How Cybersecurity Lapses Hurt Auto Dealerships and What Dealerships Can Do

By Joseph J. Lazzarotti and Mary T. Costigan

November 8, 2017

Automobile dealerships' cybersecurity vulnerabilities can drive away customers, according to a survey by auditing firm Total Dealer Compliance.

Automotive News said the survey of 200 dealerships in five states found that:

- Nearly 84 percent of consumers would not buy another car from a dealership that had a data security breach at the dealership; and
- Approximately 33 percent of consumers are not confident in the security of their personal and financial data when buying a vehicle at a dealership.

The low consumer confidence in dealerships' protection of personal data may not be the only reason to implement data security programs. Federal and state laws may mandate that dealerships have such programs. While the details may vary, this means dealerships' data located in a dealer management system (DMS) or customer relationship management (CRM) system, collected by the finance and insurance (F&I), sales, service, or human resources departments, or shared with third-party providers are subject to legal requirements. Further, because employee negligence is the cause of many data breaches, employers must include employee training when implementing a data security program.

A Significant Threat: Employees

Employee error is one of the most frequent causes of data breaches. IT employees are not the only ones with access to personal data. Employee errors can occur when employees not affiliated with the IT department share their DMS password, misplace a portable device, tape their password to the service department computer, improperly dispose of rejected financing applications, open emails from unfamiliar service vendors, pick up malware from visiting a website, or neglect to lock a file cabinet containing sensitive customer or employee information.

Even more troubling is when a disgruntled employee interested in working for a competitor removes backup tapes or another source of "prospective customer" data that could hurt the business as well as compromise the security of that data.

Dealerships collect and maintain a wealth of personal information, including customer names, addresses, phone numbers, dates of birth, Social Security and driver's license numbers, credit reports, credit card account numbers, financial account information, financing application data, proprietary sales information, and information collected from their websites. Regardless of whether a data breach is accidental or intentional, it can have catastrophic consequences, such as legal and compliance liability, damage to reputation, and loss of customers.

Employee Training is Critical ... and Required

There are a number of legal requirements that can apply to auto dealerships. Some examples are provided below. In each of these examples, employee training and security awareness is a critical component. Employee training on how to protect sensitive customer or employee information that addresses company policy, as well as best practices for maintaining the confidentiality, privacy, and security of sensitive data, is not only prudent, but often required by federal or state laws.

Examples of legal requirements include:

- The Federal Trade Commission (FTC), under the *Gramm-Leach-Bliley Act Safeguards Rule,* requires that certain financial institutions maintain comprehensive information security programs that *include* employee security awareness training. Car dealerships that provide financing to customers are subject to this rule. In 2008, the FTC charged a dealer with illegally exposing sensitive customer data. An employee had installed P2P software on a company system that uploaded the customer data. The FTC said the dealer failed to adopt reasonable security measures under the rule;
- Similarly, dealerships are subject to the identity theft protection requirements of the *Fair and*

Meet the Authors

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

Mary T. Costigan

Of Counsel
Berkeley Heights 908-795-5135
Email

Practices

Privacy, Data and Cybersecurity

Accurate Credit Transactions Act Red Flags Rule. In general, this rule requires covered entities to develop programs designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations. Employees must be trained about these programs;
- The *Payment Card Industry Data Security Standards* are a set of security standards established by the major card brands to secure credit and debit card transactions against data theft and fraud. Dealerships that accept credit or debit cards for payment have to be sure they are compliant with these standards, which include employee training as a safeguard;
- Dealerships located in certain states, or that do business with customers from those states, are required by law to have reasonable safeguards that protect residents' personal information. In some cases, training is expressly required. In others, it is a "reasonable safeguard." California, Massachusetts, and Oregon expressly require dealers to train their employees in data security awareness. Connecticut, Florida, Maryland, and others impose only general requirements for "reasonable safeguards." Regardless, "reasonable safeguards" should include employee data security training; and
- Dealerships that sponsor a self-funded *health plan,* such as one that meets the minimum value requirements for purposes of the Affordable Care Act or a flexible spending arrangement, are required to provide employee security awareness training under the federal *Health Insurance Portability and Accountability Act (HIPAA) Security Rule.*

Some federal and state laws mandate data security protection, but do not specifically require employee training. However, training provides added protection and, in the event of a data breach, demonstrate to a regulatory authority a good faith effort to comply with the law.

Trade Secrets

Personal data is not the only information a dealership might want to or is required to protect. In 2016, a U.S. Magistrate Judge in Denver allowed a dealership to pursue claims under the Computer Fraud and Abuse Act against two former managers (the general manager and the finance and insurance manager) for unauthorized access to the dealership's computer systems and stealing trade secrets (see the Automobile News report). According to the court, two former managers who went to work for a competitor used their access credentials to remove confidential trade secrets. This included information concerning sales, customer credit and financing, floorplan financing, and other data that was used to benefit their new employer.

Many dealerships maintain proprietary and confidential business information. If such information is shared outside the organization (or with the wrong people inside the organization), then substantial harm can result. In addition, a dealership's contracts (with banks, manufacturers, third-party providers, and so on) may require security safeguards to protect shared information. These contracts might expect or expressly require employee data security training as part of those safeguards. Clearly, maintaining secure systems, holding trainings, and ongoing vigilance is important not only to protect personal information, but to protect the business.

Cybersecurity Training

When the relevant laws do not specify the manner of data security training, implementing a tailored employee training program is both good security practice and sound business. The training details will depend on industry norms, but the programs should be tailored to the activities, assets, and risks of the individual dealership. Online training sources can be helpful and efficient, but rarely are they sufficient.

Consider these basic questions when designing a training program:

- What data security safeguards does the dealership currently have?
- Who in the organization is qualified to design, implement, and maintain a training program?
- Which employees should be trained?
- Who should conduct the training?
- What should the training cover?
- When and how often should employees be trained?
- How can training effectiveness be measured?
- When and how must training be documented?

The data security training program is a fundamental part of an overall data security program that will help protect your data, your customers, and your business.

Breach Preparedness

Training employees on how to prevent a breach is not the same thing as knowing how to deal with a breach. All organizations have exposure to a breach, and 48 of the 50 states in the U.S. have breach notification laws.

Accordingly, management must be prepared if a data breach occurs. It must secure the systems, continue the business, conduct an investigation, notify customers or employees, notify federal and state agencies, and mitigate harm. All of this must be done without unreasonable delay. Therefore, planning is critical and practicing those plans through tabletops and other exercises is highly recommended.

***

Cybersecurity risk is here to stay and all businesses, particularly those that handle significant amounts of sensitive personal information, need to be prepared. Jackson Lewis works with organizations in all industries, including automobile dealerships, to assess their cybersecurity risks and develop and implement cybersecurity policies, procedures, and practices, including security awareness training for auto finance managers, salespersons, service technicians, and others.

Focused on labor and employment law since 1958, Jackson Lewis P.C.'s 950+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged, stable and diverse, and share our clients' goals to emphasize inclusivity and respect for the contribution of every employee. For more information, visit https://www.jacksonlewis.com.