VAWTER, GAMMON, NORRIS & COMPANY, P.C.

Certified Public Accountants

Profit Drivers: Volume 15, Issue 6

Profitable Ideas for Automobile Dealers

Inside This Issue....

What Is Your Succession Planning Score?

Robert Vawter, Principal
rvawter@vgncpa.com

Not much demands more of a dealership owner than the challenge of passing on the business to the next generation. Findings from our nationwide survey revealed that the number one inhibitor to succession planning included the current owner's willingness to step back. Nearly one-third of dealerships we surveyed are moving toward the retirement or death of the founder with no formal plans for succession.

There are unique risks and obstacles associated with the transfer of ownership and control of a dealership. Owners often ponder, Who will run the company when I retire? How will I be paid? How will the new owners have the financing power to support the present workload of the company? Coming up with solutions to these questions requires an organized focus on the various facets of ownership several years before the actual transition. Succession planning is your chance to make the most of family assets and perpetuate the special privileges and opportunities of ownership for the next generation.

Five tips to help you begin your succession planning: *continued on page 2*

Steps to Strengthen Your Cyber Security Initiatives

It is very likely that in the past week you have received at least one, if not multiple, phishing emails containing malicious attachments or requesting large-scale wire transfers. As cyberattacks evolve and hackers become more sophisticated, cybersecurity is now more important than ever. In 2015, 6,000 breaches were reported, and that number is expected to climb to 16,000 by 2020. As cyberattacks become more frequent, they are also becoming more costly. Just a few years ago, the cost associated with cybercrimes was in the hundreds of millions. According to a recent study by Juniper Research, the cost of data breaches will reach 2.1 trillion dollars globally by 2019. So why, despite our increased awareness, do these numbers continue to grow?

Continued on page 2

Specializing in serving clients in automotive, truck and motorcycle dealerships

Past issues available at vgncpa.com/profit-drivers

Succession Planning Score

1. In the circumstance that the current leader is unable or unwilling to serve, who is next in line? Your "contingency" succession plan should identify who has decision-making authority in an emergency. Be sure your contingency plan determines a temporary leader and describes the process for selecting a permanent successor.

2. Identify who, over time and with training, has the potential to climb the ranks. Identifying future leadership potential is a major component of succession planning. Taking the time to evaluate your current team with the bigger picture in mind is critical. Doing so will reveal if you have any vulnerable positions that time and training can't mend.

3. Make your plan official by writing a formal document. It would be helpful for your contingency plan to include whether consulting with a lawyer will be necessary. This comes into play if the plan requires a change in an estate plan or institutional by-laws.

4. When you lead an organization, it is your duty to plan for the unforeseen future. The most successful leaders are supported by team members with diverse backgrounds.

5. Executive your succession plan with confidence. This is an excellent opportunity to showcase your leadership skills while simultaneously building trust among key stakeholders.

If you are starting to think about how you will exit your company, request a copy of our succession planning progress report scorecard. This easy-to-use checklist will give you an idea of where you stand, what you need to do and probably raise some questions that you can bring to us to answer. It's never too late, or too early, to plan your future. If you need assistance with your succession planning issues, please reach out to us today.

Strengthen Cybersecurity

The answer lies in the digitization of currencies, transactions, relationships, experiences, enterprise records and assets. This trend is transforming all industries, including automotive, and is past the point of return. The fact of the matter is that your dealership is vulnerable to both ransomware attacks and hijacking. Potential threats include theft of property, customer service privacy infringement, dealership reputation damage, financial penalties and lost customer trust.

Your cash and customer information are desirable targets from a cyber attacker's perspective; even small or medium-sized dealerships who outsource their IT functions are targets for cyber fraud or external hacking. While you can never be 100 percent safe, there are steps you can take to strengthen your cybersecurity initiatives. We have put together the following step-by-step guide to help you assess your dealerships incident response capabilities and vulnerabilities.

Continued on page 3

Specializing in serving clients in automotive, truck and motorcycle dealerships

Past issues available at vgncpa.com/profit-drivers

Strengthen Cybersecurity

Determine Your Security Risks - Identifying, categorizing and prioritizing potential cybersecurity threats can help protect critical assets. Begin this process by making a list of your security risks to pinpoint your vulnerabilities. What controls, if any, are already in place and what steps need to be taken?

Risk management can also help develop proactive measures for protecting your assets. Dealerships can implement risk management by having an official process for reporting risk to the appropriate person.

Another aspect of determining vulnerabilities is making a list of who has access to your information. *How many ways can the outside world access your network? Have you considered third-party vendors? Are responsibilities equally distributed?* We highly recommend dividing access to systems and facilities so that no one employee has complete and total access.

Establish Formal Policies - How often do you change your passwords? Do you have a separate wi-fi for guests? How do employees access the network outside the office? We advise having multiple policies in place to address these questions. At a bare minimum, your dealership should establish password, encryption, retention, email, mobile device and anti-virus policies.

Awareness and Training - Are your employees trained to identify suspicious patterns and inquiries? Do they know how to report their suspicions? Through training and awareness programs, dealerships can strengthen an employee's understanding of cybersecurity. Providing education to internal stakeholders on security awareness, roles and responsibilities is one way to accomplish this.

Incident Reponses Plan - Dealerships should also have a plan that clearly defines the protocol for responding to and recovering from a cybersecurity incident. One aspect of your plan should identify an incident response team that will be responsible for coordinating stabilization efforts. Performing incident simulations periodically can be beneficial in measuring preparedness.

Collaborate with Third Parties - Engaging and collaborating with third parties such as peer organizations, suppliers, cybersecurity researchers, government agencies and the Auto-ISAC can enhance cyber threat awareness within your dealership. The AICPA has a reporting framework you can use to share information about your cybersecurity initiatives with stakeholders.

Be Proactive - Conduct random tests to determine your dealership's vulnerability. We recommend regularly reviewing and updating your policies and procedures to keep up with evolving strategies used by hackers. Another proactive measure to take is investing in a cyber insurance policy. Standard insurance policies do not typically cover security breaches.

Continued on page 4

Specializing in serving clients in automotive, truck and motorcycle dealerships

Past issues available at vgncpa.com/profit-drivers

Strengthen Cybersecurity

Did You Know?

- When dealers provide financing services, personally identifiable financial information is collected from customers. Under the Payment Card Industry's Data Security Standard (PCI DSS), the dealership is responsible for protecting cardholder data.

- According to the Graham Leach-Bliley Act (GLBA), dealerships are considered financial institutions when they collect and store consumer financial information in their databases. Therefore, dealers must follow the legislation's requirements for securing client data.

- Under individual state breach notification laws, dealerships must notify government agencies and consumers when their data is compromised.

The professionals in our office understand the threat cyber fraud poses to your dealership. Call us today to discuss how we can help you strengthen your cybersecurity initiatives.

NAADA
National Alliance of Auto Dealer Advisors

Vawter Gammon Norris & Company, P.C. is a founding member of The National Alliance of Auto Dealer Advisors, a nationwide network of 11 of the most recognized and trusted accounting and business consulting firms who have pooled their resources to provide their dealership clients with the local, national and international perspective needed to prosper. Each of our member firms specialize in providing professional services to dealerships. Collectively our members service more than 1,000 dealers and related entities across the nation.

Vawter, Gammon, Norris & Company, P.C.
vgncpa.com | (907) 767-4030 | info@vgncpa.com
1316 Hardwood Trail Cordova, TN 38016