Compliance and CyberSecurity Planning Checklist

"When cyber attacks are inevitable, focus on cyber security," said *Harvard Business Review.*[i] The front line here is your employees. Train them on cyber and other compliance protection needs and proper response action.

Note, too, that personal malfeasance bears watching.

An accounting firm study once noted a third of dealership respondents had "experienced actual or attempted fraud." Of those, 62% of the fraud perpetrators were employees!

Review these best practices for your organization. Some may not be practical for your situation – and undoubtedly, you already stand tall on many of these vigilance and diligence protections against cyber threats.

Automotive Risk Management Partners brings exceptionally seasoned vigilance, diligence, and compliance intelligence to automotive dealership cyber protection and security compliance. Provide confident protection with a solid Insurance program where the dealer is named additional insured on a policy that would cover any action brought against the dealer, eliminating the loss of money due to fines or suits.

A $1,000,000 insurance policy with an A+ rated insurer backs our services for additional assurance.

If it's time to address this issue head-on or change providers. Automotive Risk Management Partners wil help you make this critical transition.

Contact us today and let us help you with all your inquiries and concerns:

AUTOMOTIVE RISK MANAGEMENT PARTNERS

Terry Dortch, Founder and CEO
info@autorisknow.com • 815-345-3629 • 60B West Terra Cotta Ave 159 • Crystal Lake, IL 60014

CONSIDER THESE GENERAL DEFENSES:

- ✓ Security cameras to watch over parts and materials inventory shelves, supply rooms, parking lots, and other outside areas to observe suspicious activities.
- ✓ Limit access to your parts department, main office, F&I office, cashier office, materials closets, and parts cores storage.
- ✓ Note employees' lifestyles, habits, and behaviors that seem suspicious or otherwise indicate they may live above their visible means.
- ✓ Employees hanging around in areas without legitimate reason to do so is a red flag.
- ✓ Enforce your internal controls policies.

For back-office defense:

- ✓ Don't let one person have complete control of bank accounts. Have one individual handle the payoffs of trade-in balances and another control license and title activities; have a third person manage the day-to-day bill paying. This would mean having multiple accounts.
- ✓ Regular audits of the books should be conducted; auditing by a third party is preferred.
- ✓ Review the DOC or Daily Operating Control sheet daily. Look at vendor expenses closely and get to know each vendor and their service. Look for any abnormalities in the expenses, e.g., is it too high for their service?
- ✓ Investigate anything that looks different or out of place on vehicle values, bank statements, inventory balances, or number of ROs.
- ✓ Don't shrug off any swing in profit, revenue, or payables --always investigate!
- ✓ Pay close attention to used inventory depreciation from purchase to current date.
- ✓ Pay close attention to your wholesaled vehicles; run a report at least monthly to see what is being wholesaled and check the price at which it was sold.
- ✓ Pay close attention to contracts in transit—again, this could mean something other than just waiting on Stips or stipulations, the documents a lender requires to fund a loan, such as proof of income, home, and insurance.
- ✓ Check bank statements personally; randomly look for abnormalities.
- ✓ Keep an eye on used car reconditioning costs; if they look out of place, dig deeper!
- ✓ Conduct monthly inventory of all vehicles, used and new, and match to the dollar amount on the books and/or floor plan.

For data defense:

- ✓ Engage a Managed Security Services Provider to track your network and alert your IT staff when an intrusion occurs so immediate action can be taken. The dealership will probably remain open to network compromise and possibly substantial loss without real-time network tracking.
- ✓ Ensure every employee knows that no internal theft will be tolerated. Also, be sure they understand violations will cause dismissal, at least, and often criminal prosecution.
- ✓ Having a third-party audit of your exposures will provide the most prevention and peace of mind.

www.autorisknow.com

Resource Citations

[i] Keri Pearison, "When Cyberattacks are inevitable, focus on cyber resilience," Harvard Business Review headline, July 18, 2024, https://hbr.org/2024/07/when-cyberattacks-are-inevitable-focus-on-cyber-resilience