HELION

AI Driven Threats:

Dealership Cybersecurity Lessons From 2025 and Advice for 2026

Erik Nachbahr
CISSP #728261

AI is Booming!

AI adoption is accelerating faster than regulation

- 76% of U.S. dealerships plan to increase AI spending
- 81% believe AI will improve operational efficiency
- AI usage in fixed ops chat + BDC automation up 40%
- 58% of dealerships are experimenting with generative AI internally

Dealers Have Lots of Questions

- How can we benefit from AI?
- Does AI increase cyber risk?
- Are there regulatory concerns?
- What policies must we implement?

Types of AI

Generative AI
Produces new content (ChatGPT-style)

Predictive AI
Forecasts outcomes using historical data (pricing, inventory)

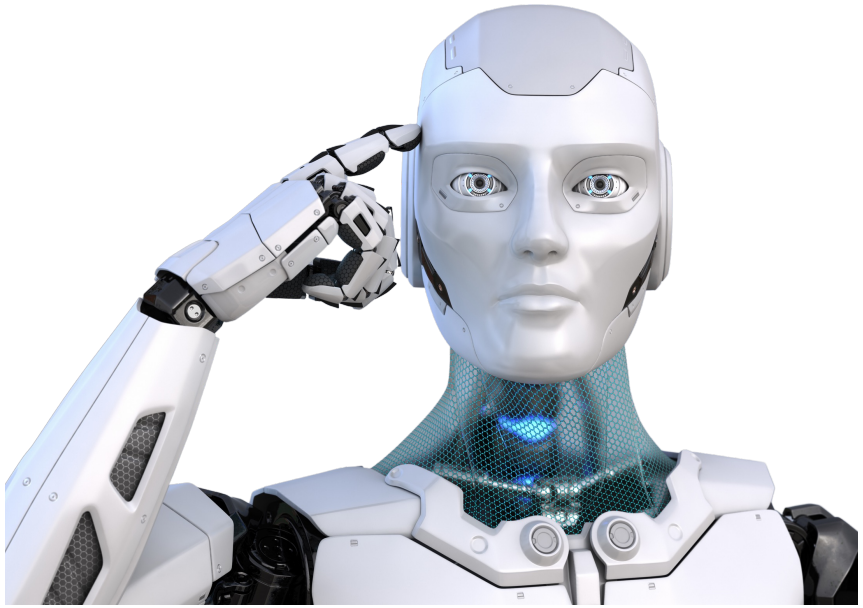
Automation AI
Improves productivity by supporting human actions (chatbots, BDC)

Embedded AI
Integrated into software (within DMS, CRM)

Benefiting From AI

- Service BDC
- Inventory Pricing
- Chat Assistant for Parts
- Warranty Claim Review

Every one of these use cases requires dealership data



And that's where the risk begins.

Your Dealership's Data Fuels AI

AI doesn't need all your data.
But it will take whatever you give it.

- Average dealership stores 150,000 - 500,000 customer records
- SSNs, driver's licenses, banking data, payroll
- DMS, CRM, service history

The Questions That Arise

- Should you let AI directly access your data?
- Where does your data reside?
- Who is responsible for the security of your data?
- Where does your data go after you upload it?

Say Hello To Your New Employee

- Never sleeps
- Has access to your systems and data (and stores them)
- Follows instructions - precisely
- Has no morality
- **Doesn’t just work for you**

A Difficult Employee To Control

38% of employees use unauthorized AI tools at work

- AI can execute API calls into your DMS
- AI can store prompts & training data
- Shadow AI use is exploding

Shadow AI

The unsanctioned use of AI results in:

- Unauthorized processing of sensitive data
- Regulatory noncompliance
- Expansion of the attack surface
- Lack of auditability & accountability
- Model poisoning & unvetted outputs
- Data leakage
- Overprivileged or insecure third-party access

AI Makes IT/Cyber More Complex

AI expands your attack surface in ways traditional tools never did.

- Model hallucination risk
- Prompt injection attacks
- Data exfiltration via AI prompts
- API key exposure
- AI supply chain risk

The Dark Side

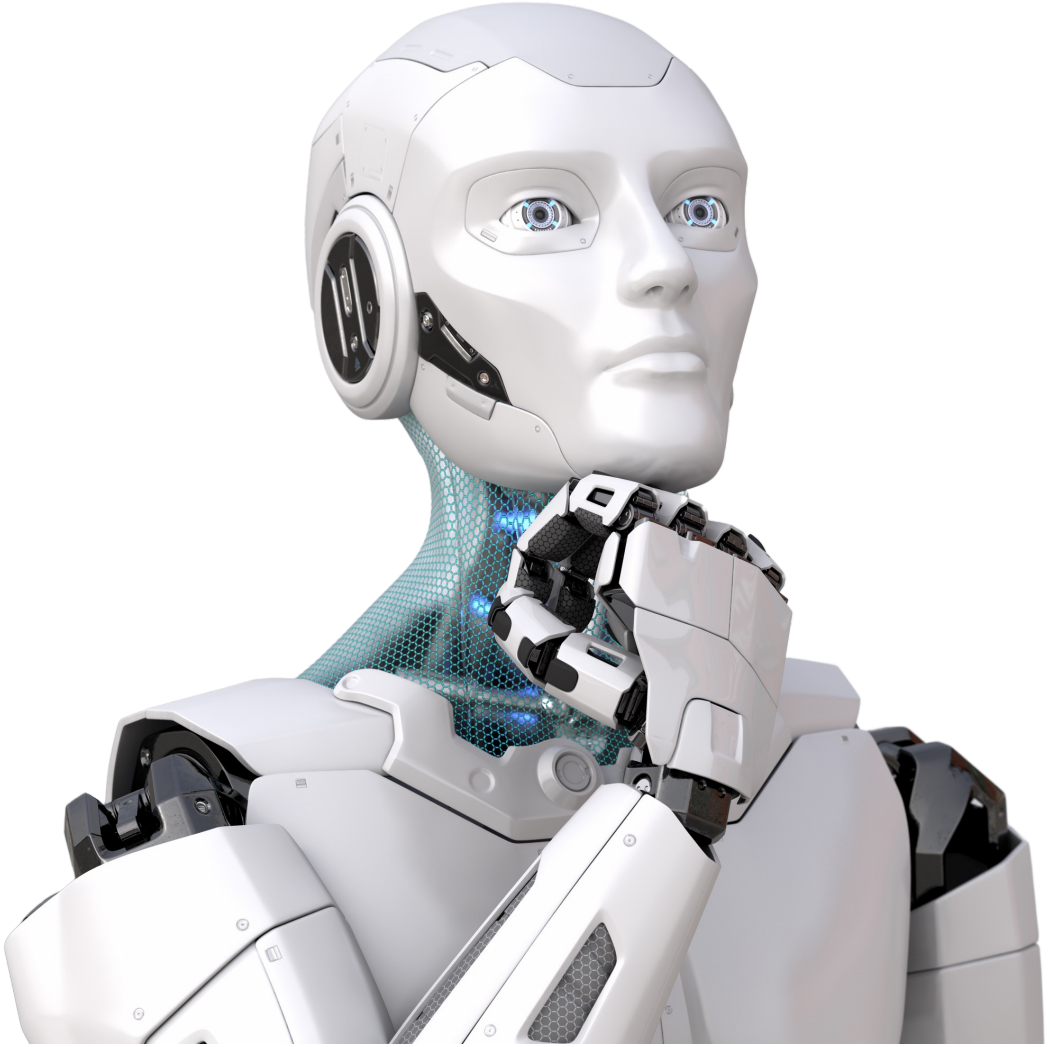
- AI-generated phishing now bypasses traditional detection
- Deepfake voice scams increasing (CFO fraud)
- AI-generated invoice fraud attacks up 3x in 18 months
- Ransomware groups using AI for adaptive targeting

Cybercriminals Also Use AI

- Automated spear phishing at scale
- AI-generated vendor impersonation
- Real-time adaptive social engineering
- AI malware that changes signatures

- 97% of breaches start with social engineering
- Business Email Compromise losses exceed $50B

AI Is Powerful & Dangerous



An Example:

Dealership wants to use PII to sell auto insurance

AI Adoption exacerbates the need …

… for cybersecurity expertise & manpower

Governance
- What is allowed and why
- Approved tool list

Data Controls
- What can/can’t be shared
- Logging and monitoring

Security Controls
- MFA
- Vendor due diligence
- Configuration control
- Continuous monitoring

Erik's 5 AI Rules for Dealerships

1. Never upload customer PII into public AI tools
2. Inventory all AI tools in use
3. Treat AI vendors as regulated service providers
4. Enforce MFA and logging on AI integrations
5. Assign clear AI governance ownership

What Should You Do *Tomorrow*

If AI is already in your dealership, governance must catch up immediately.

- Inventory AI tools in use
- Prohibit public AI use with customer data
- Assign AI governance ownership
- Require vendor AI disclosure
- Update cyber insurance information

Final thought

AI will not destroy dealerships.
Poor governance will.

Innovation without governance is just risk at scale.

Erik Nachbahr

Enachbahr@heliontechnologies.com

443.610.7640

For Slides: Marketing@heliontechnologies.com

For A Free Cybersecurity Assessment Please Visit:
www.HelionTechnologies.com/it-assessment