DATA SECURITY SIMPLIFIED

3 BEST PRACTICES TO ENSURE THAT YOUR DEALERSHIP IS WELL-PROTECTED

WWW.COMPLIANTNOW.COM
866-301-0593

Automotive COMPLIANCE CONSULTANTS INC

DATA SECURITY SIMPLIFIED

An Invitation to Dealers and their General Managers,

According to a recent NuSecure Labs report, data port scanning for potential targets by hackers is up 38% at auto dealerships over last year. Up to 95% had little to no data security "whatsoever," the FBI reports.

The cost of a data breach? An average of $217 per lost or stolen record, according to a 2015 Ponemon Institute© study sponsored by IBM.

Data network security and compliance services through Automotive Compliance Consultants will keep your data Safe. Secure. And Sure.

So let us take care of these important compliance security details for you, so you can focus on selling and servicing cars - and retaining customers.

Terry Dortch, President, Automotive Compliance Consultants, Inc.

PROTECTING YOUR DEALERSHIP'S DATA NETWORKS IS VITAL

– BUT IT NEED NOT BE COMPLICATED

Network and data security for your auto dealership is serious business! You just cannot operate an automobile dealership safely and without undue stress unless modern systems, security tools, and network protection are in place to keep good data safe and keep out bad data and cyber troublemakers.

You want and need the facts – clearly presented, to make the right decision about how to best protect you and your customers' valuable assets from data hacking and cybercrime.

Better understanding and application of just three data security best practices will keep your dealership well protected, secure, and productive. We invite you to learn more. Please turn the page.

Data risk is everywhere today.

It rides along within the smartphones your shoppers use in your dealership to showroom competitors across town. It's transferred from an infected USB drive that Charlie brought from home and plugged into a dealership PC.

And who knows who's probing your network for weaknesses to exploit.

The only valid way to ensure full protection against these threats is by having in place robust real-time network and data systems monitoring and management:

- **Robust protection**
- **Weakness isolation and remediation**
- **Prompt response to changing system needs, from new threats – and to your questions.**

For most dealerships, resourcing an internal IT staff that can provide this depth and breadth of network safety is a difficult challenge.

Speaking at NADA, Automotive Compliance Consultants and data security partner Nuspire Networks note that dealers' are pinged for unauthorized access in increasing frequency.

About 80% of dealerships lack sophisticated network protection because they do not have the expertise, resources and often the desire to do anything about it.

A recent ZDNet headline:

- **Hackers are using malware and phishing scams to steal Netflix users' passwords, bank details** *Video streaming service customers are being duped by fake offers for a cheaper service, warn researchers*

A recent TheGuardian.com headline:

- **Hugh rise in hack attacks as cybercriminals target small businesses** *Experts say consequences for small businesses that ignore security risks can be disastrous*

A recent SearchAutoparts headline:

- **Cybersecurity in the shop is a growing concern** *Author notes 'surface attacks' from connected cars to shop networks and scan tools*

"Too frequently, dealers falsely believe they are too small of a target for hackers. A business like Target may be a big fish, but a hacker can scoop vast numbers of critical personal and financial data from hundreds of auto dealerships more easily and more quickly," they advised dealers.

The National Cyber Security Alliance notes that 30% of small-to-medium-sized businesses --like car dealerships -- believe they're more likely to be struck by lightning before their computer systems fall victim to an Internet attack.

Best Practice #1

- Protect passwords, re-issue logins occasionally, and use caution when plugging USBs, disks, backup drives and other devices to your PCs and network.
- Treat smartphones, laptops, and tablets that contain dealership and customer data as attractive resources for data thieves.
- Establish hard-and-fast rules for how these devices will leave the dealership's premises and how they are to be protected when taken offsite. Have written data protection and compliance policies that spell out how these basics will be used.

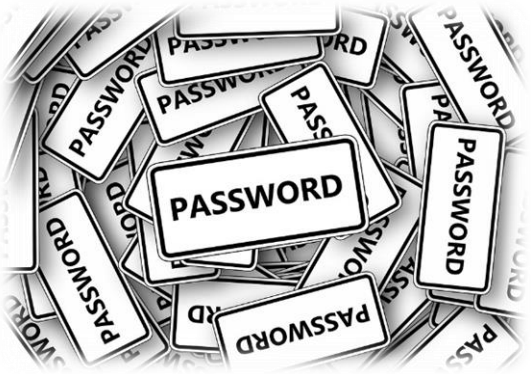
Unfortunately, basic protection measures probably won't be enough to keep out professional cyber criminals.

Best Practice #2

Dealers must take preventive measures to protect valuable data in the digital age. This checklist below, from the FBI, Experian and others, is helpful:

- Secure processes at the intersection of paper and digital mediums, such as scanners and smartphones that photograph documents and digital printers that output the paper copy.
- Use antivirus and malware software, but realize they alone will not thwart hackers who want your data.
- Use digital devices to capture driver's licenses and other personal data you collect for test-drives. Verify that no original or document copies are left behind in scanners and printers. Put the paper version in the deal jacket or scan the paperwork and then destroy the paper documents, unless otherwise required to be retained by law.
- Audit your credit and debit card nodes to ensure payment card industry (PCI) compliance.
- Secure your email servers. Hackers got into a Texas dealership's email system and sent out two million spam emails per minute until detected and stopped!

- Ensure the privacy and protection of the wireless networks you support. Provide a separate wireless system for consumer use. This will help protect dealership networks from virus infection or access through unauthorized devices.
- Institute strict policies restricting the downloading of software.
- Restrict access to the system and do away with the centrally located computer with a password of "password." This practice should be avoided on any machine that is password protected.



If e-contracting, a firewall is not enough to get that electronic contract admitted in court. You will need to show the dealership has:

- ✓ **Security:** The signature system should have bank-level security protocols to ensure documents and audit records cannot be accessed by unauthorized parties.
- ✓ **Audit Logs:** Audit logs are an important part of legal admissibility. They should be time-stamped, detailed, and secured.
- ✓ **Authentication:** The higher the level of authentication, the more likely the judge will admit the electronic contract into evidence.

Data breaches are as much a threat for auto dealers as they are retailers such as Target and Sony.

According to a recent NuSecure Labs report, port scanning for potential targets by hackers is up 38% at auto dealerships over last year. Moreover, up to 95% had little to no data security "whatsoever," the FBI reports.

The cost of a data breach? An average of $217 per lost or stolen record, according to a 2015 Ponemon Institute© study sponsored by IBM.

This study also observes factors that can help reduce data breach risk and breach costs. Business that have an "incident response plan and team in place, extensive use of encryption, a business continuity management system, [strong IT] leadership, employee training, board-level involvement, and insurance protection are viewed as reducing the cost of data breach.

Best Practice #3

This Best Practice identifies key strategic steps designed to protect a dealership at one of the highest possible levels. These steps are:

Training: Training helps to ensure everyone involved in your data compliance project is onboard, understands its importance, and knows what to expect. Having your team engaged in this process will result in a more thorough and stress-free implementation of the entire process.

Discovery: This is the point where appropriate documentation is gathered, the assessment is further defined, interviews are scheduled, and time is allocated for protection resources and client stakeholders.

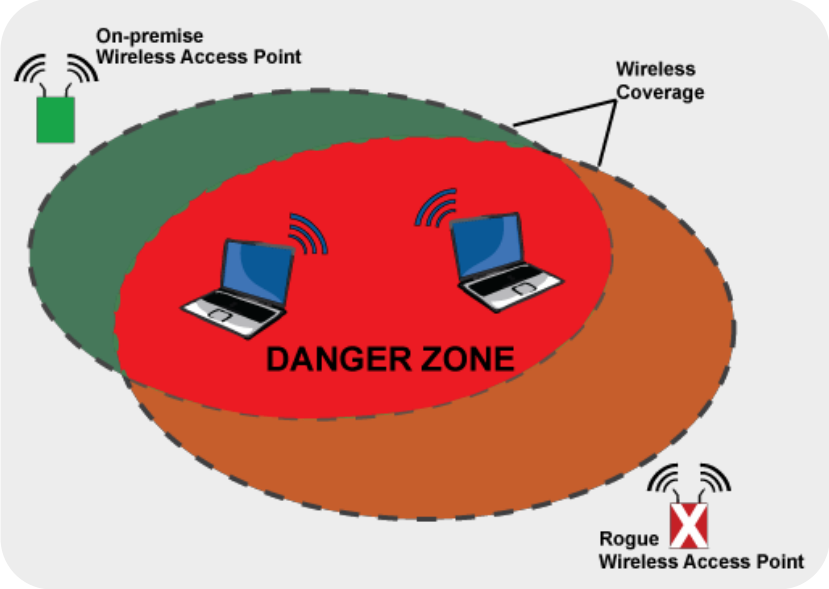
Assessment: During this phase, the systems examiner will review system integrity tests required for audits and identifies areas for further study.

Remediation: If assessment audits arise matters that need further attention, they should be addressed during this phase.

Verification: Here is when preliminary audit findings and remediation steps are taken to ensure that the network is ready for the actual completion of a satisfactory audit.

Completion: The completion of necessary documentation and audit procedures for the Report of Compliance.

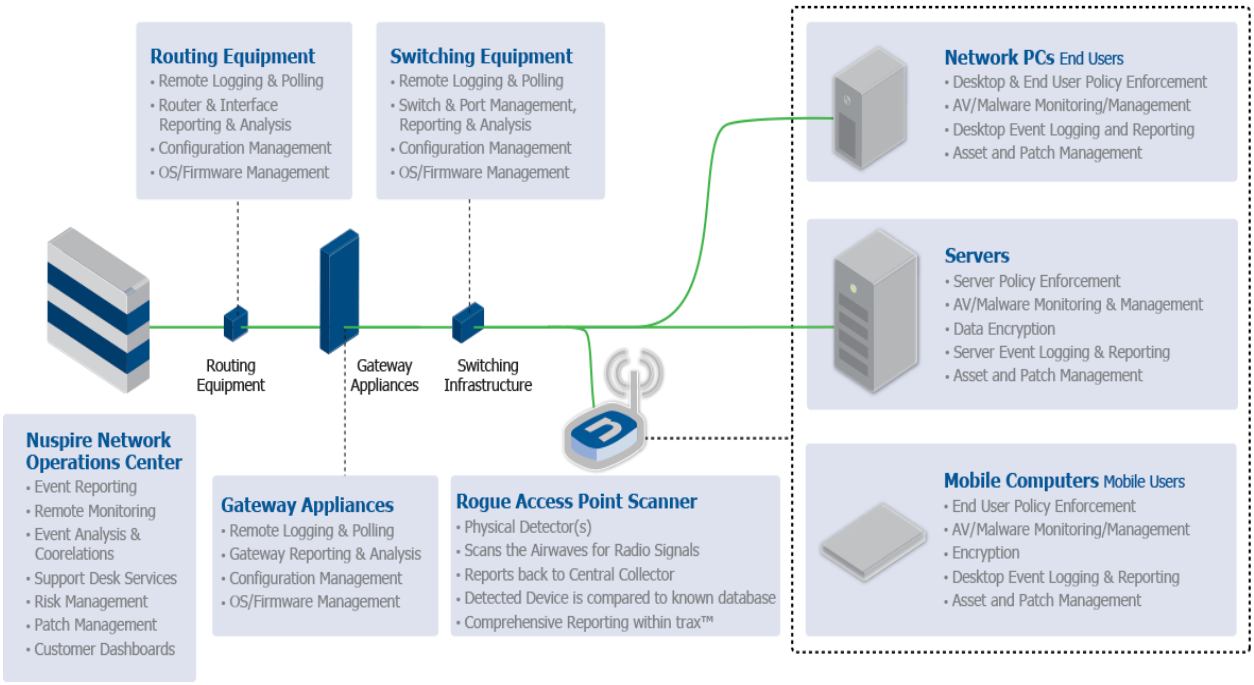
The simplest and most robust way to achieve these best practices is to partner with a professional, dealership-specific network security and compliance resource.



Many regulations - such as PCI DSS - specifically cite the need for rogue access point scanning as part of a compliant network security posture. Our wireless detection services exceed regulatory requirements for rogue access point scanning.

Whether implementing a rogue access point detection solution for a more robust security posture or compliance, our Wireless Detection Services are indispensable.

DATA SECURITY SIMPLIFIED



A turnkey dealership managed network and data protect strategy provides the rampart against viruses, trojans, worms, and malicious invasions that can cripple your business.

Managed Services Delivers Bumper-to-Bumper Coverage

Managed Security Services from Automotive Compliance Consultants and partner Nuspire Networks provide superior data-threat detection and remediation through a skilled team of experts, advanced processes, and propriety solutions that merge Big Data and deep human analytics.

This partnership ensures that dealership clients are compliant throughout their businesses, their networks, and their day-to-day data management.

nuspire networks

This collaboration allows these best-in-class providers to pair offerings in state-of-the-science Managed Security Services to meet auto dealership's data security compliance regulations. These are regulations auto dealers must abide by, such as GLBA and PCI.

This partnership ensures a quick and thorough response to any threat to clients' networks.

Both organization's in-house legal, compliance, and development teams enable Automotive Compliance Consultants and Nuspire Networks to customize solutions quickly to meet the changing compliance and data security and protection needs of today's auto dealerships.

Be sure you're compliant now - Have your dealership evaluated today – know the facts. Contact us today:

866.301.0593

compliantnow.com

Automotive COMPLIANCE CONSULTANTS INC