Helion Automotive Technologies Issues Proactive Security Recommendations for Auto Dealerships' Customer Data Breaches

TIMONIUM, MD, UNITED STATES, March 12, 2017 /EINPresswire.com/ -- Helion Automotive Technologies, a leading Information Technology (IT) Managed Services Provider, today issued proactive security recommendations for auto dealerships that may experience customer data breaches. The recommendations come on the heels of an incident that occurred last month and was widely reported in news outlets.

In February a disgruntled employee with a CRM vendor circulated an email that appeared to be from hackers threatening to release sensitive information from millions of customer records. The data was purportedly taken from several dealerships' DMS databases. The CRM vendor quickly identified the employee, determined that no security breach had occurred, and that the data the employee had in her possession was benign.

> What this incident illustrates is how most dealerships do not understand the serious consequences related to a data breach of this nature and how ill prepared they are to respond"
>
> *Erik Nachbahr, President of Helion Automotive Technologies*

"These dealers were lucky because if this hoax had turned out to be true they would be legally liable and could be on the hook for millions of dollars," said Erik Nachbahr, founder and President of Helion Automotive Technologies. "What this incident illustrates is how most dealerships do not understand the serious consequences related to a data breach of this nature and how ill prepared they are to respond."

If a hacker gains access to sensitive data in customer records such as social security numbers and birth dates, the cost to a dealership could be in the millions. That figure is based on an average cost of $30 per customer record breached.

Even if a dealership's CRM or DMS vendor is responsible for the breach of a dealership's customer records, the dealership is legally liable for all resulting costs, which may include:

- Local law enforcement and/or FBI investigations
- Computer forensic investigations
- Business interruptions; in some cases businesses are ordered to close their doors until the source and impact of the data breach is assessed
- Customer notifications and free credit monitoring for customers

• Crisis management and public relations
• Customer and class action lawsuits
• FTC action for non-compliance with the Gramm-Leach-Bliley (GLB) Act and software copyright laws

Fortunately for dealers, these consequences can be greatly mitigated by creating a security plan that includes a response to customer data breach occurrences.

The first recommendation that dealers should implement is to assign a point person in the dealership who will coordinate a planned response. The designee is typically a high-level financial executive, which in a dealership may be the CFO, Controller or Chief Compliance Officer.

The designee should have a written response plan that addresses each of the consequences listed in the bullet points above.

The designee should have a list of parties and contact information at the ready in the event of a security breach. Parties that need to be notified immediately include local law enforcement, the dealership's attorney, cyberliability insurance provider and public relations/crisis management representative.

The customer data breach response plan should also include a protocol for notifying customers that their data has been breached, which is a legal requirement. Many states also have a legal requirement that will require your dealership to pay for one or two years of free credit monitoring for the affected customers.

If your dealership does not have cyberliability insurance, get some. Immediately. The typical insurance policies that dealerships carry such as property, liability and casualty insurance do not cover costs related to data breaches.

If a dealership does not have a crisis management plan in place, create one. Costs related to litigation and compliance violations can be greatly alleviated if the dealership responds publicly, immediately and in an appropriate manner.

"Dealers need to realize this is an imminent threat, and that it's not if, but when this will happen," said Nachbahr. "Having a security plan in place is pretty much expected for every business in every industry these days, but unfortunately we find that many dealerships don't think about it until it's too late."

The likelihood that auto dealerships will experience a customer data breach is high. In the last 12 months 71 percent of Small to Mid-Size Businesses (SMBs) reported a security breach, according to a July 2016 report titled IT Security at Small to Mid-Size Businesses (SMBs): 2016 Benchmark Survey. Companies with fewer than 500 employees proved the most vulnerable with a 75 percent breach rate.

For more information contact Helion at 443-541-1500 or online at http://www.heliontechnologies.com.

About Helion Automotive Technologies

Helion...Putting Your Dealership in the FAST LANE! Helion Automotive Technologies is a leading IT solutions provider, providing auto dealers with faster, more efficient networks and secure data protection. From managed services to IT assistance and service desk help, Helion offers both short-term IT fixes and long-term planning so dealers can focus on what matters most: selling more cars. Helion has specialized in IT for more than ten years and works with 650+ auto dealers nationwide.

Dealers can request a free assessment of their IT needs at www.heliontechnologies.com.

Holly Forsberg
Carter West Public Relations
602-680-8960
email us here
