Acture Solutions

What You Should Expect from a Managed IT Services Partner (MSP)

All businesses need an MSP.

No one is safe from data leaks and the resulting domino effect that buries unsuspecting organizations in lawsuits, ransomware payments, and identity theft.

If you're in any of the following industries:

- → K-12 School Districts
- → Higher Education
- → Healthcare
- → Legal
- → Financial Services
- → Small to medium-sized businesses (SMBs)

The time to act is NOW. Though all organizations need a quality MSP to safeguard their data, the industries above are prime targets for cybercriminals.

This is because education, healthcare, legal, and financial services are subject to more regulatory compliance requirements and have extremely sensitive data that is worth lots of money on the dark web.

Finding the right managed IT Services partner is essential to keeping your data and people secure.

Unfortunately, many businesses in the above industries don't invest in their tech. If you don't have an expert MSP partner, you're at high risk for a data breach or cyberattack and that could cost you BIG. You could lose your clients' trust, face heavy fines, or even be forced to shut down.

But where do you begin?

To avoid a cyber disaster, make sure that your chosen MSP is analyzing and optimizing these five areas within your organization:

- → Security
- → Ease of Use
- → Reliability
- → Accessibility
- → Technology Roadmap

Security

Is my tech safe to operate?

A good MSP should offer a multilayered cybersecurity plan based on the NIST Cybersecurity Framework. Please learn more about NIST here. By creating a cybersecurity plan designed for every level of your organization's infrastructure, your MSP will ensure high-level protection against common and complex threats from cybercriminals, such as ransomware and phishing. A multilayered cybersecurity plan is non-negotiable because each layer supports and strengthens one another. This means that if one fails, the next one is ready to defend.

Multilayered security programs typically include:

→ Endpoint Detection and Response

→ Full Managed Detection and Response

→ MFA (Multifactor Authentication)

→ Compliance maintenance

→ Real-time monitoring

→ Technology upgrades

→ Disaster Recovery and Incident Response Planning

→ Employee security awareness certifications

→ Identity and Access Management

→ Data management (least privileges and encryption)

→ Among others, depending on organizational risk tolerance

Ease of Use

Is my tech easy to understand and use?

All technology within your organization should be user-friendly, even for those who aren't the most tech-savvy.

A good MSP ensures all hardware and infrastructure are properly standardized, fully upgraded, documented, and streamlined. It may not seem like it, but a large component of cybersecurity is having up-to-date technology in the hands of the employees, not only for efficient productivity but for overall safety. Stale, outdated technology makes it easier for cybercriminals to hack in because it lacks the latest patches and upgrades.

Technology that's easy to use and accessible to everyone is a necessary precaution, especially as we move into the age of remote work. The extra assurance that your employees are safe to connect and work over their home Wi-fi only comes with up-to-date tech and cybersecurity practices.

Reliability

Is my tech doing what I need without breaking?

In the same breath as having technology that's understandable, it should also be reliable.

If it isn't, your MSP should be stepping in for the save.

Your MSP must ensure your tech works whenever you need it to, and if it doesn't, they should have a plan to get it back on track. Reliable tech isn't limited to the kind of computer you're using. Important apps that keep the business operating, such as payroll software and email clients, shouldn't be a hassle to use. Your MSP should be regularly patching your software, keeping your network connection stable and secure, and ensuring business hours are not wasted on troubleshooting your tech just to get through the day.

Accessibility

Can my tech accommodate everyone in my organization?

Your MSP should ensure all IT systems and environments are available whenever and wherever they're needed. Humans and technology are imperfect, so there should always be support readily available if there's an accident. In addition, your organization's tech should meet the needs of all your employees, regardless of any medical condition, language barriers, and other impairments.

If your employees can't access the necessary resources to be productive during business hours, then you're losing money. Ensuring accessibility with a proper MSP partner is well worth the investment to keep everyone productive and supported based on their needs.

Technology Roadmap to Success

Every organization should have a five-year technology roadmap. Technology roadmaps are used to help organizations review, understand, and improve the state of their IT, infrastructure, software, hardware, and IT procedures. Roadmaps can define how an organization's IT tools function, the proper procedure for using them, and what action steps to take should an emergency arise.

Your MSP's Virtual Chief Information Officer (vCIO) should be more than happy to explain how to use your technology as well as provide the data and insights to aid in your IT decision-making and budgeting processes. A technology roadmap is crucial in meeting long-term business goals and initiatives. Without one, you risk implementing costly, unexpected upgrades or being unprepared when faced with unforeseen circumstances.

Ready to get serious about your IT Services and security? Take an assessment to ensure you're on the right path forward.