

# ***CYBER ENGAGEMENT 2025***

---

**PHANTOM FIGHTERS AND RED TEAMS TO THE FRONT**



**Stop Malicious  
Assaults and  
Turn Hackers'  
Attacks Back  
on Them**

**Unique analysis of cybersecurity  
protocols for auto dealerships**



**AUTOMOTIVE RISK  
MANAGEMENT PARTNERS**

**POWERED BY RIDGEBACK NETWORK DEFENSE**

info@autorisknow.com • 815-345-3629 • 60B West Terra Cotta Ave 159 • Crystal Lake, IL 60014

Cybercriminals have learned that ransoming auto dealership data can result in handsome rewards for their clandestine efforts.

The cybersecurity you're using now won't stop them; most dealership data networks are permissive, weakly defended, and wrong for your business.

It couldn't be more clear: the auto retail industry must know that cyber protection demands a combat-like mindset. It means bringing smart weapons to the front lines to protect digital assets.

There is no longer a place for naïve thinking. Invasive data missiles are launched every second against organizations like yours. A glance at a live cyber threat map shows

how many millions of attacks are in progress worldwide every minute of the day.<sup>i</sup>

As a business leader with fiduciary, market, and reputation responsibility for your dealership, you must be confident that your IT networks are orderly and resilient – and can be punitive when attacked.

Level up your game and free IT from disruption.

Create order out of cyber chaos.

*“Most dealership data networks are passive, weakly defended — and wrong for your business.”*



## Not Dad's Cybersecurity

Although traditional cybersecurity techniques evolve fast, their increasing complexity creates unseen and unmanaged coverage gaps. These gaps lead attackers to the assets you need to protect most.

There is no victory from watching and analyzing cyber activity itself, which has been the extent of protection commonly offered by security tools today. Winning the cyber war means using strategic, combat-like automated tools that counter-engage cyber adversaries to end their attacks against you!

Against traditional security solutions, cyberbullies today:

- **Outnumber you** – Perpetrator populations are vast, skilled, criminal -- and well-funded
- **Pivot faster** – Overwhelm your traditional cyber protection solutions
- **Manipulate AI** – Turn your AI-enhanced security into allies for their goals

These dated solutions rely on two main strategies: (1) blocking access to unauthorized users (e.g., firewalls) and (2) surveillance and detection solutions, including antivirus and endpoint and network detection solutions that leverage AI.

Here's how these adversaries mess with you once they gain access to your network:

- They inject signals to break or modify normal detection processes
- They escape detection by using unexpected attack vectors
- They “twist” the valuable purpose of security AI for their nefarious purposes against you.

## Cybersecurity forged by the Principles of Warfare

Cyber and combat warfare attack strategies mirror each other's offenses and defenses. The more we can understand these strategies and apply them to the new battlefield of international cyberwar the better protection we can use to insulate our businesses from these disruptive and costly attacks. No doubt the technology and application of cybersecurity will evolve. Cyber Engagement 2025 is gaining permanent ground in cyber warfare.

If this level of dealership security sounds daunting, be assured that it is—and more. However, its implementation into your network takes but minutes and uses mere megabytes of memory. Could a security campaign designed around this simplicity be too good to be true? That would be an unfortunate and risky conclusion, even if competitors urge otherwise.



*Winning the cyber war means using strategic, combat-like automated tools that counter-engage cyber adversaries to end attacks against you.*

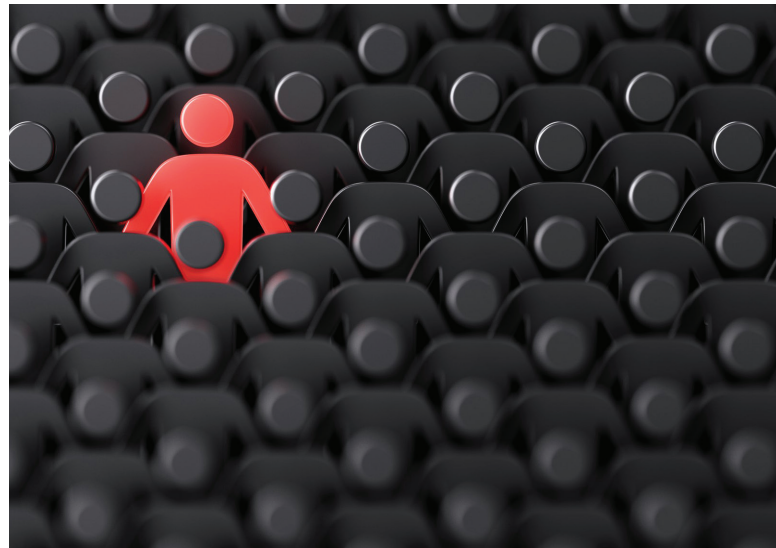
Here are but a few features that make the difference:

**Red Teams:** Our Red Teams of cyber sleuths help you improve IT network operations by attacking the same networks to isolate cybercrime penetration gaps. Red teams began with the military to evaluate the efficacy of strategies against enemies without engaging in actual combat.<sup>ii</sup> By creating a red team tasked with attacking the blue team using the most effective tactics, military organizations pinpointed problems before they reached the battlefield, helping to reduce the risk of staff and material loss.”<sup>iii</sup>

These systems instantly and quietly capture, report, and visualize all network devices, communications, and ports/services. They watch inactive IP addresses or Dark Space on networks. Systems like this help you meet regulatory requirements while safeguarding against external attacks and insider threats without complicating IT operations.

**Phantoms:** We operate Phantom “detectives” within your network’s Dark Space (the unused addresses in your network) to deter and neutralize threats and intruders. Our Phantoms, which appear as live endpoints to attackers, intercept adversary exploitation operations to detect unauthorized activities and dispatch them to the tar pits of Dark Space.

Without Phantoms identifying and neutralizing intruders, a cyber probe implanted in an IT network will not be identified by a traditional cybersecurity solution until days, weeks or months afterward.



*Red Team cyber sleuths isolate penetration gaps in your network.*

A genuinely secure dealership network delivers across three levels of network traffic:

- **Exposure:** The potential frequency of adverse events
- **Complexity:** The potential severity of adverse events
- **Capacity:** The scale of the IT footprint

**Reconnaissance agents:** that scan and probe your network to collect information about active devices, their services, open ports, IP addresses, and network topology:

- **Passive Reconnaissance:** Monitors network traffic and gathers information, sniffing network traffic without engaging with the network.
- **Active Reconnaissance:** Is direct interaction with network parts, such as ping sweeps, port scanning, or device.

You deserve protection that protects you from the first mile to the last. **Ask us to prove it.**

## Is Cyber Insurance an Answer?

Dealers may be encouraged to mitigate cyber problems by insuring that risk. According to the Insurance Information Institute, cyber insurance is expected to be one of the fastest-growing segments of the Property and Casualty insurance marketplace, globally projected at \$23 billion in 2025.<sup>iv</sup>

Citing IBM's Annual Data Breach Report, the Institute noted that average data breach costs for organizations are climbing, reaching \$10 million in the US in 2023.

Ninety-five percent of study participants experienced more than one breach.<sup>v</sup>

Premium costs are a concern. In a 2022 transcript from an insurance industry leadership forum, these experts noted:

Recent cyberattacks illustrate the significant economic cost cyber threats can pose and the importance of preparing for future incidents and their financial tolls.

Insurers, however, may not be willing or cannot offer coverage against this growing threat, which has the potential for catastrophic losses.<sup>vi</sup>

As the source of many cyberattacks is foreign, some have suggested that the federal Terrorism Risk Insurance Program (TRIP) be used to help with loss coverage. Because the terms of TRIP coverage do not meet the criteria of a violent or coercive terrorist attack, the GAO concluded that cyberattacks do not meet that criterion.

## Stop the Carnage

Noting a recent CDK Global cybersecurity report (yes, we see the irony), SecurityIntelligence<sup>vii</sup> notes that 85% of dealerships say cybersecurity is essential relative to other operational areas. Dealers who experienced ransom attacks had to pay \$228,000 to regain control of their data, which shut down their business for an average of 16 days per dealership.

The damage to retention is worse. "Some 84% of customers say they would not buy another vehicle from a dealership if a breach compromised their data," the report noted.

*"The retail auto industry must know that cyber protection demands a combat-like mindset. The incremental and passive cyber security protocols popularly used by car dealerships today are not getting the data security job done."*

In June 2024, Findlay Auto Group and CDK Global were attacked by ransomware attackers. CDK's alleged payout to ransomers was \$25 million. The attack hit the technology provider's customers with \$1 billion in lost sales, resulting in class-action damages lawsuits.

Incremental and passive cyber security protocols, which have been the tedious march of technological progression in cybersecurity for years, are not getting the data security job done that auto dealers and their vendors need.

Criminals using EDR Killer threats bypass the most critical security defenses dealerships rely on: End-Point Detection and Responses (EDR). EDR is designed to raise an alert when it detects something unusual in your network, but EDR

Killers bypass, disable, or otherwise neutralize the alert.

Another risk is activity latency. Even so-called real-time solutions are not no-latency systems.

Latency gaps present opportunities for hackers, but no-latency technology makes a network unnavigable by an intruder.

Cybersecurity providers like Automotive Risk Management Partners and Ridgeback Network Defenses do more than detect threats to your devices and networks; they deter them. They use offensive techniques to defend dealerships from ransomware attacks and strike back at attackers to inflict costs on them as they try to rob you.



*Cyberattacks can severely shake customer confidence and loyalty. Some 84% of customers say they would not buy another vehicle from a dealership if a breach compromised their data.*

## The Good/Bad Role of AI

By Scott Fogarty, CEO  
Ridgeback Network Defenses

With the ascendance of generative AI, cyberbullies now have a tool that can:

- 1) produce malicious payloads in volume rapidly,
- 2) design the payloads precisely to escape that which defensive AI is taught to identify as harmful (i.e., write the payload to avoid being detected by specific AI-based defensive tools) and,
- 3) Automate the exploitation to achieve the criminal mission before defenders even appreciate the adversary's presence and their tools based on after-the-fact detection approaches.

The most pernicious implication arises from the enormously favorable brand equity associated with AI, which often leads to defenders' overconfidence in the integrity of defensive solutions, when AI is only extending an arms race that continues to favor the attacker asymmetrically.

Our work in this area shows that even AI-supported cybersecurity measures are easily subverted and manipulated, turning dealers' security measures into turncoats. This past year, hordes of malicious actors turned their attention to the car business. We've seen the damage this has caused to dealers, major vendors, dealerships, and their customers.



# RIDGEBACK

## First Strike

Human eyes, hands, and experience remain a primary strategy against identity theft crimes in auto dealerships. No dealership can be 100% protected from compliance lapses and data breaches, even where computer systems oversee digital networks.

Yet, employees increasingly bypass the cyber security measures at their fingertips in exchange for convenience and speed. A recent survey says this challenge to your cyber security is not abating, even where organizations promote cyber awareness to internal audiences.

According to the HIPPA Journal, sixty-five percent of employees admit to circumventing employer security policies. Verizon's data breach study found that 68% of data breaches in the past year were caused by human error. An employee who falls for social engineering fraud fails to secure confidential information.

A similar Forbes report summarized the situation: How do you enforce compliance without stifling workflow? In the rush to meet deliverables, employees sometimes skip security to make the sale.

It cannot be stressed too heavily why dealership leadership must embrace this human element to data security and push it down into their stores—and assign one or two managers to implement and oversee data security training and compliance throughout all departments. What's a reasonable workaround for this dilemma? I have three to suggest:

1. Have strong cyber security technology, as discussed here, in place. The more this solution can counter cyberattacks—offensive security—the better your dealership will be protected. Make cyber security investments a priority; insurers are now scrutinizing how dealerships protect themselves from pene-

trations of their data flows, internally and in the data that moves to and from vendors.

2. Pay attention to your vulnerabilities. Never let your security lapse; never fall into the mindset that you're ready because your current cyber protection methods aren't turning up evidence of attacks. We see networks penetrated years ago siphoning off financial and personal data or waiting silently to spring into action when an incentive in their coding DNA is activated. The right security software and processes should not leave you in jeopardy like that.

3. Get and keep your people sensitized to the critical role of their diligence in cyber compliance; a quarterly refresher is not too frequent in today's rule. No dealership can be 100% protected from compliance lapses and data breaches, even where computer systems oversee digital networks.

4. Overall, be skeptical. Everyone in technical and business leadership roles must maintain vigilance with a continuous questioning of their posture. Overconfident, complacent attitudes are strongly correlated to risk of loss.

Lax information hygiene, systems auditing, and lax document handling practices expose dealers to considerable compliance and cyber risks. Anyone with a malicious spirit and camera phone wandering the store can quickly capture this information – and will rarely be seen doing so.

## Demand Better

Automotive Risk Management Partners and Ridgeback Network Defenses provide dealerships:

- The best offense against frustrating and costly cyber attacks
- 24/7, no-latency visualization of all network systems and tracking of and fulfilling FTC Safeguards Rule compliance requirements.
- Action-oriented reporting to identify network risks, pinpoint opportunities to harden security and improve function, and measure ROI compared to other IT and security tools.
- Easy to deploy and manage, so it provides impact within minutes.
- Favored cost/benefits

This industry's compliance and cyber security offerings offer various service options and costs. Don't equate price with value – you must investigate for at least two critical reasons:

1. The passion and zeal of the humans who run the company and who bring that same enthusiasm, seriousness, and integrity to your showroom and shop floor; and,
2. The experience, skills, technology, and strategy to ensure the integrity of your data platforms and provide aggressive and offensive cyber protection against entities who seek to defraud you and your customers.

**Cyber Engagement 2025 is available now.**  
**Give yourself and your dealership the network defenses**  
**required for victory in this evasive, pervasive, and**  
**perplexing combat for your business assets.**  
**Telephone or email us today for a no-obligation consultation.**

**Terry Dortch, Founder and CEO**

[info@autorisknow.com](mailto:info@autorisknow.com)

815-345-3629



*Automotive Risk Management Partners brings exceptionally seasoned vigilance, diligence, and compliance intelligence to automotive dealership cyber protection and security compliance. We provide absolute protection with a solid Insurance program where the dealer is named additional insured on a policy that would cover any action brought against the dealer, eliminating the loss of money due to fines or suits. Ridgeback Network Defense focuses on building and deploying tools to battle despicable criminals who would rob families and hijack businesses. Ridgeback is a unique and innovative enterprise security platform that enables the deployment of interactive defense on an incredibly large scale.*

#### Resource Citations

---

<sup>i</sup> Live Cyber Threat Map, CheckPoint, checked December 20, 2024, 10:22 a.m. central time, <https://threatmap.checkpoint.com/>

<sup>ii</sup> Bondeerud, Doug, “What is a red team? All you need to know,” SecurityIntelligence, March 9, 2023, <https://securityintelligence.com/articles/what-is-a-red-teamer/>

<sup>iii</sup> Ibid

<sup>iv</sup> Cyber Insurance – State of the Risk, Insurance Information Institute, February 2024, [https://www.iii.org/sites/default/files/docs/pdf/triple-i\\_state\\_of\\_the\\_risk\\_cyber\\_02062024.pdf](https://www.iii.org/sites/default/files/docs/pdf/triple-i_state_of_the_risk_cyber_02062024.pdf)

<sup>v</sup> Ibid, page 2

<sup>vi</sup> U.S. Government General Accounting Office, “Cyberattack Risks Increase, How Is The Insurance Market and Government Responding? June 2022, <https://www.gao.gov/assets/730/721076.txt>

<sup>vii</sup> SecurityIntelligence, July 11, 2024, <https://securityintelligence.com/news/hackers-increasingly-targeting-auto-dealers/>

