STAR®
Standards for Technology in Automotive Retail

STAR Dealer Data Security Guidelines
2018

INDUSTRY BEST PRACTICES AND RECOMMENDATIONS FOR AUTOMOTIVE RETAIL DATA SECURITY

1. STAR Dealer Data Security Guidelines

1.1 Overview

Purpose

The purpose of this document is to provide industry recommended security guidelines for automotive dealers to appropriately protect:

- Customer information
- Automotive dealers' and automotive OEM's information and assets
- Automotive dealers and automotive OEMs from security incidents that may disrupt business continuity.

In addition, this document provides uniform and standard practices to facilitate a consistent implementation strategy especially for multi-brand automotive dealers.

Applicability

This document applies to all automotive retail dealerships.

Use of this document

This document is organized so that it may be referenced by specific areas or topics. It is encouraged that the document initially be read in its entirety. However, it may be referenced by a specific section as needed.

The document presents the industry best practices and recommendations for data security in two "stages". Stage I is comprised of actions to be taken that include policies and procedures and can serve as the starting point and baseline in documentation and implementation for your dealership's security practices. The second Stage involves more complex safeguards, such as technologies and technical best practices, to secure the dealership network.

1.2 Disclaimer

Any company name, application, website link, or technology reference mentioned in this document should not be considered an endorsement by the OEMs or by STAR unless that endorsement is expressly stated.

This document provides a guideline for dealers to establish sound data security practices. It is important to note that network infrastructure, dealer data, and system security is the dealership's responsibility. Third-party organizations such as service providers and partners may provide guidance and recommendations. Some organizations may provide software, hardware, or proprietary network elements to help streamline network operations and secure data. However, these applications, recommendations, or tools are not a substitute for network management.

2. STAGE I – Security Policies, Procedures, and Compliance

Stage I identifies the security policies, procedures, and documentation a dealership should have in place to protect the dealer network and information residing on the dealer's network. These are often little-to-no cost actions in this stage. Stage II will aid in identifying the technologies, systems, and processes that should be in place to support the Stage I security goals.

2.1 Security Policies

The Security Policies framework of the dealership needs to be complete, consistent, and approved by the dealer's management body. It is important to ensure all stakeholders commit to the policies and agree to implement them in all relevant aspects of the dealership.

Policies should reflect the strategy for securing information - not the other way around - and understanding security requirements is the key factor here. The basic focus should be on confidentiality, integrity, and availability of sensitive data and resources including the physical environment, network infrastructure, applications, and data (both physical and digital). However, this is not a complete list, as there are many other considerations. For example, quite often non-repudiation, traceability, or authenticity should be considered.

Moreover, every industry has its own sensitive areas. For instance, we care much more about the integrity - rather than the confidentiality - of an airplane in the air or of a car on the highway in comparison to caring about the confidentiality of the medical history of a patient (which also may depend on the context). Security policies should reflect these considerations.

There are many out-of-the-box policies or framework directives for security from which to select and apply in a company. However, even though this kind of framework can provide a general baseline, a company will need to adjust and develop the policies for application within their business context.

General Guidelines

- Make sure there is a shared understanding with Management as to what needs to be protected as well as the ambition level regarding data protection. On the one hand, it is important that policies guarantee an expected level of protection. However, it is also very important that the policies are not so restrictive as to constrain the company from doing needed business.
- Make sure policies are aligned with laws and regulations (e.g., in the privacy area or industry-specific regulations).
- Develop policies to reflect actual and achievable security practices. It is better to have a small set of rules rather than a comprehensive document that is impossible to follow. Just in case the actual state is far from ambition level, develop a transition plan agreed upon by all key stakeholders to take an organization from as-is to the expected to-be level. It is very important to develop a good communication plan as a part of the overall security program.
- Policies should not be changed too often (to include the manner and language in which they are expressed). However, if needed, appropriate changes should be

applied as they should always reflect current security requirements and information security strategies.

- Policies should be expressed in such a way that there is no room for exceptions. This is related to both the commitment from all stakeholders to follow the policies as well as to the language. Otherwise, especially when many exceptions are allowed, the question may become whether the Management is really committed to the policy and/or the policy truly reflects the company's strategy for information protection.
- Policies should be expressed in such a way that there is no room for interpretation. In addition, policies need to be supported by guidelines, processes, procedures, roles with responsibilities, and interpretations so it is clear what to do in specific cases. It should also be clear to whom to turn to in case an interpretation or a decision is needed. It is also a good practice to also maintain knowledge base articles.
- Make sure appropriate solutions and technologies are available to support policy expectations. For instance, when a policy requires two-factor authentication in specific circumstances, then it is important the existing IT environment allows for an implement to this additional level of protection.
- Introduce a dashboard to track the level of policy implementation, allowing for reliable risk management as well as prioritization of efforts.

Guidelines with examples of policies deemed especially valid from a dealership perspective are as follows.

2.1.1 Acceptable Use Policy

Outlines the acceptable use of a business's physical and digital resources. Covers also ownership and control. Emphasize examples of prohibited activities.

2.1.2 Asset Management Policy

Assets represent everything what has value to the organization. Company assets are considered as both physical and logical dimensions.

Physical. Servers, hard disks, routers, mobile phones, removable media like DVDs or USB sticks, for example. It is important to keep track of the asset lifecycle with special focus being given to asset disposal and re-use.

Logical. It is important a company develop standards governing appropriate data collection, retention and use. These standards should consider what information is collected, how long it is kept, how it is stored, who may access it, and how access is achieved. This is very connected to the increased role of privacy regulation in different countries.

Additionally, an information classification policy with clear information ownership and protection requirements at different levels should be developed. It is so very important, it is sometimes considered in a separately, identifiable policy.

2.1.3 Business Applications Policy

Introduce a business application classification policy. Describe the requirements for protection on the application level for different levels of criticality (e.g., security zones placement, connectivity methods, identity and access control, applying defense in depth, fail securely, least privilege, and similar principles). Include the expectations regarding application architecture, communication with other systems, and separation of data between customers. Define expectations toward cloud-based solutions (which are becoming more and more popular).

Other aspect to specify is the way in which an application is procured by the company, what are the mandatory steps, what are the common requirements towards suppliers both functional and non-functional (e.g., SLA, security, identity management, integrations). Define expected audits of the acquired application (e.g., Pentest or Vulnerability Scan reports). Support policies with templates and guidelines to be shared with suppliers.

2.1.4 Electronic Communication Policy

In today’s technological age, companies have many options for communication and exchange of information. However, risks are associated with these options. For instance one may use a cloud service to communicate but it is also collecting data with malicious intention. It is important to regulate electronics communication such as emails and instant messaging, using boards like Trello, file exchange over Dropbox, and similar solutions and platforms.

2.1.5 Identity and Access Management Policy

One of the most critical areas. More details can be found in the relevant section of this guideline. Password policy should be included in this section.

2.1.6 Security Incidents Management Policy

There is no IT environment that can be secured 100%. A company needs to be ready for when there is a security incident. The Security Incidents Management Policy should be part of - or contribute to - overall incident management. Provide the definition of a security incident, introduce processes and procedures (i.e., response plan) for what to do in case of a security incident (depending on the incident category, e.g., hacking, wrong behavior, equipment failure), and the criticality. Define the exact procedures for response and action. For example:

- If a computer is compromised, disconnect it immediately from the network.
- If someone is entering without access card, ask about identity.
- Consider further forensic investigation.
- Consider emergency fixes to support Service and Business Continuity Plans.
- Consider who to notify in the event of an incident, both inside and outside the organization. The following parties may need to be informed: consumers, law enforcement, customers, and credit bureaus and other businesses that may be affected by the breach.

- Quite often there are also laws and regulations which require a specific behavior in case a data breach occurs and will depend on the country, state, and industry.

Policy may also expect to introduce appropriate technical solutions to support policy implementation.

More specific information on incident response can be found at: https://www.sans.org/reading-room/whitepapers/incident.

Sample incident handling forms and documentation can be found at https://www.sans.org/score/incident-forms.

2.1.7 Network Policy

Network policy is another very important aspect of the overall security. In development of a network policy, it is recommended to consider the following aspects:

- Define network zone classes with supporting organization (zone owner, zone operator, etc.), assign level of trust to every class, define allowed connections between different trust levels. Introduce more restricted network segments for more sensitive applications and data.
- A list of the network devices and the associated configurations as well as what is to be allowed to connect and to where.
- External network connections, VPNs (both for employees and external partners)
- DNS including naming structure as well as supporting infrastructure and scope
- Firewalls, reverse proxy and proxy configurations (e.g., all outbound traffic to go through a proxy, all sensitive inbound traffic to go over the reverse proxy)
- Wireless classes and standards on authentication and protection in transit. Separate, specific, and very limited segments for customers.
- Remote maintenance
- VoIP, telephony, and conferencing

2.1.8 Risk Management and Audit Policy

Define the risk framework and supporting auditing considerations. Describe the requirements for risk assessment and audits of the business' information and resources.

2.1.9 Threat and Vulnerability Management Policy

Define requirements on malware protection, security event logging and appropriate SIEM solution, intrusion detection, and vulnerability scanning. Establish the right ambition level on schedules of scanning as well as other supporting systems; all should be connected to risk management.

Aside from the examples listed above, there are other security policies and procedures a company should consider implementing to safeguard data. More information on such policies may be found throughout this document. Additionally, the SANS Institute is a great resource for developing and implementing such policies. For a variety of sample Security Policy templates, please visit: https://www.sans.org/securityresources/policies. There is also a great article on introducing security policies in a company: https://www.csoonline.com/article/2124114/it-strategy/strategic-planning-erm-how-to-write-an-information-security-policy.html.

2.1.10 Dealer Guidance on Security Policies

When determining the next steps to mature a dealership's security policies, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have identified and documented policies around acceptable use, audit, access management (including password) and basic network consideration (including external access and wireless standards).
- **Intermediate Maturity Level:** Dealerships have identified and documented policies for all expected areas. Moreover, have processes in place to deliver, educate, and support dealership personnel with documented security policies.
- **Advanced Maturity Level:** Dealerships regularly test, audit, and refine security policies and procedures.

2.2 Identity and Access Management

Cover identity and access management in a comprehensive way. Start with introduction and basic concepts followed by subsections: identity management, authentication, authorizations and why they are so important, access management process, end users and physical consideration and protection levels. Close with an introduction to the three levels of maturity.

2.2.1 Introduction

Gartner, Inc. defines Identity and Access Management (IAM) as a security discipline that enables:

- the right individuals to access
- the right resources at
- the right times for
- the right reasons.

Even though the definition is quite simple, it captures the essence and implies many considerations in different areas.

2.2.2 Basic Concepts and definitions

To set a baseline, define the basic terms related to Identity and Access Management.

- **Entity**: a real person or information system
- **Identity**: entity in a specific context (e.g., at work or in social media)
- **Identifier**: set of attributes which identifies identity (e.g., SSN, email, fingerprint)
- **Authentication**: a process of confirming identity claimed by an entity (e.g., by providing password)
- **Authorizations**: set of permissions assigned to someone or something (e.g., "you are authorized to see the medical records of patient XYZ")
- **Accounting/Auditing**: history of what happened

The above is to be considered in both physical and logical dimensions where physical refers to limiting access to buildings, rooms, and other physical IT assets, and logical refers to limiting access to the virtual computer world such as connections to computer networks, information systems, files, or data. Once the above is implemented, introduce the key element in this puzzle.

- **Access control**: is to make sure authorization rules are executed. One can think of it as the implementation of authentication, authorization, and accounting (AAA) in both physical and logical dimensions.

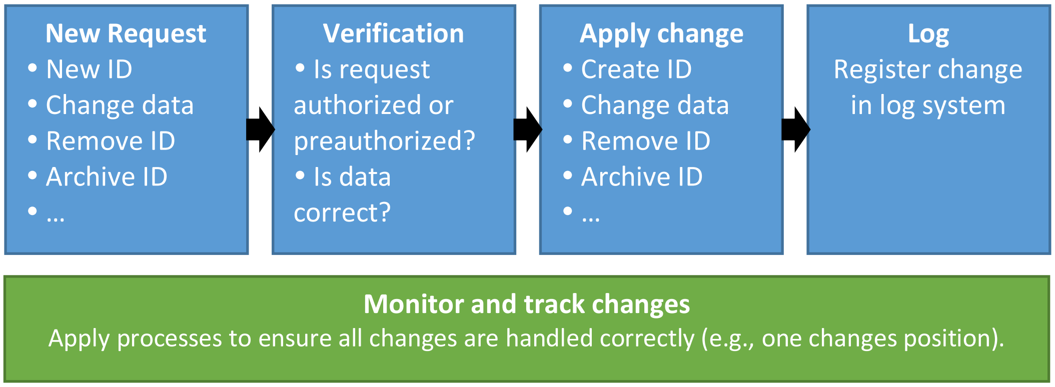
2.2.3 Identity Management

The following aspects of the identity management should be carefully considered:

- Lifecycle of identities
- Management and storage of identities
- Password management
- Identity Federation

Lifecycle of identities

Lifecycle should be considered from the moment a relationship starts till the moment when it is terminated and monitored over time for context changes (e.g., employee is changing assignment). The process can be illustrated as follows:


New Request
• New ID
• Change data
• Remove ID
• Archive ID
• …
Verification
• Is request authorized or preauthorized?
• Is data correct?
Apply change
• Create ID
• Change data
• Remove ID
• Archive ID
• …
Log
Register change in log system
Monitor and track changes
Apply processes to ensure all changes are handled correctly (e.g., one changes position).

- Limit the number of identities related to a specific entity and centralize management of them (e.g., try to avoid situations where there are application-specific accounts).
- Try to avoid group accounts. In case it is really needed, again, make sure that each one has its own custodian responsible for it.
- Remember that identities are related not only to end-users, but also to services or networks and these kinds of identities need to also be managed and maintained with care. Make sure that every non-personal identity has its own custodian responsible for it.
- Make sure storage of identities is protected, especially when confidential information is stored. Usually passwords are referred to as an example, but it can also refer to sensitive user information (e.g., GPS coordinates of visited locations).

It is recommended to follow common market standards and security protocols as well as products.

Password Management

Passwords need to be secured both in transit and storage. Additionally, procedures around passwords need to be designed with care. Storage of passwords can be considered from two perspectives.

- **From the server side** where identity is managed (e.g., Active Directory, business application, etc.).
    - Key aspects
        - Password must not be stored in a plain text and - in case it is encrypted in a reversible way, key for decryption needs to be protected in a correct way.
        - All vendor-supplied default passwords must be changed before any information system is put into operation.
- **From the client side** where a password is used to access resources. If there is a need to store a password, it is highly recommended to store that in an encrypted form (e.g., in a KeyPass application, encrypted Excel file). Then, it is important to protect the master password in a secure manner. It is very important to discourage employees from
    - writing down passwords and keeping them in a place visible to others (e.g., on a Post-it Note close to the workplace)
    - divulging passwords to anyone unless absolutely necessary (e.g., helpdesk assistance); and then remembering to change the password after divulging

All passwords should be promptly changed if suspected of/are being comprised, or disclosed to vendors for maintenance/support.

It is also important to make sure that all backups where passwords are stored are also secured with care.

Common procedures which need to be designed in a secure way:

- Sending the initial password in a secure way
- Password recovery in case it is forgotten
- Unlocking in case it is locked
- Self-service for password change
- Policies around password lifecycle (see policies section for passwords); but remember that too restrictive policies can also have negative consequences.

Identity Federation and Single Sign-On

Just in case a company is established with other partners on the IT systems level, it is worth a look at the Identity Federation policy. In short, it is about sharing the same identity between companies based on some level of trust. There is a set of mature technologies supporting the approach. These are the immediate benefits:

- Single Sign-On: end-user needs to authenticate once and gets access to a number of applications (without a need for re-authentication)
- Less cost related to managing identity lifecycle
- Less risk related to the need of keeping separate identities by an end-user

In the end, a calculation needs to be performed to determine whether or not it is worth the investment in Identity Federation in a specific context.

2.2.4 Authentication

The most common proof in authentication is the password, but there is also a problem: passwords are hard to remember. Therefore, it has become more and more popular to use passphrases instead. One needs to remember that recommending passphrases requires changes in policies as well as IT systems to support the new policies.

There are other options to authentication than the password such as biometry, one-time-passwords, or smartcards supported by RSA Tokens, mobile applications like Google Authenticator, or Yubikey. Every method is usually classified into one of three categories:

- Something you know (passwords, visual patterns)
- Something you have (smartcard, RSA token, smartphone)
- Something you are (biometry, behaviour)

There are 2 reasons for applying different authentication methods:

- Better user experience (e.g. biometry)
- Better security (smartcard)

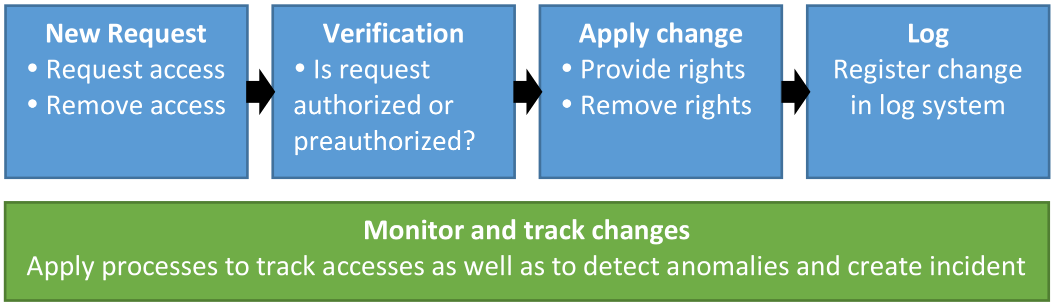
When two or more methods from different categories are combined, this is defined as ***multi-factor authentication*** which is about increasing the level of security.

2.2.5 Authorizations and Access Management Process

Correct authorizations - i.e., permissions' definition and its representation in IT systems - are one of the most important of the overall IT security landscape. The following aspects should be correctly secured:

- Define a structure of roles and access levels
- Define a set of permissions for given role
- Make sure authorizations are documented and easily accessible
- Make sure authorizations are implemented in access control systems
- Access requests are approved by correct people and it is clearly defined who are approvers
- Monitoring and reviews (audits) of access rights and authorizations

In addition, the ***Access Management Process*** needs to be established and implemented to make sure that defined authorizations are applied in every place at any point of time. The process is similar to the identity Lifecycle Management process and can be illustrated as follows:


New Request
• Request access
• Remove access
Verification
• Is request authorized or preauthorized?
Apply change
• Provide rights
• Remove rights
Log
Register change in log system
Monitor and track changes
Apply processes to track accesses as well as to detect anomalies and create incident

The key elements of such a process which should be considered:

- Access is revoked or modified anytime an employee departs the company or changes positions.
- Access should be updated in a timely manner reflecting business needs.
- Access should be reviewed periodically on a documented cadence (quarterly, semi-annually, annually). This evaluation, not prompted by employee exit or transition, is to determine if the level of access presently granted corresponds with the person's position in the business. Please note that frequency of reviews may vary depending on asset criticality which are protected.
- A good practice is also to apply "need to know" principle i.e., access to resources should be given only if there is a business need.

Once again, the importance of monitoring and auditing authorizations and access rights, especially to make sure that access removal is implemented correctly, cannot be overemphasized. Unfortunately, it is very common that access rights are provided and then never removed.

2.2.6 End users and Physical Consideration

It is a common knowledge that most problems with security are often caused by wrong people/user behaviour. (The ones related to the logical dimensions (like clicking dangerous emails) are covered in other sections.) The elements related to physical access control follow and should also be the basis for appropriate education strategy.

- Server/equipment rooms should be locked. Employee access should be limited to only those who have a legitimate business need. Mechanisms should be in place to know if and when someone accesses the site.

- Require that files containing sensitive data and information are kept in locked file cabinets at all times, other than when an employee is working on the file. Moreover, when an employee is working on the file, make sure that unauthorized people are not able to see the file (e.g., when flying on the plane).
- Remind employees not to leave sensitive documents/information out on desks when away from workstations.
- Require employees to put files away, log off computers, and lock file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building. Tell employees what to do and whom to notify if an unfamiliar person is seen on the premises.
- If offsite storage facilities are maintained, limit employee access to those with a legitimate business need. Mechanisms should be in place to know if and when someone accesses the site.
- If devices that collect sensitive information are used, such as PIN pads, secure the equipment to reduce the risk of tampering. Such equipment should also be secured to reduce the risk of an attacker switching equipment with a dummy device.

2.2.7 Protection Levels

Access control (including identity consideration) should be considered at many different levels.

- **Business applications**: applications needed to manage orders, schedule work, organize HR and finance, etc. Focus is on protection of sensitive business information and functionalities. Identities usually relate to end users.
- **Operating systems**: base for running applications on laptops, desktops, servers, phones, tablets, etc. Focus is on protection of files and data, against malware, what access control can support. Identities usually relate to end users (laptops, phones, etc.) and services (servers).
- **Infrastructure devices and supporting services**: routers, switches, access points, authentication services, etc. Focus is on protection of correct network traffic, keeping the communication secured, and keeping intruders away. Identities usually relate to technical users and services.
- **Mobile devices**: devices like phones, tablets, even laptops. Focus is on protection of data stored on devices and making sure it is accessible securely including scenarios like offline usage or theft of device.
- **Premises/physical**: buildings, server rooms, print rooms, offices, workshops, showrooms, etc. Focus is on making sure that people can enter the right places and get access to the right assets.

Moreover, one can map the above to the different network layers:

- Application layer (e.g., HTTP)

- Transport layer (e.g., TCP)
- Internet layer (e.g., IP)
- Network layer (e.g., Ethernet)

It is important make sure that there is full coverage of the IAM in different layers and areas according to the requirements which should be based on information criticality.

2.2.8 Dealer Guidance on Identity and Access Management (IAM)

When determining the next steps to mature a dealership's IAM, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

Basic Maturity Level

- Explicit processes for managing identities' lifecycle and access rights
- Regular audits and reviews of permissions for critical systems
- Explicit processes for password management
- Basic education of employees (at least for newly hired)
- Access control system for critical physical premises

Intermediate Maturity Level

- Explicit processes for managing identities' lifecycle and access rights
- Regular audits and reviews of permissions for critical systems
- Explicit processes for password management and recommendations on storing passwords on the client side
- Regular education of employees
- Access control system for all physical premises
- Level of protection (e.g., multi-factor authentication, defence in depth) related to the criticality of information and business functions

Advanced Maturity Level

- Automated processes for managing identities' lifecycle and access rights
- Centralized identities' storage and management including right level of identities' federation
- Centralized processes for password management and authentication
- Strong recommendations (or policies) on storing passwords on the client side
- Level of protection (e.g., multi-factor authentication, defence in depth) related to the criticality of information and business functions
- Centralized access control system for all physical premises
- Regular education of employees
- Regular audits and reviews of permissions and identities
- Comprehensive protection on all layers and for all types of applications and devices both on physical and logical dimensions

2.3 Patch Management

The operating systems on the local servers/computers require updates from time to time, many of which are due to security risks. Patches sent out by the manufacturer often provide protection from new or previously unknown exploits. It is critical these patches be managed, implemented, and verified to ensure a reliable, secure application. Furthermore, dealerships should pay special attention to the following:

- End of Life (EOL) systems
  - Keeping current with End of Life (EOL) of operating systems will assist in making sure the location is not using operating systems that no longer receive security updates or other kinds of updates because the supplier discontinued support.
  - Generally, suppliers provide notice of EOL and this can always be verified on their respective websites.
- Mobile devices
  - Mobile devices will often leave the protection of a dealership network and connect to another, often less secure network. Because of this, these devices can be considered more vulnerable. It is important that mobile devices are patched quickly to limit risk and exposure to threats and vulnerabilities.

2.3.1 Guidance with Patch Management

When determining the next steps to mature a dealership's patch management solution, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have each system set to automatically update for critical or security patches.
- **Intermediate Maturity Level**: Dealerships have an enterprise-wide patch management system in place.
- **Advanced Maturity Level:** Dealerships test, rollout, and validate patches as they become available as soon as possible.

2.4 Disaster Recovery

How will business continue to be conducted if something fails? Business continuity better describes the circumstances to an entity engaged in providing products or services. Disaster recovery is the answer to the question: how would the organization continue to operate if a business essential service/asset was not available (i.e., internet, telephones, computer access, power, and etc.)?

- The solution does not have to provide for all services 100% of the time, but it should enable a business to continue to conduct business in a "limp" mode until the issue is resolved.
- Essential retailer data should be backed up and verified regularly, using a backup service that has the following capabilities:
  - Offsite secured storage of media
  - Regular daily backups along with daily reviews of all system recovery events
  - Monthly reports summarizing the previous month's activities should be kept and reviewed by the Retailer

2.4.1 Dealership guidance with Disaster Recovery

When determining the next steps to mature a dealership's disaster recovery/ business continuity, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships regularly back up all systems.
- **Intermediate Maturity Level:** Dealerships perform regular incremental backups and store backup images offsite.
- **Advanced Maturity Level:** Dealerships deploy a business continuity system to include full system backups off site in a virtual environment that will allow the dealership to spin up the backup image immediately in case of an outage or failure.

2.5 Security Awareness Training

The vast majority of security incidents, including data breaches, are the result of human error – like clicking on a phishing email, for example. Just technicians are trained on the latest vehicle developments and sales people on new vehicle features and sales techniques, all your employees need to be trained on how to protect your business from theft, data breaches, and other security issues.

The goal of the training program is not just to educate your employees, but to influence their behavior. They are to become a human firewall for the company.

Security should not be boring – if people don't pay attention, the message will not permeate – so do not be afraid to get creative with the training and awareness program. Humor, real life examples, and contests and games are a few ways to keep it interesting and gain employee engagement.

To keep employees engaged, consider using shorter online security training modules more frequently rather than one long training sessions once a year. This will also help the training keep up-to-date on the latest developments in malware and attacks.

- Training should be annual, at minimum, and cover topics that include:
  - Social engineering awareness: phishing, Business Email Compromise (BEC), vishing, ransomware, safe web browsing
  - Passwords
  - Sensitive Data – PII, PCI, PHI, etc. – and data handling
  - Data sharing and acceptable use policies
  - Data protection and destruction
  - Mobile device security
  - Safe social networking
  - Workplace violence
  - Security-related company policies
- Further training may be necessary depending on the employee's role in the company. For example, employees that handle company finances may benefit from understanding the unique ways they are targeted by cyber criminals for the access they have to bank accounts. Consider role-based training to help employees understand the role they play in protecting the company in their daily activities.
- Use security awareness materials in break rooms and other employee-only spaces such as posters or fliers reminding employees of safe handling of customer data, social engineering awareness, training reminders, etc.

- Use company newsletters, emails, live training sessions, and other company functions to continually reinforce the security message.
- Regularly review training programs and adjust for new technologies, dealer business changes, and employee feedback.
- Resources. These can be free or paid, but some of your business partners may offer online security training for your employees.
  - DMS provider
  - Insurance provider
  - Accounting firm
  - Legal firm
- Leading security training vendors. These companies all offer online training modules. Pricing is usually based on the number of employees.
  - Wombat Security Technologies
  - SANS
  - KnowBe4
  - PhishMe
  - Security Mentor
  - Inspired eLearning
- Other resources:
  - https://staysafeonline.org/business-safe-online/train-your-employees
  - SANS Ouch – a free monthly security newsletter for employees https://securingthehuman.sans.org/resources/newsletters/ouch/2016

2.5.1 Dealer Guidance on Security Awareness Training

When determining the next steps to mature a dealership's security awareness program, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** All employees take annual security training. Training completion is documented and reporting is available for audit. Employees may be unsure of their role in protecting the organization. Organization may be compliant, but not secure. There is no established process for and/or employees do not feel empowered to report suspicious behavior or accidental data loss.
- **Intermediate Maturity Level:** Training program may be more frequent than annual, and follow up is conducted to ensure all employees participate as a condition of employment. Topics covered focus on the greatest risks to the organization. Awareness materials are posted in employee break areas. Employees are aware of company security policies and know how to recognize and report a security incident.
- **Advanced Maturity Level:** Training program for all employees and contractors includes short but frequent modules on timely topics relevant to their role. Employees are tested on their ability to defend against various social engineer tactics like phishing, USB drops, fraud, etc. Employees know how to report a security incident and when tested, at least 50% of employees report something suspicious. When tested, less than 10% click on phishing test emails. Dealership has a culture of security – employees understand their role in protecting the organization, seek out secure processes, and encourage their co-workers to

conduct business in a way that values security and protecting the organization from fraud, theft, and accidental data or financial loss.

2.6 Compliance with Federal Legislations

Ensure the dealer complies with all federal, state, local, and industry regulations for financial and retail institutions such as the Gramm-Leach-Bliley Act, Safeguards Rule, PCI DDS, etc.

2.6.1 Gramm-Leach-Bliley(GLB) Act *and* Safeguards Rule

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. The Gramm-Leach-Bliley (GLB) Act requires businesses defined as "financial institutions" to ensure the security and confidentiality of sensitive information. Because dealers lease and lend (even if through a 3rd party), they must adhere to the GLBA Act.

The Safeguards Rule was issued by the Federal Trade Commission (FTC), as part of the GLB Act. The Safeguards Rule requires financial institutions to have measures in place to keep customer information secure.

For more information on these legislations and the requirements, please visit: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

2.6.2 Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise.

All merchants storing, accepting, processing, and/or transmitting cardholder data must comply with technical and operational requirements set forth by PCI DSS. All dealerships must adhere to the PCI DSS. However, there are different requirements for reporting and auditing for dealerships based upon merchant level. Merchant level is determined by the number of credit card transactions at the dealership. For more information on PCI DSS and these requirements, please visit: https://www.pcisecuritystandards.org

2.6.3 Dealer Guidance on Compliance with Federal Legislations

When determining the next steps to mature a dealership's compliance with security legislations, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have researched PCI and GLBA to determine compliance with federal legislation. Dealers have documented policies and processes to meet compliance.
- **Intermediate Maturity Level:** Dealerships regularly review and revise compliance with federal security legislation

- **Advanced Maturity Level:** Dealers perform regular audits on systems and track results back to legislation requirements.

2.7 Additional Resources

The following organizations have information to help implement appropriate safeguards for data:

- *Computer Security Resource Center National Institute for Standards and Technology (NIST)* - http://csrc.nist.gov
- *National Strategy to Secure Cyberspace, Department of Homeland Security* - http://www.dhs.gov/files/publications/editorial_0329.shtm
- *The SysAdmin, Audit, Network, Security (SANS) Institute the Twenty Most Critical Internet Security Vulnerabilities* - www.sans.org/top20
- *United States Computer Emergency Readiness Team (US CERT)* - www.us-cert.gov/resources.html
- *Carnegie Mellon Software Engineering Institute CERT Coordination Center* - www.cert.org

3. STAGE II – Security Systems and Technologies

Stage II focuses on the systems and technologies that should be in place at a dealership to to support the policies, procedures, and compliance goals stated in Stage I of this document.

3.1 Network Security

Dealerships need to focus on the security and data integrity of the dealership local area network (LAN). This starts with policies on network usage for employees and guests. These policies should include what data each user has access to, what resources on the network each user can access, and where data is stored on the network. The policies should also deliberately state which devices company data is stored on. See stage I for more guidance on security policies and practices. General guidance for policies should be followed:

Internet Usage Policy should be enforced for customers and dealership employees.

- An internet Usage Policy stipulates the rules and guidelines related to appropriate use of company equipment, network, and Internet access. Having such a policy in place helps to not only protect the business but its employees as well. The policy will help to inform employees that certain behaviors are prohibited (such as downloading files, visiting certain websites, etc.) and failure to comply with the policy could result in serious repercussions.
- The Internet Usage Policy is an important document that should be signed by all employees upon employment commencement.

Beyond policies, the network should be configured and segmented as securely as possible to avoid unwanted access. This starts with the network gateway. For more information on proper network gateway security, see section 3.4 on Unified Threat Management (UTM).
A UTM can help with the following:

Encryption, Segmentation, and remotes access to the dealership network:

- Payment Card information, customer information, dealership traffic, and customer traffic should be segmented via network segmentation (such as VLAN, Layer 2 switch, etc.) or a different network (such as a dedicated circuit for guests) to ensure no communication can take place between the networks.

- Wireless networks should be encrypted with the most current and secure encryption standard (such as WPA2 with RADIUS authentication and AES Encryption).
- Remote access to the dealership network should be limited to secure VPN connections from known sources such as employees and trusted vendors. Two factor authentication should be enforced when possible.

Finally, the security of the dealership network should be monitored 24x7 by network experts. Experts should have the tools and ability to respond to network security events in near real time. A documented incident response plan should be followed upon any network indication of compromise. More information on security information event management is found in section 3.5 of this document.

3.1.1 Dealer Guidance on Network Security

When determining the next steps to mature a dealership's network security, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have developed and documented an internet usage policy. Dealerships have protection at the network gateway and have configured and segmented the network to avoid unwanted access to network resources. The network is monitored by security information event management technologies in real time to protect against unwanted network access. Remote access is monitored and restricted on the network.
- **Intermediate Maturity Level:** Dealerships have used documented policies and processes to set up a secure, segmented dealership network. Dealerships regularly test the network against known risks. The network is monitored 24x7x365 by security experts using security information event management technologies. Remote access monitored and restricted to known vendors and employees.
- **Advanced Maturity Level:** Dealerships have used documented policies and processes to set up a secure, segmented dealership network. Dealerships regularly test the network against known risks. The network is monitored 24x7x365 by a SOC 2 certified service provider. The network is monitored 24x7x365 by security experts. Remote access monitored and restricted to known vendors and employees. Employee VPN access is achieved by two factor authentication.

3.2 Antivirus

In this section Antivirus refers to software services running on end points, severs, firewalls, and other devices connected to the dealership's network that manage threats to those devices. This includes threats for ransomware, application exploitations, and software vulnerabilities. Dealerships need a robust end point management solution to ensure the security of the device and data residing on the device itself. The following best practices are recommended:

- Maintain active subscription to Enterprise class antivirus solution that uses regular automatic signature updates. The software should have the capabilities to:

  • Download and install most current virus signature updates
  • Actively monitor for viruses
  • Quarantine and eradicate infected files
  • Antivirus solution should include antivirus, anti-spyware, intrusion prevention, application control, spam control and rootkit detection

- Software should be used on all firewalls, servers, and clients to help prevent damage to dealership data.
- In the case of an indication of compromise on the machine, and alert should be sent to a network administrator or security engineer to immediately investigate and remediate the potential threat.

3.2.1 Guidance with Dealership Antivirus

When determining the next steps to mature a dealership's AV security, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have identified all systems and applied antivirus software to each system on the network.
- **Intermediate Maturity Level:** Dealerships have an enterprise antivirus system in place. This includes enterprise-wide license management, an enterprise portal for reporting and response, and audit and reporting across the entire network.
- **Advanced Maturity Level:** Dealers perform proactive, immediate response to alerts generated by the corporate AV solution.

3.3 Email Security

- **Overview**: Email security is a critical risk for many of the world's largest organizations. Today, 91% of all successful attacks on enterprise networks involve the use of email. An email security solution will provide inbound and outbound content inspection, encryption, and security alerting to mitigate many of these risks.
- **Outbound Email Security**: identify and respond to malware, inappropriate emails, unauthorized content, and company-private information before it leaves the network.
- **Inbound Email Security:** Apply filters to stop malware, phishing, or malicious emails before entering the network.
- **Encryption:** TLS Email Encryption is recommended to make it more difficult for third parties to read email in transit.

3.3.1 Dealer Guidance on Email Security

When determining the next steps to mature a dealership's email security, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have taken steps to implement technologies to protect dealer email systems.
- **Intermediate Maturity Level:** Dealers perform active inbound and outbound email security inspection and protection. Dealers encrypt sensitive data through email.
- **Advanced Maturity Level:** Dealerships have active email monitoring and response to email threats.

3.4 Unified Threat Management (UTM)/Firewall/Intrusion Detection System (IDS)

At a minimum, implement at the network edge with regular subscription signature updates. Ideally, the solution should include the following features:

- Fully-managed security device that continually monitors threats through Intrusion Detection System "IDS" and Intrusion Prevention System "IPS" and other mechanisms such as packet filtering, antivirus, and stateful packet inspection.
- Firewalls should support Network Address Translation/Process Analytical Technology (NAT/PAT).
- Firewalls should also support dynamic routing using RIPv2, OSPF, and BGP.
- Keep on backup configuration on file in the case of a software failure or hardware replacement.

3.4.1 Guidance with UTM/Firewall/IDS

When determining the next steps to mature s dealership's unified threat management, firewall, and intrusion detection system, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships deploy a fully managed and licensed UTM which includes licensing for AV, SPAM, and IDS/IPS. Signatures are automatically updated in real time.
- **Intermediate Maturity Level:** Dealerships respond to alerts and events from the UTM 24x7x365 in real-time. Dealerships utilize a SIEM (see section 3.5) to alert and respond to events at the network gateway.
- **Advanced Maturity Level:** Dealerships turn to a managed security service provider (MSSP) for proactive, 24x7x365 UTM management, monitoring, and response.

3.5 Security Information Event Management(SIEM)

A SIEM solution provides visibility beyond AV or firewall protection. The ultimate goal of a SIEM solution is to collect and inspect network security traffic to find indications of compromise. This indication should be sent, as an alert, to a qualified resource to perform investigation and potential remediation activities immediately. It is important to note that the adoption of SIEM software alone is not adequate to protect the dealer network. Dealerships must have processes and resources in place to respond to the information generated by the SIEM technology. General guidance for dealership security information management is as follows.

Dealerships must have:

- Proactive, real-time event monitoring that utilizes a SIEM service.
- SIEM needs to be able to collect data with capability to aggregate and correlate varying security data from the network in real-time.
- The SIEM service provider needs to be able to notify the network administrator in the case of a security event as well as provide the proper documentation for compliance purposes.
- The ultimate purpose of a SIEM service is to aid in identifying or preventing an intrusion into your network. Immediate response to a breach can greatly reduce or prevent data loss.

Note: Reactive management software (i.e., Desktop firewall or antivirus) is not to be confused with a proactive SIEM service

3.5.1 Guidance with SIEM

When determining the next steps to mature a dealership's security information event management, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships install and utilize SIEM software. All alerts are responded to in near real-time 24x7x365. All system logs are stored in accordance with federal legislation (see section 2.6 on compliance with federal legislations).
- **Intermediate Maturity Level**: Dealerships utilize a managed security service provider for advanced monitoring and response. Dealerships integration threat intelligence for advanced monitoring and alerting.
- **Advanced Maturity Level:** Dealerships turn to a SOC 2 certified managed security service provider (MSSP) for proactive, 24x7x365 UTM management, monitoring, and response. Dealerships integrate threat intelligence into the SIEM solution. Tickets, alerts, and activity is regularly reviewed by dealership management and MSSP for security posture refinement, documentation, and improvement.

3.6 Wireless Detection Systems

Scan, identify, and remove any rogue wireless access points that may be on the retailer network. A rogue wireless access point is defined as a wireless point of entry into the dealership network that has is not authorized, secured, or known about by dealer IT, management, and ownership.

- All rogue wireless networks must be detected, found, and removed immediately.
- STAR recommends the use of a managed wireless detection service that is continuously scanning the network for wireless threats.

3.6.1 Dealer Guidance on wireless detection systems

When determining the next steps to mature a dealership's wireless detection, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships perform physical inspection for rogue wireless networks at least quarterly.

- **Intermediate Maturity Level**: Dealerships utilize technology to scan and alert the dealership of potential rogue wireless networks.
- **Advanced Maturity Level:** Dealerships turn to a partner or technology to identify, investigate, and respond to alerts for potential rogue wireless networks immediately.

3.7 Application Security

In the below consideration, assume that all applications are acquired from external vendors and deployed either without any modification, or only a small customization is applied. Moreover, by an application, it is understood to be business applications and the application security is to make sure that all data processed - and all business functions offered by the application - are protected appropriately.

3.7.1 Areas and key activities

Recommend consideration of the following areas:

- Perform an inventory of applications. Document what applications are on the dealership network, what their purpose is, who is responsible for, and how to get support. Perform Business Impact Analysis (BIA) including information classification to understand business criticality and apply correct prioritization. This catalog will also help in finding and eliminating rogue applications that can become a threat to the dealer network and data security.
- Protect processed information in transit and in storage. Make sure that sensitive and critical data is well protected both from a confidentiality and integrity perspective. Review both application-to-application integrations as well as internal communication applications, especially connections to database, which are very often forgotten. If needed, make sure correct cryptography is used for protection in storage. Finally, make sure information flows are protected from end-to-end perspective.
- Consider additional business requirements such as authenticity, non-repudiation, or traceability; often required to meet privacy regulations (e.g. GDPR).
- Apply the defense in depth principle by introducing right security zones setup and application components placement, additional infrastructure services like reverse proxies or web application firewalls, and access control layers like multi-factor authentication, etc.
- Introduce right identity and access management strategy (see more in the IAM section). Apply the least privilege and need to-know principles.
- Expect from a supplier the result of an application vulnerability scanning conducted by an independent third-party company. Make sure all high and medium risks are addressed.
- Part of security is also to make sure that business transactions are handled without errors and on the expected level of quality. By that, one can expect a supplier company to provide test results or audits reports.
- Introduce processes for handling incidents, access requests, etc. Consider introducing monitoring of business applications to trace or even prevent unwanted events. Usually this is a part of an IT service management implementation.

- Perform, on a regular basis, threat modeling activities to make sure application landscape risks are documented, mitigated, and kept under control.
- Apply application updates and patches as soon as possible to limit exposure to potential exploits.

3.7.2 Dealer Guidance on Application Security

When determining the next steps to mature a dealership's application security, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

Basic Maturity Level

- Introduce an application catalogue.
- Maintain basic identity and access management.
- Apply application updates and patches on a regular basis.

Intermediate Maturity Level

- Maintain application catalogue with understanding of business impact analysis and information classification.
- Implementation of mature identity and access management strategy.
- Protection of information flows from the end-to-end perspective both in transit and storage.
- Introduce processes for handling incidents and access requests.
- Apply defence in depth strategy.

Advanced Maturity Level

- Apply all items from the previous section.

3.8 Mobility

This area is strongly connected to other areas like application security or email security. However, it is considered separately due to the additional risks it introduces by much less control of these kind of devices. Mobile devices defined here as smartphones, tablets, laptops, and any other specialized devices which processes or stores company data.

3.8.1 Areas and key activities

Consider the following:

- Create policies and procedures on who, when, and how to remotely access the company environment (network, servers, applications, etc.) and which parts of it. For instance, a policy can allow smartphones and tablets to access an external company network and restrict access to the internal company network; and allow access to the internal company network for managed laptops over VPN. Deploy an appropriate technical solution to support established approach.
- Define what information can be processed and stored on the mobile devices, include considerations related to managed and unmanaged devices.
- Introduce policies, procedures, and technical capabilities to define what software can be installed and executed on all types of mobile devices. In case of unmanaged devices, introduce conditions where company data is not exposed to unacceptable risks (e.g., by installing solution like MobileIron or Microsoft Intunes for smartphones).

- Access to devices should be restricted, requiring user authentication. Most devices can be locked with a screen lock, password, or PIN.
- Apply the appropriate identity and access management strategy.
- Make sure about the correct configuration and hardening of device and operating system (e.g., BIOS password, device level encryption, availability of USB and SD ports). Make sure that (especially in case of Android and iOS devices) the device is not rooted and jailbroken.
- Keep an updated and, preferably, centrally managed antimalware software both on laptops and smartphones.
- Update the mobile OS with security patches. More information on patch management can be found in section 3.2.
- Apply appropriate encryption of data both on laptops and mobile devices with special care of key management for decryption.
- Review all connectivity methods, being careful with automated wireless connectivity since passwords may be exposed as well as man-in-the-middle attacks can be executed.
- Enable remote data wipe option if available.
- Regularly back up the mobile device.

3.8.2 Dealer Guidance on Mobility

When determining the next steps to mature a dealership's security in mobility, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

Basic Maturity Level

- Keep updated antimalware software.
- Define what information can be processed and stored on the mobile devices, include considerations related to managed and unmanaged devices.
- Access to devices should be restricted, requiring user authentication. Most devices can be locked with a screen lock, password, or PIN.
- Update the mobile OS with security patches. More information on patch management can be found in section 3.2.

Intermediate Maturity Level

- All items from Basic Maturity Level.
- Apply appropriate encryption of data both on laptops and mobile devices with special care of key management for decryption.
- Review all connectivity methods, be careful with automated wireless connectivity since passwords may be exposed as well as man-in-the-middle attack can be executed.
- Create policies and procedures on who, when, and how to remotely access remotely the company environment (network, servers, applications, etc.) and which parts of it. Deploy appropriate technical solution to support established approach.
- Regularly back up the mobile device.

Advanced Maturity Level

- Apply all items from the previous sections.

4. Glossary

802.11: 802.11 is a group of wireless specifications developed by the IEEE for wireless local area network (WLAN) communications. It details a wireless interface between devices to manage packet traffic to avoid collisions. Some common specifications include the following: 802.11a, 802.11b, 802.11g, 802.11n, etc. The 802.1X standard is designed to enhance the security of wired and wireless local area networks that follow the IEEE standard.

Access Control: A security technique that refers to the process of regulating who and what has access to resources, objects, or data. Access control can be both physical and logical. Physical access control limits access to buildings, rooms, and physical IT assets. Logical access limits connections to computer networks, files, and data.

Antenna: A device for transmitting and receiving radiofrequency (RF) signals. Often camouflaged on existing buildings, trees, water towers, or other tall structures, the size and shape of antennas are generally determined by the frequency of the signal they manage.

App (Application): Downloadable tools, resources, games, social networks, or almost anything that adds a function or feature to a wireless device that are available for free or a fee. Some applications may also offer users the ability to purchase content or enhanced features within the application. Parents may limit their child's ability to download or make these in-app purchases by password protecting those features on a wireless device.

Broadband: A transmission facility having a bandwidth (capacity) sufficient to carry multiple voice, video, or data channels simultaneously. Broadband is generally equated with the delivery of increased speeds and advanced capabilities including access to the Internet and related services.

Cat 5: A twisted pair cable type designed for high signal integrity. Many such cables are unshielded but some are shielded. Category 5 has been superseded by the Category 5e specification. This type of cable is often used in structured cabling for computer networks such as Ethernet and is also used to carry many other signals such as basic voice services, token ring and ATM (at up to 155 Mbit/s, over short distances).

Cat 5e: The category 5e specification improves upon the category 5 specifications by tightening some crosstalk specifications and introducing new crosstalk specifications that were not present in the original category 5 specifications. The bandwidth of category 5 and 5e is the same - 100 MHz.

Cat 6: A cable standard for gigabit Ethernet and other network protocols that is backward-compatible with the Category 5/5e and Category 3 cable standards. Cat 6 features more stringent specifications for crosstalk and system noise. The cable standard provides performance of up to 250 MHz and is suitable for 10BASE-T / 100BASE-TX and 1000BASE-T (gigabit Ethernet). It is expected to suit the 10GBASE-T (10gigabit Ethernet) standard, although with limitations on length if unshielded, Cat 6 cable is used. STAR recommends Cat 6 cabling when running new cable or replacing new wired network segments.

DSL (Digital Subscriber Line): A digital line connecting the subscriber’s terminal to the serving company’s central office, providing multiple communications channels able to carry both voice and data communications simultaneously.

Encryption: Digitally scrambling information so it can be transmitted over an unsecure network. At the other end, the recipient typically uses a digital "key" to unscramble the information so it is restored to its original form.

Handheld/Tablet PCs: These devices are computers that can be carried by a user. These are typically much smaller than a typical laptop and do not have the full capability of desktop computers, but can still perform most necessary tasks. They will also allow a user to perform work in various locations of a dealership, which can increase productivity.

IEEE (Institute of Electrical and Electronics Engineers): A professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence. It has about 425,000 members in about 160 countries, slightly less than half of whom reside in the United States (http://www.ieee.org).

LAN (Local Area Network): Local Area Network (LAN) is a small data network covering a limited area such as a building or group of buildings. Most LANs connect workstations or personal computers. This allows many users to share devices such as laser printers as well as data. The LAN also allows easy communication by facilitating email or supporting chat sessions.

Malware: Malware (“malicious software”) is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, and Trojan horses as well as spyware (programming that gathers information about a computer user without permission).

Megahertz: Megahertz (MHz) is a unit of frequency equal to one million hertz or cycles per second. Wireless mobile communications within the United States generally occur in the 800 MHz, 900MHz, and 1900MHz spectrum frequency bands (Wi-Fi = 250, 400).

Operating System: The software component of a computer system responsible for the management and coordination of activities and the sharing of the resources of the computer. The operating system (OS) acts as a host for application programs that are run on the machine. As a host, one of the purposes of an operating system is to handle the details of the operation of the hardware.

Patch management: The process of updating servers or PCs. This is often done to update machines to the latest security patches and service packs. Writers of viruses, spyware, and other malicious software exploit existing flaws in software loaded on a PC to spread and to do damage. STAR recommends dealerships apply critical patches, such as security, as soon as possible.

Rogue wireless access point: A wireless point of entry into the dealership network that is not authorized, secured, or known about by dealer IT, management, and ownership. Any rogue wireless networks must be detected, found, and removed immediately.

Routers: Allow computers from different networks and subnetworks to communicate. In dealerships, routers may be used to connect an OEM LAN, dealership LAN, and DMS LAN to the Internet.

Security policy: A formal plan that addresses how security will be implemented within an organization. The policy should describe the approaches taken to ensure the confidentiality, availability, and integrity of sensitive data and resources including the physical environment, network infrastructure, applications, and data (both physical and digital).

Spectrum: The radio frequencies that are designated for a specific use such as personal communications services and public safety.

Spyware: Any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a Spybot or tracking software), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Dealers must deploy systems to detect and remove spyware to protect customer data, and network security integrity.

SSID (Service set identification): In computer networking, a SSID is a set consisting of all the devices associated with a IEEE 802.11x wireless local area network. SSIDs must be associated with a specific VLAN.

TCP/IP (Transmission Control Protocol/Internet Protocol): A protocol permitting communications over and between networks. The TCP/IP protocol is the basis for the Internet communications.

Transport Layer Security (TLS): A protocol that provides privacy and data integrity between communicating applications and their users on the Internet. When a server and client communicate, TLS safeguards Dealers from eavesdropping or tampering with the message. Secure Sockets Layer (SSL) is the predecessor to TLS.

Trojan (Trojan horse): Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining a certain area on your hard disk.

VPN (Virtual Private Networks): A VPN allows a user to conduct secure transactions over a public or unsecure network. By encrypting messages sent between devices, the integrity and confidentially of the transmitted data is kept private.

VLAN (Virtual Local Area Network): In computer networking, a single layer-2 network (switch-based) may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN. This is usually achieved on switch or router devices.

VoIP (Voice over Internet Protocol): VoIP is not simply capable of delivering voice over IP, but is also designed to accommodate two-way video conferencing and application sharing as well. Based on IP technology, VoIP is used to transfer a wide range of different type traffic.

WAN (Wide Area Network): A general term referring to a large network spanning a country or around the world. The Internet is a WAN. A public mobile communication system such as a cellular or PCS network is a WAN. Dealerships can network remote locations and buildings via WAN technology. In most dealer terms, WAN refers to the dealership Internet service provider.

Worm: A worm is a self-replicating virus that does not alter files, but duplicates itself. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Wi-Fi: Wi-Fi provides wireless connectivity over unlicensed spectrum (using the IEEE 802.11a or 802.11b standards), generally in the 2.4 and 5 GHz radio bands. Wi-Fi offers local area connectivity to Wi-Fi-enabled computers. STAR recommends WiFi 802.11n standard.

WPA (Wi-Fi Protected Access): A security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA is not secure and should not be used by dealers.

WPA-2 (Wi-Fi Protected Access II): WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. WPA-2 is the STAR wireless security standard.

Wireless Local Area Network (WLAN): Using radio frequency (RF) technology, WLANs transmit and receive data wirelessly in a certain area. This allows users in a small zone to transmit data and share resources, such as printers, without physically being connected.