FTC Safeguards Rule:

A Guide for Auto Dealerships

cyberdefenselabs.com

CYBER DEFENSE LABS

TABLE OF CONTENTS:

500 Crescent Court, Suite 300
Dallas, TX 75201
+1.972.737.8200
CyberDefenseLabs.com

CYBER DEFENSE LABS

To our auto dealer friends –

We have spent the past several months working with your colleagues nationwide in response to recent updates made to the FTC's Safeguards Rule. We understand the anxiety many of you are experiencing as you realize how big an undertaking compliance will be.

We are here to help.

Cyber Defense Labs will work together with you as trusted partners to strengthen your information security program, ensure compliance with the updated Safeguards Rule and provide peace of mind so you can focus on keeping your business moving forward.

If you are concerned about your level of compliance with these new guidelines, or have questions about how the Safeguards Rule may impact your dealership, please give our team a call at 972.737.8200. You can also email us at experts@cyberdefenselabs.com.

Thank you,

Katy Montgomery

Katy Montgomery

Executive Vice President

INTRODUCTION TO THE SAFEGUARDS RULE

The Federal Trade Commission's (FTC) "Safeguards Rule" was created to ensure data collected by non-banking financial institutions – a designation that includes auto dealerships – are protected from security breaches. It requires dealerships to implement and maintain a comprehensive security program to keep customer data safe.

The original Safeguards Rule was born out of broader federal data protection legislation passed in the late 1990s. Despite the rule's recommendations, data breaches and cyberattacks targeting dealerships and other non-banking institutions continued to escalate. This prompted the FTC to strengthen the rule in late 2021.

The newly updated Safeguards Rule includes more stringent regulations on what protections dealerships must implement to secure and protect their data. It could include steep consequences for non-compliance.

Timeline:

- November 1999 – Gramm-Leach-Bliley Act (GLBA) enacted
- May 2003 – FTC enacts first Safeguards Rule
- 2003 to 2019 – Data breaches increase, regulatory environment evolves
- March 2019 – FTC proposes updates to Safeguards Rule
- January 2022 – Updates to Safeguards Rule finalized
- December 2022 – All Safeguards Rule requirements in full effect

WHY DO CYBERCRIMINALS TARGET AUTO DEALERSHIPS?

There are multiple reasons why cybercriminals target auto dealerships:

- Dealerships collect, store and share enormous quantities of sensitive customer data – particularly financial data.
- There tends to be multiple points of entry available to criminals searching for this type of data – which is considered very valuable.
- Dealerships nationwide are experiencing a rapid digital transformation accelerated by the COVID-19 pandemic. This digital transformation is creating vulnerabilities that criminals are exploiting.

Threat Actors Involved

Criminal actors: Often motivated by financial gain, criminal actors typically conduct nefarious activity through computers and online systems. The cyberattack of choice for many of these criminal actors is ransomware, often delivered by phishing attack.

Insider threats: These are employees, vendors, and customers whose access to your physical location or digital environment is wittingly or unwittingly leveraged to do harm.

Hacktivists: Hacktivists disrupt, interrupt, or shut down a company's business operations in order to promote a social or political belief.

Nation-state actors: Some foreign states use cyber operations as a tool of national power to steal information, influence populations, and damage industries. Over the past decade, state-sponsored hackers have compromised software and IT service supply chains to facilitate espionage and sabotage operations.

AUTO CYBERSECURITY DEALERSHIP STATS

85% of dealerships worldwide have experienced a cyberattack since 2018 *(CDK Global)*

70% of surveyed dealerships do not have up-to-date antivirus software *(Total Dealer Compliance)*

Only 27% of dealerships are testing incident response plans. *(CDK Global)*

84% of customers would not buy another vehicle from a dealership after their data has been compromised *(Total Dealer Compliance)*

SIGNS YOUR DEALERSHIP IS AT RISK OF A CYBERATTACK

Dealerships face a constantly evolving cyber threat landscape due to the increasing amount of financial and personal data gathered and stored as a part of normal business operations. How your dealership collects, stores, shares and protects this information can determine your level of cyber risk and exposure to harm.

Are any of these statements true about your dealership?

- You do not currently have a cybersecurity program in place
- You are not familiar with the specific cyber risks impacting your dealership
- You haven't conducted a risk assessment within the past 12 months
- You are not reviewing risks associated with your third-party partners and vendors
- You have not conducted a data and systems inventory
- You do not have an incident response plan outlining how you would respond to a cyber-related incident or loss of service
- You do not have 24x7x365 security monitoring in place to detect cyber threats and malicious events

If any of the above statements are true, then you are at greater risk of experiencing a cyberattack.

CHANGES TO THE SAFEGUARDS RULE IN 2022

Previous Rule	Updated Rule
Requires dealerships to undertake a risk assessment	Requires written risk assessment including risk criteria and how the dealership's information security program will address and mitigate risks Requires additional periodic risk assessments
Requires dealerships develop, implement and maintain an information security program (based on the risk assessment) to address the identified risks	Requires the information security program to include: • Access controls • Data and systems inventory • Data encryption • Multi-factor authentication • Customer information disposal procedures • Change management procedures • Policies, procedures, and controls to monitor and log activity • Regularly test/monitor key controls, systems, procedures • Continuous monitoring of information systems or – Annual pen testing – Vulnerability assessments every six months • Employee training • Evaluate safeguards from third-party service providers • Written incident response plan
Allows dealerships to designate one or more employees to coordinate the information security program	Requires the designation of a single "qualified individual" to oversee and implement the program and provide periodic reports to boards of directors or governing bodies

THREE KEY TAKEAWAYS FOR DEALERSHIPS ABOUT THE SAFEGUARDS RULE

1 **Time is running out to achieve compliance:** The updated Safeguards Rule goes into full effect in December of 2022. This means dealerships need to begin working now to be ready in time. If your dealership does not have the internal bandwidth or resources to achieve compliance, you need to a engage with an expert cybersecurity services provider.

2 **Virtually all data is covered by this rule:** The FTC has a very broad definition of data as covered by the updated Safeguards Rule. This includes data provided directly by customers to obtain products or services, any data that is customer-related, and data resulting from or in conjunction with a transaction. Hardly any data are excluded.

3 **Boards of directors will have to be engaged:** The new rule requires regular reports to company boards including the overall status of the dealership's information security program, the dealership's current level of compliance with Safeguards Rule, the most recent risk assessment, any new management and control decisions, service provider arrangements, test results, information on security events or violations (and management's responses thereto), and recommendations for changes.

PENALTIES FOR NON-COMPLIANCE

Violations can result in publicly-filed complaints against the dealership, consent or settlement orders in which the FTC requires certain activities and recordkeeping and monitors the dealership for a period of years, and monetary fines for violating the consent order.

WHO'S EXEMPT FROM THE SAFEGUARDS RULE?

If an auto dealership collects information on **fewer than 5,000 customers**, then it is exempt from certain requirements of the newly updated Safeguards Rule including the written risk assessment, the incident response plan, and the annual report to a board of directors.

HOW SHOULD DEALERS APPROACH COMPLIANCE?

For many dealerships in the United States, complying with the updated Safeguards Rule may seem like a daunting challenge. Here are a few tips for how to get started:

- **Be strategic:** No one knows more about your unique dealership environment than you. It is important to ensure any cybersecurity investments you make support your overall business strategy and protect the assets most critical to your strategic business objectives and operations.
- **Start with a risk assessment:** This assessment will validate your current state, identify any existing gaps and vulnerabilities which are creating exposure to risk, and prioritize actionable recommendations based on ease of implementation and criticality to reduce risk quickly and effectively.
- **Complete a data and system inventory:** The risk assessment for your dealership along with the risk assessment for the vendors you work with are contingent upon a complete understanding and inventory of your assets, data and dataflows.

Q&A: PENETRATION TESTING

What is it? A pen test is a concentrated effort to exploit security weaknesses from internal and external entry points.

What's the goal? The goal of a pen test is to proactively hack a dealership's environment to identify weaknesses and security gaps that can be fixed before a criminal actor can discover and exploit them.

How does it work? Pen tests can be conducted from different perspectives and entry points. External pen testing involves a white hat hacker trying to compromise a network from outside your dealership – as a typical, unethical hacker would. Internal pen testing is an effort to compromise your network from within your digital environment – as an insider threat would. Wireless pen testing leverages your WiFi as an entry point to your digital environment.

How long does it take? A pen test can usually be completed within a few days to a couple of weeks, depending on the size of the dealership involved and the methods of testing.

What does the Safeguards Rule require? The Safeguards Rule requires that dealerships conduct an annual pen test.

Q&A: VULNERABILITY ASSESSMENTS

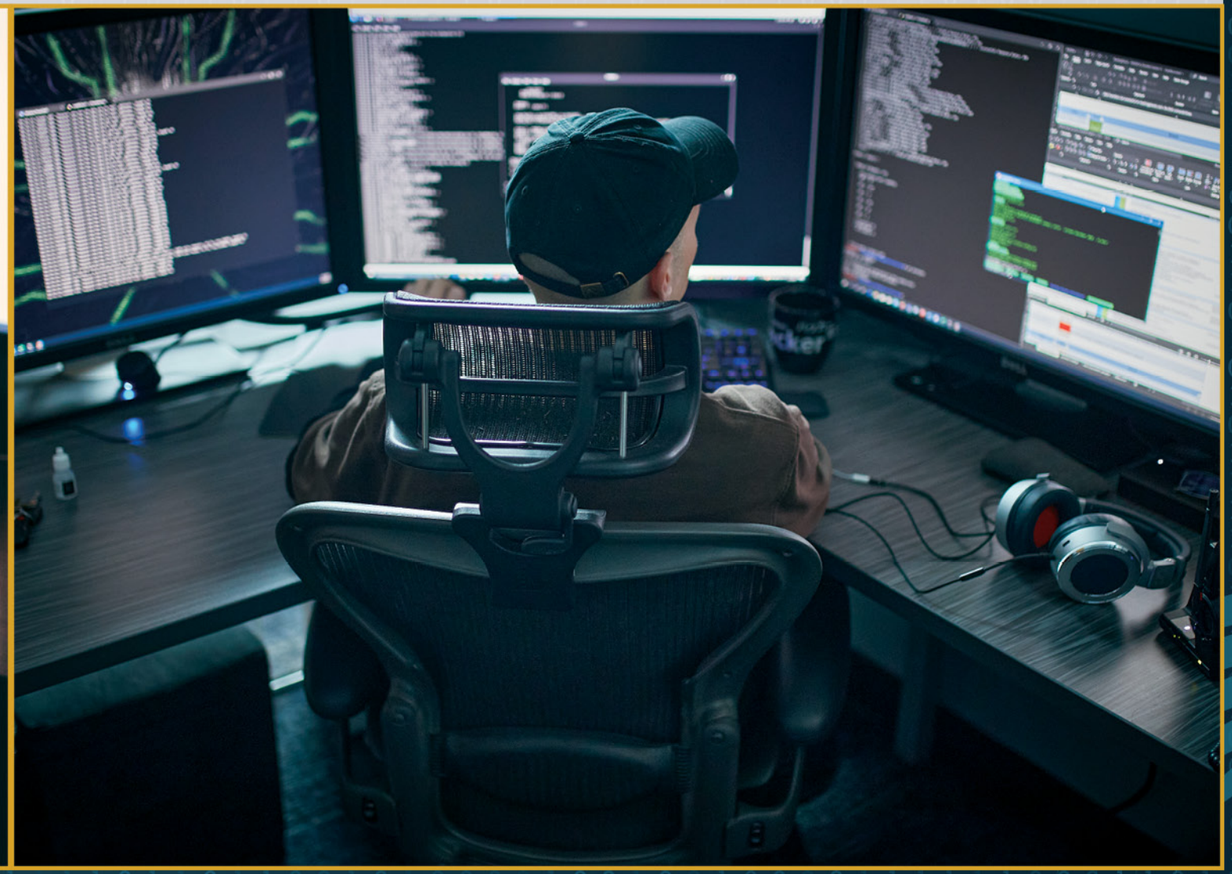
What is it? A vulnerability assessment is a broad non-invasive overview of your organization's security weaknesses.

What's the goal? A vulnerability assessment identifies the areas of your IT environment that are vulnerable to attack so that they can be addressed and fixed.

How does it work? Vulnerability assessments begin by identifying a security framework as a benchmark, which will guide the exercise of evaluating people, process, and technology. Within the technology analysis, the team conducting the assessment will attempt to determine how your organization's security protocols will fare in the event of a cyberattack. Any weaknesses discovered during the assessment are reported back to your organization, as well as potential ways to correct them.

How long does it take? For a small organization, most assessments can be completed within days or a few weeks. For a larger organization, vulnerability assessments may require slightly more time given the size and scope of their operations.

What does the Safeguards Rule require? The Safeguards Rule requires that dealerships conduct continuous monitoring of information systems or vulnerability assessments twice yearly.



ENLISTING A PARTNER

Cyber Defense Labs works closely with auto dealerships across the U.S. to strengthen their security posture and help monitor their environment around the clock for malicious threats. **We can help you ensure compliance with the FTC's updated Safeguards Rule.**

Our team allows you to run your dealership without having to worry about your cybersecurity plan. We provide:

- Written risk assessments
- Continuous, around-the-clock cyber monitoring, enabling early threat detection and rapid remediation
- Vulnerability assessments and penetration testing
- Vendor and third-party risk assessments
- Creation and implementation of robust information security programs
- Real-world experience and expertise addressing security, compliance, and governance challenges
- Best-in-class technology and customer service

Schedule an assessment today with the experts from Cyber Defense Labs and gain peace of mind knowing that we've got your back.

ADDITIONAL RESOURCES

For more information on the FTC Safeguards Rule, free auto dealership cybersecurity resources, or to contact an expert, please visit cyberdefenselabs.com/automotive.

Cyber Defense Labs is your trustworthy partner providing expert cybersecurity services at all times – before, during and after a cyber incident.

Scan the QR code below with your smartphone to schedule a complimentary consultation with Cyber Defense Labs experts.

We are the trusted experts in cybersecurity.

For additional resources on how to reduce cyber risk and protect your dealership, visit www.cyberdefenselabs.com/autodealership or email experts@cyberdefenselabs.com.

CYBER DEFENSE LABS