VicOne 2026 Automotive Cybersecurity Report Finds Cyber Incidents No Longer Stay Inside One Organization

Automotive cyber incidents tripled in 2025. New data shows automotive cyber risk now spans vehicles, cloud, and enterprise IT, reshaping governance priorities.

Crossroads-Automotive-Cybersecurity-Report

DETROIT, MI, UNITED STATES, February 11, 2026 /EINPresswire.com/ -- VicOne, a leading automotive cybersecurity company, today released its 2026 Automotive Cybersecurity Report, revealing that automotive cyber incidents are increasingly escalating beyond individual systems and teams to impact entire organizations. Compared to 2024, cross-region, multi-business incidents more than tripled in 2025, accounting for 161 of 610 recorded cases, as centralized software platforms and OTA infrastructures amplified the impact of a single security failure across subsidiaries and regions.

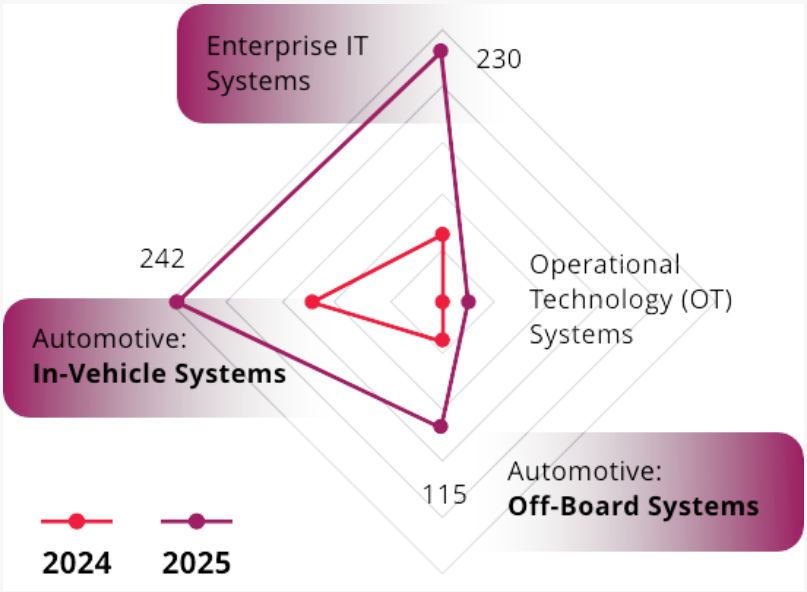
> In the Overlap Era, vehicles, cloud, and enterprise IT form a single operational fabric. Governing them as silos is no longer sustainable—cybersecurity is now a board-level issue.”
>
> *Max Cheng, CEO at VicOne*

The report finds that automotive cyber risk is no longer a localized technical issue. Attacks now routinely span enterprise IT, cloud services, and in-vehicle systems simultaneously, transforming cyber incidents into enterprise-wide governance challenges that directly affect operational continuity, brand trust, and executive accountability.

“In the Overlap Era, vehicles, cloud platforms, and enterprise IT systems function as a single operational fabric,” said Max Cheng, CEO at VicOne. “Governing these environments as isolated silos is no longer sustainable. Cybersecurity has become a board-level accountability issue.”

Key Findings from the VicOne 2026 Automotive Cybersecurity Report

- Cross-organization automotive cyber incidents more than tripled year-over-year, shifting attacks from localized breaches to enterprise-wide disruption.
- 33% of observed cyber risk now directly impacts driver-facing systems, increasing visibility, customer impact, and brand trust implications.
- Fragmented cybersecurity ownership is weakening organizational resilience, as attacks propagate across IT, off-board, and in-vehicle domains by design.



Cyber incidents in 2025 increasingly span multiple system domains, underscoring the growing disconnect between integrated automotive architectures and fragmented risk governance

VicOne defines this convergence of cyber risk as the “Overlap Era”, a period in which traditional vehicle platforms remain in service at global scale, even as software-defined vehicles, cloud-connected ecosystems, and AI-enabled features are rapidly deployed. In this environment, vehicles, backend services, enterprise IT systems, and external infrastructure are tightly coupled by design, while cybersecurity ownership and governance often remain fragmented.

As a result, automotive cyber risk is no longer shaped solely by technical weaknesses, but by how effectively organizations govern risk across overlapping domains.

The report further examines how expanding software ecosystems, emerging AI technologies, and evolving regulatory requirements are reshaping automotive cyber risk. Beyond the vehicle itself, EV charging infrastructure is emerging as a growing source of exposure, as chargers connect vehicles, backend services, mobile applications, and power grid at scale.

At the same time, AI-enabled features and continuously learning systems are accelerating how cyber risk propagates and persists across connected platforms, introducing dynamic behavior that challenges static threat models and traditional testing assumptions. While regulations such as UN R155 and ISO/SAE 21434 have raised baseline cybersecurity maturity, the report finds that domain-specific compliance alone cannot address cross-platform risk propagation in modern software-defined vehicle architectures, reinforcing the need for lifecycle-oriented cyber risk governance beyond patch-centric approaches..

Read the VicOne 2026 Automotive Cybersecurity Report, Crossroads: Automotive Cybersecurity in the Overlap Era, or listen to the accompanying audiobook, for a deeper insight into the forces reshaping automotive cyber risk.

For more information on VicOne’s holistic approach to cybersecurity, please visit https://vicone.com/solutions.

About VicOne
With a vision to secure the vehicles of tomorrow, VicOne delivers a broad portfolio of cybersecurity software and services for the automotive industry. Purpose-built to address the rigorous needs of automotive manufacturers and suppliers, VicOne solutions are designed to secure and scale with the specialized demands of the modern vehicle. As a Trend Micro subsidiary, VicOne is powered by a solid foundation in cybersecurity drawn from Trend Micro’s 30+ years in the industry, delivering unparalleled automotive protection and deep security insights that enable our customers to build secure as well as smart vehicles. For more information, visit vicone.com

Ling Cheng
VicOne
+81344002265 ext.
email us here
Visit us on social media:
LinkedIn
YouTube