BDO Driving Profits
NEWSLETTER

INSIGHTS FROM THE BDO AUTO AUTO DEALERSHIPS PRACTICE

WHY DEALERSHIPS MUST PRIORITIZE CYBERSECURITY

BDO

While the day-to-day operations of a dealership might vary greatly from other types of businesses, they all still have one thing in common: the need for cybersecurity. Every business, no matter what line of work they are in, needs to secure their data and do everything they can to prevent accidental leakage or malicious attacks.

The threats to dealerships are pervasive. There are so many moving parts to keep track of (and we're not just talking about the vehicles here). Dealerships have relationships with **financial institutions**, for lending purposes, and across the **supply chain**. They deal with a wealth of **sensitive customer data** such as names, social security numbers, and credit card information. Their **service scheduling** could be automated. They are taking part in **marketing activities**.

When talking about cybersecurity, so many different relationships can only mean one thing: greater risk. So, how can your dealership protect against cyber threats? Here are a few tips to get started:

1 CONTINUOUS PREPARATION IS A DEALERSHIPS BEST DEFENSE

The biggest thing that is going to affect a dealership is a hit on their brand. No dealership wants to see themselves in the media with the news they were subject to a breach. News like that could affect consumer confidence in the dealership thereby hurting business, as well as the overall brand.

The cyber landscape is constantly changing, and simple defenses are not enough. All companies, especially dealerships, need to continuously evolve to keep up. They don't want anything suspicious touching their credit card transactions, supply chain relationships, and so on. Therefore, it's important for dealerships to review cybersecurity measures that are in place and improve upon them as needed.

2 DRAFTING AND PRACTICING AN INCIDENT RESPONSE PLAN

Simply having an **incident response** plan is just the beginning. Once you develop a plan, you must put it into practice, question it, and make revisions as you see fit. If an incident occurs, ask yourself, "what lessons did we learn from this? What can we do better next time?" By testing and practicing the plan, your dealership will learn the best and most efficient way to respond to incidents.

3 A DISASTER RECOVERY COMMUNICATION PROCESS

A disaster recovery plan must also be developed, implemented, and practiced just like an incident response plan. It should clearly outline how your dealership responds and quickly resumes work following an unforeseen disaster. In the plan, document who dealership employees should communicate with and how they should communicate with each other during different phases. Additionally, make sure everyone within your dealership is educated about how the plan works

While an incident response plan is similar to a disaster recovery plan, there are key differences which is why each one requires a separate document.

An **incident response** plan is for a specific type of incident (data breach, ransomware attack, phishing, etc.).

Disaster recovery plans are drafted specifically for disruptions (equipment outage, natural disasters, cyberattacks). They outline how an organization would resume normal operations in these instances.

4 OFFERING CONTINUING EDUCATION TO ALL PROFESSIONALS

In addition to having documented plans for incidents and disasters, it's also important to offer continuing education to all employees. All it takes is one human error for disaster to ensue within a dealership. If your people aren't educated, they can be the biggest threat to the organization.

5 CYBER INCIDENT EXERCISES FOR ALL EMPLOYEES

Beyond continuing education, employees must also be prepared for any scenario that may present itself. What is the best way to make sure they're prepared? With realistic exercises. Practice makes perfect, and the more practice your employees have, the less vulnerable you'll be to cyber threats.

6 CREATING A CULTURE OF AWARENESS AND REPORTING

Creating a culture within the dealership that not only makes employees aware of cybersecurity but also encourages them to report incidents will only help you. Cybersecurity shouldn't just be a top priority among executives, make sure it's a part of the culture within your organization.

7 ROBUST AND TIMELY THREAT DATA

Knowing how to respond to threats is important, but you must also effectively manage risk. This means having access to robust and timely threat data. Does your dealership have access to information about significant risks that are affecting the business? Are you constantly reviewing these to improve your security posture? If not, it's time to start doing so.

8 ADEQUATE INSURANCE COVERAGE

No matter how confident you are in your security posture, your mindset should never be, "what will we do if a cyber incident occurs?" But rather, you should ask yourself, "what will we do when a cyber incident occurs?" Any business can fall victim to cyber threats, and because of that, it's smart to have insurance. This can offset any financial losses that may happen because of a cyber-attack.

Most dealerships don't have people on staff that understand the current realities of what cyber is today. With an ever-evolving threat landscape, it is imperative that investments in cybersecurity are smart and pragmatic to protect your dealership.

The cyber specialists within BDO Digital can lend their experience and help you improve your dealership. BDO Digital's **security maturity quiz** can give you an idea of how secure you are currently. Additionally, we recommend engaging in a deeper conversation around your threat landscape as it relates to cyber to find the comprehensive solution that is right for you. **Contact us** today to get started.

CONTACT:

RIC OPAL
Cybersecurity National Practice Leader
630-846-8645
ropal@bdo.com

JORDAN ARGIZ, CPA
Audit Partner, Auto Dealerships Group Co-Leader
305-503-1039
jargiz@bdo.com

MEGAN CONDON, CPA
Tax Partner, Auto Dealerships Group Co-Leader
206-382-7825
mcondon@bdo.com

ABOUT BDO

BDO USA, LLP is a professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 70 offices and over 750 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 97,000 people working out of more than 1,700 offices across 167 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. www.bdo.com