

# Automotive Dealerships Are Cybercrime Targets



by **BRAD BONO**, Chief Executive Officer, Helient Technologies

Any type of business can find itself the victim of cybercrime, but automotive dealerships have been particularly targeted in recent years, likely due to the amount of data dealerships handle.

According to CDK Global's State of Dealership Cybersecurity in 2025, "one in five dealerships reported being targeted in 2025." Notably, CDK itself was the target of a much-publicized cyber incident in 2024, in spite of ongoing threats from cyber criminals. Fortunately, there are preventative actions your dealership can take to protect itself and its assets.

Here are three immediate steps your dealership can consider:

- 1. Audit Your Current IT Security:** The first step toward safeguarding your dealership against cybercrime is to assess your current security situation. For most dealerships, this means bringing in an outside cybersecurity specialist to analyze your current practices. A good consultant can inspect your IT infrastructure to look for security holes, including any outdated protocols that leave you exposed to cyber threats. Automotive dealerships handle just as much sensitive customer data as a bank or a hospital, so an assessment of your current security is a must-do first step.
- 2. Secure Your Data:** Whether you're working off localized files or the cloud — likely both — the security of your customers' data is only as strong as the network you've built around it. A trained cybersecurity consultant can make sure your dealership's encryption, firewalls, and WiFi networks are up to date against the newest threats. This can include monthly security patching and updates to anti-virus as well as intrusion prevention and endpoint security.

- 3. Train Your Employees:** You must train your team to be aware of the latest and most common cybercrime tactics. This can include training against malware and password attacks via phishing, but it could also include preparation against more sophisticated AI-impersonation attacks that have been predominant as of late. Employee training is important for all parts of your business. Just as your marketing team needs to be aware of suspicious inquiries, your IT department needs to be on the lookout for unusual network activity. Consider quarterly sessions with your team to stay on top of the latest tactics to make sure that new hires are up to speed on your security-first protocols.

At Helient, we're cybersecurity experts. We believe it's important for your dealership to have a qualified Managed Security-Solutions Provider (MSSP), with specific expertise in dealership security on your team. Helient has been an MSSP for more than 15 years, and we work with more than 70 dealerships, giving us the experience needed to assist with ongoing efforts and secure dealerships against cyberthreats.

*For more information, please visit our website at [helient.com](https://helient.com) or contact us at (856) 470-1369 | [bbono@helient.com](mailto:bbono@helient.com).*

