ENDPOINT SOLUTIONS

Technology Leadership Assessment — Delivery Report

NORTHSHORE
REALTY GROUP

Client: Northshore Realty Group

Date: June 20, 2026

Prepared by: Michael-Paul Hart, Endpoint Solutions

ENDPOINT SOLUTIONS

NORTHSHORE
REALTY GROUP

ENDPOINT SOLUTIONS

Technology Leadership Assessment — Delivery Report

Client: Northshore Realty Group · Date: June 20, 2026 · Prepared by: Michael-Paul Hart

OVERALL MATURITY

30

Reactive

Combined maturity across the assessed stages.

ENGAGEMENT

Industry: Real Estate — Residential Brokerage
Primary sponsor: Grant Mills — Broker/Owner

Executive summary

Northshore Realty Group is a successful residential brokerage whose agents move fast and win business — but the brokerage's technology and, more importantly, its security have not kept pace with the money and sensitive data flowing through it. Agents operate as independent contractors on their own phones and laptops, client and transaction data is scattered across personal devices and inboxes, and there is no internal IT owner or governance.

The single most serious exposure is wire fraud: real estate is the top target for business email compromise, and Northshore's inconsistent email security, missing MFA, and informal closing communications leave clients' funds and the brokerage's reputation at real risk. Close behind is the sprawl of client data across unmanaged agent devices. Neither is difficult or expensive to address, and doing so is also a differentiator with clients. This report lays out a prioritized plan that fits how a brokerage actually operates.

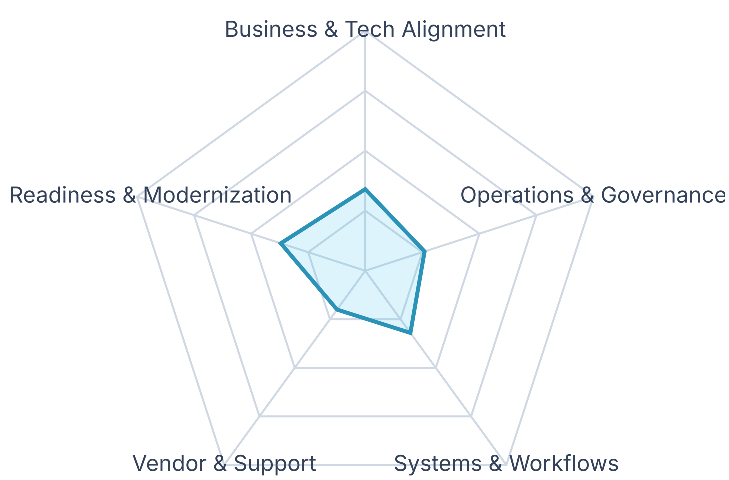
Current-state overview

Northshore's agents work largely on personal devices with a mix of the MLS, a CRM, a transaction-management platform, e-signature, and email — much of it adopted agent by agent. Staff use Microsoft 365 (mostly for email) and QuickBooks. There is no managed IT provider, no internal owner, and no device management: brokerage and client data lives on agents' personal phones and laptops and in personal inboxes. MFA is inconsistent, email security is minimal, and closing and wire communications happen over ordinary email. There is no central view of the tools agents use, what the brokerage pays, or where client data resides, and backups of shared brokerage data are informal.

Maturity scorecard

STAGE	SCORE	INTERPRETATION
01 Business & Tech Alignment	34%	Reactive
02 Operations & Governance	26%	Reactive
03 Systems & Workflows	32%	Reactive
04 Vendor & Support	20%	Reactive
05 AI Readiness & Modernization	37%	Reactive

Maturity profile



Top findings & business implications

1. **High wire-fraud / business-email-compromise exposure at closings.** — Real estate is the leading BEC target; with minimal email security and informal wire communications, a single compromised or spoofed email could divert a client's funds — a catastrophic financial and reputational risk.
2. **Client and transaction data lives on agents' personal, unmanaged devices.** — Lost or compromised agent devices expose client personal and financial information the brokerage is responsible for, with no way to control or recover it.
3. **No internal IT owner, governance, or device management.** — Security and technology decisions have no home; the brokerage cannot enforce even basic protections across its agents.
4. **Inconsistent MFA and minimal email security.** — Account compromise — the entry point for wire fraud and data theft — is far more likely than it should be.
5. **No visibility into agent tools, spend, or where client data resides.** — The brokerage cannot see its cost, its risk, or its obligations across a fragmented, agent-driven toolset.

Domain observations

01 · BUSINESS & TECH ALIGNMENT — 34%

Leadership is focused on recruiting agents and closing deals, and technology is viewed as each agent's own affair. There is little visibility into how technology and security support (or endanger) the brokerage, and no plan connecting them to growth or risk.

02 · OPERATIONS & GOVERNANCE — 26%

This is a weak area. There is no internal or external IT owner, no governance, and no leadership reporting — technology and security are entirely reactive. For a business moving client funds and handling personal financial data, the absence of any security governance is a serious gap.

03 · SYSTEMS & WORKFLOWS — 32%

Agents adopt tools individually, so the MLS, CRM, transaction platform, and e-signature are disconnected and client data is scattered across personal devices and inboxes. Microsoft 365 is barely used beyond email, there is no device management, and continuity for shared brokerage data is unproven.

04 · VENDOR & SUPPORT — 20%

Vendor and tool management is essentially absent: agent-by-agent adoption, unclear support, no view of spend, and no renewal tracking. Establishing a baseline brokerage toolset and a basic vendor inventory would reduce both cost and risk.

05 · AI READINESS & MODERNIZATION — 37%

Agents already use consumer AI informally for listing descriptions and marketing, with no policy — a modest data risk today and an opportunity later. As with everything here, guardrails and security come first; AI for marketing and transaction support is a fast follow once the foundations exist.

Risk register

RISK	AREA	SEVERITY	OWNER
Wire fraud / business email compromise at closings — funds diversion	Operations & Governance	Critical	Broker/Owner
Client and transaction data on unmanaged agent personal devices	Systems & Workflows	Critical	Broker/Owner
Inconsistent MFA and minimal email security	Operations & Governance	High	Office Manager
No internal owner, governance, or device management	Operations & Governance	High	Broker/Owner
No visibility into agent tools, spend, or client-data location	Vendor & Support	Medium	Finance

Recommended priorities

02 · OPERATIONS & GOVERNANCE

Shut down wire-fraud exposure at closings

Harden email security (MFA, anti-spoofing, impersonation protection), adopt verified closing/wire communication procedures, and train agents and staff — the single highest-value protection for clients and the brokerage.

03 · SYSTEMS & WORKFLOWS

Protect client data across agent devices

Put basic device management and secure, managed storage in place so client and transaction data is protected and recoverable even on agents' personal devices.

02 · OPERATIONS & GOVERNANCE

Establish an IT owner and baseline security governance

Engage managed IT and name an internal owner so the brokerage can enforce baseline protections and has a home for security decisions and incidents.

04 · VENDOR & SUPPORT

Define a baseline brokerage toolset and vendor inventory

Standardize a core, integrated toolset for agents and inventory tools and spend, reducing sprawl, cost, and where client data can scatter.

Technology leadership roadmap

0–30 days

ACTION	OWNER	PRIORITY	EFFORT
Harden email security (MFA, anti-spoofing, impersonation protection) Outcome: Sharp reduction in wire-fraud and account-compromise risk · Vendor: Endpoint Solutions	Managed IT	High	Medium
Adopt verified wire/closing communication procedures and train everyone Outcome: Client funds protected at the most dangerous moment · Vendor: Endpoint Solutions	Broker/Owner	High	Low
Engage managed IT and name an internal technology owner Outcome: A home for security decisions and enforcement · Vendor: Endpoint Solutions	Broker/Owner	High	Medium

31–90 days

ACTION	OWNER	PRIORITY	EFFORT
Deploy basic device management and managed, backed-up storage Outcome: Client data protected and recoverable across devices · Vendor: Microsoft 365 · Depends on: IT engaged	Managed IT	High	Medium
Inventory agent tools, spend, and where client data resides Outcome: First view of cost, risk, and data location · Vendor: Endpoint Solutions	Finance	Medium	Medium
Run security-awareness training focused on wire fraud Outcome: Agents recognize and stop fraud attempts · Vendor: Endpoint Solutions	Office Manager	High	Low

91–180 days

ACTION	OWNER	PRIORITY	EFFORT
Standardize a core, integrated brokerage toolset for agents Outcome: Less sprawl and fewer places client data scatters · Vendor: Software vendors · Depends on: Tool inventory	Technology owner	Medium	High
Adopt secure, tracked client document exchange to replace email Outcome: Safer transaction documents and an audit trail · Vendor: Transaction platform	Office Manager	Medium	Medium

181–365 days

ACTION	OWNER	PRIORITY	EFFORT
Publish an AI acceptable-use policy for client and transaction data Outcome: Safe use of AI for marketing and listings · Vendor: Endpoint Solutions	Broker/Owner	Medium	Low

ACTION	OWNER	PRIORITY	EFFORT
Establish a simple quarterly technology & security review Outcome: Ongoing oversight of risk and spend	Broker/Owner	Low	Low

Vendor & support ecosystem

VENDOR	ROLE / COVERAGE	RENEWAL / NOTES
(No managed IT provider)	Agent-by-agent, ad-hoc support	None
Regional MLS	Listing service	Annual dues
kvCORE CRM (assorted agent plans)	Lead & client management — adopted per agent	Various
Dotloop / transaction platform	Transaction management & e-signature	01/2027
Microsoft 365 (Business Basic)	Email — mostly unused beyond mail	05/2027
QuickBooks Online	Brokerage finance & commissions	Monthly

Documentation reviewed: Software / application list · Device count / inventory · Employee count by role or location · Known projects, issues, or planned purchases

Evidence notes: No managed IT agreement, security policy, or wire-fraud/closing procedure exists — all findings given the brokerage's exposure. There is no inventory of agent tools or of where client data resides, which should be built as a first step. Cyber and errors-and-omissions coverage should be reviewed against the wire-fraud exposure identified here.

Renewal & contract calendar

RENEWAL	VENDOR	ROLE / COVERAGE
01/2027	Dotloop / transaction platform	Transaction management & e-signature
05/2027	Microsoft 365 (Business Basic)	Email — mostly unused beyond mail
None	(No managed IT provider)	Agent-by-agent, ad-hoc support
Annual dues	Regional MLS	Listing service
Various	kvCORE CRM (assorted agent plans)	Lead & client management — adopted per agent
Monthly	QuickBooks Online	Brokerage finance & commissions

Next steps

1. Review this report with leadership and confirm the priorities.
2. Assign owners and target dates to the roadmap actions.
3. Decide where ongoing technology advisory support is appropriate.

Appendix — discovery responses

01 · Business & Tech Alignment

Does technology clearly support your business strategy?	Somewhat
Leadership visibility into technology	Blind spots
Confidence making technology decisions	Some
Is there a technology plan tied to business goals?	None

02 · Operations & Governance

Is ownership of systems and risks clear?	Partly
Is IT reactive or governed?	Reactive
How are tech decisions made?	Ad-hoc
Leadership gets regular technology reporting?	Never

03 · Systems & Workflows

How much do tools or workflows slow people down?	Somewhat
Are core systems integrated?	Siloed
Microsoft 365 used to its potential?	Barely
Confidence in continuity if a key system fails	Low

04 · Vendor & Support

Is it clear who covers what for support?	Unclear
Visibility into total technology spend	None
Are vendors aligned to business needs?	No
Awareness of upcoming contracts or renewals	None

05 · AI Readiness & Modernization

Are employees using AI tools today?	Some, informal
AI acceptable-use policy?	None
Identified automation opportunities?	A few ideas
Is your data ready to support AI?	Not ready

How scoring works

Each answer maps to a 0–100 maturity value based on what it signals. Stage scores are the average of the answered, scored questions in that stage; the overall score is the average of assessed stages. Some questions are informational context and are not scored. Bands: Strategic 80+ · Governed 60+ · Developing 40+ · Reactive 20+ · Ad-hoc 0+.

Prepared by Endpoint Solutions for client leadership review. For the cleanest PDF, turn browser print dialog **Headers and footers** off.