Co. requested a preliminary security review through our free-assessment page. This report combines the requester's stated environment with publicly observable technical signals for ridgewaydistribution.ca, benchmarked against the CIS Controls v8 baseline that North Star runs on every managed client. No internal access was used and no systems were tested intrusively. Every finding below is reproducible by an attacker with a laptop and a coffee break.

Risk scorecard

Domain	Score	Rating	Headline finding
Identity & access	2 / 5	HIGH RISK	MFA not enforced tenant-wide. No Conditional Access. Contractors on personal email.
Email trust & anti-phish	1 / 5	CRITICAL	DMARC absent, DKIM absent, SPF soft-fails. Your domain is spoofable right now.
Endpoint & device	2 / 5	HIGH RISK	BYOD contractors, no MDM, no verified encryption, inconsistent EDR coverage.
Backup & recovery	2 / 5	HIGH RISK	No independent M365 backup. Ransomware or an insider deletes SharePoint and it stays gone.
Network & perimeter	3 / 5	MEDIUM	Public hosting control panel exposed. No documented segmentation between office and warehouse.
Data governance	2 / 5	HIGH RISK	PIPEDA-regulated data handled without formal classification or IR plan.
Detection & response	1 / 5	CRITICAL	No SIEM. No log retention beyond 90 days. No named incident-response arrangement.

Composite posture: 2.1 / 5.0 · HIGH RISK. Scoring rubric follows CIS Controls v8 Implementation Group 1 minimums for organizations of this size.

Top 5 risks to close now

01	Domain impersonation. Any attacker can send email that appears to come from `@ridgewaydistribution.ca`. Direct path to invoice fraud and vendor payment redirection.
02	Credential theft with no MFA net. A single phished password grants full mailbox access, including customer pricing and employee PII.
03	Unmanaged contractor devices. Company data on personal laptops with no encryption, patching, or EDR. One lost laptop is a notifiable breach under PIPEDA.
04	No independent M365 backup. Ransomware or a malicious insider can wipe SharePoint and mailboxes within Microsoft's retention window with no clean restore point.
05	No incident-response plan. During a live breach, hours matter. There is no named team, no pre-approved containment authority, and no evidence retention.

RECOMMENDED ENGAGEMENT

How we would close the gap

For an organization of this size and risk profile, we recommend a fixed-fee onboarding project followed by an ongoing monthly managed service. The onboarding phase closes every critical and high-risk item in this report. Ongoing service keeps them closed, adds monitoring, and gives you a named team when the next incident lands.

Phase	Duration	What is delivered	Type
Phase 0 · Discovery	1 week	30-minute assessment call, tenant read-only audit, device inventory, existing-tools review, refined scope and firm quote.	No cost
Phase 1 · Stabilize	30 days	DMARC + DKIM + SPF hardening, tenant-wide MFA + Conditional Access, password-manager rollout, external attack-surface lockdown.	Fixed fee
Phase 2 · Foundation	60-90 days	Contractor identity cleanup, MDM + endpoint baseline, independent M365 backup, advanced email security, data-handling guardrails.	Fixed fee
Phase 3 · Managed	Ongoing	24/7 monitoring, patching, backup verification, quarterly security reviews, named IR team, annual re-assessment.	Monthly

Specific pricing is quoted after Phase 0 discovery so we are not guessing at seat counts, contractor arrangements, or existing tools you may already own. Typical engagements of this size fall in the $8,000 to $15,000 one-time range for Phases 1-2, plus a monthly managed-service tier scoped to user count.

Standards our baseline aligns to

CIS Controls v8	Implementation Group 1 minimums across all 18 controls, with IG2 hardening on identity, email, and endpoint.
PIPEDA	Reasonable safeguards, breach-notification readiness, and record-keeping duties for Canadian private-sector organizations.
Cyber insurance	Common carrier prerequisites: MFA, EDR, offline/immutable backup, email security, and IR retainer.
Microsoft Secure Score	Target >= 65% after Phase 1, >= 80% after Phase 2 (industry median for SMB tenants: 42%).

02

External findings

What an attacker sees when they type ridgewaydistribution.ca into their tools. DNS records, email authentication, hosting exposure, certificates, breach corpora. Reproducible from any laptop with an internet connection.

EMAIL AUTHENTICATION

Your domain is spoofable today.

Email authentication is the single highest-leverage control for an SMB. It costs nothing beyond DNS changes, stops the most common attack path (business email compromise), and is a hard requirement for every cyber insurance policy in market today. Ridgeway currently fails on the two most important records.

Observed DNS records

Record	Observed value (RDATA)	Status
MX	`ridgewaydistribution-ca.mail.protection.outlook.com. (pref 0)`	OK
SPF	`"v=spf1 include:spf.protection.outlook.com ~all"`	WEAK
DMARC	`(no _dmarc.ridgewaydistribution.ca record)`	CRITICAL
DKIM	`(no selector1/selector2 CNAME to onmicrosoft.com)`	CRITICAL
MTA-STS	`(no _mta-sts TXT, no mta-sts.ridgewaydistribution.ca policy)`	MISSING
TLS-RPT	`(no _smtp._tls TXT)`	MISSING
DNSSEC	`Not signed (parent zone .ca allows it)`	MISSING
CAA	`(no CAA records; any CA can issue certs for the domain)`	MISSING

Queried against ridgewaydistribution.ca on the report date. TTLs range 300-3600s.

What each finding means in dollars

SPF soft-fail (~all)	Recipients are told to accept-but-flag mail from unauthorized senders. Modern mailbox providers still deliver these messages, often to inbox. Tighten to -all once DKIM and DMARC are aligned.
DMARC absent	No policy tells recipient mail servers what to do with spoofed messages. Attackers can send email that appears to come from `finance@`, `procurement@`, or ownership addresses with high delivery success. This is the direct path to invoice-fraud and payroll-diversion attacks that cost Canadian SMBs a median of $70,000 per incident (CAFC 2025).
DKIM absent	Mail is not cryptographically signed by the sending server. Even when DMARC is added later, it has nothing to align against on the DKIM side, weakening the policy to SPF-only enforcement.
MTA-STS / TLS-RPT missing	Inbound mail can be delivered over downgraded TLS. Passive network attackers on a compromised upstream can capture invoices, contracts, and pricing in transit.
DNSSEC unsigned	Anyone controlling a resolver in the path can forge DNS answers for ridgewaydistribution.ca. Fix is a one-time registrar step at Ridgeway's .ca provider.
CAA absent	Any certificate authority can issue a valid TLS cert for the domain. A CAA record restricts issuance to Ridgeway's chosen CAs, blocking impersonation via mis-issued certs.

WEB & HOSTING EXPOSURE

Public-facing surface

External review of ridgewaydistribution.ca web presence, TLS configuration, and hosting infrastructure. Findings shape the risk of website defacement, credential-stuffing on admin panels, and TLS downgrade attacks.

Area	Observed	Status	Recommendation
Web server	Apache 2.4.x on shared hosting (banner suppressed but fingerprintable)	INFO	Acceptable for a brochure site. Move admin to VPN or IP-restrict.
TLS version	TLS 1.2 and 1.3 only, TLS 1.0/1.1 disabled	GOOD	Maintain. Add HSTS preload once the site is stable.
Cert issuer	Let's Encrypt, 90-day validity, auto-renewed	GOOD	Add CAA records to restrict issuance to Let's Encrypt only.
HSTS	Missing (Strict-Transport-Security header not present)	MEDIUM	Add max-age=31536000, includeSubDomains, preload.
Security headers	Missing: CSP, X-Content-Type-Options, Referrer-Policy, Permissions-Policy	MEDIUM	Baseline security header set via web-server config or CDN.
Hosting panel	cpanel.ridgewaydistribution.ca reachable on public internet, port 2083	HIGH	IP-allowlist or move behind VPN. Rotate the panel password.
Directory listing	/backup/ and /old/ return 200 with index (no sensitive files observed)	MEDIUM	Disable Options +Indexes. Remove stale directories.
Admin login	wp-login.php reachable, no rate limiting observed on 10 test attempts	HIGH	Rate-limit, MFA the WP admin, or move to WAF (Cloudflare rules).

Passive breach exposure

Six email addresses on `@ridgewaydistribution.ca` appear in one or more historical breach corpora (LinkedIn 2021, Dropbox 2016, and a 2023 marketing-tool breach). Two of those are executive addresses. Without enforced MFA on the tenant, any reused password is a live account-takeover risk today.

03

Stated environment

The environment as described by the requester on the intake form. Not verified against internal systems. Presented so leadership can confirm our understanding matches reality before deeper work begins.

STATED ENVIRONMENT

What the requester told us

Organization snapshot

Business	Regional B2B distributor of industrial supplies. Founded 2011.
Locations	Head office (Kelowna, BC), branch (Prince George, BC), branch (Calgary, AB). One shared warehouse per branch.
Headcount	~35 total: 22 employees on payroll, ~13 contractors and drivers, seasonal peak +6.
Data at risk	Customer records, vendor terms, negotiated price lists, quoting history, employee PII, payroll data, banking details.
Regulated data	PIPEDA-regulated personal information. Payment card data handled via a hosted gateway (no PAN storage claimed).
Compliance drivers	Cyber insurance renewal in 4 months. One enterprise customer has begun sending vendor security questionnaires.

Current tooling and gaps

Domain	What is in place	What is missing
Identity	M365 Business Standard, ~35 licenses. Global admin on one account (owner).	MFA not enforced. No Conditional Access. No break-glass account. No PIM.
Endpoint	Windows 11 on ~20 laptops. Defender basic. Warehouse workstations on Windows 10.	No MDM (Intune not deployed). No BitLocker enforcement. No EDR beyond default. Win10 devices past support.
Email	M365 Exchange Online. Anti-spam at defaults.	No anti-phishing tuning. No impersonation protection. No safe-links / safe-attachments.
Backup	SharePoint version history, OneDrive recycle bin.	No independent third-party M365 backup. No air-gapped or immutable copy. No verified restore test.
Network	Consumer-grade firewalls at each branch (mixed brands). Guest wifi separate at HO only.	No documented segmentation. No VPN for remote access. No IDS/IPS. No logging retention.
Contractors	Ad-hoc access via shared folders and personal email.	No identity governance. No offboarding process. No audit trail.
Detection	Default M365 audit log only (90-day retention on Business Standard).	No SIEM. No long-term log retention. No alerting. No documented IR runbook.

THREAT SCENARIO · HOW THIS ENDS

30 days from the intake form.

The following is not hypothetical fear-mongering. It is a step-by-step reconstruction of how a common SMB compromise would unfold against Ridgeway's current posture. Every step below uses only techniques observed in real Canadian SMB breach reports in the last 18 months. Timeline is compressed to 30 days because that is the median dwell time for BEC campaigns targeting Canadian SMBs.

DAY 0 Reconnaissance

Attacker enumerates ridgewaydistribution.ca via public sources. LinkedIn identifies the controller and 3 procurement staff. The domain has no DMARC. One executive's password was exposed in the 2023 marketing-tool breach.

What stops this: DMARC enforcement, tenant-wide MFA, dark-web credential monitoring.

DAY 1 Spoofed invoice

Attacker sends an invoice from ap@ridgewaydistribution.ca to a real vendor, redirecting payment to an attacker-controlled account. Because there is no DMARC record, the mail lands in the vendor inbox with no warning.

What stops this: DMARC policy at p=reject, DKIM signing, vendor bank-change verification policy.

DAY 2 Credential harvest

Attacker phishes the controller with a fake M365 login page hosted on a look-alike domain. Controller enters credentials. No MFA is required. Attacker has full mailbox access within minutes.

What stops this: Tenant-wide MFA, Conditional Access blocking non-corporate IPs, advanced anti-phishing.

DAY 3–7 Inbox rules and lateral movement

Attacker creates hidden inbox rules to auto-forward finance mail and delete replies. Uses the compromised account to phish 3 additional staff, capturing procurement and shipping mailboxes.

What stops this: Impossible-travel detection, inbox-rule auditing, SIEM with M365 alerts.

DAY 14–30 Wire fraud and data theft

Attacker impersonates the controller to authorize a $47,000 wire to a new vendor account, and downloads the customer pricing spreadsheet from SharePoint. When Ridgeway notices, the attacker deletes the audit trail (retention is 90 days, no long-term SIEM).

What stops this: Segregation of duties on wire approvals, independent M365 backup, long-term log retention, IR retainer.

ESTIMATED FINANCIAL IMPACT

$47,000 direct wire loss · $12,000 IR + legal · $8,000 PIPEDA breach notification · $20-40,000 insurance premium increase at renewal · indeterminate reputational cost with the enterprise customer running vendor questionnaires.

Median Canadian SMB BEC loss: $70,000. Median dwell time before detection: 18 days. Source: Canadian Anti-Fraud Centre 2025 statistics.

04

Remediation roadmap

Every finding mapped to a concrete remediation item with effort estimate, impact, and dependency ordering. Sequenced so the highest-impact fixes ship first.

REMEDIATION ROADMAP

Prioritized remediation items

#	Item	Effort	Impact	Phase	CIS v8
R-01	Publish DKIM selectors for M365 (selector1, selector2) and enable signing in Exchange Online.	S	CRITICAL	P1	9.5
R-02	Publish DMARC record at p=none with rua/ruf reporting. Monitor 2 weeks. Move to p=quarantine, then p=reject.	S	CRITICAL	P1	9.5
R-03	Tighten SPF to -all after DKIM + DMARC alignment confirmed.	XS	HIGH	P1	9.5
R-04	Enable tenant-wide MFA via Security Defaults or Conditional Access. Enforce for all users including contractors.	S	CRITICAL	P1	6.5
R-05	Conditional Access baseline: block legacy auth, require MFA outside trusted IPs, block high-risk sign-ins.	M	HIGH	P1	6.7
R-06	Roll out 1Password Business or Bitwarden Teams. Migrate shared credentials. Retire browser-saved passwords.	M	HIGH	P1	5.2
R-07	IP-allowlist cpanel.ridgewaydistribution.ca or move behind VPN. Rotate panel and WP admin passwords.	S	HIGH	P1	4.5
R-08	Add security headers (HSTS, CSP baseline, X-Content-Type-Options, Referrer-Policy) to the marketing site.	S	MED	P1	16.10
R-09	Deploy Intune MDM. Enrol all Windows devices. Enforce BitLocker + Defender for Endpoint P1.	L	CRITICAL	P2	10.1, 3.6
R-10	Retire Windows 10 warehouse workstations or move to Win 10 IoT LTSC. Document EOL replacement plan.	M	HIGH	P2	2.2
R-11	Deploy Datto Backupify (or equivalent) for M365: Exchange, OneDrive, SharePoint, Teams. Verify 3 restore tests.	M	CRITICAL	P2	11.1-11.4
R-12	Deploy Defender for Office 365 P1: safe-links, safe-attachments, anti-phishing + impersonation protection.	S	HIGH	P2	9.6
R-13	Contractor identity cleanup: guest accounts or cheapest licensed tier, MFA-required, off-boarding SOP.	M	HIGH	P2	5.1, 6.2
R-14	Network segmentation review. Replace consumer firewalls with managed UniFi or Fortinet. Document VLANs.	L	MED	P2	12.2
R-15	Stand up centralized logging (Microsoft Sentinel or equivalent) with 12-month retention.	L	HIGH	P2	8.1-8.11

#	Item	Effort	Impact	Phase	CIS v8
R-16	Data classification policy. Label pricing, PII, financial data. DLP rules in Exchange + SharePoint.	M	MED	P2	3.7, 3.12
R-17	Named incident-response arrangement with 4-hour response SLA. Annual tabletop exercise.	S	HIGH	P3	17.1-17.9
R-18	Quarterly security review + Secure Score reporting to leadership.	S	MED	P3	18.1
R-19	Annual third-party re-assessment against CIS Controls v8 IG1.	M	MED	P3	18.5

Effort scale: XS = <2h, S = 2-8h, M = 1-3 days, L = 4-10 days. Impact reflects risk reduction in Ridgeway's context. CIS v8 column references the Center for Internet Security Controls v8 safeguard number.

APPENDIX

Method, references, next step

A · Method & scope

This preliminary assessment was produced from: (1) intake form data submitted by the requester on the assessment date, (2) public DNS record queries (MX, SPF, DMARC, DKIM, MTA-STS, TLS-RPT, DNSSEC, CAA), (3) HTTP header and TLS handshake inspection of the requester's public web presence, (4) passive review of publicly indexed content and directory listings, and (5) public breach-corpus lookup for email addresses on the requester's primary domain. No internal access was granted or used. No credentials were tested, no vulnerabilities were exploited, and no intrusive scanning was performed.

A full assessment following signature of a mutual NDA and scoping agreement would validate these findings from inside the environment and add: authenticated M365 tenant audit, endpoint posture review, network topology and firewall configuration review, backup restore test, phishing simulation, and interview-based process review.

B · Reference standards

CIS Controls v8	Center for Internet Security. Safeguards referenced throughout the remediation table map to CIS v8 numbering.
NIST CSF 2.0	Function mapping (Identify, Protect, Detect, Respond, Recover) available on request.
PIPEDA	Personal Information Protection and Electronic Documents Act. Applies to all Canadian private-sector organizations handling personal information in commercial activities.
Microsoft Secure Score	Microsoft's tenant-level security posture score. Recommendations aligned to score-improving actions.
CAFC 2025	Canadian Anti-Fraud Centre 2025 SMB fraud statistics. Business email compromise remains the top-loss category for Canadian businesses.

C · About North Star IT

North Star IT Services Ltd. is a Prince George, BC based managed services and security provider. We run a standard security baseline across every client (enforced MFA, advanced email security, independent M365 backup, endpoint protection, patch management, monitored backup and recovery) and we operate our own group of businesses on the same stack. Every recommendation in this report reflects controls we run in production, not theoretical guidance.

NEXT STEP

Book a 30-minute assessment call to validate these findings from inside your environment. No obligation, no pitch deck, no scripted sales process.

northstarit.ca · keegan@northstarit.ca