

Managed IT Blind Spots

They will put your office technology dealership at risk

by: Jonathan Blakey, Technology Assurance Group (TAG)

There is an uncomfortable reality many office technology dealers do not want to admit: A surprising number of dealerships are one neglected IT process away from a catastrophic business interruption. And the scary part? Most owners would never see it coming. Why? Because most successful office technology dealers are not deeply technical.

Once a dealer hires an IT manager to run his (or her) managed IT services division, he assumes the basics are being handled properly. But “assuming” and “verifying” are two very different things. And in managed IT, the basics are everything — one forgotten process, one unchecked backup or one compromised account is all it takes.

There was a recent case where an office technology dealership delivering managed IT services “assumed” backups were functioning correctly — until ransomware hit one of its clients. When the dealership employees attempted to restore the environment, they discovered the backups had not actually been working properly.

The client’s systems were locked. Operations stopped. The business was crippled. And the client may go out of business.

That kind of failure does not just hurt the customer. It can destroy reputations overnight. So if you are an office technology dealer selling managed IT services, these are the kinds of mistakes that can put your dealership out of business.

When a client trusts you with his technology infrastructure, he trusts you with the operational heartbeat of his business. If you are not obsessively focused on the fundamentals of properly running a managed IT services business, your client does not have an IT strategy. He has a liability.

Here are the bottom-line fundamentals every office technology dealer offering managed IT services should verify regularly. If a prospective client’s provider is not doing these



things, it is your way into a sales conversation.

(1) Backups are not enough. You must verify they actually work — One of the biggest misconceptions in managed IT is believing that “having backups” means you are protected. It does not. A backup that has not been verified is just a theory. Many organizations discover this the hard way after ransomware, accidental deletion, hardware failure or a cyberattack. They assume their systems are recoverable — until they actually try restoring them. That is why mature IT organizations do not just run backups; they constantly test them.

Office technology dealership owners should be asking questions like:

- “Are backups being checked and how frequently?”
- “Are backup reports being reviewed by leadership?”
- “When was the last time we did a full restore to a virtual environment to prove recovery actually works for all of our customers?”

If those conversations are not happening in your business,

that is a major red flag. Because when disaster strikes, “We thought it was backing up” is not a strategy.

Here is a useful question to ask your IT manager: “When was the last time we fully test-restored our customer backups — and could they confidently get their businesses operational again if something catastrophic happened tomorrow?” That question tends to separate providers that simply run backups from those that actually verify business continuity.

(2) Weak multifactor authentication (MFA) policies are leaving the front door open — Many cyberattacks do not begin with sophisticated hacking. They begin with a stolen password. That is why MFA has become one of the most important baseline protections in modern IT environments. And, yet, many office technology dealerships have not implemented MFA on all of their customers’ IT networks.

Sometimes MFA is enabled for email but not remote access. Sometimes executives bypass it because it is “inconvenient.” Sometimes legacy systems are left exposed. Those gaps matter because cybercriminals do not need every door unlocked. They only need one.

For office technology dealers, this is especially important because your business is likely to have access to:

- Customer data
- Financial information
- Device credentials
- Admin access across multiple environments
- Sensitive employee information

A compromised customer could quickly become a compromise across your client base. That is why strong MFA policies should not be optional. They should be nonnegotiable.

A useful question to ask your IT manager: “Are all of our managed IT services accounts leveraging MFA?” That question alone can reveal a lot.

(3) If your managed IT services team members are not talking strategy, they are probably just reacting — Most office technology dealerships’ IT service departments spend all day putting out fires — tickets, password resets, printer issues, software problems, etc. But great IT leaders do not just react to problems, they prepare customers for what is coming next.

Your IT leadership team members should be conducting strategic business reviews with your accounts, and discussing strategy and customer objectives. If those strategic conversations never happen, your dealership may be stuck in reactive mode instead of building a long-term technology road map. That becomes dangerous very quickly in an industry evolving as quickly as managed IT. A useful question to ask is:

Your IT leadership team members should be conducting strategic business reviews with your accounts, and discussing strategy and customer objectives.

“How often are we meeting with customers to discuss a strategic technology plan for the next year?”

Are You Checking the Boxes?

The question many office technology dealership owners eventually need to ask themselves: “Are these basics truly being handled — or am I simply assuming they are?”

Many owners hand technology responsibility to their IT managers and trust that everything is covered. But trust without verification can create blind spots, and those blind spots can put customers and, ultimately, you, out of business. Some internal IT team members become very good at sounding technical without consistently executing basic operational disciplines that keep businesses protected. The fundamentals may not be flashy, but they are what keep companies operational.

No Basics, No Business

Managed IT is not just another revenue stream for office technology dealerships anymore. It has become a foundational part of the dealership business model. And with that opportunity comes responsibility. Because when clients trust you with their technology, they trust you with:

- Their operations
- Their productivity
- Their customer data
- Their financial systems
- Their reputations
- Their livelihoods

It is very easy for your IT manager to skip the basics. If you do not ask, you do not know. You are the leader and ultimately responsible and liable, not your IT manager. The office technology dealerships that will thrive in managed IT services in the coming years have already made a commitment to implementing sound IT processes, cybersecurity protocols, achieving compliance like ISO 27001 and HIPAA, and ensuring their customers’ IT environments are checked consistently. Those that do not have already put their dealerships at risk. ■

Jonathan Blakey is vice president of technology at Technology Assurance Group (TAG).

He is responsible for driving the implementation of operational best practices, adoption of new technology and enhancing service delivery.

Blakey can be reached at jonathan@tagnational.com. Visit www.tagnational.com.

