

SEPTEMBER 25, 2026 | PUBLICATION

Client Resource: Selling Your Business? Data Privacy and Cyber Due Diligence Could Make or Break the Deal

If you are considering selling your business, you are probably thinking about financial statements, customer contracts, and employee matters. But there is another area that today's buyers scrutinize closely, and it can derail a deal or significantly reduce your purchase price: your **data privacy and cybersecurity** posture.

What Buyers Are Looking For

Modern acquirers treat cyber due diligence with the same rigor they apply to financial audits. A buyer's diligence team will typically request your written privacy policies (both internal and

customer-facing), a description of every category of personal information you collect and store, a list of every vendor or software platform that touches that data, and evidence that you have contracts, specifically data processing agreements, governing how those vendors handle it.

Buyers will also want to know which privacy and security laws apply to your operations, whether you have conducted any security risk assessments or audits, and whether you have ever experienced a data breach or received a regulatory inquiry. If you cannot answer these questions clearly, the buyer sees risk, which gets priced into the deal or, worse, kills it.

Why It Matters More Than Ever

The regulatory landscape has expanded dramatically. Even a small Florida business may be subject to the Florida Information Protection Act's 30-day breach notification requirement, the Payment Card Industry Data Security Standard (PCI DSS) if it processes credit cards, and potentially the Federal Trade Commission's (FTC) Safeguards Rule if it handles consumer financial information. Buyers know that inheriting a company's data also means inheriting its compliance gaps and breach exposure. A single undisclosed incident or a

INDUSTRY SECTOR

Technology

SERVICE LINE

Corporate, Tax & Transactions
Technology, Data Privacy,
Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

missing security program can become a post-closing indemnification claim.

How Sellers Can Prepare

Start early. Well before you go to market, take these steps:

- **Audit your data inventory.** Know what personal information you collect, where it lives, and who has access.
- **Review your vendor agreements.** Confirm you have written contracts addressing data security with every third-party platform that processes personal data on your behalf.
- **Update your privacy policies.** Ensure your external privacy notice actually reflects your business operations, not just a boilerplate template.
- **Document your security practices.** Even if you lack a formal certification, write down what you do: access controls, encryption, employee training, and incident response procedures.
- **Confirm your breach history.** Be prepared to affirmatively represent whether you have experienced any incidents.

A clean data privacy and cybersecurity profile signals to buyers that your business is well managed and low risk. The time to address these issues is before a buyer's diligence team starts asking—not after. If you would like to learn more about Data Privacy or Cybersecurity, check out the Shumaker Digital Risk Report.

Jade Davis is a partner at Shumaker, advising clients on technology, data privacy, cybersecurity, and artificial intelligence in mergers & acquisitions (M&A), incidents, investigations, and general counsel. She can be reached at jadavis@shumaker.com.