MDR, the Human Component to Cybersecurity

By Richard Preston, Preston Office Solutions

As the owner of Preston Office Solutions, I spend a lot of time talking with business owners about cybersecurity. One thing I hear often is, "We're a small business in a small city. Are we really at risk?" Because our city is smaller, it's easy to assume cybercriminals are focused elsewhere. But make no mistake. If your business is connected to the World Wide Web, it doesn't matter where you're located or how big your company is. Your network is visible, reachable, and vulnerable.

Many businesses believe they're protected because they've invested in cybersecurity tools like firewalls, antivirus software, and multi-factor logins. Those tools are important, but on their own, they're not enough. Most of today's security solutions do one main thing: they send alerts. And without someone actively watching, understanding, and responding to those alerts, real threats can go unnoticed.

That's where Managed Detection and Response, or MDR, becomes the most important piece of cybersecurity. In my experience, MDR isn't just another layer of protection; it's what makes all the other tools actually work. MDR adds trained cybersecurity professionals who are watching your systems around the clock and responding the moment something looks suspicious.

Cybercriminals don't usually succeed because businesses have no security at all. They succeed because alerts get missed, delayed, or misunderstood. Hackers overwhelm systems with activity and wait for someone to slip up. MDR prevents that by putting real people in charge of detection, investigation, and response before small issues turn into major incidents.

I often compare cybersecurity to playing chess. Technology and automation are powerful, but without human strategy, you're always reacting instead of staying ahead. MDR combines advanced technology with experienced professionals who know how attackers think and how to shut them down. When hackers realize a business is actively monitored, they move on to easier targets.

This matters even more for businesses in smaller cities, like ours. The idea that "we're too small to be noticed" is one of the biggest risks out there. Cyberattacks aren't targeted by location. They're automated, constant, and global. MDR ensures someone is always watching your business, no matter the time of day or night.

With MDR in place, our team monitors devices, reviews alerts, investigates threats, and takes action immediately on behalf of our clients. Business owners don't have to guess what an alert means or scramble to respond. That responsibility is handled for them.

At the end of the day, cybersecurity isn't really about software. It's about response. MDR is the piece that turns tools into true protection. It allows business owners to focus on running and growing their company, knowing that experts are actively defending their systems behind the scenes. That's why, at Preston Office Solutions, we see MDR as the core benefit of modern cybersecurity—not an add-on, but the foundation.

Prosperity & Purpose

ABOUT THE AUTHOR

Richard Preston, owner and CEO of Preston Office Solutions in St. George, Utah, has been a trusted name in business technology for over forty years. Under his leadership, Preston Office Solutions has earned a solid reputation for exceptional sales, service, and support of office multifunction printers and large-format printing products across Southern Utah and southern Nevada. Preston Office Solutions is more than just a print solutions provider. As a dependable IT partner, the company delivers a comprehensive suite of technology products and services—all designed to support the success and growth of every client. To learn more, contact Preston Office Solutions at 435-628-2997 or visit www.prestonoffice.com.