2021

# State of Cybersecurity in the Dealership

# Table of Contents

# Intro

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 or reputation damage have never been higher. Now is the time to assess, reassess and improve cybersecurity at your dealership.

In this report, we've 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 strategy.

# Key Findings

The online survey administered by CDK Research & Insights confirmed that dealers' cybersecurity concerns are high and rising every day. **Here are the key findings from this report.**

## Dealers are more worried than ever about cybersecurity threats.

**85%** say it is **very or extremely important** relative to other operational areas

**77%** say it is **more important** than it was a year ago

## Dealers are confident, but gaps remain.

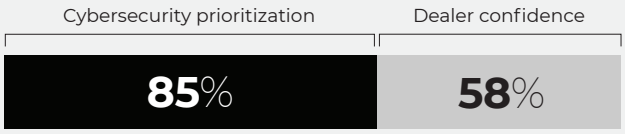
**58%**

**Only 58% feel very or extremely confident in their protection.**

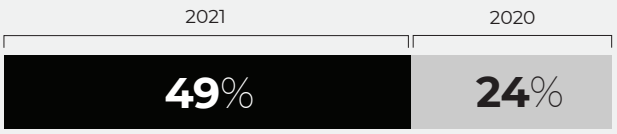
**1/3**

**Email phishing is their biggest worry, but less than 1/3 train employees on how to avoid it.**

## Dealers want to take action, but don't know where to start.




**Increased sense of urgency to prioritize cybersecurity outpaces dealer confidence.**




**Twice as many say they would increase budget for cybersecurity now than they did a year ago.**

# What the National Security Advisor Says About Cybersecurity

After a series of ransomware attacks targeting the energy, banking, healthcare and food processing sectors, the White House issued a letter explaining the threats to businesses and outlining a series of best practices to follow.

The letter, written by Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, asked all businesses to take the threat seriously and immediately implement the practices outlined in the President's Executive Order on Improving the Nation's Cybersecurity.

## What are dealers saying?

*Auto dealers are constantly under attack by cyber criminals because of the large quantities of customer data stored on our DMS systems.*

IT DIRECTOR

**BACK UP**
your data, system images and configurations, regularly test them, and keep the backups offline

**UPDATE & PATCH**
systems promptly

**TEST**
your incident response plan

**CHECK**
your security team's work (Penetration Test)

**SEGMENT**
your networks (business, customer, vendor)

# What You Need to Know

The good news is that dealers are implementing a lot of the best practices outlined on the previous page. However, 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

**More and more dealers are backing up their data while keeping their systems updated and patched.**

**65%**

are backing up data, system images and configurations while regularly testing them and keeping the backups offline.

**Hackers are on the lookout for unpatched devices and out-of-date software because they have known vulnerabilities.**

**63%**

are updating and patching systems promptly.

## Where dealers can improve

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

**27%**

are testing their incident response plan.

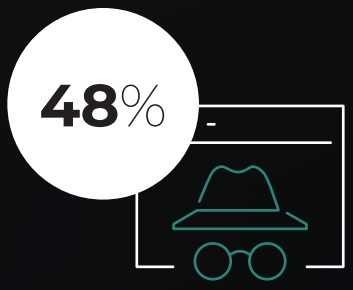
**45%**

are segmenting their networks.

**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.**

# Top Dealer Perceived Threats


EMAIL PHISHING

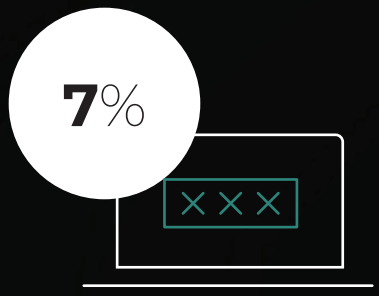



RANSOMWARE


PC VIRUS / MALWARE


LACK OF EMPLOYEE AWARENESS


CUSTOMER DATA THEFT




STOLEN / WEAK PASSWORDS

## What are dealers saying?

*A breach can mean losing millions of dollars as well as customers' trust.*

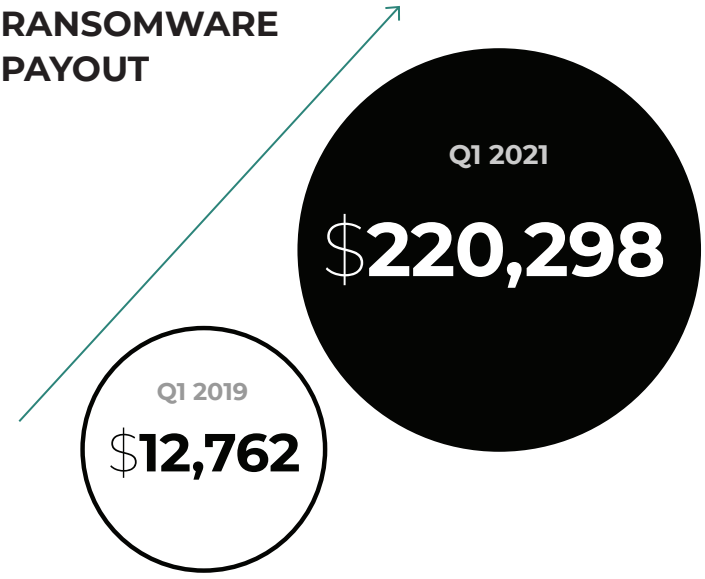
> CONTROLLER

# The Cost of Inaction

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

The increase in payout amount during 2020 is most likely due to COVID, 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**




## Spend

**49%**

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

**24%**

of suveyed dealers said they **increased their spending** on cybersecurity last year.

**16%**

**average increase in spend preferences** by CDK Global customers.

# How Dealers Are Taking Action

## Preventive measures

**Installing and maintaining** backup systems remain the most popular preventive measures taken by dealers.

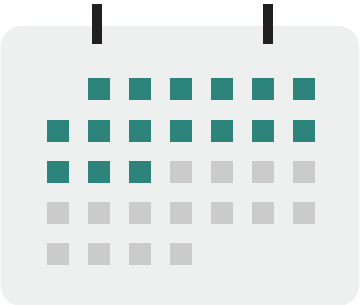
## Responsive measures

**Monitoring for and detecting** threats before they happen is an efficient way to ensure your dealership is safe.

## Employee-facing measures

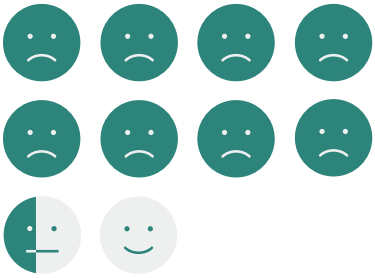
**Investing** in secure remote access for employees is money well spent in a work from anywhere environment.

# Dealership Impact



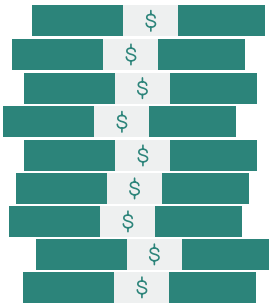
**16** days

**average length of downtime** due to a ransomware attack.[1]



**84**%

of consumers said they would **not go back to buy another vehicle** after their data had been compromised.[2]



**$220,298**

**average payout to thieves** in a ransomware attack.[1]

[1] Coveware Ransomware Marketplace report [2] CDK Global Market Research study

## Business Never Sleeps and Neither Should Your Cybersecurity

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.**

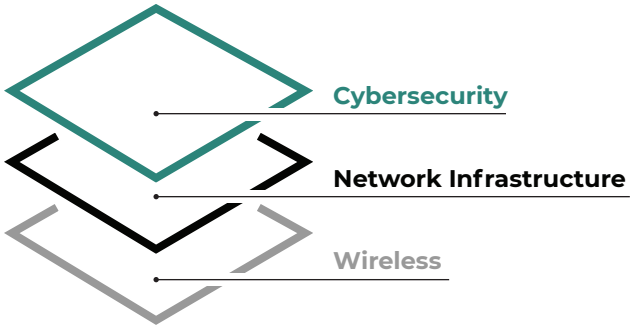
- Recovery
- Rollback or return computers to a known good state
- Remediation
- Containment
- Response plans

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.

# Getting 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 assessment 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 assessment, reach out to your CDK Sales Representative or call 888.424.6342.**

**For more information on CDK cybersecurity solutions, visit cdkglobal.com/cybersecurity.**

CDK GLOBAL®

Learn more at **CDKGlobal.com**