CDK GLOBAL

The State of Dealership Cybersecurity
2023

Table of Contents

Defending Against Cyberthreats Is More Important Than Ever

Cybercriminals continue to target dealerships with ever-evolving methods to steal user and client data, from simply stealing passwords to sophisticated phishing schemes. Protecting your data to avoid IT-related business interruptions, ransom demands and reputation damage has never been more important. Now is the time to assess and reassess to improve your security and be up to date on the latest cyberthreats.

For this e-book, we compiled 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 how other dealers are addressing cybersecurity.

"With all of the manufacturer, customer and our own data stored, it's extremely important to protect it all."

> IT DIRECTOR

Key Findings

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

Top Threats of 2023
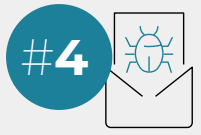
#1 EMAIL PHISHING
(SAME RANK AS 2022)

#2 LACK OF EMPLOYEE AWARENESS
(UP FROM #3 IN 2022)

#3 RANSOMWARE
(DOWN FROM #2 2022)

#4 PC VIRUS OR MALWARE
(UP FROM #5 IN 2022)

#5 THEFT OF BUSINESS DATA
(DOWN FROM #4 IN 2022)
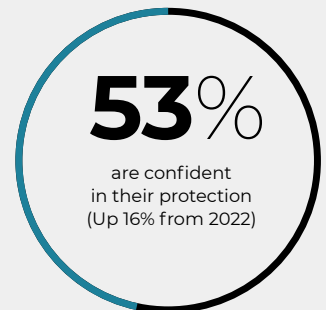
#6 STOLEN / WEAK PASSWORDS
(SAME RANK AS 2022)

#7 VEHICLE CYBERATTACKS
(SAME RANK AS 2022)

Dealers Are Serious About Cybersecurity, But Half Are Not Confident They're Protected

90%
say it is **very or extremely important** relative to other operational areas
(Up 1% from 2022)

53%
are confident in their protection
(Up 16% from 2022)
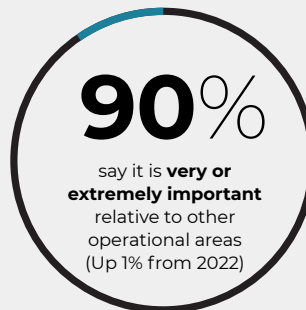
Most Dealers See Cybersecurity As an Ongoing Need

"Cybersecurity is not a destination, but a journey. It's always something that will need work and will never be done."

> **DEPARTMENT HEAD**
> *(3 TO 5 ROOFTOPS)*

Dealership Cyberattacks Increased in 2023

Experience

17% of dealers **experienced a cyberattack or incident in the past year**

Yes, at Our Dealership/Group

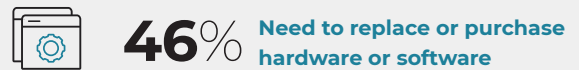|		
2023		**17%**
2022		**15%**

"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

46% of dealers experienced a cyberattack that **resulted in a negative financial/operational impact** (down by 17%)

Top Three Impacts on the Dealership's Financials/Operations

69% **Employee downtime**

46% **Need to replace or purchase hardware or software**

31% **Damaged reputation**

32% of dealers experienced a cyberattack that **resulted in information theft** (down by 8%)

Top Three Impacts Resulting in Information Loss

56% **Sales transaction data**

22% **Customer personally identifiable information (PII)**

22% **Finance and Insurance data**

FTC Compliance Improves Dealer Confidence

The updates many dealers made to their security policies to meet compliance requirements has helped them better protect their dealership and customer data.

75% of dealers said the **quality of their security improved post-compliance**

"The FTC passed the newest legislation because dealerships were found to be frequent targets for hackers and phishing campaigns. Mandating security principles ensure that dealerships are taking the necessary steps to ensure this protection."

> DEPARTMENT HEAD
(6 TO 10 ROOFTOPS)

Completed Actions To Achieve Compliance

Identified a qualified individual to oversee and be accountable for cybersecurity
85%

Implemented ongoing cybersecurity training for employees
73%

Integrated multifactor authentication throughout the network
72%

Performed a written risk assessment or had one performed by reputable source
67%

Created an informed security program based on that assessment
65%

Developed an incident response
63%

None, we have not taken any action to become compliant
6%

The Cost of Security

Dealers understand the importance of having protections in place. They plan to continue to invest in cybersecurity, with many focusing on training their staff to spot and avoid potential threats.
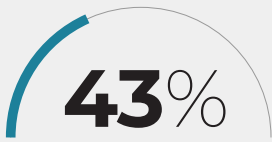
"Educating employees, since they're our first line of defense. Also, staying current with any updated security policies."

> DEPARTMENT HEAD
> *(11+ ROOFTOPS)*

Investment

51% of dealers say they **plan to increase their budget for cybersecurity** in the next year.

43% of dealers say their budget for cybersecurity will **stay the same** next year.

6% of dealers say they plan to **decrease their budget for cybersecurity** in the next year.

Higher Focus on MSPs

59% dealerships using **Managed Service Providers for cybersecurity and IT infrastructure** (11% increase from 2022)

Tools and Training

Focus on Email Security and Staff Training Increased in 2023

Antivirus and Malware Protection
2023 **89**%
2022 **91**%

Secure Network
2023 **89**%
2022 **85**%

Email Security
2023 **84**%

Update and Patch
2023 **74**%
2022 **72**%

Staff Training
2023 **74**%
2022 **54**%

Real-Time Monitoring
2023 **67**%
2022 **53**%

Secure Endpoint Devices
2023 **63**%
2022 **58**%

Formal Response Plan
2023 **53**%
2022 **31**%
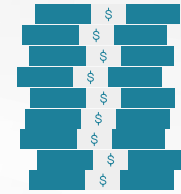
Cybersecurity Insurance
2022 **59**%

Dealership Impact
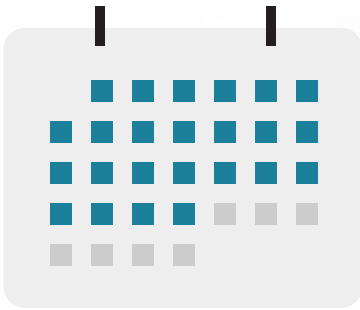
3.4 weeks
average length of downtime due to a ransomware attack.[1]

25%
of businesses that paid ransom **did not get their data back.**[1]

$740,144
average payout to thieves in a ransomware attack.[2]

Up 126% from Q1 2023

> " *This aspect of technology is quickly becoming the most important aspect of ongoing IT operations. Data theft and extortion are growing at a seemingly exponential rate. Low-hanging fruit are the ideal victims.* "
>
> ⯈ **DEPARTMENT HEAD**
> *(11+ ROOFTOPS)*

[1] https://www.veeam.com/ransomware-trends-report-2023 [2] CovewareRansomware Quarterly Report, July 21, 2023

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 this kind of protection 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 direct money maker, there are many successful dealers who would agree that if the computer systems aren't secure, then everything else will fall apart.

CDK GLOBAL
State of Cybersecurity in the Dealership

Next Steps

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

"Allocating funds to the cybersecurity department is a MUST. It may be considered expensive or unnecessary to some, but it's a truly important measure to keep information secure and a company free of risk."

> **DEPARTMENT HEAD**
> *(6 TO 10 ROOFTOPS)*

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.

CONNECTIONS THAT MOVE YOU

9

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 provided by skilled experts that examines three key areas of your business:

Cybersecurity

Network Infrastructure

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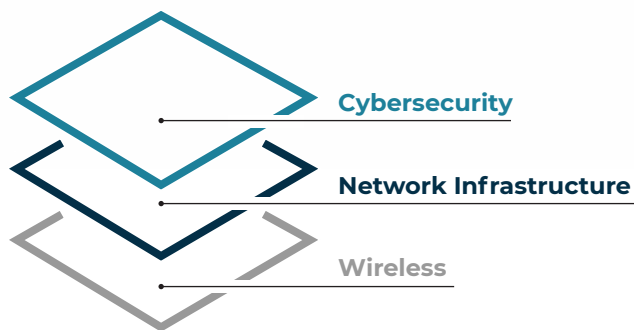
Your results will show how well your business is performing and protected, including:

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

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 Gold Certified** *Global Partner*

✓ **More than 10,000 sites** *supported with IT services*

✓ **Over 4,000 dealers** *use our Managed IT Services*

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

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

CDK GLOBAL.®

Learn more at **CDKGlobal.com**