Seeing the Future of Data Security and Protecting Customer Information

The Business of Mitigating the Risk

Bob Schaefer
Vice President, OEM Relations and Data Services
Reynolds and Reynolds

Seeing the Future of Data Security and Protecting Customer Information

Last year, more than 700 data breaches occurred in the U.S. and exposed more than 169 million records...

"... a hacker can scoop vast numbers of critical personal and financial data from hundreds of auto dealerships more easily and more quickly."

The New York Times reported in June that banks are moving away from traditional passwords to the next generation of protecting customer information and data security: biometrics.[1] Once relegated to science fiction, biometric verifications – from voice and eye scans to touch ID on a cell phone – are becoming a more preferred way to identify users and protect their information.

Those of us who use banks would likely applaud that added level of security. And with good reason.

Last year, more than 700 data breaches occurred in the U.S. – from the business sector to government, healthcare, and education. Those breaches exposed more than 169 million records and compromised confidential and financial information for millions of individuals.[2]

So if there's any business where consumers expect the most vigilant focus on safe, secure information, it's a bank.

Now, consider this: What other retailer is considered by law to be a "financial institution" and typically stores as much personally identifiable financial information as a bank?

Automotive retailers.

So far, automotive retailers have been fortunate to have avoided a major data breach splashed across the news (the most visible incident being Franklin Toyota).[3] But dealerships aren't immune from the threat.

As one security expert put it: "Too frequently, dealers falsely believe they are too small of a target for hackers. A business like Target may be a big fish, but a hacker can scoop vast numbers of critical personal and financial data from hundreds of auto dealerships more easily and more quickly." [4]

In fact, seven of the top 10 categories of personal and financial information most often stolen in data breaches are commonly found in the dealership management system (DMS).[5] Is it any wonder then that dealership vulnerability would be tested?

More to consider: The average cost of a data breach for retailers in 2015 was $221 for each lost or stolen record.[6] Multiplying the tens of thousands of customer records in the DMS by $221 is a calculation no dealer wants to do. And what's the accompanying cost to the dealership's reputation and future business? What's that figure?

But there are proven steps that will help avoid having to make those calculations. For dealerships, the best practices to mitigate risk and protect the business extend well beyond the realm of the IT team and the world of passwords and log-in screens.

First, approach data security as a *business* issue, not an *IT* issue.

...implement a "strict data 'push' system for sharing data" with third parties as a way to limit data access.

Second, approach data security as a *management* issue, not an *IT* issue.

A Business Issue, Not an IT Issue

First, approach data security as a *business* issue, not an *IT* issue.

As dealers adopt a more retail-oriented focus, they are turning more often to outside specialists to help harness the data in their dealership's customer database in order to reach the right customers at the right time through the right channel with the right message.

This business initiative also invites more scrutiny on how customer data from the DMS is handled, protected, and used. It also implies that dealerships must be more guarded in determining who can access DMS data, when, and under what circumstances.

The FTC has weighed in on the importance of placing limits on third-party access to a retailer's network. "Not everyone who might occasionally need to get on your network should have an all-access, backstage pass. That's why it's wise to limit access to what's needed to get the job done." [7]

The National Automobile Dealers Association (NADA) also recommends that dealers limit access to only the data necessary for the third party to provide the service and that dealers implement a "strict data 'push' system for sharing data" with third parties as a way to limit data access.[8]

NADA further notes the FTC may consider any third-party access to Non-Public Personal Information (NPPI) to be the same as sharing that information, which puts a burden of responsibility on everyone in the chain of handling consumer data.

In dealerships, inevitably there will be tension between the need to operate efficiently without disruption and the need to adhere to regulatory guidelines in safeguarding customer and business data. Managing this tension as a *business* issue and business risk, not simply an *IT* issue, will help keep the right emphasis on the need to follow best practices in protecting the data – and the dealership.

A Management Issue, Not an IT Issue

Second, approach data security as a *management* issue, not an *IT* issue.

As the U.S. Attorney for the Southern District of New York put it: "If you relegate the issue of cyber and protecting against the threat to the IT people and think of it just only as a security matter, you're going to fail in how you prepare yourself for it. It has to be, like everything else, a corporate-governance matter." [9]

In other words, it has to be part of how you run your business.

And with good reason. Recovering from a data breach is not just a *technical* issue; it's an all-consuming business *management* issue.

Eight out of 10 consumers would *not* buy another car from a dealership where their personal information had been exposed in a data breach.

Typically, the costs associated with a data breach are relatively well known: the technical investigation, customer notification, added regulatory compliance and penalties, attorney fees and even litigation.[10]

But there are also less visible costs that can take an exacting financial and business toll that businesses typically don't realize until they're actually in the situation of a data breach. Those consequences can range from lingering business disruption issues to more expensive insurance premiums, increased financing costs, and lost value of reputation and customer relationships.[11]

In fact, a recent survey of dealerships across five states found that more than eight out of 10 consumers would *not* buy another car from a dealership where their personal information had been exposed in a data breach.[12]

Finally, approaching data security as a management issue also forces the issue of how to prepare now for the day when you discover a data breach. Do you have a business management plan in place if there is a breach?

A People Issue, Not an IT Issue

Third, approach data security as a *people* issue, not an *IT* issue.

As a people issue, the responsibility for data security becomes a business imperative for every employee – from the dealer principal to the most recently hired service technician.

As a best practice in information security, dealerships should consider policies and procedures for all employees who have access to the dealership network and information. Examples include:[13]

- Training for all employees.
- Restrictions on the ability to download software and connect devices to the dealership's computers and network.
- System guidelines and restrictions for users.
- Password protection policies to prevent duplicating passwords; prevent allowing multiple individuals to log-in with the same user ID; and prevent work-arounds to avoid security protocols.
- Consistent ways to monitor compliance and a process for enforcing the policies.

While technology can help monitor and control how IT systems are used, technology is only as good as the people and processes in place to protect those dealership systems and the information in them.

Consumers will expect *more* protection for their information, not less.

What Won't Change

Jeff Bezos, the CEO of Amazon, once remarked that when you can identify what *won't* change in your business over the next five to 10 years, "you can afford to put a lot of energy into it," because you know it will continue to pay dividends – for your customers and the business.[14]

When it comes to data security in dealerships, we know this will not change: Consumers will expect *more* protection for their information, not less. Government regulators will put *more* scrutiny on how businesses handle consumer data, not less. And it's likely that the costs of *not* paying attention to the first two certainties will increase exponentially – in dollars, lost business, employee retention, and tarnished business reputations.

When you know something *isn't* going to change, "you can afford to put a lot of energy into it."

Are you?

Visit ***reyrey.com/whitepapers*** to read more about how the automotive industry is changing.

Footnotes:

[1] "Goodbye, Password. Banks Opt to Scan Fingers and Faces Instead," Michael Corkery, New York Times, June 21, 2016.
[2] Wells Fargo Dealer Services, "Preventing data theft and fraud," Spring 2016.
[3] FTC News Release: "FTC Charges Businesses Exposed Sensitive Information," June 7, 2012.
[4] David Missimer, "How to stop a data breach before it stops you," Dealer Marketing Magazine, May 20, 2016.
[5] Symantec, "Internet Security Threat Report," April 2015, pg. 83.
[6] Doug Olenick, "Ponemon puts a $4 million price tag on mitigating data breaches," SC Magazine, June 15, 2016.
[7] Federal Trade Commission, "Start with Security: A Business Guide," June 2015.
[8] National Automobile Dealers Association, "Dealer Data Guidance," August 28, 2013.
[9] The Wall Street Journal, "U.S. Attorney on the biggest threats businesses face," June 17, 2016.
[10] Deloitte, "Beneath the surface of a cyberattack: A deeper look at business impacts," 2016.
[11] Deloitte, "Beneath the surface of a cyberattack: A deeper look at business impacts," 2016.
[12] Vince Bond Jr., "Dealers vulnerable to hackers, survey warns," Automotive News, June 20, 2016.
[13] David Missimer, "How to stop a data breach before it stops you," Dealer Marketing Magazine, May 20, 2016.
[14] Jillian D'Onfro, "Jeff Bezos' brilliant advice for anyone running a business," Business Insider, Jan. 31, 2015.

Bob Schaefer is vice president of OEM Relations and Data Services at Reynolds and Reynolds. In that role, he and his team are responsible for OEM sales and Data Services, including the secure movement of data for all Reynolds products and services. During his 37-year career with Reynolds, he has led initiatives in dealership management and dealer communications systems, data integration structures, and worked closely with automobile manufacturers throughout a number of his roles.

Retail Management System

Reynolds & Reynolds®