

MONTHLY NEWSLETTER

MARCH 2025

TECH "KNOWLEDGY"

Why Are More Small And Medium-Sized Businesses Using Managed IT?

A newsletter article by Berry Solutions Group

In today's fast-changing digital landscape, small and medium-sized businesses (SMBs) are increasingly recognizing the value of managed IT services. While some SMBs have in-house IT staff or rely on a break-fix approach, many are turning to managed IT service providers (MSPs) for cost-effective solutions to their IT challenges. Managed IT services offer a comprehensive stack of network, data, device, and security management tools, along with expert IT professionals, all at a predictable monthly cost.

One of the key reasons SMBs are partnering with MSPs is to enhance their cybersecurity measures. MSPs assess the entire IT environment for vulnerabilities and implement robust cybersecurity measures, including the latest software, equipment, practices, policies, and employee security awareness training. This helps businesses stay compliant with ever-changing federal and state cybersecurity and privacy laws, as well as insurance requirements². Additionally, MSPs provide ongoing maintenance, strategic planning, and budgeting guidance for future IT investments, ensuring that businesses can quickly recover from disasters and minimize downtime.

By outsourcing their IT management, SMBs can save time, resources, and headaches associated with managing IT in-house. MSPs offer strategic business continuity and disaster recovery planning, ensuring that businesses have the necessary data backups and can quickly recover if disaster strikes. This allows business owners to focus on running their operations smoothly and efficiently, knowing that their IT environment is in capable hands.

Another significant advantage of managed IT services is the ability to monitor and maintain network performance continuously. MSPs establish systems to gain complete visibility into the IT network, tracking performance and identifying issues such as unusual network traffic, device configuration problems, DNS issues, or slow Wi-Fi. This proactive approach ensures that the IT environment runs smoothly and efficiently, allowing businesses to focus on their core operations.

Finally, managed IT services offer cost savings by providing a predictable monthly expense for comprehensive IT management. This eliminates the need for businesses to hire and maintain an in-house IT team, which can be costly and challenging to manage. With managed IT services, businesses can access a team of expert IT professionals who ensure that their technology infrastructure is up-to-date, secure, and aligned with their long-term business goals.

EMPLOYEE CELEBRATIONS & SPOTLIGHT



Stephen Cermak is the support team leader for BSG's Hagerstown office. He joined the company in 2023 and has used his passion for problem solving to quickly rise through the ranks and deliver the best possible IT service to clients!

Stephen studied classical history for the University of Maryland transfer program at Montgomery College. Prior to BSG, he was in the private sector for 10 years as a VP of a well-known home remodeling company in the Washington DC area but has since decided to turn his lifelong hobby of IT into a career!

Stephen is an avid hiker, gamer, and car enthusiast. On the weekends, he can often be found going on adventures with his dogs, Moo and Daisy. He is also a student pilot and hopes to obtain his private pilot's license soon!

March 14, 2025 marked Brandon Stephens's three-year anniversary with Berry Solutions Group. Thanks for everything you do, Brandon!



WELCOME OUR NEW EMPLOYEES



Nicholas Geedy

BSG IN TRAINING

With a brand-new year, BSG is jumping into brand-new opportunities to work with our partners and vendors. In February alone, BSG employees had the chance to attend three training sessions.

First being welcoming partners from Hubbell Incorporated, Wesco Anixter, and Reclamere for a day of insightful discussions on information technology and cybersecurity. Collaborating with industry leaders who understand the evolving challenges of IT security allows us to strengthen solutions and drive innovation in the field. We're proud to work alongside these outstanding partners to help businesses stay secure in today's digital landscape. We also had the pleasure of hosting our friends from Hubbell Incorporated a second time for an engaging Cable Certification training session!

Lastly we had the pleasure of hosting our partners from Motorola Solutions and Avigilon, strengthening our collaboration in advancing technology solutions. We appreciate their partnership and look forward to continuing our work together in the ever-evolving world of security and communications.

SECURITY CORNER

How Zero Trust Can Streamline NIST & CMMC Compliance For Your Business

The new U.S. Department of Defense (DoD) regulation is designed to confirm the existence and effectiveness of the cybersecurity measures used to protect federal contract information (FCI) and controlled unclassified information (CUI) by nongovernment entities. Adopting a Zero Trust architecture is one way businesses can satisfy many of the essential security requirements of CMMC 2.0, which went into effect on December 16, 2024. Zero Trust follows the mantra, "never trust, always verify." Rather than trust automatically and verify later, Zero Trust does away with the traditional implicit trust approach. Instead, it is centered around the notion that a breach has happened or will happen.

Under the new CMMC rule, federal contractors and their subcontractors must demonstrate exactly how they are safeguarding FCI and CUI within their organizations. CMMC is a federal regulation that heavily leans on the National Institute of Standards & Technology (NIST) framework, which provides a set of guidelines and essential security controls⁵. Businesses are split into three certification levels based on the type of information they handle: Level 1 (Foundational), Level 2 (Advanced), and Level 3 (Expert). Each CMMC tier has specific controls and assessment requirements needed for certification.

Zero Trust incorporates five pillars: identity, devices, applications, networks, and data. These core components help enforce the Zero Trust philosophy of trusting no one and nothing to protect your sensitive information and systems from malicious actors constantly looking for new ways to gain access. Because of the strong cybersecurity protections that are rolled into Zero Trust, businesses that establish a Zero Trust architecture will essentially satisfy many of the CMMC requirements for Level 1 assessments by default.

TECH TIPS & TRICKS

Tech Tips and Tricks

General Shortcuts:

- 💡 **Create a New Email:** Ctrl + N
- 💡 **Reply to an Email:** Ctrl + R
- 💡 **Reply All:** Ctrl + Shift + R
- 💡 **Forward an Email:** Ctrl + F
- 💡 **Send an Email:** Alt + S
- 💡 **Open Address Book:** Ctrl + Shift + B
- 💡 **Search:** Ctrl + E or F3
- 💡 **Mark as Read:** Ctrl + Q
- 💡 **Mark as Unread:** Ctrl + U
- 💡 **Delete an Email:** Delete
- 💡 **Open Calendar:** Ctrl + 2
- 💡 **Open Contacts:** Ctrl + 3
- 💡 **Open Tasks:** Ctrl + 4
- 💡 **Switch to Mail:** Ctrl + 1
- 💡 **Check for New Mail:** Ctrl + M or F9

