ADAMS BROWN
Technology Specialists
above+beyond

FAQS ON MANAGED IT SERVICES & CYBERSECURITY

As you navigate the evolving landscape of today's digital world, you are probably juggling a lot—from day-to-day operations to looking out for what's on the horizon. One thing's for sure: technology's at the core of it all. And with that reliance comes a slew of questions, especially when it comes to managing IT and ensuring your company's cybersecurity. Here are some of the most frequently asked questions to provide clarity and assist business owners in making informed decisions.

TOP QUESTIONS ON MANAGED IT & CYBERSECURITY ANSWERED

Q: What exactly does "managed IT services" entail?

A: Managed IT services refer to an external provider's proactive management and maintenance of IT systems. This often includes network monitoring, software updates, data backups, cybersecurity measures, help desk support and other essential IT tasks, all designed to optimize a business's IT environment and minimize disruptions.

Q: What kind of support can I expect? Is it 24/7?

A: Managed IT services offer 24/7 support to ensure any critical issues are addressed promptly, no matter the hour.

Q: What's the difference between cybersecurity and IT security?

A: While often used interchangeably, there's a subtle difference. IT security refers to securing information systems, digital data and IT assets. Cybersecurity is a broader concept, focusing on protecting data from threats in the cyber realm, including the internet, networks and digital devices.

Q: What is one of the most pressing cybersecurity challenges for businesses?

A: A challenge many businesses grapple with is the continuous evolution of cyberthreats and the necessity of staying informed and educated about cybersecurity. One of the prevalent tactics hackers employ is deceiving employees into revealing their login credentials. It's not so much about "stealing" in the traditional sense; it's more about skillfully manipulating users into inadvertently handing over their access. Once these cybercriminals infiltrate the system, they often lie in wait, biding their time until they spot an opportune moment to launch a damaging attack.

By prioritizing cybersecurity education and embedding best practices throughout the company, businesses can significantly fortify their defenses against these commonplace cyber threats. Among the most potent tools in this educational arsenal is Security Awareness Training, which equips employees with the knowledge and vigilance needed to thwart such deceptive tactics.

Q: Why should my business consider managed IT services instead of hiring in-house?

A: Managed IT services offer several advantages over an in-house team, including:

- Cost-Efficiency
- Expertise
- Scalability
- Latest Technology

Q: I already use managed IT services. What should I expect from my provider?

A: A managed IT services provider should elevate your technological framework and cybersecurity posture, ensuring optimal performance and peace of mind. Here's what you should expect:

- Proactive Monitoring: Continuous surveillance of your IT infrastructure to identify and address issues before they escalate.
- Regular Maintenance: Scheduled updates, patches and tuneups to ensure all systems are running efficiently and securely.
- Cybersecurity Measures: Implementation of robust security protocols such as firewalls, intrusion detection, encryption and multi-factor authentication.
- Data Backup & Recovery: Routine backups to both local and off-site locations, and swift recovery processes in case of data loss.
- 24/7 Support: Round-the-clock help desk support to address any queries or issues you might encounter.
- Strategic IT Planning: Guidance on future IT investments, scalability considerations and technology roadmaps tailored to your business goals.
- Compliance & Industry Standards: Ensuring your IT setup aligns with your domain's legal regulations and industry standards.
- Employee Training: Regular sessions to educate your team on best practices, cybersecurity awareness and usage of new technologies.
- Vendor Management: Coordinating with third-party vendors on your behalf, ensuring all technology integrations are seamless and beneficial.
- Regular Reporting: Providing analytics and reports on IT system performance, potential vulnerabilities and other key metrics to keep you informed.
- A technology partner isn't just about maintaining the status quo; they're about actively enhancing your technological environment and positioning your business for future growth and innovation.

Q: Is there downtime when transitioning to a different managed services company?

A: The goal is to ensure a seamless transition with minimal disruption and no downtime. While there might be brief periods of downtime for certain tasks, these are typically scheduled during off-peak hours.

Q: How do you ensure the cybersecurity of data and systems?

A: Adams Brown Technology Specialists utilize a combination of best practices, including regular vulnerability assessments, intrusion detection systems, multi-factor authentication, encryption, regular software updates and employee training to maintain a robust cybersecurity posture.

Q: How do you handle data backups and recovery?

A: In case of data loss, systems are in place to ensure rapid data recovery, minimizing downtime and data loss.

Q: What measures are in place in case of a data breach?

A: An incident response plan is in place in case of a breach. This involves identifying the source of the breach, containing the threat, communicating with relevant stakeholders, recovering lost data and taking steps to prevent future incidents.

Q: Can managed services and cybersecurity be tailored to fit specific industry needs?

A: Absolutely. Different industries have unique requirements, and services can be customized to align with your specific industry regulations, standards and needs.

Managed IT and cybersecurity services are more than just protective measures. It's a strategic partnership that ensures your company's continuous growth and resilience against threats. It's about having a knowledgeable ally by your side, dedicated to keeping your tech infrastructure running smoothly while you focus on what you do best: driving your business forward.