NADC
NATIONAL ASSOCIATION OF DEALER COUNSEL®

NADC • 1800 M Street, NW, Suite 400 South • Washington, DC 20036 • Phone: 202-293-1454 • Fax: 202-530-0659 • www.dealercounsel.com

The National Association of Dealer Counsel (NADC) is a nationwide professional organization of attorneys who represent automobile and other vehicle dealers. For more information please visit www.dealercounsel.com.

Reprint from DEFENDER, May 2021.

Cybersecurity and Auto Dealerships – An Often Overlooked and Unmitigated Risk

By Christopher Arkin, *Senior Director, Investigations and Compliance at Guidepost Solutions*

When it comes to the day-to-day operations of selling vehicles, an auto dealership's level of cybersecurity protection might not be the first thing that comes to mind. Given the myriad of business, legal, and reputational risks, auto dealers, their counsel and other advisors should have this pressing issue top of mind–this was the case prior to the COVID-19 pandemic, and the pandemic has only amplified the need for proactive and other cybersecurity efforts.

Unfortunately, the threat of bad actors targeting auto dealerships is something of an inevitability. Due to the nature of the business, and a prevalence of relatively immature cybersecurity infrastructure overall–-whether due to a lack of emphasis, awareness of the full scale of the risks, or reluctance to invest in something that will not necessarily drive revenue growth--auto dealerships are prime targets for cyber-attacks. All too often, dealers, like other businesses, do not realize the need for adequate cybersecurity efforts until they are a victim of an attack or find themselves in a full-blown crisis.

Through security breaches, cybercriminals can readily access valuable information such as bank account numbers, login credentials, and customer data including credit card numbers, social security numbers, and more. Viruses in email attachments, phishing and social engineering attempts, and false login prompts are just a few examples of how bad actors can use their nefarious skills to pry high-value information and monetary assets from dealerships, largely through unwitting, unaware, or busy employees, some of whom may be working remotely and even more susceptible. While the media reports on some of these attacks, they are far more prevalent than the level of reporting would suggest.

The risks are not just limited to cyberattacks. Auto dealerships regularly handle sensitive personal information and have affirmative legal and other regulatory compliance obligations to handle such data appropriately, securely, and responsibly-–whether from individual OEMs or the government. Data security and related obligations can be complex and ever changing, particularly as more U.S. jurisdictions adopt and enact their own (often parallel, but slightly different) regulatory regimes. Failure to comply with these obligations can result not only in regulatory or related government actions, but also in private actions, including by the plaintiffs' class action bar. The financial and reputational risks of these actions can be significant.

With all that said, there are a few initial practical steps auto dealerships, their counsel, and other advisors can take to mitigate cybersecurity risks.

Assess Weak Spots

One of the first steps to take when assessing and enhancing cybersecurity efforts is to conduct a comprehensive threat vulnerability risk assessment (TVRA). The TVRA process identifies, quantifies, and documents the probability of various types of potential disruptive threats related to a specific dealership location.

A recent survey of auto dealership IT-related employees identified that most dealerships have not conducted a formal risk assessment to identify foreseeable internal and external cybersecurity risks; do not conduct regular tests for security systems and processes; or do not have a formal process to respond to security incidents. A regular TVRA process can help address these issues. Indeed, most dealership IT professionals agree it is not a matter of "if" but "when" the next auto dealership will fall victim to a data breach or cyber-attack involving malware, social engineering, or other schemes.

As part of the comprehensive TVRA process, seek to develop a prioritized list of risks and corresponding adequate risk-mitigation controls (e.g., technology, services, or additional procedures). Depending on the dealership's current cybersecurity posture, these controls may need to be developed or enhanced. In our experience, identifying top-level risks can serve as a catalyst for additional controls or defenses in the future, further bolstering a dealership's cybersecurity infrastructure.

The TVRA process will necessarily be different from dealership to dealership, and depending on past cybersecurity issues or emphasis, auto dealers may find that at least some of their risks and corresponding controls may already be sufficiently fleshed out and implemented.

It is crucial to revisit the TVRA process on a regular basis (perhaps annually), as risks and appropriate mitigation controls are constantly evolving. Doing so can put closure on previously identified risks, ensuring that they have been mitigated to an acceptable level, and determine whether new risks have evolved since the prior TVRA process. In addition, being able to point to a regular TVRA process and corresponding prioritized mitigations can be a pivotal part of an auto dealership's defense in legal and regulatory actions.

Additional Steps

In addition to implementing a regular TVRA process, conduct periodic security-awareness training for all personnel. Employees are critical to cyber defense and educating them on relevant topics will strengthen their ability to detect and prevent future cyber-attacks. Employees should understand the sensitivity of the data they handle and the risks their dealerships face.

Auto dealerships can also greatly benefit from developing a management playbook that details how to respond to incidents, including how to communicate a breach to affected parties. Having an organized, thoughtful plan, developed in advance of any incident, can help not make an already stressful situation worse and compound mistakes.

An objective cybersecurity company can be critical in supporting an auto dealership's efforts to adequately mitigate these significant risks. When vetting potential firms, look for those that do not sell cybersecurity products. These firms may push dealers to purchase tools that may not be ideal for their dealership's specific security issues or environment. They tend to focus on products and not on cybersecurity assessments and planning. In addition to looking for firms with specific automotive-industry expertise, dealers should review the backgrounds of the project team that will be working with the dealership. Their credentials and experience should include providing overall cybersecurity assessments, plan development and implementation, and specific cybersecurity consulting. ■

Christopher A. Arkin has extensive experience working with clients in connection with sensitive and high-stakes regulatory matters, internal investigations, and criminal and civil litigation. He has represented global companies, financial institutions, boards, executives, and directors involving a wide variety of substantive issues and areas of the law, including anti-bribery and corruption, securities and financial fraud, environmental and safety-related laws, and corporate governance. He has conducted investigations and other assessments in Latin America, Asia, Africa, and throughout the United States.