



THE STATE OF DEALERSHIP CYBERSECURITY 2024

The following information is based on publicly available information and customer interviews.



TABLE OF CONTENTS

4

THE IMPORTANCE OF DEFENDING
AGAINST CYBERTHREATS

6

KEY FINDINGS

8

DEALERSHIP CYBERATTACKS
INCREASED IN 2024

9

CONSEQUENCES OF ATTACKS
ON DEALERSHIPS

10

FTC COMPLIANCE AND
DIGITIZED INTEGRATIONS

11

INVESTMENT IN CYBERSECURITY

12

TOOLS AND TRAINING

13

NEXT STEPS

14

LET US HELP YOU GET STARTED

15

NETWORK AND COMMUNICATION SERVICES

THE IMPORTANCE OF DEFENDING AGAINST CYBERTHREATS

Cybercriminals continue to attack dealerships with ever-evolving techniques, such as complex phishing campaigns or the theft of passwords. **It is crucial to protect your data from ransom demands, reputational harm and IT-related business disruptions.** It's time to evaluate and reevaluate your security now in order to strengthen it and stay informed about the most recent cyberthreats.

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

We've included quotes from dealer participants throughout the book so you can see what other dealerships are doing to address cybersecurity.



KEY FINDINGS

The online survey administered by CDK Research and Insights confirmed that although dealers feel confident about the security of the dealerships, protecting against cyberthreats remain a continued priority for dealers. **Below are some key findings from this year's survey compared against last year's survey results.**

Top Threats of 2024



Most Dealers See Cybersecurity as an Ongoing Need

“Besides the costs involved, it’s making employees understand and adhere to policies to keep the business safe.”

DEPARTMENT HEAD
(3 TO 5 ROOFTOPS)



Dealers Are Serious About Cybersecurity, but More Than Half Are Not Confident in Their Protections

91%

say it is very or extremely important relative to other operational areas.

40%

are confident in their protection.

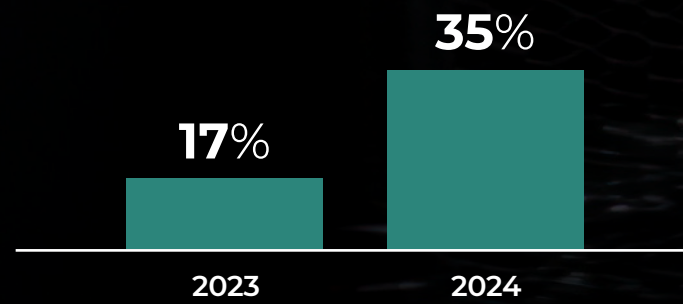
DEALERSHIP CYBERATTACKS INCREASED IN 2024

Experience



of dealers experienced a cyberattack or incident in the past year.

Yes, at Our Dealership/Group



“We’ve personally experienced fake emails going out from trusted sources, such as an email from the Dealer Principal asking to confirm if the attached information is correct. When the employee clicks on the link or attachment, they get hacked. Thankfully we’ve been able to catch these pretty quickly as our team is slowly becoming more aware of these issues.”

DEPARTMENT HEAD
(3 TO 5 ROOFTOPS)

Consequences of Attacks on Dealerships

Of those dealers that experienced a cyberattack on their dealership:

92%

said it resulted in a negative financial/operational impact (up from 46% in 2023).

Of those dealers that experienced a cyberattack on their dealership:

42%

said it resulted in a negative information theft impact (up from 32% in 2023).

Top Three Impacts on the Dealership’s Financials/Operations

63% Employee downtime

27% Need to replace or purchase hardware or software

24% Damaged reputation

Top Three Impacts Resulting in Information Loss

36% Dealership financial records

32% Inventory records

32% Personal and employee records



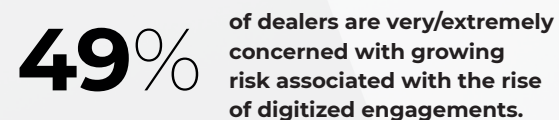
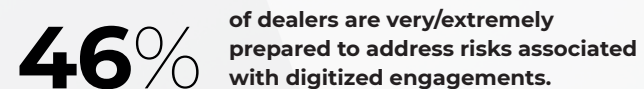
61%
of dealers said the quality of their security improved post-compliance.

The FTC regulations were established to protect businesses, including third-party integrations. For dealers who use outside platforms, services or partners in their business operations, FTC compliance with regard to third-party integrations is essential.

Businesses can successfully manage the FTC compliance risks related to third-party integrations by proactively addressing these factors. This improves overall operational integrity and helps preserve consumer trust, in addition to guarding against possible legal problems.

Within the FTC rules, dealers should complete an assessment to ensure all their vendors are compliant.

Dealers concerned with third-party integrations mentioned trust, security, access control and customer data protection as their top concerns.



“Navigating and adhering to constantly changing data protection laws and cybersecurity regulations adds significant complexity to maintaining compliance.”

DEPARTMENT HEAD
(6 TO 10 ROOFTOPS)

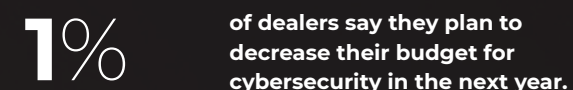
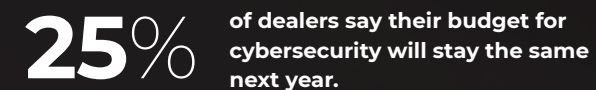
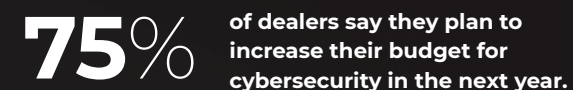
Dealers understand the importance of having protections in place. They plan to continue to invest in cybersecurity.

Higher Focus on Auto-Specific Providers



58%
of dealerships are using auto-specific providers for cybersecurity and network infrastructure (17% increase from 2023).

Investment

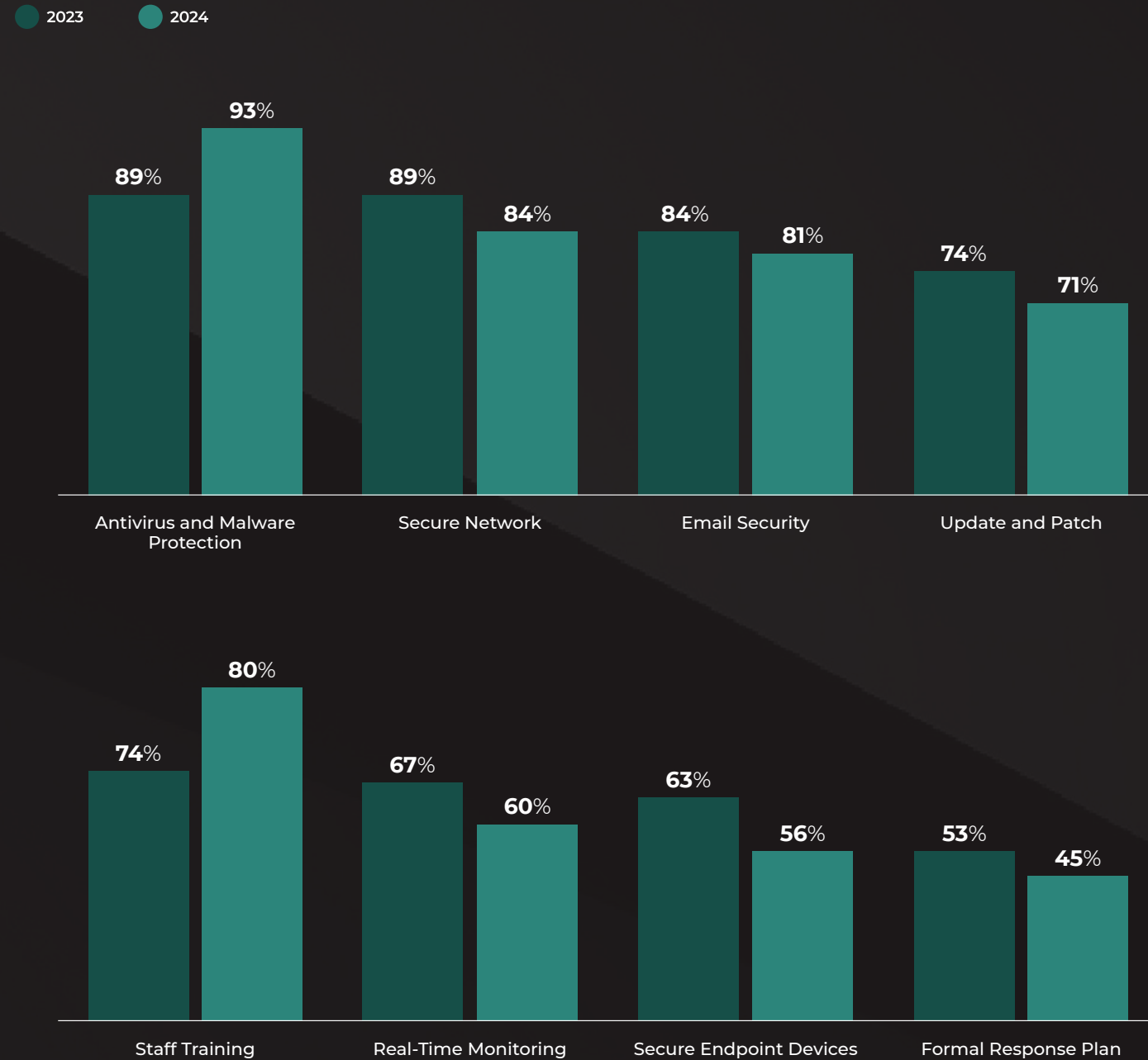


“With the growing cyber threat around the world, we don’t want to be caught off guard or become a victim due to the financial impact it would have on our company.”

DEPARTMENT HEAD
(3 TO 5 ROOFTOPS)

TOOLS AND TRAINING

Many dealers are focusing on training their staff to spot and avoid potential cybersecurity threats. Focus on antivirus, malware protection and staff training increased from 2023.



NEXT STEPS

Don't be fooled into thinking "it won't happen to our dealership." All dealerships are targets and need to be protected. A layered approach to cybersecurity can help to make you more secure.



Prevention

Stopping or minimizing potential problems before they start



Protection

Blocking or stopping threats as they attack



Response

Containing threats and recovering quickly

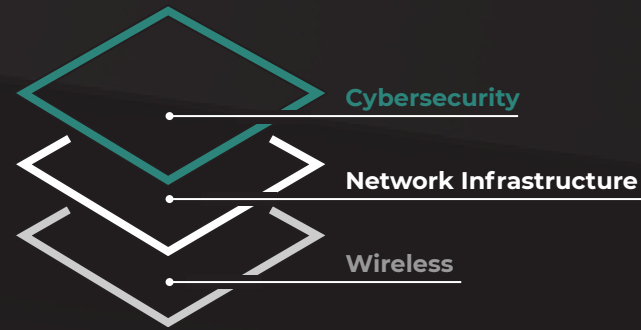
There's no one-size-fits-all approach to cybersecurity.

It's a moving target that requires constant attention. Your dealership is unique, and your cybersecurity requires an approach to match your needs.

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 security and network evaluation provides a **three-tiered health check** at your dealership, 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

NETWORK AND COMMUNICATION SERVICES

Our team assists dealers so they can focus on selling vehicles and servicing their customers by providing reliable, trusted and secure solutions that help reduce expenses, protect against cyberthreats and increase productivity.



Cisco Gold Certified
Global Partner



More than 10,000 sites
supported with IT services



Over 4,000 dealers use
our Managed IT Services



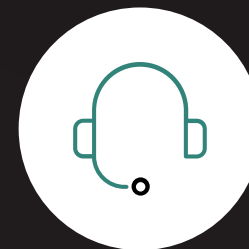
25+ years of proven
experience with over
200 certifications



**Largest Network and
Communication Services
provider** in the industry




Over 8,500 networks
built and monitored



Talk with one of our cybersecurity experts to get an evaluation of your security and network systems.

For more information on Cybersecurity, visit cdkglobal.com/security.



CONNECT WITH US  [CDK.COM](https://www.cdk.com)