VAWTER, GAMMON, NORRIS & COMPANY, P.C.
Certified Public Accountants
Profit Drivers: Volume 15, Issue 3

Profitable Ideas for Automobile Dealers

Make Cybersecurity a Top Initiative in 2017

Bishop Norris
Principal
bnorris@vgncpa.com

One only needs to read the daily news to realize that hackers are getting better and cybersecurity is more important than ever for dealerships. Potential threats include theft of dealership property, customer service privacy, 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.

Dealerships are vulnerable to both ransomware attacks and hijacking. The FBI indicated there was over a 300% increase in ransomware attacks between 2015 and 2016. Dealerships can no longer afford to overlook cybersecurity. To protect yourself, it is essential to be proactive with cybersecurity measures. This article will explore how dealers can strengthen their cybersecurity initiatives.

Did you know?

- 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.
- When dealers provide financing services, personally identifiable financial information is collected from customers. Under the Payment Card Industry's Data Security Standard (PCI DSS), they are responsible for protecting cardholder data.
- Under individual state breach notification laws, dealerships must notify government agencies and consumers when their data is compromised.

In July of 2016, the auto industry issued its first set of cybersecurity best practices. The Automotive Information Sharing and Analysis Center (AUTO-ISAC) identified seven key areas on which dealers should narrow their focus.

Continued on page 2

Specializing in serving clients in automotive, truck and motorcycle dealerships

Past issues available at vgncpa.com/profit-drivers

1. Governance

Consider aligning your cybersecurity program with the dealership's broader mission and objectives of the dealership. This strategic alliance can help adopt a culture of cybersecurity. Establishing processes to ensure compliance with regulations, internal policies, and external commitments is just one-way strong governance can help.

2. Risk Management

Identifying, categorizing and prioritizing potential cybersecurity threats can help protect critical assets. Risk management can also help develop proactive measures for protecting these assets. Dealerships can implement risk management by having an official process for reporting risk to the appropriate person.

3. Security by Design

Integrating cybersecurity features, such as testing hardware and software vulnerability, during the product development process is another best practice. The enterprise selling the car is accountable for design security rather than the dealership.

4. Threat Detection and Protection

Having processes in place for early detection empowers dealerships to decrease risk. Threat detection processes include raising awareness of suspicious activity and enabling preparedness and recovery. Dealerships can detect threats using a defined process that aligns with their overall risk management procedures.

5. Incident Response

Dealerships should have a plan in place that clearly defines the protocol for responding to and recovering from a cybersecurity incident. One aspect of your plan should be to identify an incident response team. They would be responsible for coordinating the response. Performing incident simulations periodically can be beneficial in measuring your response team's preparedness.

6. Awareness and Training

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 just one way to accomplish this.

7. Information Sharing and Collaboration

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.

Continued on page 3

Specializing in serving clients in automotive, truck and motorcycle dealerships

Past issues available at vgncpa.com/profit-drivers

This article may serve as a reality check for many of you. Cybersecurity should not be overlooked, there is an established, well-organized and well-funded underground economy for cybercrimes. While 100% protection is not possible, there are steps you can take now to prepare.

- Identify what exactly you are protecting: customer database, personally identifiable information, employee records, financial information.
- Implement security practices: Complex passwords, firewall, anti-malware, back up data, limit administrator rights.
- Offer security training.
- Perform security assessment.
- Develop a response program.
- Review (or get) cybersecurity insurance!

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