NATIONAL AUTOMOBILE DEALERS ASSOCIATION

Data Security Breaches — A Dealership's Biggest Risk

Randy Henrick

Associate General Counsel

Dealertrack. Inc.

Lake Success, New York

516-734-3644

Randy.henrick@dealertrack.com

The views and opinions presented in this educational program and any accompanying handout material are those of the speakers, and do not necessarily represent the views or opinions of NADA. The speakers are not NADA representatives, and their presence on the program is not a NADA endorsement or sponsorship of the speaker or the speaker's company, product, or services.

Nothing that is presented during this educational program is intended as legal advice, and this program may not address all federal, state, or local regulatory or other legal issues raised by the subject matter it addresses. The purpose of the program is to help dealers improve the effectiveness of their business practices. The information presented is also not intended to urge or suggest that dealers adopt any specific practices or policies for their dealerships, nor is it intended to encourage concerted action among competitors or any other action on the part of dealers that would in any manner fix or stabilize the price or any element of the price of any good or service.

Learning Objectives

1. **Learn** about new ways hackers target small and mid-size companies and how the paradigm for doing so has dramatically changed putting you more at risk than in the past.
2. **Understand** steps you can take beginning immediately to make your system and customer information less susceptible to being compromised.
3. **Learn** how to manage, identify and contain system risks.
4. **Learn** best practices for responding quickly and efficiently to a data breach to minimize damages and mitigate risks.

Three Takeaways: New Security Risks; New Strategies to Protect Data; Critical Response Strategies if You are Breached

1. Hackers look to exploit users through social engineering (phishing), password compromises, and installation of malware to obtain entry into your systems through an end user and their computer. The "human factor" of untrained or unmonitored users is the most likely point of entry.

2. Know where data is located and its pattern through your system. Monitor users and network traffic. Irregular behavior may suggest a compromise. Segregate customer information onto secure dedicated servers.

3. If breached, have a Security Incident Response Plan to implement with assigned roles, consultants on retainer, and immediately take action to identify and control the damage and manage the legal and PR fallout.

Part One: Understanding the Terms

Security event and **security incident** are often used interchangeably. A security event is a change in the everyday operations of a network or Information Technology service, indicating that a security policy may have been violated or a security safeguard may have failed.

A **security breach** is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying Security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized system or network. A security breach is also known as a **security violation**.

A **data breach** is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), personally identifiable information (PII), trade secrets of corporations or intellectual property. For our purposes, we will focus on PII data breaches.

Part Two: The Real World Risk of a Data Breach

A data breach is your biggest dealership risk in terms of costs to remediate, notices to consumers and regulators, PR and legal ramifications, and loss of management time and good will among customers.

2015 was a record year for data breaches in companies of all sizes. One study found that 62% of targets are small and mid-size businesses (Travelers 2015).

Another study indicated the “all-in” cost of a data breach is $214 per record compromised (The Ponemon Institute 2015).

Another study found that 60% of small to mid-size businesses that experienced a data breach went out of business within six months (Experian 2015).

Dealers are a prime target because of their wealth of customer information and the likelihood of not having as sophisticated security tools, technologies and processes as banks and other large financial institutions.

A data breach is the biggest threat to your dealership's existence.

Part Three: The Primary Causes of Data Breaches

With firms investing more in firewalls, anti-virus software, and system protections, user endpoints are the most significant threat for a security event. It is easier to get in via one user's negligence or wrongdoing than trying to break into the system as a whole. Traditional perimeter fortress security of the system won't stop this and new malware attacks can bypass anti-virus programs. Home Depot's breach was caused by an external user who had malware on his PC that allowed hackers to get into Home Depot's systems and create data privileges to compromise over 56 million credit cards (source: Wall Street Journal). You have the same kind of risks from your users' activity.

Compared to intentionally stolen data, twice as much critical data is lost accidentally. Insider threats vary significantly and have different causes and sources. Some are without question motivated by financial reasons or personal or political conflicts with the organization. Often, however, a data breach is due to an employee inadvertently engaging in risky behavior out of habit, ignorance or both. Whatever the motivation or cause, insider threats will continue to cause devastating data losses to many dealers.

Part Four: Initial Steps You Can Take Immediately

The FTC has brought > 50 Safeguards Rule enforcement actions but securing your system and customer information goes well beyond what is required for Safeguards compliance. Here are some initial steps you can take immediately to begin the process.

Step One
Know where all of your customer PII data is located and implement protections to prevent loss of this data. Do not allow this data to be copied to external storage devices. Store your most sensitive consumer PII information on a dedicated system and require "two factor" authentication for access to this system. Encrypt this data at rest and in transit.

Step Two
Limit users who can access customer information on a "need to know" basis. Train them on security best practices (like using complex passwords and not clicking on links in phishing emails) and monitor their access to both paper and electronic files whenever possible. Quickly resolve any data access or network irregularities (large amounts of data entering or exiting your dealership network) as these may be indicators that a hacker has gotten in.

Step Three
Include a secure data destruction and data retention policy in your Safeguards Program. The FTC has warned not to keep sensitive customer information any longer than you need it and then to systematically and securely destroy it in both paper and electronic form. This is particularly true for sensitive customer data such as Social Security numbers, driver's licenses, customer birthdates, and payment card information.

Step Four
Implement, practice, and refine a security incident response program. Involve senior management. Assign tasks to functional officers (IT, security, legal) and engage consultants on retainer (forensics, legal, PR) with a predefined plan to take steps to identify, contain, and correct the incident, determine whether a security breach or data

breach has occurred, and, if so, the extent of compromised data to determine and manage the need for notices to regulators and affected consumers. Test the plan through tabletop exercises and make changes to reflect and prioritize workflows. This is a critical element of a Safeguards Program and may mean the difference in whether and how you survive a security breach.

Part Five: System Issues You Can Promptly Address

Step One

Is your system outdated, unsupported, or unpatched? If so, upgrade to current technology. Windows 2003 and XP are no longer supported by Microsoft with security patches and the like. Windows 8 is 21 times more secure than Windows XP and 7 times more secure than Windows 7. Windows 10 is more secure than both and provides real time patch management. Have a thorough patch management process. Installing patches on a real time basis for all your systems is a critical security requirement.

Step Two

Install Data Loss Prevention Software to prevent data from leaving your systems. Install software that monitors log-in and account usage activity. Once cybercriminals break into a computer, they deploy malware that searches for the credentials of more privileged users, until they hit a mother lode of valuable information. You want to be able to identify irregular system, network, and application activity and suspect log-ins. Ensure audit and system logs are available on all applications and systems where sensitive consumer information can be accessed. Wipe the hard drives of digital copiers, PCs, and fax machines before exchanging them.

Step Three

Test your system regularly such as by using “whitehat” hackers to attempt to break in, identify, and recommend necessary corrections to your systems. Penetration testing is critical. Also develop a vulnerability management process to scan your systems for known security vulnerabilities. Ensure you have up-to-date endpoint and anti-virus software to identify malware, spyware, or viruses that have made their way in or sit on

your PCs. Look for vulnerabilities that require a patch, upgrade, configuration changes, etc. When critical malware is detected, immediately remove the computer from your network but keep the computer intact so that your IT team or a forensics expert can analyze the malware and determine the impact of the malware.

Step Four

Manage employee use of personal devices with a BYOD policy that allows you to define what mobile devices can, and cannot, connect to your dealership network. Employ Mobile Device Management (MDM) software to register authorized mobile devices connecting to your network and place a "container" for secure flow of information to and from your system to the device. This will allow you to better control access to your data and systems as well as provide you the ability to remotely wipe mobile devices that are lost, stolen, or if an employee leaves their employment of your dealership. It will also allow you to enforce good security controls on all dealership owned mobile devices such as passcodes, encryption, etc. Also be sure to encrypt all laptops and make sure all security software, web browsers, and plug-ins (e.g., Adobe Acrobat, JAVA) are patched and up-to-date. Use two-factor authentication to better protect external access into your internal network.

Part Six: Non-System Issues You Can Promptly Address

Step One

Manage the "human factor" (users) which some studies have found account for over 70% of hacker break-ins (Verizon 2013). Train your people frequently on security best practices such as not opening phishing email attachments and using complex passwords. Prohibit their downloading of software not approved by your IT Department such as P2P software. Implement a proxy server or web-filtering technology to prevent users from going to Web sites that are typically associated with malware. Cut off access immediately for employees to be terminated or who give notice of leaving.
Make training a regular process and link compensation to effective security practices. Security is everyone's responsibility.

Step Two

Paper files and deal jackets also present a security risk. Files should be locked up and access monitored by a gate-keeper much as access to electronic files is monitored by system log events. Review spikes in any user's access activity. Implement a clean desk policy so that no confidential information is on desks, copiers, fax machines, or otherwise out in the open. Securely cross-shred paper records in accordance with your document destruction policy on a consistent basis. "Dumpster diving" remains a threat to data security if paper records are just discarded.

Step Three

Manage vendors and other third parties who will have access to your customer files. Do a "due diligence" on the vendor's security practices and contractually obligate them to meet your security standards and retain a right of immediate audit if you suspect an irregularity or security incident. Try to get an indemnity if their act or omission causes a data breach.

Step Four

Consider looking into a cyber-insurance policy to cover risks and costs of a security incident or breach. Most policies cover specified risk elements such as the cost of a forensics team to remediate a breach and restore the compromised systems; the cost to notify affected consumers; legal costs; and other components of a loss. Policies can be customized to fit your needs and budget.

Part Seven: What to Do if a Security Incident, Security Breach, or Data Breach Occurs

Step One

Immediately bring together your Security Incident Response Team and assign roles and responsibilities. Prioritize and assign tasks among simultaneous workflows. Inform the Board and senior management immediately. Designate one point of contact who will communicate with the press and media. Fully understand the situation before making

any statements. Don't speculate. Many security incidents do not result in data breaches. The goal is to understand what occurred or is occurring, stop the bleeding, identify necessary actions, and have the team meet regularly so an overall process is maintained and understood by all. The process may take some time. If you have cyber-insurance, notify the carrier immediately.

Step Two

Identify a small circle of trusted people to prevent leaks of misinformation. Events and circumstances will dictate many different workflows. Try to identify systems, servers, and databases compromised and passwords used. Is email safe? Analysis of a forensic system image may take up to two weeks or longer. Try to identify if the hackers are still in the system or can get back in. Consider contacting law enforcement. The FBI has established experts at all 56 regional offices to offer technical/investigative support to help. If the event is publicized, you may need to bring in a dedicated call center team and prepare FAQs and scripts. All of this will consume a great amount of management time and expense of third parties.

Step Three

Once the workflows are resolved, the system restored with the hack mitigated, and other legal and regulatory notices and issues are addressed, the Security Incident Response Team should meet and review the incident in detail. What was done well and what could have been done better? Were priorities properly allocated? Managing the customer fallout will be a long-term process, whether or not lawsuits are filed. This is why doing mock tabletop incidents is critical prior to the time it is necessary to convene the Security Incident Response Team for a suspected security incident. Try to learn lessons in a mock drill to identify best practices for the types of security incidents you are most at risk of facing. What happens and how quickly you identify and fix the problem will go a long way towards determining the time, cost, and activities you will need to promptly take. There is no template for a response as no two security incidents or data breaches are the same.


Access
Information
Security
RISK
CONTROLS
institutions
MONITORING
appropriate
Management
may
Handbook
Booklet
Authentication
ASSESSMENT
EXAMINATION
firewall
Key
Network
Page
FFIEC
Software
whether
institution's
include
user
use
control
PROCESS
PROCEDURES
System
can
Data
Systems
institution
financial
determine
Policies