

Does Meeting Compliance Requirements Mean You're Safe?

Compliance vs. Security in the Auto Industry

Compliance and security are two pivotal yet often misunderstood aspects of the modern auto industry. Many auto dealership leaders mistakenly believe that merely checking off compliance boxes ensures their business is secure.

However, compliance and security serve distinct purposes and have different implications for auto dealers. Understanding the nuances between these two concepts is crucial for effectively safeguarding your dealership against a range of potential threats.

While compliance focuses on meeting regulatory requirements, security is about fortifying your dealership against potential threats. Although many compliance requirements include security measures, they often represent only a baseline level that fails to align with best practices or provide the necessary protection.



Complying with Regulations

Compliance involves adhering to laws, regulations, and industry standards mandated by governing bodies. Achieving compliance ensures that your dealership operates within the legal boundaries, shielding it from hefty fines, legal entanglements, and reputational damage.

Regulations frequently lag behind the issues they aim to address, and cybersecurity regulations are no exception. For example, Verizon's Data Breach Investigations Report found that 85% of breaches involved human error, highlighting the importance of comprehensive security measures beyond mere compliance.

Securing Your Dealership

Cyber criminals continuously evolve, developing new methods to attack businesses.

The security measures required for compliance are insufficient for robust protection. Ensuring your dealership goes beyond compliance to implement advanced security practices is crucial for safeguarding against evolving threats.

Effective security measures go beyond the compliance checklist. They involve implementing robust cybersecurity protocols, conducting regular security assessments, and fostering a culture of security awareness among employees. Security measures act as your defenses against cyber criminals seeking to exploit vulnerabilities within your dealership's infrastructure.

The Disparity: Compliance ≠ Security

The critical distinction between compliance and security lies in their objectives. Compliance ensures your dealership operates within the confines of the law. It's the baseline—a necessary but insufficient condition for providing comprehensive security.

Security is a proactive stance — a constant battle against evolving threats.

A compliant dealership may still fall victim to sophisticated cyber threats due to the lack of robust security measures.

Many auto dealerships may need more in-house expertise to navigate the complexities of cybersecurity effectively. Relying solely on compliance may create a false sense of security,

leaving your dealership susceptible to costly cyber attacks.

If your dealership lacks the in-house resources or expertise to manage security, hiring a managed service provider could be your best option. They can implement and maintain robust security measures for your dealership.

Building Resilience

It's clear that cyber attacks will only increase as businesses become more reliant on technology and auto dealerships must prioritize both compliance and security.

Compliance is just the beginning—proper security requires a proactive stance, constant vigilance, and a commitment to staying one step ahead of cyber threats.

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

Connect with us at:
@onestepsecureit