protiviti®
Global Business Consulting

DRIVE SECURE

NAVIGATING CYBER SECURITY & PRIVACY IN CONNECTED VEHICLES

Face the Future with Confidence®

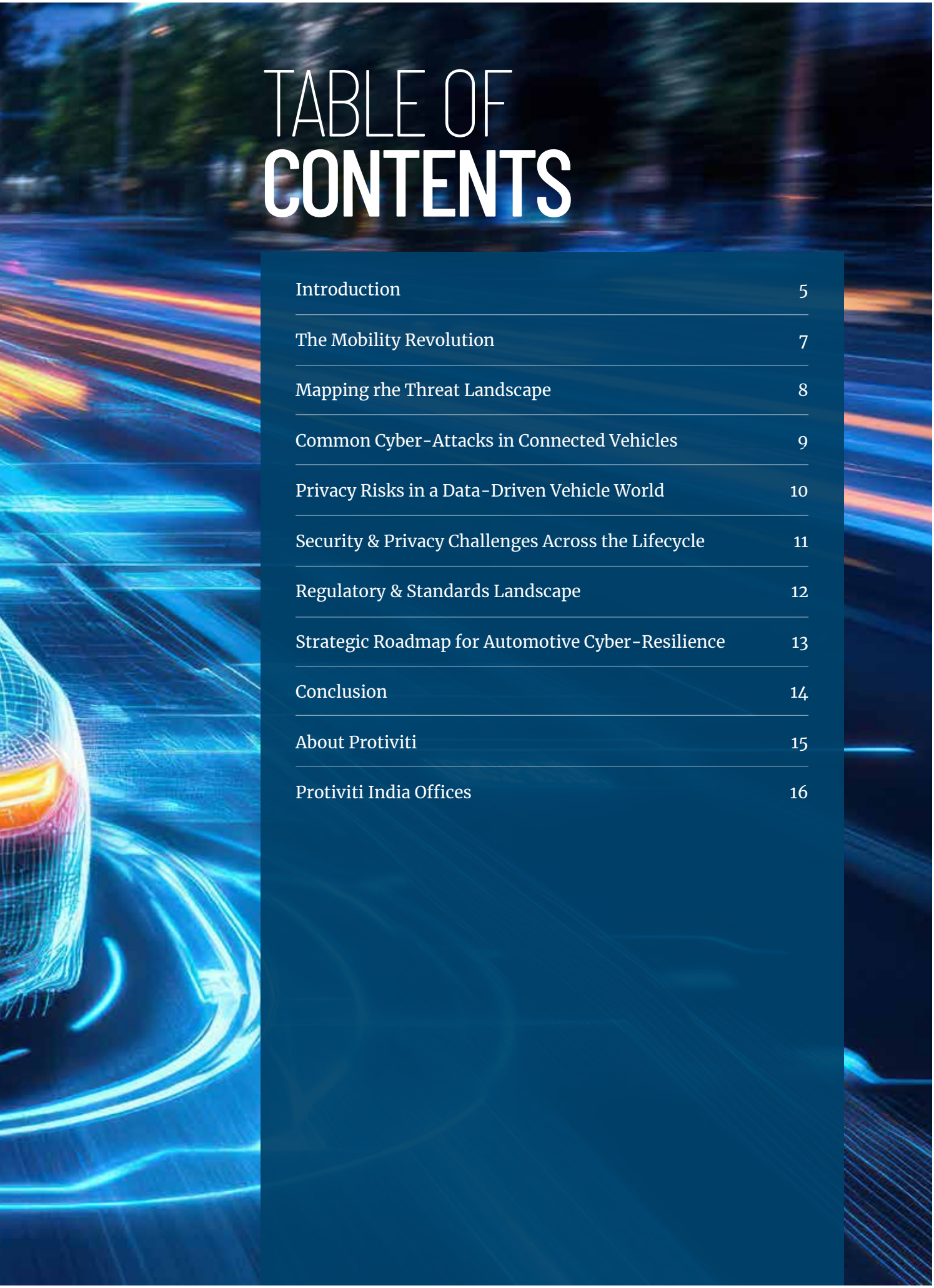
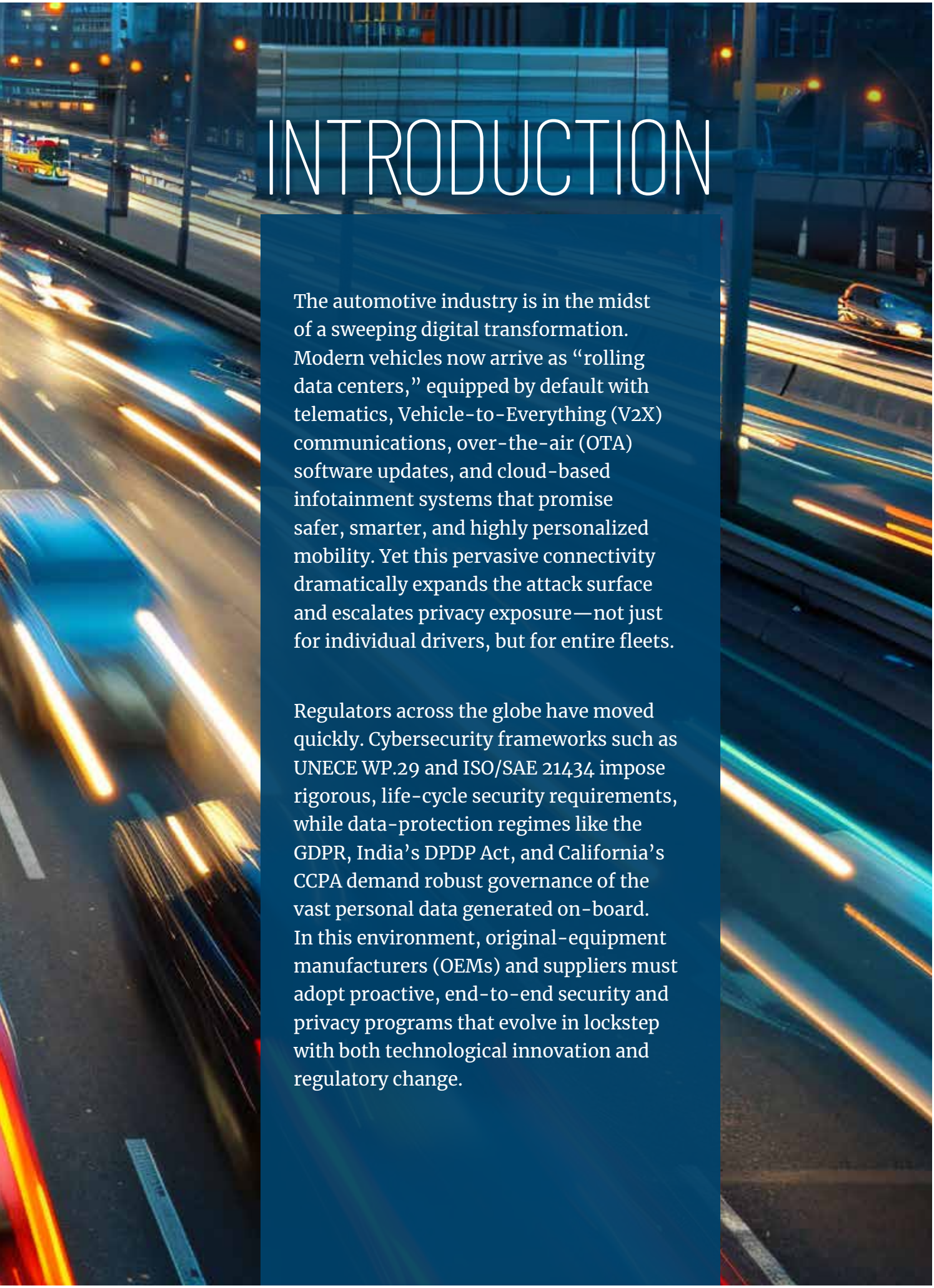


TABLE OF CONTENTS



INTRODUCTION

The automotive industry is in the midst of a sweeping digital transformation. Modern vehicles now arrive as "rolling data centers," equipped by default with telematics, Vehicle-to-Everything (V2X) communications, over-the-air (OTA) software updates, and cloud-based infotainment systems that promise safer, smarter, and highly personalized mobility. Yet this pervasive connectivity dramatically expands the attack surface and escalates privacy exposure—not just for individual drivers, but for entire fleets.

Regulators across the globe have moved quickly. Cybersecurity frameworks such as UNECE WP.29 and ISO/SAE 21434 impose rigorous, life-cycle security requirements, while data-protection regimes like the GDPR, India's DPDP Act, and California's CCPA demand robust governance of the vast personal data generated on-board. In this environment, original-equipment manufacturers (OEMs) and suppliers must adopt proactive, end-to-end security and privacy programs that evolve in lockstep with both technological innovation and regulatory change.

THE MOBILITY REVOLUTION — AND WHY CYBERSECURITY NOW SITS IN THE DRIVER'S SEAT

Vehicles have accelerated from purely mechanical machines to **software-defined, perpetually connected platforms**. A single modern car packs **100 + million lines of code, 70 + ECUs, multiple wireless radios, and an always-on cloud tunnel**. Safety-critical functions—once governed by gears and hydraulics—now update over the air as frequently as smartphone apps via edge-AI and ADAS routines.

Today's automobile is effectively a rolling technology hub, seamlessly blending:

- **Cloud-powered infotainment**
- **Telematics & predictive diagnostics**
- **Vehicle-to-Everything (V2X) communication**—vehicle-to-vehicle and vehicle-to-infrastructure
- **Mobile**-device convergence for remote commands and personalization
- **Secure, large-scale Over-the-air (OTA) firmware and feature updates**

These capabilities elevate convenience and efficiency, yet they also introduce **digital, physical, and supply-chain attack surfaces** that adversaries can exploit.

Against this backdrop, **cybersecurity and data privacy have moved from nice-to-have options to non-negotiable pillars of business resilience and consumer trust**. Automakers and suppliers that embed robust cyber-privacy controls across the vehicle life-cycle will define the next era of safe, trusted mobility.

Decoding the Connected-Vehicle Ecosystem

Before cyber-hardening a modern vehicle, security teams must first grasp the **digital tapestry that links hardware, software, cloud, and user touch-points into a single mobility platform**. Key building blocks include:

- **Telematics Control Unit (TCU)** — cellular gateway that powers eCall, remote diagnostics, and fleet-management telemetry.
- **Infotainment / Head Unit** — hosts navigation, app-store content, streaming media, and Bluetooth or Wi-Fi pairing.
- **In-Vehicle Networks** — Controller Area Network (CAN), FlexRay, and Automotive Ethernet weave power-train, chassis, body, and ADAS ECUs into one real-time backbone.
- **V2X Module** — DSRC or C-V2X radio exchanging millisecond-level safety messages with roadside units and neighboring vehicles.
- **OTA Update Manager** — cloud orchestration plus an in-car agent that delivers signed firmware, maps, and feature activations.
- **Mobile Companion Apps & APIs** — provide remote lock/unlock, climate pre-conditioning, charge status, and geo-fencing services.
- **Cloud Platforms & Data Lakes** — aggregate high-volume telemetry for predictive maintenance, usage-based insurance, and product analytics.

Each element is a **business enabler and, simultaneously, a potential attack vector**. Effective protection therefore relies on layered, defense-in-depth controls that span the entire ecosystem—from ECU silicon to cloud micro-services and every wireless hop in between.

MAPPING THE THREAT LANDSCAPE

Key Attack Vectors

A connected vehicle is only as secure as its most overlooked interface. Every cellular antenna, Bluetooth stack, cloud micro-service, and in-car network segment represents a **potential point of entry for adversaries**. Threat actors routinely probe for the softest target—an open TCU port, an unpatched infotainment OS, an over-privileged mobile-app token, or a misconfigured OTA server—and then pivot laterally toward safety-critical ECUs or valuable data stores.

Systematically charting these vectors is the first step in crafting an effective, defense-in-depth strategy.

ATTACK SURFACE	TYPICAL RISK SCENARIO	PRIORITY RECOMMENDATIONS
Telematics Interfaces	Default credentials or outdated firmware allow remote root access.	Mutual TLS, credential rotation, rigorous patch SLAs, fuzz-testing.
Infotainment Systems	Media-parsing or browser flaws enable code execution and lateral movement to safety ECUs.	Containerize apps, enforce least-privilege, continuous vulnerability scanning.
Controller Area Network (CAN) / In-Vehicle Networks	Lack of message authentication lets attackers spoof braking or steering commands.	Segmentation, CAN-MAC, gateway firewalls, anomaly-detection ECUs.
Mobile Apps & Cloud APIs	Hard-coded tokens or excessive permissions expose vehicle controls.	OWASP MASVS compliance, OAuth2 short-lived tokens, API monitoring.
OTA Infrastructure	Compromised update servers push malware to entire fleets.	Sign & encrypt every payload, hardware root-of-trust validation, staged rollout with rollback.
Keyless Entry / Ultra - Wide Band (UWB)	Relay attacks silently unlock and start cars.	Distance-bounding, motion-aware fobs, UWB-based ranging.
Diagnostic Ports On Board Diagnostic (OBD-II)	Physical access yields firmware dumps or message injection.	Disable write commands in production, encrypt debug interfaces, port hard-covers.

COMMON CYBER-ATTACKS IN CONNECTED VEHICLES

High-profile vehicle hacks—from the car takeover to the remote compromise of electric-car charging apps—reveal **a distinct playbook that attackers reuse and refine**. Whether the end goal is theft, extortion, espionage, or sheer disruption, most exploits fall into recognizable categories: remote-code execution via infotainment, relay attacks on keyless systems, CAN-bus spoofing, malicious OTA payloads, GPS spoofing, or large-scale data breaches.

An effective defense therefore begins with a clear taxonomy of these techniques and an equally clear mapping to **practical, field-tested countermeasures**. By analysing the adversary's patterns and closing each corresponding gap—through secure boot, signed firmware, message authentication, intrusion detection, and robust cloud access controls—OEMs and suppliers can convert past lessons into future resilience.

ATTACK TECHNIQUE	REAL-WORLD IMPACT	EFFECTIVE MITIGATION
Remote Code Execution (RCE)	Full ECU takeover; attacker pivots to drivetrain.	Secure boot, stack canaries, ASLR, frequent patching.
Relay Attacks on Keyless Systems	Stealth vehicle theft in < 30 seconds.	UWB fobs, motion-sensing activation, RF shielding garages.
CAN Message Injection	Disable brakes, spoof speedometer, or steer.	Message authentication codes (MAC), CAN IDS, bus segregation.
OTA Malware Injection	Fleet-wide ransomware or spyware.	End-to-end signed & encrypted OTA, multi-sig approvals, rollback protection.
OTA Infrastructure	Compromised update servers push malware to entire fleets.	Sign & encrypt every payload, hardware root-of-trust validation, staged rollout with rollback.
GPS Spoofing / Jamming	Navigation misguidance or autonomous path disruption.	Multi-GNSS validation, inertial navigation fallback, RF monitoring.
Cloud Credential Theft	Mass location tracking or remote command abuse.	MFA on admin portals, secrets vault, continuous anomaly detection.

PRIVACY RISKS IN A DATA-DRIVEN VEHICLE WORLD

Every connected vehicle now doubles as a mobile sensor suite, streaming terabytes of raw telemetry each year—GPS breadcrumbs, inertial data, biometric voiceprints, cabin images, driver-behaviour metrics, app-store clicks, and streaming-media preferences. Much of this data is indispensable for safety functions, predictive maintenance, usage-based insurance, and personalized services. Yet the same abundance also creates a rich target for advertisers, stalkers, cyber-criminals, and over-zealous data brokers. As a result, the connected-car ecosystem confronts four core privacy challenges:

- **Surveillance & Profiling** — Persistent VIN-to-driver linkage enables granular tracking, behavioral analytics, and potentially discriminatory scoring.
- **Unauthorized Data Monetization** — Telematics or infotainment datasets may be repackaged and sold to third parties without meaningful, informed consent.
- **Cross-Border Data Transfers** — Roaming vehicles routinely shuttle personal data across jurisdictions, invoking conflicting requirements under GDPR, India's DPDP Act, CCPA/CPRA, LGPD, and other regional laws.
- **In-Cabin Sensor Exposure** — Microphones and cameras can inadvertently record private conversations, children, or sensitive documents, leading to accidental over-collection and heightened regulatory scrutiny.

Mitigating these risks demands a Privacy-by-Design framework—data minimization at the edge, on-device aggregation, granular consent dashboards, encryption in transit and at rest, strict retention limits, and transparent user controls—to ensure that the data fueling tomorrow's mobility does not simultaneously erode consumer trust.

SECURITY & PRIVACY CHALLENGES ACROSS THE LIFECYCLE

Building a secure vehicle is not a one-time engineering milestone; it is a **continuous, cradle-to-grave discipline**. From the first concept sketch to end-of-life recycling, every phase introduces new assets, new stakeholders, and new attack surfaces. A single lapse—an unsecured flashing station on the factory floor, an out-of-date third-party library, or an ignored CVE in a ten-year-old ECU—can unravel the most sophisticated controls deployed elsewhere. **Cyber-resilience, therefore, is capped by the weakest lifecycle link**

LIFECYCLE STAGE	KEY CHALLENGE	FOCUSED RECOMMENDATION
Concept & Design	Feature-rush sidelines threat modeling.	Embed secure-by-design gates, abuse-case storyboarding.
Development	Open-source or supplier code introduces hidden vulns.	Secure SDLC, SAST/DAST, continuous SBOM generation.
Manufacturing	ECU flashing stations may be tampered with.	Secure factory networks, code-sign firmware, hardware attestation.
Supply Chain	Third-party stacks (Bluetooth, Wi-Fi) harbor zero-days.	Supplier security scorecards, contractual clauses, pen-tests.
Operation & Maintenance	10–15-year support window strains patching.	Vehicle SOC, remote telemetry, automated OTA cadence, CVE watch.
End-of-Life	Data remnants persist after vehicle resale or scrap.	Secure data wipe, cryptographic key revocation, scrap-yard guidance.

Only by weaving consistent security and privacy controls through every lifecycle milestone can OEMs and suppliers ensure that connected-car innovations remain trustworthy—today, tomorrow, and a decade from now.

REGULATORY & STANDARDS LANDSCAPE

From Compliance Burden to Blueprint for Excellence

The connected-car industry now operates under a rapidly maturing rulebook that does more than threaten fines; it **codifies a roadmap for secure and trustworthy mobility.**

- **UNECE WP.29 (R155 & R156)** — Makes type approval contingent on a demonstrable Cybersecurity Management System (CSMS) and a Software-Update Management System (SUMS), forcing OEMs to institutionalize threat analysis, secure OTA pipelines, and post-production monitoring.
- **ISO/SAE 21434** — Extends this mandate into engineering practice, prescribing risk-based cybersecurity processes across concept, development, production, operation, and decommissioning. Compliance here not only satisfies auditors but also synchronizes cross-functional teams on a common security vernacular.
- **Auto-ISAC Best Practices** — Encourages industrywide threat-intelligence sharing and coordinated incident response, effectively raising the herd immunity of the automotive ecosystem.
- **NIST CSF & SP 800-161** bring supplier depth, mapping "identify-protect-detect-respond-recover" to every ECU and back-end micro-service, while NIST AI RMF layers on trustworthy-AI controls for vision, voice, and driver-assist models.
- **Global Data-Protection Statutes (GDPR, CCPA/CPRA, Brazil LGPD) and India's DPDP Act, 2023 & Draft Rules 2025)** — Shift the narrative from "who owns the data?" to "who protects the data?" by enforcing explicit consent, purpose limitation, data-minimization, and 72-hour breach-notification requirements.

The cost of non-compliance is material: GDPR can levy up to **€20 million or 4% of global turnover**, while India's DPDP Act authorizes penalties up to **₹150-250 crore per incident**. Beyond fines, regulators may revoke production licenses or block vehicle sales in non-compliant markets.

Forward-leaning OEMs are leveraging these mandates as **design baselines**, integrating WP.29 and ISO/SAE 21434 controls directly into their product-development pipelines and using privacy laws to justify robust data-governance budgets. In effect, **regulation is evolving from a compliance afterthought into a competitive differentiator**—one that rewards companies able to demonstrate verifiable cyber and privacy stewardship to regulators, insurers, and increasingly security-savvy consumers.

STRATEGIC ROADMAP FOR AUTOMOTIVE CYBER-RESILIENCE

Achieving meaningful risk-reduction demands a dual-track game plan:

- Long-horizon strategic initiatives that embed security and privacy into the vehicle DNA, and
- Tactical quick wins that harden the current fleet and demonstrate immediate ROI.

A. High-Impact Strategic Initiatives

KEY FOCUS AREA	WHAT "GOOD" LOOKS LIKE	PRIORITY ACTION ITEMS
Security-by-Design	Cyber risks are addressed as system requirements, not post-launch patches.	• Mandate threat-modelling in concept phase • Secure-coding gates in CI/CD pipelines
Zero-Trust Vehicle Architecture	Every ECU, domain, and cloud API is authenticated and least-privileged.	• Physically & logically segregate infotainment from safety domains • Mutual-TLS or MACed traffic on in-vehicle networks
Secure OTA Governance	Updates are tamper-proof, rollback-safe, and audit-ready.	• End-to-end payload signing & encryption • Staged rollouts with health telemetry and automatic rollback
Fleet Threat Monitoring (vSOC)	Real-time detection of anomalies across millions of vehicles.	• Telemetry baselining & ML-driven anomaly scores • 24 × 7 incident-response playbooks
Privacy-by-Design	Data practices engender consumer trust and regulatory compliance.	• Granular consent dashboards • On-device aggregation & data minimization • Automated deletion workflows
Supply-Chain Assurance	Third-party code/hardware meets the same rigor as in-house assets.	• SBOM-driven vulnerability scanning • Contractual security KPIs • Regular supplier pen-tests & red-team drills

B. Tactical Quick Wins

- **Drop-in CAN IDS ECUs** – Add intrusion-detection gateways in next-gen models to flag spoofed brake/steer messages.
- **Deploy Hardware Security Modules (HSMs)** – Secure ECU key storage and cryptographic ops without full redesign.
- **Harden the OTA Pipeline** – Enforce payload signing + encryption today; add staged rollout/rollback logic tomorrow.
- **Tighten Cloud & API Hygiene** – Replace long-lived tokens with least-privilege, short-life credentials; enable continuous anomaly monitoring.

Implementing these quick wins delivers **visible risk reduction within 6–12 months**, while the strategic track builds a sustainable, audit-ready security posture that will stand up to evolving threat actors and regulatory scrutiny.

CONCLUSION

Trust is the New Horsepower

Connected cars will define the next decade of mobility—but only if security and privacy are engineered in, not bolted on. A single breach can trigger recalls, fines, and reputational crash-tests the industry can't afford. Automakers that embed Zero-Trust architectures, secure OTA pipelines, and privacy-by-design controls will convert compliance pressure into market advantage.

The mandate is simple: keep innovating, but protect every byte and every passenger. Tomorrow's vehicles must be more than smart; they must be unequivocally secure and trusted.

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.
Named to the 2024 Fortune 100 Best Companies to Work For® list for the past 10 years, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACT US

SANDEEP GUPTA
Managing Director,
Technology & Digital
Sandeep.Gupta@protivitiglobal.in

VAIBHAV KOUL
Managing Director,
Technology & Digital
Vaibhav.Koul@protivitiglobal.in

AJU SEBASTIEN
Managing Director,
Technology & Digital
aju.sebastian@protivitiglobal.in

SAHIL CHANDER
Senior Director,
Technology & Digital
sahil.chander@protivitiglobal.in

NAGESH AKULA
Senior Director,
Technology & Digital
nagesh.akula@protivitiglobal.in

SARITA PADMINI
Senior Director,
Technology & Digital
sarita.padmini@protivitiglobal.in

PROTIVITI INDIA **OFFICES**

Ahmedabad
6th Floor, West Gate, E-Block,
Near YMCA Club, SG Highway,
Gujarat, 380 015, India

Bengaluru
Umiya Business Bay - 1, 9th Floor
Cessna Business Park, Outer Ring
Road, Kadubeesanahalli, Varthur
Hobli Bengaluru – 560 049
Karnataka, India

Bhubaneswar
1st floor, Unit No 104, 105, 106
Utkal Signature, Chennai Kolkata
Highway Pahala, Bhubaneswar
Khordha - 752 101
Odisha, India

Chennai
10th Floor, Module No. 1007
D Block, North Side, Tidel Park
No. 4, Rajiv Gandhi, Salai,
Taramani, Chennai - 600 113
Tamil Nadu, India

Coimbatore
TICEL Bio Park, (1101 - 1104)
11th floor Somaiyapalyam
Village, Anna University Campus,
Maruthamalai Road, Coimbatore
North Taluk, Coimbatore – 641046
Tamil Nadu, India

Gurugram
15th & 16th Floor, Tower A,
DLF Building No. 5, DLF Phase III
DLF Cyber City,
Gurugram – 122 002
Haryana, India

Hyderabad
Q City, 4th Floor, Block B,
Survey No. 109, 110 & 111/2
Nanakramguda Village
Serilingampally Mandal, R.R.
District Hyderabad – 500 032
Telangana, India

Kolkata
PS Srijan Corporate Park,
Unit No. 1001 10th & 16th Floor,
Tower - 1, Plot No. 2
Block - EP & GP Sector-V,
Bidhannagar Salt Lake
Electronics Complex
Kolkata –700 091,
West Bengal, India

Mumbai
1st Floor, Godrej Coliseum
A & B Wing Somaiya Hospital Road
Sion (East) Mumbai – 400 022
Maharashtra, India

Mumbai - Goregaon
The Westin Garden City,
13th Floor, Commerz 1-
International Business Park,
Behind Oberoi mall, South Side,
Goregaon, Mumbai - 400063,
Maharashtra, India

Noida
Windsor Grand, 14th & 16th Floor
1C, Sector - 126 Noida
Gautam Buddha Nagar- 201313
Uttar Pradesh, India

KS_ 123658_APR2025

Face the Future with Confidence®