MN Risk Advisory
Cybersecurity, risk management, and vCISO support

Minnesota Business Technology & Email Security Snapshot

A public-signal review of 389 organization profiles, highlighting common DNS, email, vendor, and security-hardening patterns visible from outside the network.

389	148	4,161	498
organization profiles	unique providers	configuration findings	high-severity findings

Key message: public DNS and email records show that most organizations rely on mainstream cloud providers, but many still have basic hardening opportunities in certificate issuance, domain authentication, inbound mail TLS policy, and SPF/DMARC governance.

At-a-glance findings

Top DNS providers

Cloudflare DNS	**23.9%**
GoDaddy DNS	**19.3%**
Amazon Route 53	**5.9%**
Google Domains DNS	**3.6%**
Network Solutions	**3.6%**

Email services

Microsoft Exchange Online	**43.2%**
Unknown external mail	**34.7%**
Google Workspace	**8.7%**
Custom SPF include	**4.4%**
SendGrid	**3.9%**

Registrar signals

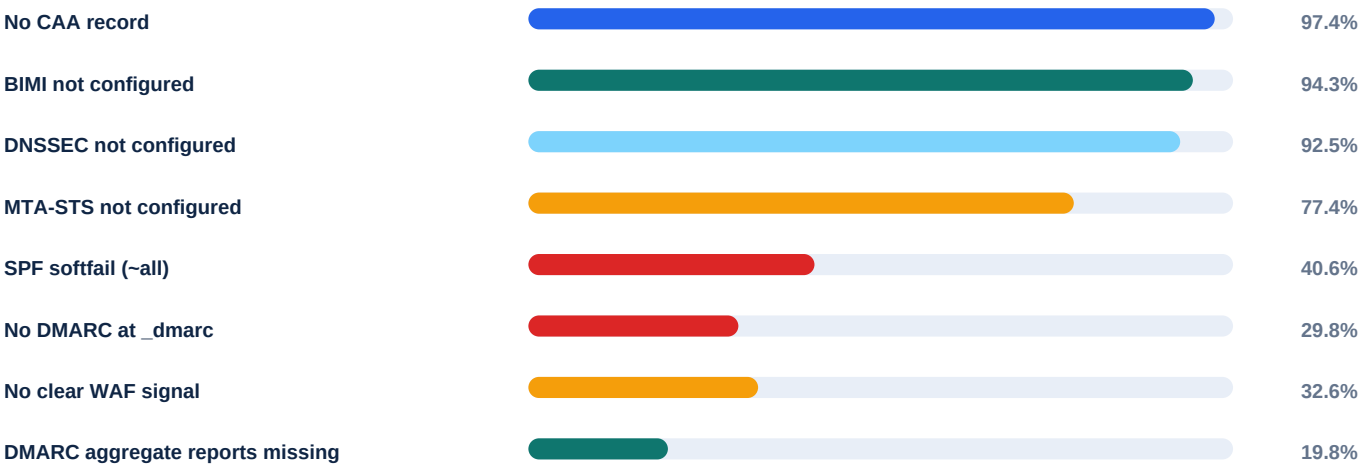
GoDaddy	**17.7%**
eNom	**14.1%**
Network Solutions	**13.9%**
Tucows	**5.4%**
Squarespace Domains	**4.6%**

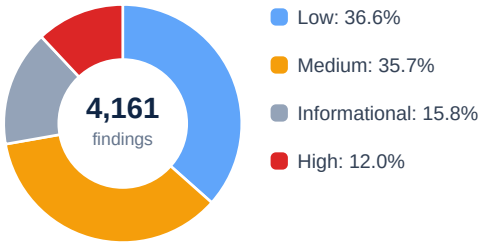
SaaS/vendor signals

Google verification	**37.8%**
Microsoft verification	**29.3%**
Meta/Facebook	**7.5%**
HubSpot	**3.6%**
KnowBe4	**3.1%**

Security-hardening gaps visible in public records

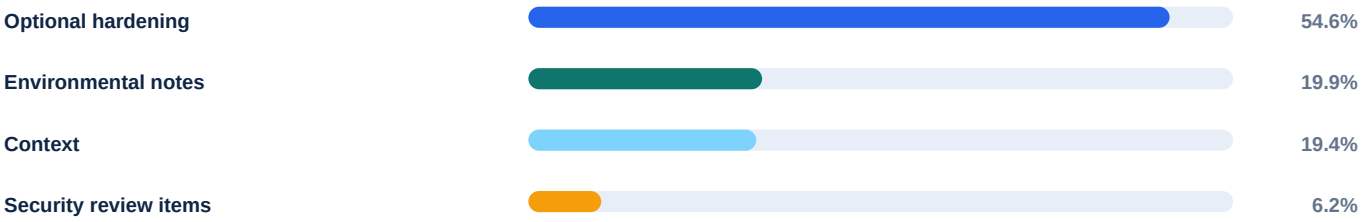
These findings are not breach claims. They are externally observable configuration signals that often indicate where an organization should review ownership, vendors, and policy maturity.





Severity mix: 12.0% of findings were high severity, while most findings were low or medium hardening and governance items. That is common in public DNS/email reviews: the goal is not panic, but a prioritized roadmap.

Most common review themes



What this means for small and mid-sized businesses

Theme	Finding	Practical action
Certificate issuance controls	97.4% had no CAA record.	Define which certificate authorities may issue certificates for your domain.
Email authentication maturity	40.6% used SPF softfail and 29.8% had no DMARC record.	Validate legitimate senders, publish DMARC reporting, then move toward stronger enforcement.
Inbound mail transport policy	77.4% had no MTA-STS signal in this scan.	Consider MTA-STS and TLS reporting where mail flow and provider support make it practical.
DNS integrity hardening	92.5% had no DNSSEC signal.	Evaluate DNSSEC with your DNS provider, registrar, and operational recovery process.
Vendor sprawl	148 unique providers appeared across the dataset.	Maintain an owner-approved list of DNS, email, SaaS, and sending services.

Recommended 30-day review plan

- Inventory DNS hosting, registrar, email platform, and third-party senders.
- Publish or validate SPF, DKIM, and DMARC records; enable aggregate reporting.
- Review CAA, MTA-STS/TLS-RPT, and DNSSEC applicability with current providers.
- Remove stale SPF includes and unknown third-party sending services.
- Assign a business owner for DNS/email changes and require change documentation.

Important caveat: Public records do not show every internal control. A missing signal may be intentional, unsupported by a provider, or mitigated elsewhere. Treat this as a starting point for review, not a final security rating.

Methodology and scope

The snapshot summarized 389 valid customer profile JSON files. Counts are unique organizations per provider/category per file, even when a provider appears more than once in a record. Categories were derived from vendor category strings and public DNS/vendor fingerprints.

This is a public-signal review: DNS, email, verification, registrar, vendor, and externally visible configuration patterns. It is separate from vulnerability scanning and does not imply a breach or confirmed exploitable condition.

Dataset summary

Files reviewed	389
Valid JSON files	389
Skipped files	0
Unique providers	148
Customers with at least one finding	389 / 389
Total configuration findings	4,161
High-severity findings	498

Need help interpreting your records?
MN Risk Advisory helps small and mid-sized businesses understand cybersecurity risk, prioritize what matters, and make practical security decisions without replacing the existing IT provider.

mnrisk.com/contact