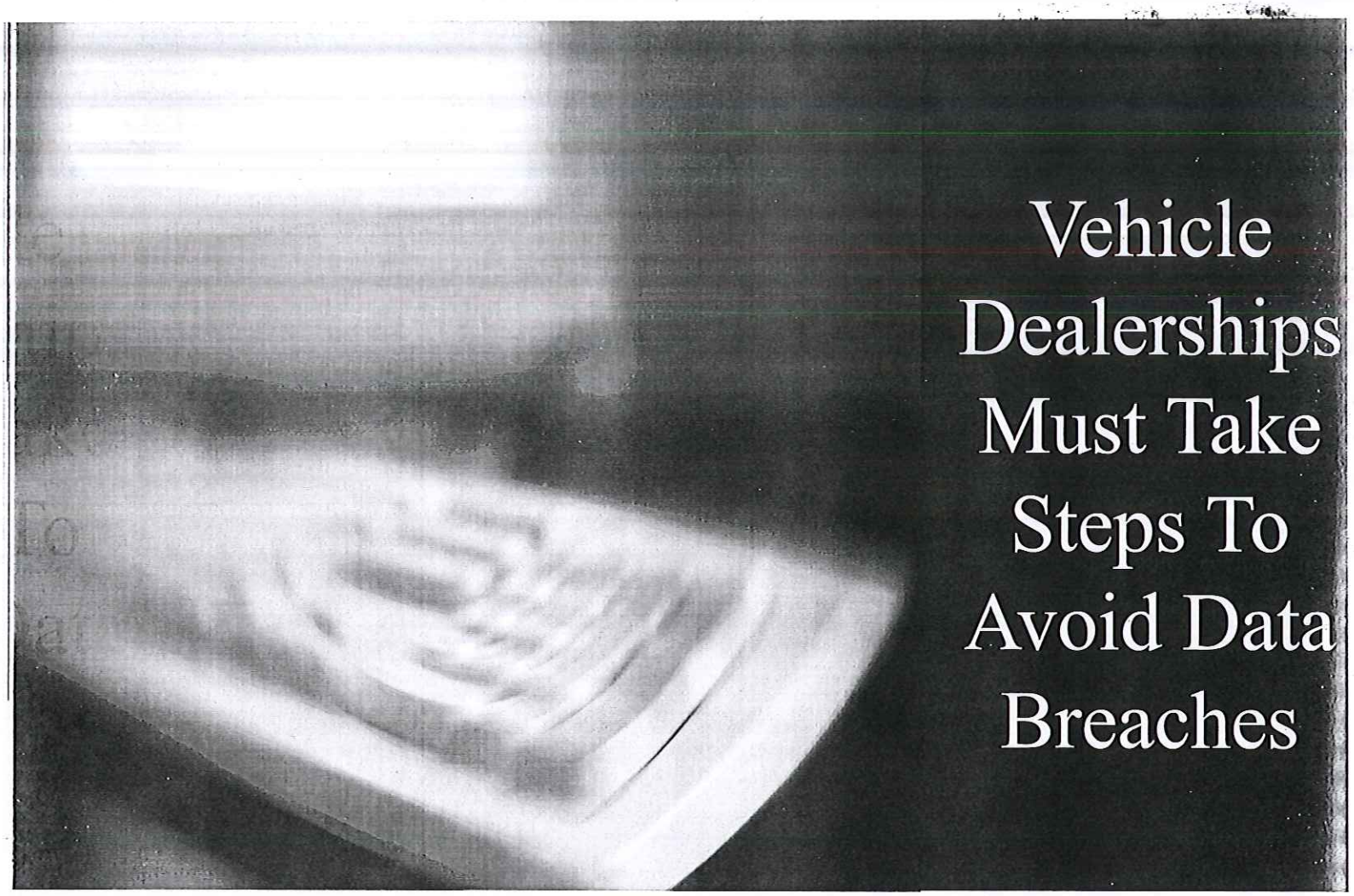


Vehicle Dealerships Must Take Steps To Avoid Data Breaches

By Devin Chwastyk and Elaine A. Stanko, McNees Wallace & Nurick

Imagine this: computer hackers (virtually) "break into" your vehicle dealership. Using a favorite software tool of cyber thieves, they monitor the keystrokes of the dealership's controller. Then, they remotely log onto the controller's computer, and, using the controller's user name and password, access the dealership's bank accounts and transfer funds out of the country. This doomsday scenario struck a dealership in Kansas recently. In another instance, a consultant, sitting across from a vehicle dealership in an Arby's restaurant, was able to access the dealership's network through the free internet wireless service it provides as a courtesy to customers in their waiting lounge.

Vehicle dealerships routinely collect and maintain files of private and confidential information about their customers. Personally-identifiable information (PII) includes names, addresses, dates of birth, and Social Security numbers. When this information ends up in the wrong hands, it can be used to perpetrate identity theft and other fraudulent activity. Helion Automotive Technologies, a national IT service provider that serves over 20,000 vehicle dealerships across the U.S., is reporting an increased threat to auto dealerships and their accounting and finance departments, and warning that the greatest threat to dealerships are scams designed to trick employees.

Legal Obligations For Protection Of Data

The primary legal obligation that arises when a data breach occurs is to notify all individuals whose records were exposed. While there is no federal law addressing data breaches, forty-seven states and the District of Columbia now have laws requiring data security breach notifications.

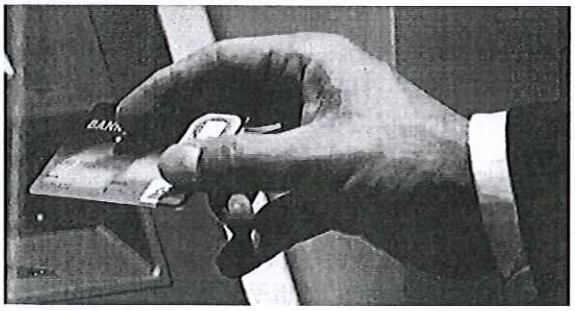
Pennsylvania's notification requirements are set forth in its Breach of Personal Information Notification Act, 73 P.S. §2302. That Pennsylvania law requires that any entity that maintains, stores, or manages computerized data containing PII provide notice to the affected individuals if their system is breached and information is exposed to unauthorized third parties. Most states impose similar requirements on businesses that collect PII belonging to their residents.

PII is commonly defined to include an individual's name, in combination with any of the following: (1) Social Security number; (2) driver's license or state identification number;

or, (3) financial account information, such as credit or debit card or bank account numbers, in combination with a security code or password. Generally, an entity that stores computerized data is required by these state data breach notification laws to provide notice whenever it discovers or reasonably believes that unauthorized persons have accessed and acquired unencrypted files containing un-redacted PII.

In a few states, however, notification is required as soon as unauthorized access is detected, regardless of whether there is any proof that the information has been acquired by third parties.

Responding to a data breach therefore requires careful scrutiny of the notification requirements of multiple states, as each state's law governs the notification that must be provided to its residents. A dealership's computer network could contain PII of customers who reside in, or have moved to, states other than where the dealership operates and where the vehicle was purchased. Data privacy attorneys must ensure that the specific requirements of each state law are met, which may require distribution of multiple notices. Some states require not only that notice of the breach be sent to the individuals affected, but also to the state attorney general's office, consumer affairs division, or police agencies.



The Costs Of Data Exposure

While notification alone can be expensive, the cost of mailing notices is not the only direct cost of a data breach. A dealership that is hacked will need to pay IT experts to investigate, repair, and secure the breached data network, in addition to attorneys' fees for outside data security counsel. Although it is not legally required, many businesses that suffer a breach offer to provide their affected customers with identity theft monitoring and protection, which can also be expensive.

Several reliable studies have examined the costs of responding to a data breach. According to Helion Automotive Technologies, one cyber attack resulting in theft of customer PII can cost a dealership anywhere from $100,000 to several million dollars.

Steps To Limit The Risk Of Data Breaches

Vehicle dealerships must proactively seek to limit the risks of data breaches and the ensuing liabilities. Privacy lawyers and IT professionals agree that data breaches are virtually inevitable, and so businesses must seek to be "compromise ready." This can be accomplished through training and education, security assessments and IT support, having strong data security policies and appropriate breach response plans, and by paying careful attention to insurance and indemnification issues.

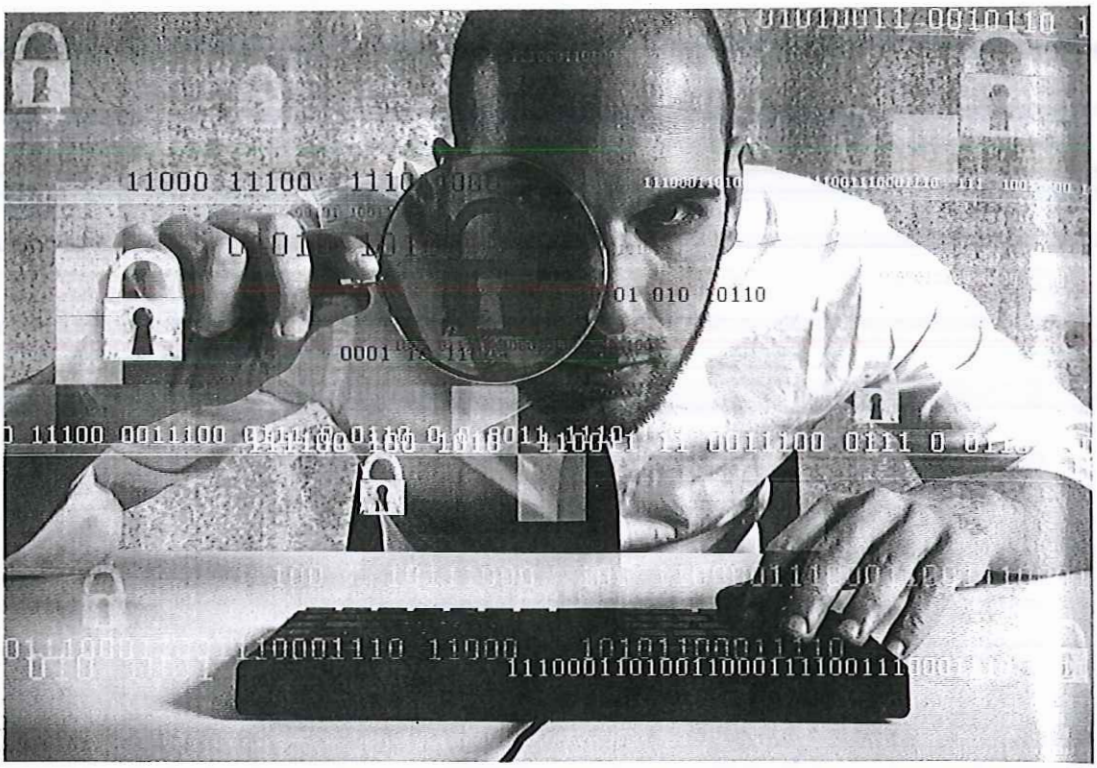
Training and education of employees about the importance of data security and risks of data breaches is essential. Employees must be instructed about the importance of using strong passwords and changing them on a routine schedule, and the dealership's systems should require the same. Training employees to recognize "phishing" attempts and to avoid opening emails or attachments from unfamiliar addresses will greatly reduce the opportunity for hackers to introduce malware or ransomware into a dealership's computer networks.

While IT costs will further burden the dealership's budget and overhead, the importance of devoting adequate funds to internal IT staff and resources, together with appropriate third party vendors, cannot be overstated. Most hackers gain access to computer systems when inadequate attention is devoted to their upkeep. Internal IT staff must have the resources to ensure that anti-virus, anti-spyware, and monitoring software, together with software patches and hardware updates, are kept current. Outside vendors, meanwhile, can conduct independent penetration testing and probe the dealership's network for files that may inadvertently have been left unencrypted and accessible to the public.

The process of creating a data security policy can force a business to confront the categories and amount of personal information that they are collecting and storing. The best way to avoid a breach that exposes such information is not to collect it at all, or to retain it only so long as needed to serve a necessary purpose.

A properly constructed data security policy should be written, disseminated throughout the organization so that all employees are familiar with the policy, and should address certain key topics.

The policy should designate an employee to coordinate the organization's data security efforts, including implementation, training, and testing of the policy.



The policy should limit the categories of PII that will be collected, limit access to those records to the employees whose duties require such access, and require that such records be destroyed or deleted at the earliest opportunity (consistent with organizational needs and legal retention requirements). The policy should include or reference a document retention policy that addresses the full gamut of records the organization may collect or create. The data security policy must also provide for levels of disciplinary measures to be imposed if employees break or ignore the mandates addressing information security.

The policy should address technical requirements, such as the updating and patching of software and firewalls, strong password requirements, and mandatory use of anti-virus protections. It is also crucial to prohibit the transfer of unencrypted personal information by e-mail or to portable devices, including storage media. All of the requirements regarding the security of electronically-stored PII apply equally to the storage of such information in paper records and files.

In addition to a data security policy, auto dealerships should have in place a data breach response plan. When a breach occurs, the plan will designate the key decision makers, and should include executive and management officers, legal and IT staff members, and outside vendors and consultants. The plan should refer these leaders to a preselected forensics firm that can identify the scope of the compromise and repair the system without compromising digital evidence. And it will walk them through a decision tree that touches upon issues including contacting law enforcement, retaining outside counsel, determining notification obligations, documenting response steps, and addressing public relations. The breach response plan should require occasional drills to simulate a breach, with follow-up to make sure the plan is kept current and is updated for training purposes.

The purchase of cyber insurance for data breaches should also be considered. Nearly all general commercial liability policies exclude coverage for data breaches, so a dealership must select additional endorsements or separate policies for cyber-liability coverage. Coverage under an appropriate cyber-liability policy should include the costs of forensic analysis, repair of systems, data breach notifications, offers of credit monitoring, and, if necessary, legal defense of claims arising from a breach.

In addition to adequate insurance coverage, exposure also can be limited through inclusion of appropriate indemnification provisions in contracts with vendors. If any outside vendor or contractor is provided access to a dealership's physical office spaces, computer systems, or stored information, the contractor or vendor should be required to indemnify the dealership if their negligence (or intentional acts of their employees) results in any exposure of government data.

Vehicle dealerships need to be mindful of the wealth of personal information they collect and maintain about their customers and insure that substantial attention is devoted to the security of their computer networks and to preparation for the creeping inevitability of a data breach.

Devin Chwastyk, CIPP/US, is Chair of the Privacy & Data Security group at McNees Wallace & Nurick and Elaine A. Stanko, is a member of the Financial Services & Public Finance Group, Corporate & Tax Group, and Privacy & Data Security Group at McNees Wallace & Nurick. Attorneys Chwastyk and Stanko counsel the firm's clients with regard to privacy issues, including the development of data security policies and data breach response plans. They also assist clients in responding to data breaches, including in rectifying, investigating, and reporting hacking and other data exposure events.