onestep
Secure IT Services

Securing Your Auto Dealership: **Essential Cybersecurity FAQs Answered**

In the auto dealership industry, it's easy to assume that your systems are secure if there are no visible issues. However, many cyber threats are hidden and only become apparent after causing significant damage.

We'll clear up these misconceptions by addressing common questions about dealership cybersecurity, such as the limitations of relying solely on cloud storage, DMS, or cyber liability insurance, based on the most frequent inquiries we receive as an IT and cybersecurity Managed Service Provider (MSP).

How do we create a balance between security and productivity?

Balancing security and productivity involves strategic planning and the right technology. Use user-friendly security solutions that integrate with existing systems to minimize disruptions. Regularly train staff on security best practices, automate routine tasks like updates and backups, and focus on protecting critical data and systems. Continuous monitoring and expert support from an MSP can significantly enhance your security while helping maintain productivity.

We haven't had any issues; how do I know I am exposed?

The absence of visible issues doesn't mean your dealership is not at risk. Cyber threats often go unnoticed until significant damage occurs. Regular security assessments can identify hidden vulnerabilities. Your dealership should conduct thorough risk assessments, monitor for suspicious activity, and ensure your systems are up-to-date with the latest security protocols to address potential threats proactively.

Everything is in the cloud; what could be my exposure?

Even with cloud services, your dealership isn't immune to risks like data breaches, misconfigurations, and unauthorized access. Employees might use weak passwords or fall victim to phishing attacks, while issues with your cloud provider could disrupt access to critical data. It's important to implement strong access controls, regular security audits, employee training, and continuous monitoring to secure your cloud environment.

I spent a lot on tools; what else do I need?

Investing in tools is a great start, but tools alone are not enough. You need a comprehensive strategy with regular security assessments, continuous monitoring, and employee training. Tools must be properly configured, updated, and managed by skilled professionals. Partnering with an MSP provides expert guidance, 24/7 support, and ensures your security investment is fully utilized and effective.

My Document Management System (DMS) is protecting me. It is their responsibility, isn't it?

Your DMS provider secures their platform, but you are responsible for managing access controls, user permissions, and data security. They handle the system's infrastructure, but you need to ensure it's used securely. This means implementing strong passwords, keeping software up to date, and training your staff on security protocols to protect your dealership effectively. Remember, if a hacker gains access to your computer system, they, too, have access to your DMS and all the data within.

onestep
Secure IT Services

I have cyber liability insurance; I have nothing to worry about, correct?

Cyber liability insurance is valuable but not a substitute for comprehensive cybersecurity measures. Insurance can mitigate financial losses but doesn't prevent cyber incidents and the subsequent downtime and loss of customer trust. Implement robust security practices, regular risk assessments, employee training, and proactive monitoring to reduce cyber threats and maintain policy standards for full coverage, ensuring comprehensive protection for your dealership.

Learn more about securing your dealership at
https://www.onestepsecureit.com

Is your dealership's security strategy providing proper protection?

Find out with our Free 27-Point Inspection.
www.onestepsecureit.com/27point-inspection

(623) 227-1997
hello@onestepsecureit.com
www.onestepsecureit.com

Conect with us at:
@onestepsecureit