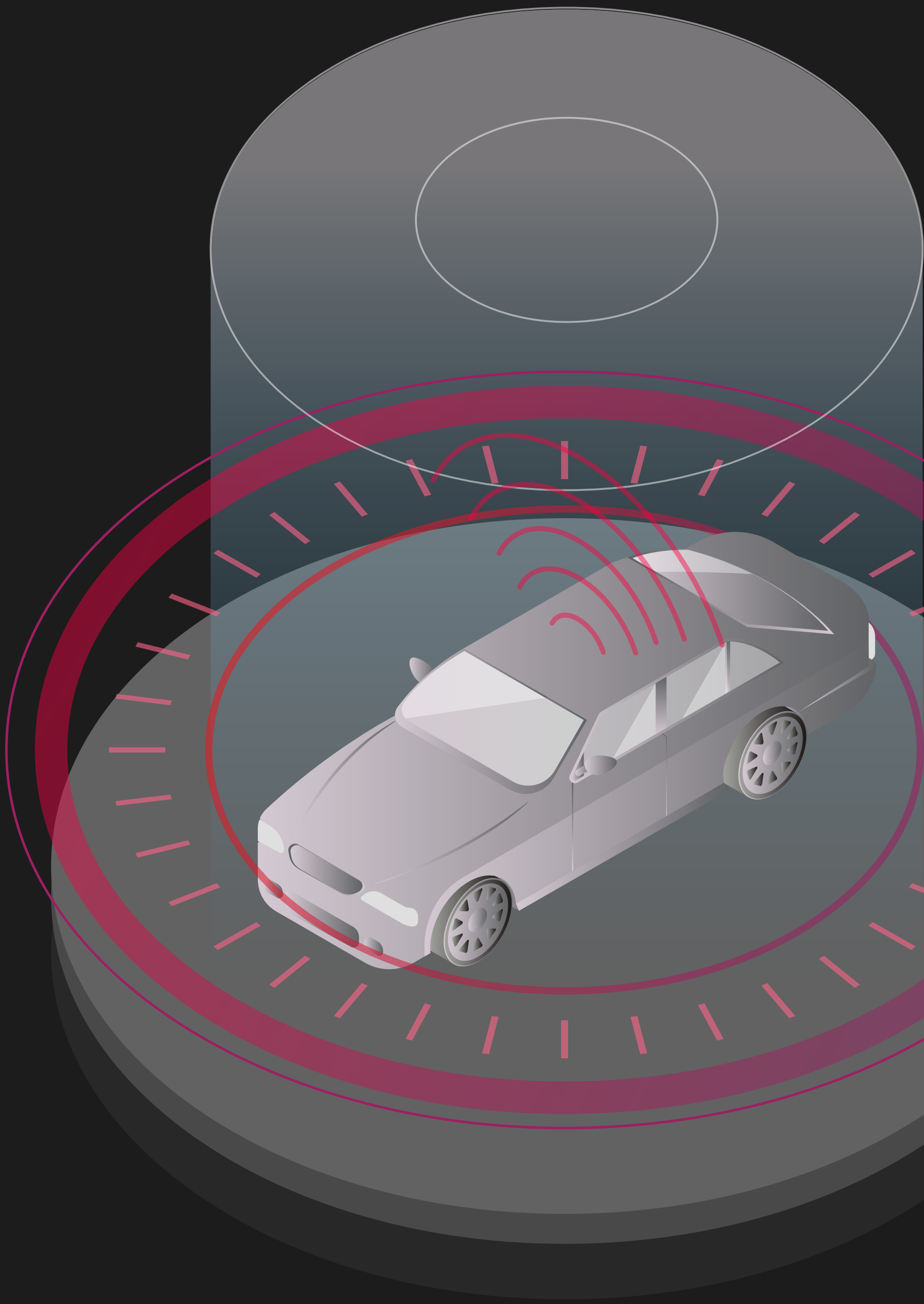
VicOne

AUTOMOTIVE CYBERSECURITY SNAPSHOT



WHAT YOU NEED TO KNOW

In 2023, the automotive industry remained a prime target for evolving cyberthreats. While 2024 was relatively quiet — largely due to law enforcement disrupting active cybercriminal groups[1] — this should not be seen as an assured decline in overall risk. **Persistent activity** suggests this might only be a temporary reprieve before a resurgence.

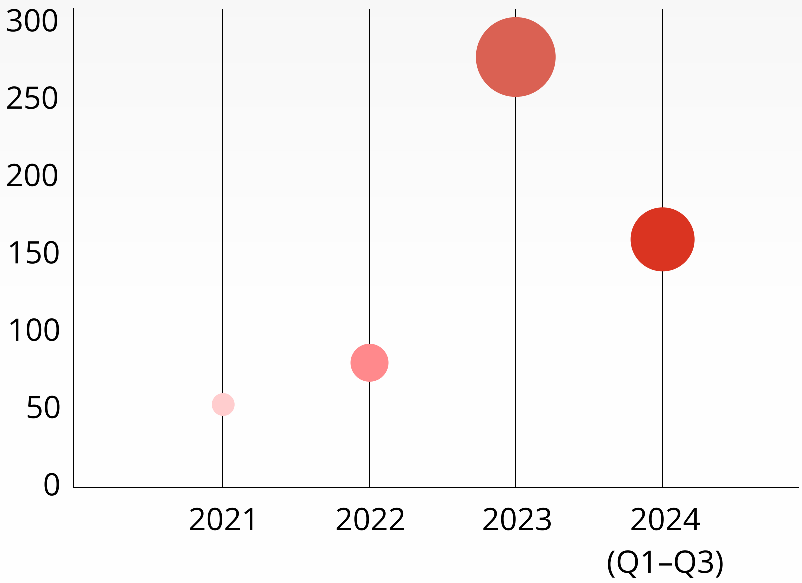
As vehicles enter a transformative era of mobility — powered by AI, cloud services, advanced driver assistance systems (ADASs), and other cutting-edge technologies — **vulnerabilities and risks** continue to emerge and grow. Drawing on our insights from the first three quarters of 2024, this VicOne report highlights the **critical factors** shaping today's automotive cybersecurity landscape.

[1] https://thehackernews.com/2024/11/interpols-operation-synergia-ii.html

SUSTAINED VOLUME OF CYBERSECURITY INCIDENTS

In 2024, the volume of cybersecurity incidents remained significant. Although the total number of incidents was unlikely to reach the record high of 2023, this **sustained level of activity** underscores the persistent threat landscape facing the automotive industry.

● 2021	● 2022	● 2023	● 2024 (Q1–Q3)
52 incidents	81 incidents	285 incidents	162 incidents, suggesting ongoing significant threat levels



Most of these cyberattacks involved **ransomware**, aligning with broader trends across industries where ransomware groups had intensified their operations. This uptick has had a profound impact on the automotive industry, emphasizing the urgent need for robust cybersecurity measures.

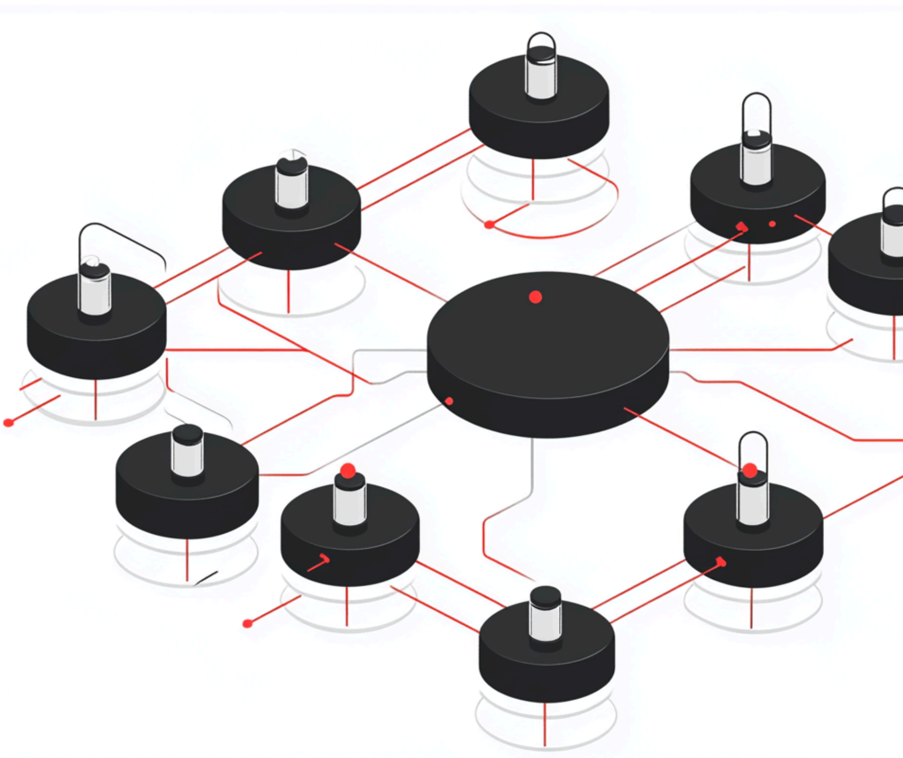
A VULNERABLE SUPPLY CHAIN

In 2024, cyberattacks focused on suppliers and third-party providers, exposing **critical weak links** in the automotive supply chain.

41 incidents	55 incidents	45 incidents	21 incidents
Third-party providers	**Suppliers**	**Dealerships**	**OEMs**

The data reveals that suppliers and dealerships were the primary targets in 2024, with incidents far surpassing those aimed at OEMs. This stresses the need to prioritize security across all supply chain partners to prevent the **cascading effects of cyberattacks.**

The attack on a **dealership software provider** in June 2024 exemplifies this trend. The ransomware attack disrupted operations at **over 15,000 dealerships** in North America, highlighting the far-reaching consequences of supply chain risks.[2]

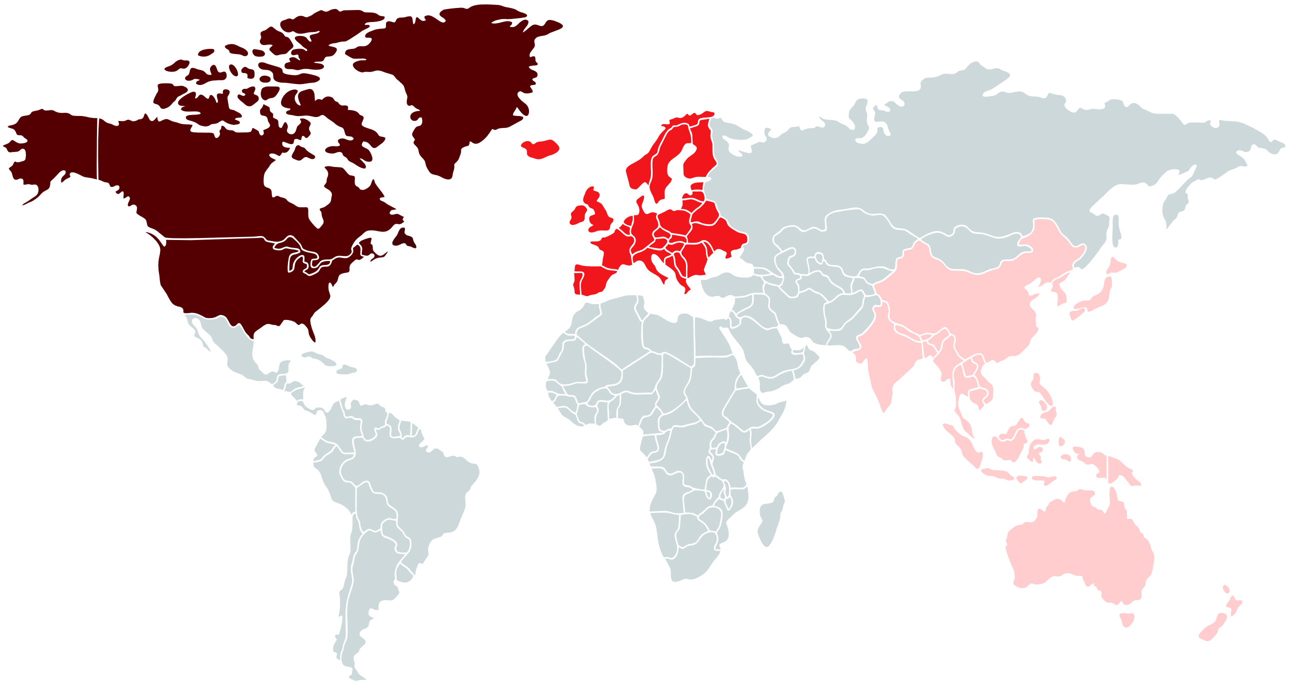


*Suppliers are entities providing vehicle components, while third-party providers include those offering other vehicle-related services, such as software, applications, and dealership management systems.

[2] https://vicone.com/blog/securing-the-automotive-supply-chain-lessons-from-the-ransomware-attack-on-a-car-dealership-software-provider

THIRD-PARTY RISKS IN FOCUS: A REGIONAL PATTERN

The 2024 threat landscape revealed a consistent **pattern across regions**: Third-party incidents outnumbered supplier incidents. While North America reported the highest overall number of incidents, Europe and Asia-Pacific followed with notable activity levels. This pattern reflects the **significant role of third-party providers** in the automotive supply chain and their heightened vulnerability to cyberthreats.



● **North America**
2024 (Q1–Q3)
18 third-party incidents
5 supplier incidents

● **Europe**
2024 (Q1–Q3)
16 third-party incidents
6 supplier incidents

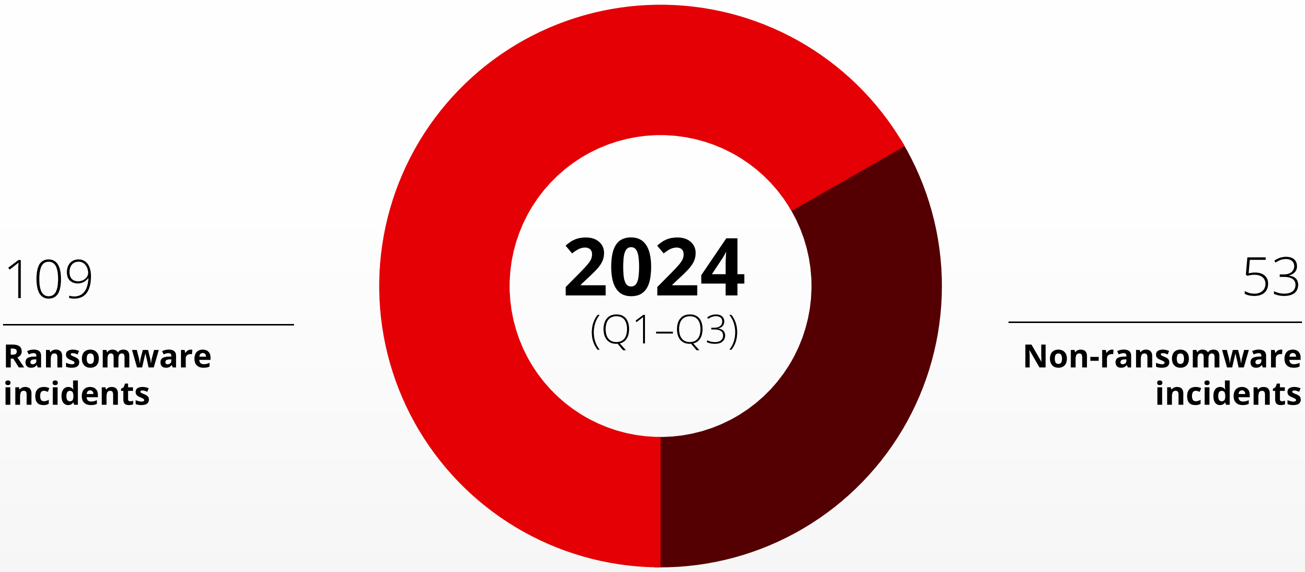
● **Asia-Pacific**
2024 (Q1–Q3)
13 third-party incidents
8 supplier incidents

The consistent prevalence of third-party incidents across regions highlights the need for enhanced security strategies to address **vulnerabilities at this level**, which could otherwise disrupt the entire supply chain.

*These figures represent the number of attacks reported by global and mainstream news outlets, rather than the total actual incidence of attacks.

THE ENDURING THREAT OF RANSOMWARE

Ransomware remained the **most prevalent type of cyberattack**, significantly outpacing non-ransomware incidents in frequency.



Although the total number of ransomware incidents declined compared to the previous year, this reduction should not be interpreted as the threat diminishing. Historically, ransomware groups have paused activity to recalibrate and implement longer-term strategies. This calls for **ongoing vigilance and strong cybersecurity measures** to address the evolving risk.

THE ESCALATING COST OF RANSOMWARE AND DATA LEAKS

The **financial impact of cyberattacks** continues to grow, with ransomware accounting for the largest share of losses.

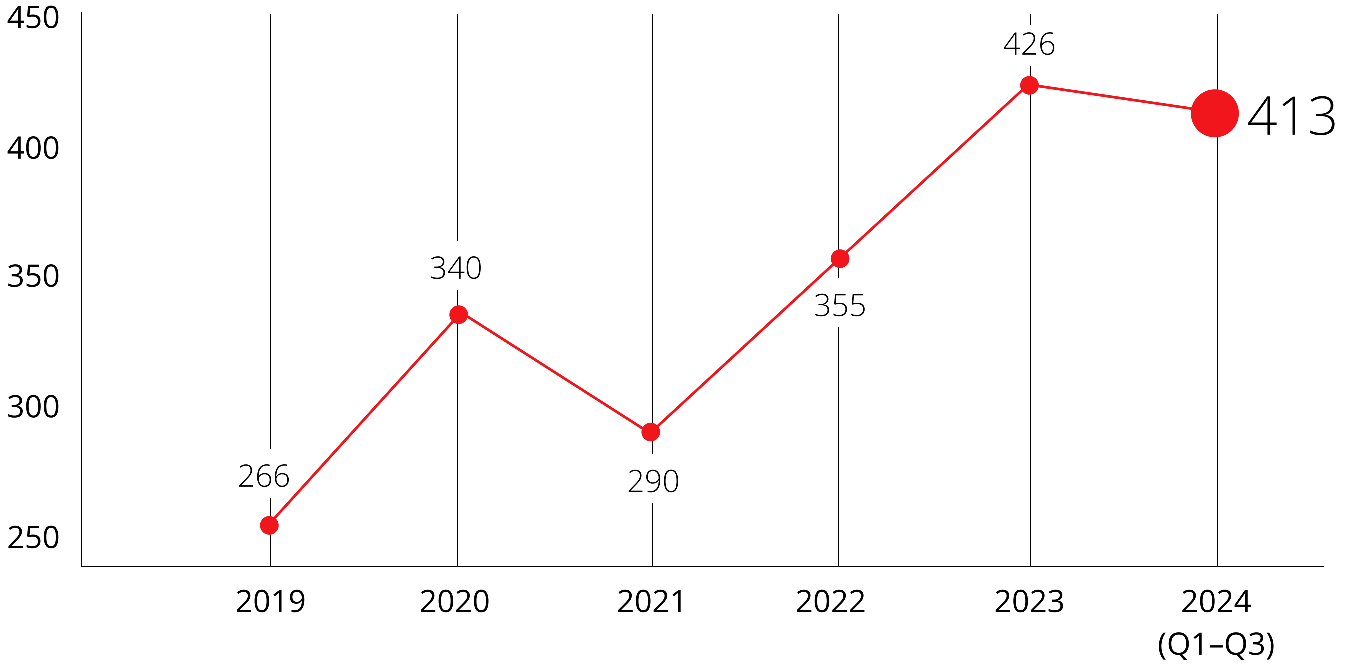
Year/Period	2021	2022	2023	2024 (Q1–Q3)
Ransomware damage cost	$74,755,025	$242,834,110	$523,644,411	$167,591,200
Data leakage cost	$13,795,000	$4,000,000	$9,714,214,350	$601,238,200
System downtime cost	$1,300,385,123	$802,688,630	$2,529,479,231	$867,354,184
Total cost	$1,388,935,148	$1,049,522,740	$12,767,337,992	$1,636,183,584

The relative decrease in ransomware damage cost in 2024 can be attributed to **law enforcement crackdowns** on major ransomware operations. However, this decline does not suggest a reduced threat level. Instead, it is likely a **strategic recalibration** by ransomware-as-a-service (RaaS) groups, reflecting their ability to adapt and evolve.

*All monetary values are in US dollars (US$). VicOne's calculations consider variables across different forms of cyberattacks, particularly ransomware and data leakage, to estimate these costs. The significant growth in costs reflects the cascading nature of these threats, particularly stolen data.

PERSISTENTLY HIGH LEVELS OF AUTOMOTIVE VULNERABILITIES

The number of reported vulnerabilities (CVEs) remained high, following the surge in the previous year. This reflects the **growing complexity of automotive systems** and their increased exposure to cyber risks.



Vulnerabilities began shifting from chipset-related issues to those involving in-vehicle infotainment (IVI) platforms, operating systems, and electric vehicle (EV) charging infrastructure. This trend highlights the need to secure both **vehicle safety** (which largely depends on chipsets) and the functionality and resilience of other **critical automotive technologies**.

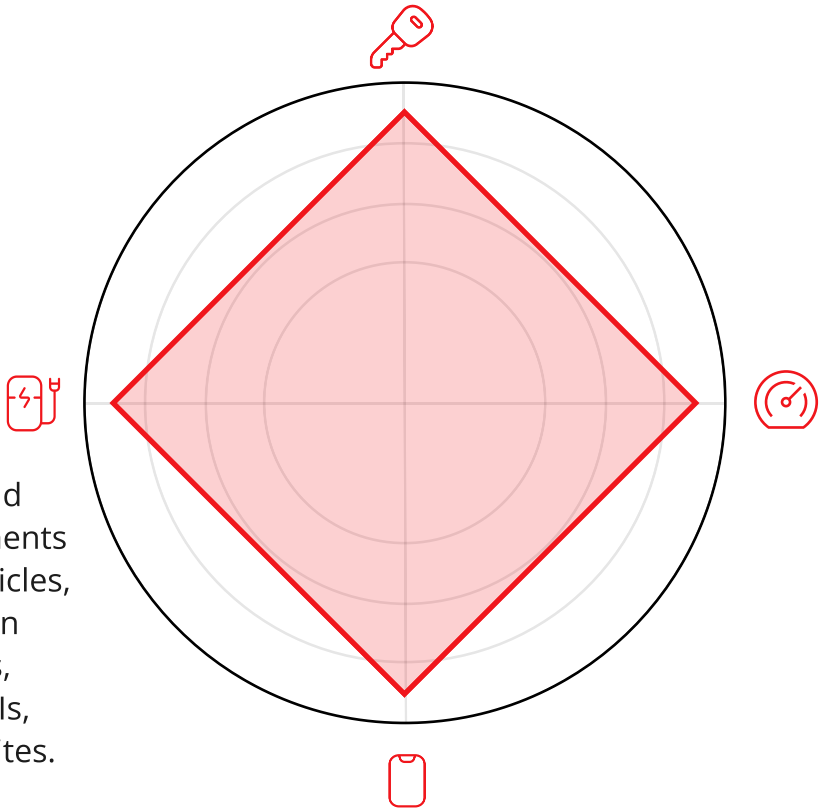
*The graph reflects the number of automotive-related CVEs published per year.

TOP TARGETS FOR AUTOMOTIVE VULNERABILITIES

The reported vulnerabilities point to the **evolving risks** tied to the complexity of modern automotive technologies. **Key areas** most frequently targeted include:

Immobilizer systems

Attacks on immobilizer systems can lead to vehicle malfunctions or car theft through wireless keyfob hacking. Such incidents compromise vehicle functionality and safety.



EV charging

Protocol vulnerabilities and low-cost components pose risks to vehicles, including issues in charging stations, related apps, GUIs, and associated sites.

Infotainment systems

Exploits can grant access to vehicle operations and sensitive data, leading to serious security concerns.

APIs and connected apps

Breaches can expose personal data and enable remote vehicle control through compromised accounts, threatening both user privacy and safety.

PRIORITIZING CYBERSECURITY IN THE AUTOMOTIVE ECOSYSTEM

The data makes it clear that the automotive industry must embrace a **proactive, comprehensive approach** to address vulnerabilities and secure its supply chain.

Key Recommendations

Enhance supply chain security.

Strengthen cybersecurity across all levels of the supply chain by addressing third-party vulnerabilities, establishing industry-wide standards, and supporting smaller suppliers with resources and training.

Protect advanced vehicle technologies.

Mitigate emerging threats by implementing multilayered defenses for technologies such as autonomous systems, AI-powered smart cockpits, and EV chargers.

Adopt proactive cybersecurity measures.

Invest in real-time monitoring, timely software updates, and robust anti-ransomware solutions to stay ahead of evolving threats.

Ensure transparency and data security.

Clearly communicate data usage practices, and secure exchanges through encryption and stringent access controls.

Align with global standards.

Collaborate with international regulatory bodies and actively participate in global cybersecurity initiatives.

VicOne

VicOne.com