


**CDK GLOBAL**

# **State of Cybersecurity in the Dealership 2022**

CONNECTIONS THAT MOVE YOU

 IT Solutions / Digital Sales / CRM / F&I / Fixed Operations / DMS / Intelligence

## Table of Contents

---

**03** **INTRO**  
Why cybersecurity is more essential than ever.

**04** **KEY FINDINGS**  
Key findings from the CDK Research and Insights security survey.

**05** **FTC SAFEGUARDS:  
WHAT YOU NEED TO KNOW**  
Learn how these amendments have a direct impact on your dealership.

**06** **FTC SAFEGUARDS RULE MAY  
CATCH DEALERS UNPREPARED**

**07** **IMPROVING DEALERS'  
CYBERSECURITY OUTLOOK**  
What dealers are doing well and where they can improve.

**08** **THE COST OF INACTION**  
What an attack could cost your dealership.

**09** **DEALERSHIP IMPACT**  
The impact attacks can have on a dealership.

**10** **NEXT STEPS**  
Where to focus your strategy.

**11** **LET US HELP YOU  
GET STARTED**  
Learn how CDK Global can help your cybersecurity strategy.

# Why Cybersecurity Is More Essential Than Ever

From ransomware to data breaches, dealerships are experiencing an unprecedented number of cybersecurity concerns. Protecting your data has never been more important. The stakes for avoiding IT-related business interruptions, reputation damage and fines from not being compliant with the FTC has risen. Now is the time to assess and reassess to improve your security and be a compliant dealership.

For this e-book, we compiled automotive-specific data from dealership personnel and market research based on a recent survey conducted by CDK Global. Our goal is to provide dealerships with key insights to consider when evaluating their cybersecurity posture and ongoing strategy.

We've also scattered quotes from dealer participants throughout the book so you can read, in their own words, how other dealers are addressing cybersecurity.

*“Ransomware attacks could cripple our infrastructure and result in loss of sales and productivity.”*

> IT DIRECTOR

# Key Findings

The online survey administered by CDK Research & Insights confirmed that dealers' cybersecurity concerns are high and rising every day. **Below are some key findings from this year's survey compared against last year's survey results.**

## Top threats of 2022



**#1 EMAIL PHISHING**  
(SAME RANK AS 2021)



**#2 RANSOMWARE**  
(SAME RANK AS 2021)



**#3 LACK OF EMPLOYEE AWARENESS**  
(UP FROM #4 IN 2021)



**#4 THEFT OF BUSINESS DATA**  
(UP FROM #5 IN 2021)

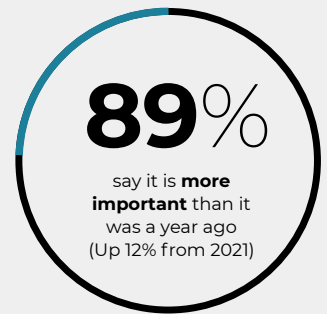
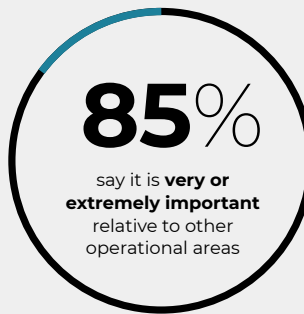


**#5 PC VIRUS OR MALWARE**  
(DOWN FROM #3 IN 2021)



**#6 STOLEN / WEAK PASSWORDS**  
(SAME RANK AS 2021)

## Dealers are more worried than ever about cybersecurity threats



## Dealers are confident, but gaps remain.



Only **37%** feel very or extremely confident in their protection.  
(Down 21% from 2021)



Of data breaches are **phishing attacks,\*** but less than 1/3 train employees on how to avoid it.

\*Verizon data breach report 2021

## FTC Safeguards: What You Need to Know

The Safeguards Rule amendments have set a deadline of December 9, 2022 for implementing mandatory security measures for your dealership. CDK has a comprehensive FTC Safeguards Guide\_for Dealers which you can find [here](#) to help you navigate. Make sure that you are also collaborating with your software vendors to meet these requirements and that you have a comprehensive and flexible plan in place for both your IT infrastructure and cybersecurity protection. When you can't do it all on your own, enlist the help of a reliable partner such as CDK to do the heavy lifting.



### 16 UPDATES TO FTC SAFEGUARD RULES

- 1 A qualified individual to oversee cybersecurity accountability
- 2 Information security program to be based on a written risk assessment
- 3 Data and systems inventory
- 4 Data encryption at rest and in transit
- 5 Adoption of secure development practices
- 6 Multifactor authentication
- 7 Required audit trails
- 8 Secure disposal procedures
- 9 Adoption of procedures for change management
- 10 Unauthorized activity monitoring
- 11 Penetration testing and vulnerability assessments
- 12 Employee training and security updates
- 13 Periodic assessment of service providers
- 14 Incident response plan
- 15 Written CISO report
- 16 Implementation of access controls

# FTC Safeguards Rule May Catch Dealers Unprepared

*“New revisions to FTC safeguarding rules create more need from a compliance perspective. Makes sense and is the right thing to do, just more complicated than it ever has been.”*

> IT DIRECTOR



# 35%

According to a CDK Global survey, only 35% **know the rule well.**

Of those who are familiar, the more complex parts still need work.

# 71%

Very/Extremely Familiar

**Protection Includes:**

- Multifactor authentication
- Data encryption
- Access of controls
- Data and systems inventory

# 54%

Very/Extremely Familiar

**Mitigation Includes:**

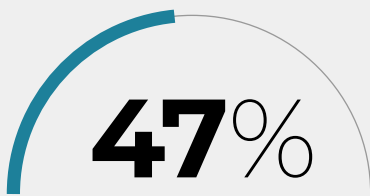
- Qualified employee (CISO)
- Written risk assessment
- Intrusion detection and vulnerability testing
- Security training verification

# 58%

Very/Extremely Familiar

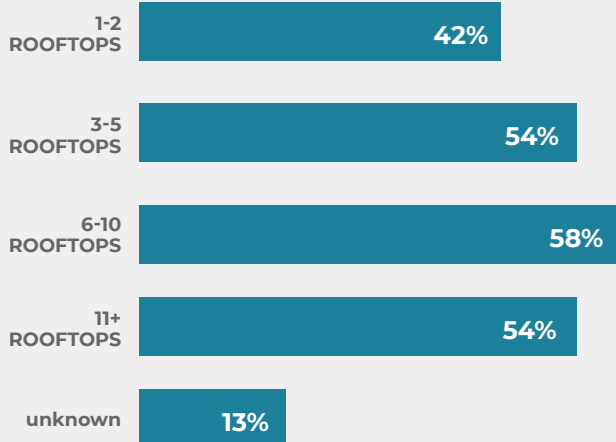
**Threat Detection and Response includes:**

- Systems monitoring & logging (including unauthorized activity)
- Secure development practices (including data disposable and change management)
- Written incident response plan
- Annual written report to board of directors



Less than half say they are well-prepared to be compliant

Larger groups are more prepared than smaller



## Improving Dealers' Cybersecurity Outlook

The good news is that dealers are implementing a lot of the best practices outlined on the previous page. With ransomware on the rise, dealerships should step up their efforts to combat attacks by updating their security policies, vetting their data security practices and training their employees.

### What Dealers Are Doing Well

Dealers are backing up their data while keeping their systems updated and patched. Anti-virus & malware protection increased by 31% in 2022.

#### Antivirus and Malware Protection



#### Secure Network



#### Update and Patch



#### Cybersecurity Insurance



#### Secure Endpoint Devices



#### Staff Training



### Where Dealers Can Improve

Very few have a plan for dealing with an attack while more need to segment their networks.

#### Real-time Monitoring



#### Formal Response Plan



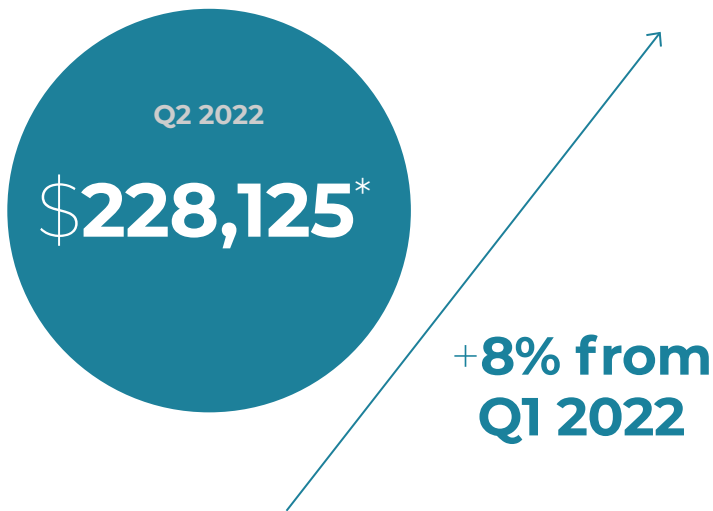
It's no longer *if*, but *when* an attack will occur. Leaving your dealership's computers accessible from your guest network is like an open invitation.

# The Cost of Inaction

Ransomware has become a major point of discussion, thanks to hackers hitting bigger and bigger targets. Looking at the average payouts over time (see chart) there is some volatility, although the costs still remain high and are an enormous burden for the average dealership.

The increase in payout amount is most likely due to the increase in work from home and the increased reliance on the distributed networking and applications needed to support this change in worker behavior. Here, the law of economics applies and hackers thrive in a business model that is financially attractive for them — low overhead and high profits. Dealerships fit the bill and are a prime target.

## AVERAGE RANSOMWARE PAYOUT IN Q2 2022



\* Source: coveware.com, 2022



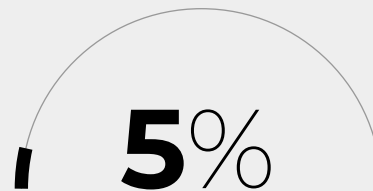
## Spend



of dealers say they plan to **increase their budget** for cybersecurity in the next year.



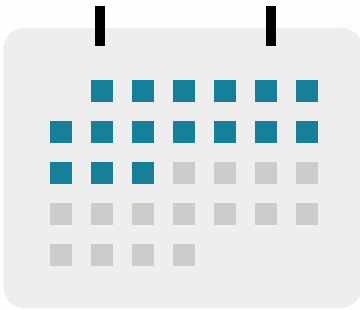
of dealers say their budget for cybersecurity will **stay the same** next year.



of dealers say they plan to **decrease their budget** for cybersecurity in the next year.



# Dealership Impact



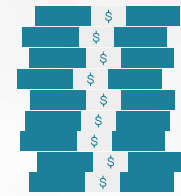
16 days

average length of downtime due to a ransomware attack.<sup>1</sup>



84%

of consumers said they would **not go back to buy another vehicle** after their data had been compromised.<sup>2</sup>



\$228,125

average payout to thieves in a ransomware attack.<sup>1</sup>

*“With the recent surge of ransomware attacks around the world and the advancement of security protocols we have made cybersecurity a huge priority for Team Automotive. The risk to businesses and our industry is at an all time high and we take that risk very seriously.”*

GENERAL MANAGER

<sup>1</sup>Coveware Ransomware Marketplace report <sup>2</sup>CDK Global Market Research study

## Securing Your Network and Business Goals

Your network and internet connectivity are the backbone of your dealership. These critical systems and pipelines must be secure for you to do business and satisfy your customers on a daily basis. Some dealers believe that security isn't important because it doesn't generate revenue. That is, at best, outdated thinking. While it may be true that cybersecurity isn't a money maker, there are many successful dealers who would agree that if the computer systems aren't secure, then everything else will fall apart.

## Next Steps

Cybersecurity can seem like climbing a mountain without knowing where to begin. To help you cut through the complexity and create a path forward, CDK has created a layered approach for thinking about cybersecurity.

### What are dealers saying?

*The stakes for avoiding IT-related business interruptions or reputational damage have never been higher.*

IT DIRECTOR

#### PREVENTION



**Stopping or minimizing potential problems before they start.**

- 24x7x365 monitoring
- Web content filtering
- Employee awareness training
- Authentication
- Systems and PCs patched and updated
- Compliance

#### PROTECTION



**Blocking or stopping threats as they attack.**

- 24x7x365 monitoring
- Detecting incoming threats
- Rogue device detection
- Securing devices, network, etc.

#### RESPONSE



**Containing threats and recovering quickly.**

- Recovery
- Rollback or return computers to a known good state
- Remediation
- Containment
- Response plans

There's no one-size-fits-all approach to cybersecurity. It's a moving target that requires constant attention. It's no longer *if* you get attacked, but *when*. And unfortunately, all it takes is one weak link to bring down the entire system. Your dealership is unique, and your cybersecurity requires an approach to match your needs.

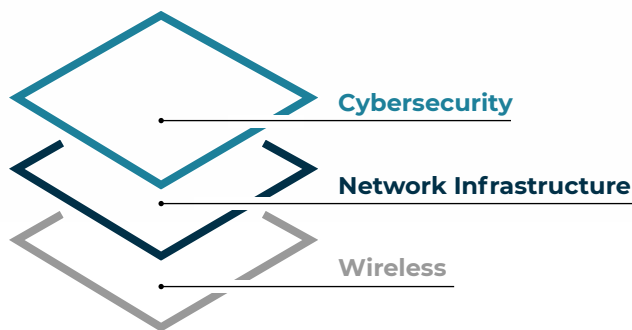
# CDK GLOBAL

State of Cybersecurity in the Dealership

## Let Us Help You Get Started

CDK helps you get a clear view of your IT environment at any stage of your journey and gives you a roadmap to the best path forward.

Our free security and network evaluation provides a three-tiered health check provided by skilled experts that examines three key areas of your business:



Your results will show how well your business is performing and protected, including:

- Strengths and gaps of your current environment
- A roadmap for current and future improvements
- Scope and cost estimates for next steps

To take advantage of this free evaluation, reach out to your CDK Sales Representative or call 888.424.6342.

For more information on CDK Cybersecurity, visit [cdkglobal.com/security](https://cdkglobal.com/security).

### CDK IT SOLUTIONS

## Why Choose CDK Global?

Our IT Solutions help you stay competitive with an enterprise-grade, secure network designed to meet your needs and budget. Our team enables dealers to focus on selling vehicles and servicing their customers by providing reliable, trusted and secure IT solutions that help reduce expenses, protect against cyberthreats and increase productivity.

- ✓ **Largest IT Solutions provider in the industry**
- ✓ **20+ years of proven experience**
- ✓ **Over 8,500 networks built and monitored**
- ✓ **Cisco "Top 10" Gold Certified Global Partner**
- ✓ **More than 10,000 sites supported with IT services**
- ✓ **Over 4,000 dealers use our Managed IT Services**

**CDK GLOBAL®**

Learn more at [CDKGlobal.com](https://www.CDKGlobal.com)