These guidelines are provided for informational purposes only and are not intended as legal advice. It is imperative that you stay abreast of developments in this area and consult with an attorney who is familiar with dealership compliance legislation in your jurisdiction.
Purpose and Intended Audience

If you are responsible for the security of your dealership’s data, and your customer’s data, then this document is for you. Its primary focus is information security. Other aspects of securing your operations, such as physical security, are also important parts of your security plan but will not be specifically addressed in this document.

The purpose of this document is to teach you best practices to help you build your organization’s own information security plan.

Every dealership is unique. Whether you are a publicly traded “megadealer” group or a family-owned single store, the information security measures you employ must be a fit for your organization and will not necessarily be the same as the dealer next door.

Security measures to protect your data—arguably your most valuable assets—can range from simple well-known practices to highly sophisticated and expensive technology solutions. However, industry experts generally agree that implementing security measures always involves tradeoffs and “more” security is not necessarily better.

For example, consider what you will pay to protect the cars on your back lot awaiting pickup by the auto auction vs. the cars in your showroom. The same may be true for data in your dealership. If someone stole the data that tracks how much oil was dispensed from your shop oiling system, would you stand to lose any more than the cost to replace the data?

On the other hand, if someone took your entire set of customer F&I records for the past year, you might find yourself facing very high costs to protect those clients from identity theft and more. Yet it is not wise to just write off smaller systems either. Is that oiler attached to your network? Could it be used as an undetectable launching point for a more significant attack on your Dealer Management System (DMS) data? Everything on your network must be considered as a potential risk until you have assessed it.

What you must do depends on:

- The type of data you have
- Its inherent value
- Where that data is stored
- Who has access to it
- How you authenticate and control that access
- How often it is backed up
- Where backups are stored
- Processes you have defined for the cases when bad things happen

There is no single solution that can be applied to every dealership.

Establishing and maintaining information security is a journey, not a destination. New threats to information security surface daily, and these threats continue to evolve into ever more complex designs. It is no longer good enough to protect only what is considered Sensitive Personal Information (SPI). New laws are emerging that say that all data elements, if they help someone “connect the dots” to a unique person, may be considered sensitive. This is how the problem becomes very complex. So, all data should be protected.

Regulatory requirements will have a direct influence on what you must do, verses what a dealer 10 miles away, or across a state line, may need to do. Any vehicle retailer who provides financing is classified as a financial institution and, therefore, the rules of the Graham-Leach-Bliley Act (GLBA) apply to you. The North Carolina data access disclosure law is an example of a state regulation that affects dealers in one state. The dealers in neighboring South Carolina may have other regulations. Dealers must be aware of and comply with their state’s data privacy laws. Credit report reporting obligations may also apply.

The bottom line is RISK. A risk-centric approach is important to ensure that all your assets that affect, use and protect your data are taken into account. These assets include hardware, software, people, processes and business partners. You must first identify your risks and then decide how much risk you can afford in each case. It is a
balancing act that every business owner must define for their business. There are three perspectives that must be considered:

- What must I protect by law? (What are your most valued assets? Are some assets more valuable than others?)
- What are the primary threats to my assets?
- How much time, effort and money am I willing to spend to protect these assets?

Once the risks and their magnitudes are well understood, a viable security plan can be drafted. You probably make these risk decisions every day without much thought. Now is the time to put them in writing and determine their relative importance, so you can put your money where it counts most or is most needed. You can start simple and build your plan, or hire an expert to assess all your assets at once and build a plan for you. Either method works, but the most important thing is to get started and keep working on it.

What are the Common Risk Areas?

This document assumes that your data is your most valuable asset. Verizon Business publishes an annual Data Breach Investigation Report [PDF] that includes breach statistics. Many other organizations conduct research on data breaches and provide statistics that may be useful in your efforts to identify and quantify your risks. One best practice is to read these briefs annually, or as released, to ensure your plan is up-to-date. The Verizon report notes the following statistics in data breach cases. In 2011 (as documented in the 2012 report), the second-highest data loss total was reported since Verizon started keeping track in 2004.

- 98% were from outsiders, organized crime and activist groups—up 6% from 2011
- 81% used some form of hacking—up 31% over 2011
- 79% were targets of opportunity—targets with known weaknesses

Also of note, breaches resulting from privilege misuse were only 5% of the total—down 12% over 2011.

Implementing basic security best practices is important!

We have all seen the media publications and know that breaches do occur, and when they do, the damage can be great. We suspect that the actual number of these events is under-reported, as the resulting publicity would be very bad for any business. The following are some areas you should address:

- Fraud due to lack of checks and balances in handling your data and finances
- Insider threats from staff or consultants with more data access than necessary to do their job
- Third-party partner access to your data that is not controlled, monitored or contractually governed
- Government data privacy legislation that mandates fines, or even jail time in non-compliance cases!
- Fines resulting from failure to perform contractual obligations, such as for Payment Card Industry Data Security Standards (PCI DSS), discovered in an audit or worse, after a breach

When basic security practices are not followed, you also become a target of opportunity. So, the first best practice is improving access controls. Requiring strong passwords, implementing random password aging, and password rotation are controls that generally should be followed. For more details on effective password management, see the section titled Employee, Workstation and Mobile Best Practices.

This is not an exhaustive treatment of all the risk areas that must concern you. Depending on your situation, your risk areas may be more, less or even different.
Roles and Responsibilities

Before you begin, decide who in your organization will be accountable for your security program and assign them the task!

Set your expectation with them, such as:

• Building/maintaining your security plan
• Conducting annual reviews
• Updating the plan when business processes change
• Observing daily operations
• Training staff, certifying their knowledge, and coaching anyone who is not following guidelines

Active governance is a requisite to success in security. You must certainly be involved in defining the scope of your plan.

Some Key Data Security Plan Considerations

• Hire or consult an expert to help you write your plan
• Assign someone on your staff the responsibility of managing it
• Keep it fresh, review compliance often and update it, annually, at a minimum
• Recognize that making tradeoffs is reality—no security measure is perfect
• Continually look for weak links and ways to strengthen them—multiple counter-measures implemented in a series make it harder for a hacker to attack your systems and get at your data; reward employees for finding and then immediately as well as discretely reporting vulnerabilities
• Learn about the challenges from free resources and be sure you or someone in your dealership is tuned into the changing nature of threats that may be important to you
  – FCC Cyber Security Planning guide [PDF]
  – The Verizon Business report [PDF] previously referenced
Identify and Quantify Your Data Risk Areas

A key part of your data security plan will be a written record of all the data you have, what kind of data it is, where it is stored, and other pertinent information. Think about your whole business. While your DMS may contain the bulk of your data, you may find that there are other places where important data is stored, depending on the applications you use.

A simple table is a good tool:

<table>
<thead>
<tr>
<th>Application</th>
<th>Data Types</th>
<th>Where Stored</th>
<th>Current Protection</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMS</td>
<td>Client data, Personnel data, Financials, Service records</td>
<td>DMS – ASP hosting center</td>
<td>Passwords, restricted access</td>
<td>Very High</td>
</tr>
<tr>
<td>Payroll</td>
<td>Salaries, SSN, Bank Account Numbers</td>
<td>Payroll provider</td>
<td>Authentication and Authorization credentials</td>
<td>High</td>
</tr>
<tr>
<td>F&amp;I</td>
<td>Client finance info, bank account numbers, SSN, etc, etc.</td>
<td>Cloud</td>
<td>3rd party F&amp;I company manages it, contractual</td>
<td>Very High</td>
</tr>
<tr>
<td>Third party data services</td>
<td>Sales info, vehicle make, model, client demographics</td>
<td>DMS</td>
<td>Contracts, token authentication</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Once you complete this table, the next step is to determine what the impact will be to your business if the data be lost, stolen or otherwise compromised. This ranking exercise will help you prioritize the order of your risk mitigation efforts.

The general thinking in the security field today is that a broad, high-level assessment and weighting of your risks is more important than a complex mathematical risk calculation that can lead to incorrect conclusions. Keep it simple and address the most important areas first, then the rest.

Include this table in your security plan and keep it updated. It will be the baseline that you will use when updating your security processes during your periodic reviews. If you hire a consultant to help you assess your data security and risks, they will begin by building a similar table. Having this ready for them may save some effort and streamline your engagement.
Domains of Risk and Best Practices

Implement Best Practices

Implement the basics! These are the first lines of defense for your data and if done well can protect you from 80% of the threats known today. The four cornerstones of a good plan include addressing the following:

- **Prevention** – How are you stopping potential attacks?
  - Firewalls
  - Strong passwords
  - Authentication

- **Detection** – If an attack happens, will you know about it in a timely fashion?
  - Unified threat management devices and management software
  - Someone looking at the reports
  - Security Information and Event Management systems (SIEM)

- **Containment** – What are your processes to limit the spreading of a virus found on a PC?
  - Anti-malware software
  - Email use policies
  - Employee reporting requirements

- **Response** – Do you have a plan to resume normal operations?
  - What about regulatory reporting requirements?

According to the Verizon Business Data Breach Investigation Report [PDF], there are some simple things you can do to shore up your defenses. These are very basic, well-known best practices many businesses have adopted:

- Smaller organizations
  - Implement a firewall or access control list (ACL) on remote access services (RAS)
  - Change *default credentials* of all Internet-facing devices
  - If a third-party vendor is handling the two items above, make sure they actually did them

- Larger organizations
  - Eliminate unnecessary data; keep tabs on what is left
  - Ensure essential controls (PCI, et al) are met; regularly check that they remain that way
  - Monitor and mine event logs
  - Evaluate your threat landscape to prioritize your treatment strategy

However, consider that recent litigation outcomes indicate that *best practices alone are not enough*. Fine-tuning best practices to particular environments, third parties or contract employees, among many other possible scenarios, may be necessary to limit your legal liabilities.
Perform periodic network scans to find network vulnerabilities and “back doors” on your network

Usually performed using specialized software, they search the network to see what devices are currently connected to the network, such as PCs, network printers, routers, switches, or access points. A network scan can also mean performing an external vulnerability test of your network to determine if there are any potential weaknesses that a hacker could exploit; an example would be performing a network “port scan.”

Did your last IT Manager or consultant set up a back door to ensure they could provide support from a home office or remote work location? Is it still there? Is it secured or open to whoever stumbles upon it? It will be far less expensive to discover it now and fix it than it will be later after a breach.

Use UTM devices, web filtering, in-series

Secure networks deploy several layers of security to assist in preventing unwanted access, viruses, malware or spam from infecting your network.

Unified Threat Management (UTM) devices typically include several different security features, including web filtering, malware protection, virus protection and spam blocking. Some devices have an active email virus scanner. This prevents infected email from being opened by quarantining the infected email, so that it will not be able to infect the network with a data-stealing bot or similar malware.

Web filtering keeps your employees from inadvertently surfing to a malicious site that could wreak havoc on your systems or simply take a copy of your data without you knowing anything happened at all. Web filtering is a critical component for any business that must use the Internet to conduct business. Web filtering should be backed up by an Internet Use Policy for your organization.

Change default passwords for all network devices

Routers and wireless access points are a common place for hackers to begin their attack on a network and its systems. Sadly, many businesses do not change the default passwords either, because they forget to or because the system integrator left them as-is for your IT person to update after the installation. It is best to check if you are not sure and then change all default passwords you find.

Secure third-party access with strong authentication

Third-party vendors should always have uniquely identifiable authentication and authorization. In the case of a breach, you want to know where the breach occurred, and without these controls over third parties, you may never really know where the breach originated.

Firewall your Internet connection

An actively managed firewall is still the best first line of defense for you network. Firewalls should be deployed and managed. They are typically deployed between the local area network (LAN) and the Internet connection used by that LAN.

Restrict your customer Wi-Fi Hotspots

Customer wireless networks should be segregated from the rest of the business’s network to keep consumers from having access to your business systems. Typically, customer wireless networks are stand-alone networks that include a firewall and web filtering as well as utilize an Internet connection independent of your business network.

Wireless Security

Your wireless business network requires special attention to ensure strong security. Locking it down to only support your known users should be seriously considered. Default passwords on wireless routers should always be changed and you may want to consider a wireless device management system that can detect and alert you to the installation of rogue access points as well as provide you with a way to audit the use of your wireless network. Implementing strong wireless security, configuring strong wireless network access security keys, and segmenting your wireless network are parameters, which should all be considered.
Use SSL to protect data exchanges
While Secure Sockets Layer (SSL) is still a common practice, be aware that SSL breaches have and can occur. Be prepared to adopt better VPN technology when it becomes available. Take note, a virus sent to you in an email over an SSL connection may easily pass through your state of the art firewall and give you fits. Hence, it is still a best practice to install and maintain anti-malware on your workstation or virtual workstation environment server as well as also implement a UTM device that scans emails for viruses.

Physical Information Security Considerations
• Restrict access to your on-site systems and servers
• Regularly back up your data on a schedule you determine that fits your needs
• Ensure backup media is stored safely off-site in a timely fashion
• Implement a clean-desk policy; do not allow papers with clients’ confidential information to sit on desks when staff is not there (NOTE: If you accept credit cards, this is an important PCI compliance requirement, and it also applies to credit report information)

Employee, Workstation and Mobile Best Practices
Use of mobile computing devices is expanding at an unprecedented rate. Maintaining security of your data where mobile devices are in play is not easy. Mobile devices are one of the new primary attack vectors for hackers and cyberthieves. Recent analysis shows that the device of choice may make only a small difference in the risk from this threat.

Here are some best practices to consider:
• Implement and enforce a strong password policy for desktops and systems; consider implementing a random password rotation schedule verses a fixed one
• Require that employees log off the DMS and other systems when they leave their workstation
• Never allow login or password-sharing, or storage in clear-text files, on email or Post-it® notes
• Prohibit the use of “Sleep,” “Standby” and “Lock” modes on laptops when employees leave your facility at any time; appropriate actions include “power down” or “Hibernate”
• Update desktop PC software regularly
• Implement a system that allows you to wipe the data from a mobile device remotely
• Ensure that all mobile device users lock the device with a password
• Businesses have tried to optimize their desktop technology investments by using them as long as possible. However, when the security patching of your legacy operating system or applications ends, your risk exposure will grow rapidly as newly discovered security flaws are publicized. Your security plan should outline: 1) a patching plan, and 2) a technology refresh plan, to ensure obsolete desktop hardware and software does not become your Achilles heel.
Include all of the following in your patching plan:
- Windows® and mobile device operating systems
- Adobe® software [Flash and Reader as applicable]
- All browsers
- Anti-virus/anti-malware software
- Java™ if required by any of your applications

• Implement mobile device requirements:
  - Require that mobile devices be set up with a password
  - Require that mobile SIM cards be locked
  - Most SIM cards will be tied to your physical phone and number and locked by the carrier; however, an unlocked SIM card from a lost or stolen phone can be used in another phone to make calls, which would be billed on your account; check with your carrier to determine if you are at risk

• Manage employee permissions in a timely fashion
  - Immediately remove credentials of terminated employees
  - Regularly audit user IDs to ensure that no former employees still have access
  - Frequently review employee authorizations and relevance to their position

Employee Security Awareness Training
Training programs can be developed for your organization and delivered as online courses. Consult with your attorney to structure the program and how often staff should review it. It should be mandatory for all new hires and be re-administered annually. The program should cover all aspects of:
• Proper handling and protection of your customers’ data
• Email use, detecting phishing attacks, never sending sensitive personal info in an email, and never responding to unsolicited email
• PCI DSS compliance and ongoing validation, if you accept credit cards
• Password requirements (see Employee, Workstation and Mobile Best Practices section above)

Fraud Risk
We have all read in Automotive News and other industry journals about the trusted General Manager or CFO who has used their position to steal or alter information, which they were authorized to manage, to their own gain. This is clearly a risk to consider. This kind of theft occurs during normal working hours while the employee is doing the job they were hired to do. [See the Risk Based Security and Open Security Foundation information in the appendix.]

Insider Threats
Have you had a Salesperson quit only to discover later that they are working down the road at your competitor’s store—and YOUR old clients are buying from him? Did he really know all of them, or did he take a customer list with him from your store?

According to The CERT® Guide to Insider Threats:
“Very few insiders steal intellectual property in order to sell it. Instead, they steal it for business advantage: either to take with them to a new job, to start their own competing business, or to take to a foreign government or organization.”

It may be lower on the risk scale, but you should consider mitigation of this risk, perhaps in your employee contracts. Your attorney should be consulted on this action.

Your best first line of defense against insider threats is to implement strong computer account and password management policies, as previously noted.

In addition, you might consider the following:
• Respond immediately to suspicious or disruptive personnel behavior, beginning with the hiring process
• Enforce separation of duties and least privilege [see glossary for definition], especially where critical information changes are required or technical modification of critical systems is necessary
• Use extra caution with System Administrators and technical or privileged users
• Immediately deactivate computer and network access following termination
• Include an insider incident response plan in your security plan
• Track and secure your physical environment assets
**Third-party Data Access**

Giving the keys to your most valuable asset—your customer database—should be done with careful planning and attention to detail. Your attorney should be engaged in writing these contracts. Put everything in writing; do not just take their word for it that they will not access data you have not given them permission to see.

*Never allow third parties to use your user ID or “screen-scrape” your data.*

Suppose there is a breach and you have a forensics team trying to find out where it came from. Ah ha—it was you! Third parties should always have unique IDs and be required to authenticate to the system before they can access the data. These credentials should be carefully managed.

_Do you have contracted employees?_ Many dealers hire certain skills on contract, because they are not considered a long-term need. How do you manage contract employees? Have you set clear expectations of them? Do you have a copy of the source code written by these contractors? Is it well documented so that it can be modified in the future? Is the source code stored off-site in a secure location with your backup data? These are all questions to need to ask yourself.

**Third-party Applications**

Third-party applications can also pose a significant risk to your DMS data and operations. Specifically, these are applications running on the DMS that are not written, provided or maintained by your DMS provider. They may be written by you, your consultant or a third-party vendor in the market.

The risk is primarily operational risk. For example, do you have processes in place to track and maintain this software and keep it functioning properly? Whom do you call when there are issues? Are you making sure that it is keeping pace with the evolution of the DMS? Some key areas of focus that you or your third party must address include:

- Updating
- Patching
- Validation with the current DMS platform
- Maintaining compatibility with evolving platforms
- Code vulnerability reviews
- Application penetration testing

**File Sharing**

Even everyday file sharing can be a risk, so how you do it can be important depending on if the sharing is inside your network or with external parties. Encryption is the most common best practice and should be considered as a minimum watermark. Here are some things to take into account in your information security plan:

- Encrypt all files you share or ensure they are shared over encrypted VPNs
- Review your contracts with third parties you share data with and be sure that the third party cannot also share your data with others, unless this is your intent
- Be sure that when you share customer information, you are being consistent with your customer GLBA Privacy Policy notices.
DMS Platform Changes

- Regulatory legislation drives a continuous effort to enhance information security controls both in the DMS platform and to the application suite; these changes can include the implementation of new logging or the sun-setting of legacy programs and system access with replacement solutions that are deliberately more restrictive; these changes can impact your legacy applications, depending on assumed access to certain functions.

- Changes are also necessary to give you the ability to implement generally accepted security best practices to protect your data, or better.

- All DMS platforms are changing, so adoption of new technologies, faster hardware and improved software are all requirements for DMS providers to maintain a viable product that can efficiently help you manage your business; changes, which at one time came in annual or longer cycles, will now be made in smaller bites and as often as monthly; some will be application-specific and others will be related to the platform and how it integrates with your network and Active Directory environments, as examples.

- Most DMS providers today have security programs in place that require periodic code reviews and penetration tests for all platforms and applications to ensure any code vulnerabilities are addressed; with the threat landscape changing daily, a DMS security program is vital today.

Your security plan should include a requirement to maintain a list of all mission-critical applications in use. Program code no longer needed should be removed. All other code should be reviewed often, kept updated and patched as required as well as storing the source code and related documentation in a safe place. ADP receives client requests for help where an IT Manager has left the dealership and the source code was lost. There is little we can do in these cases.

Third parties should be required to subject their code to vulnerability reviews and penetration tests. Your DMS is only as secure as its weakest link.

Credit Cards

An important consideration when a security incident occurs is deciding who will be “on your side” and who will be “after you.” These incidents may not even be your fault, but the credit card issuer may decide that there is enough commonality in the event with your business to subject you to an audit. You must be prepared!

Case in point: If you handle credit card data, be ready! The forensics investigator sent by the credit card company is not looking out for your best interests—even though you are contractually obligated to pay for his services. In the case you are subjected to an audit, a best practice is to immediately engage an independent Payment Card Industry Qualified Security Assessor (PCI QSA) to lead the investigation and manage the credit card company’s forensics team.

A new credit card solution referred to as ‘Chip and PIN’ is now being rolled out by banks in the U.S. This system is in use globally and may be mandated by banks by October 2015. You may want to talk to your payment processor about the enhanced security benefits this solution provides, and if/when they plan to mandate it.

Conclusion

This is by no means an exhaustive treatment of data security. We hope that it will give you a sense of the things you need to do to secure your business data. ADP has chosen to embrace information security and because of that, changes will be forthcoming that may impact how ADP clients use their DMS and other applications. These changes are intended to help them conduct business more securely.

Note: These guidelines are for general information purposes only. Neither the author nor the publisher intends to provide any legal advice. Please contact your legal counsel if you have any legal questions or concerns.
<table>
<thead>
<tr>
<th><strong>Glossary of Terms</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control List (ACL)</strong> (Routers)</td>
<td>A table that filters network traffic based on the IP address of the traffic.</td>
</tr>
<tr>
<td><strong>Active Directory (AD)</strong></td>
<td>A directory service created by Microsoft for Windows domain networks; it is included in most Windows Server operating systems.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Generally, the act of confirming the identity of a person or software program and includes verifying the validity of at least one form of identification and possibly more (e.g. A password + a token).</td>
</tr>
<tr>
<td><strong>Authorization</strong></td>
<td>The privileges a user has after they have successfully been authenticated (e.g. the General Manager can see the employee data, the Parts Manager cannot. The General Manager has authorization).</td>
</tr>
<tr>
<td><strong>Application Service Providers (ASP)</strong></td>
<td>Computer-based services and applications delivered to customers over a network. Software offered using an ASP model is sometimes called Software as a Service (SaaS).</td>
</tr>
<tr>
<td><strong>Back doors, network and systems</strong></td>
<td>In this document, the reference is to unapproved, unaccounted for and possibly unprotected connections to a business network that may have been set up to provide a specific person access to the network from a remote location to provide support. In the systems sense, a back door could be software that hides itself from Systems Administrators but allows a hacker access to the system. A rootkit is a form of a system back door.</td>
</tr>
<tr>
<td><strong>Bot</strong></td>
<td>Botnets are comprised of computers whose security defenses have been breached and a third party has gained control of them. Each compromised device is known as a “bot.” The controller of a botnet is able to direct the activities of these compromised computers generally through the Internet.</td>
</tr>
<tr>
<td><strong>Default credentials</strong></td>
<td>Commonly known administrator credentials that manufacturers use for their products, such as the password initially shipped with a router or wireless access point.</td>
</tr>
<tr>
<td><strong>DMS platform or platform</strong></td>
<td>Dealer Management System (DMS) applications such as Accounting or Service applications reside on a platform; the platform is the hardware, operating system (such as Linux or Windows), and software that is common to all applications.</td>
</tr>
<tr>
<td><strong>Event logs</strong></td>
<td>Computer data logging is the process of recording events with a computer program. By logging events, they can be audited at a later date in the case there is a need to determine what events led to a breach or abnormal software action.</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>Can be implemented in software or hardware; it is used to help keep a network secure. It controls the incoming and outgoing network traffic by analyzing the data packets and only allowing data that is allowed, based on a predetermined rule set.</td>
</tr>
<tr>
<td><strong>Financial Services - Information Sharing and Analysis Center (FS-ISAC)</strong></td>
<td>The only industry forum for collaboration on critical security threats facing the financial services sector</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Graham-Leach-Bliley Act (GLBA)</strong></td>
<td>Requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data</td>
</tr>
<tr>
<td><strong>Least privilege</strong></td>
<td>In information security, this principle (also known as the principle of minimal privilege or least authority) states that processes, users or programs must have access to only the data that is necessary for its intended purpose.</td>
</tr>
<tr>
<td><strong>Legacy programs or applications</strong></td>
<td>Old software or application programs no longer being updated or patched for security reasons because they have been replaced with newer software</td>
</tr>
<tr>
<td><strong>Malware</strong></td>
<td>Short for malicious software, it is used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.</td>
</tr>
<tr>
<td><strong>North Carolina data access disclosure law</strong></td>
<td>North Carolina General Statutes §20 305.7 – Protecting dealership data and consent to access dealership information <a href="http://www.ncga.state.nc.us/enactedlegislation/statutes/html/bysection/chapter_20/gs_20-305.7.html">http://www.ncga.state.nc.us/enactedlegislation/statutes/html/bysection/chapter_20/gs_20-305.7.html</a></td>
</tr>
<tr>
<td><strong>Payment Card Industry Data Security Standard (PCI DSS)</strong></td>
<td>A multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures; this comprehensive standard is intended to help organizations proactively protect customer account data specific to credit cards from the major brands, including American Express, Visa, MasterCard, Discover and Japan Central Bank.</td>
</tr>
<tr>
<td><strong>PCI Qualified Security Assessor (PCI QSA)</strong></td>
<td>A company approved by the PCI SSC to conduct PCI DSS on-site assessments</td>
</tr>
<tr>
<td><strong>Penetration testing</strong></td>
<td>A method of testing a network, system or application by simulating a malicious attack in order to find vulnerabilities</td>
</tr>
<tr>
<td><strong>Personally Identifiable Information (PII)</strong></td>
<td>Information that can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual</td>
</tr>
<tr>
<td><strong>Privilege misuse</strong></td>
<td>The act of using privileges for other purposes than the intended purpose for which they were given</td>
</tr>
<tr>
<td><strong>Regulatory requirements</strong></td>
<td>Requirements mandated by federal, state or local regulations.</td>
</tr>
<tr>
<td><strong>Remote Access Services (RAS)</strong></td>
<td>Refers to any combination of hardware and software employed to enable the remote access tools or information by a user outside of the business network</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Screen-scrape</td>
<td>A technique in which a computer program extracts data from human-readable output coming from another program.</td>
</tr>
<tr>
<td>Separation of duties</td>
<td>The concept of having more than one person required to complete a task (e.g. approving and signing large monetary transactions).</td>
</tr>
<tr>
<td>Spam</td>
<td>Junk email or unsolicited bulk email involving nearly identical messages sent to numerous recipients by email.</td>
</tr>
<tr>
<td>Secure Sockets Layer (SSL)</td>
<td>A protocol for encrypting information over the Internet.</td>
</tr>
<tr>
<td>Sun-setting a product</td>
<td>To end all support and maintenance of a product or application.</td>
</tr>
<tr>
<td>Technical or privileged users</td>
<td>User who, by virtue of function, has powers within the computer system that are significantly greater than those available to the majority of users. Such persons might include: System/Network Administrators, Chief Financial Officer or General Manager of a dealership, and programmers with special access to install, compile and run code on the system.</td>
</tr>
<tr>
<td>Unified Threat Management (UTM) device</td>
<td>Combines multiple threat prevention controls in one box or system, including but not limited to: web filtering, content filtering, email scanning, virus and malware scanning</td>
</tr>
<tr>
<td>Web filtering</td>
<td>A method of controlling access to the Internet by blocking Internet sites that are known to contain malware; can also be used to restrict users to only the sites of interest to a business (e.g. music sites can be blocked).</td>
</tr>
</tbody>
</table>
Appendix
