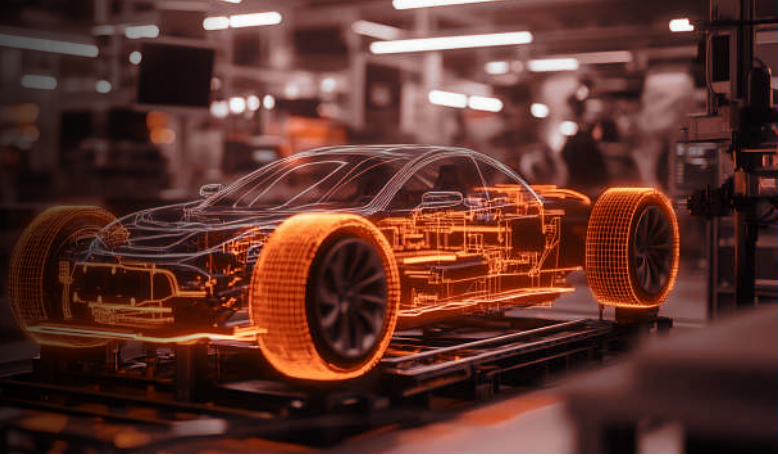


QUANTUM THREAT INTELLIGENCE REPORT: AUTOMOBILE INDUSTRY 2025



THREAT LEVEL EXTREME

The global automobile industry faces a critical quantum cryptographic vulnerability with 400M+ connected vehicles operating on encryption breakable by quantum computers expected 2026-2031.

KEY FINDINGS:

- Timeline Crisis**
Vehicles produced in 2025 operate until 2035-2040, beyond quantum computer arrival (2026-2031)
- Active Attacks**
"Harvest Now, Decrypt Later" (HNDL) collecting vehicle telemetry, OTA updates, proprietary designs NOW
- Global Mandates**
EU requires quantum-safe infrastructure by 2030; US federal systems by 2027
- Financial Impact**
\$130-193B industry cost for quantum transition; \$150-300B breach exposure
- Fleet Vulnerability**
300M+ vehicles globally at risk during 4-15 year quantum exposure window

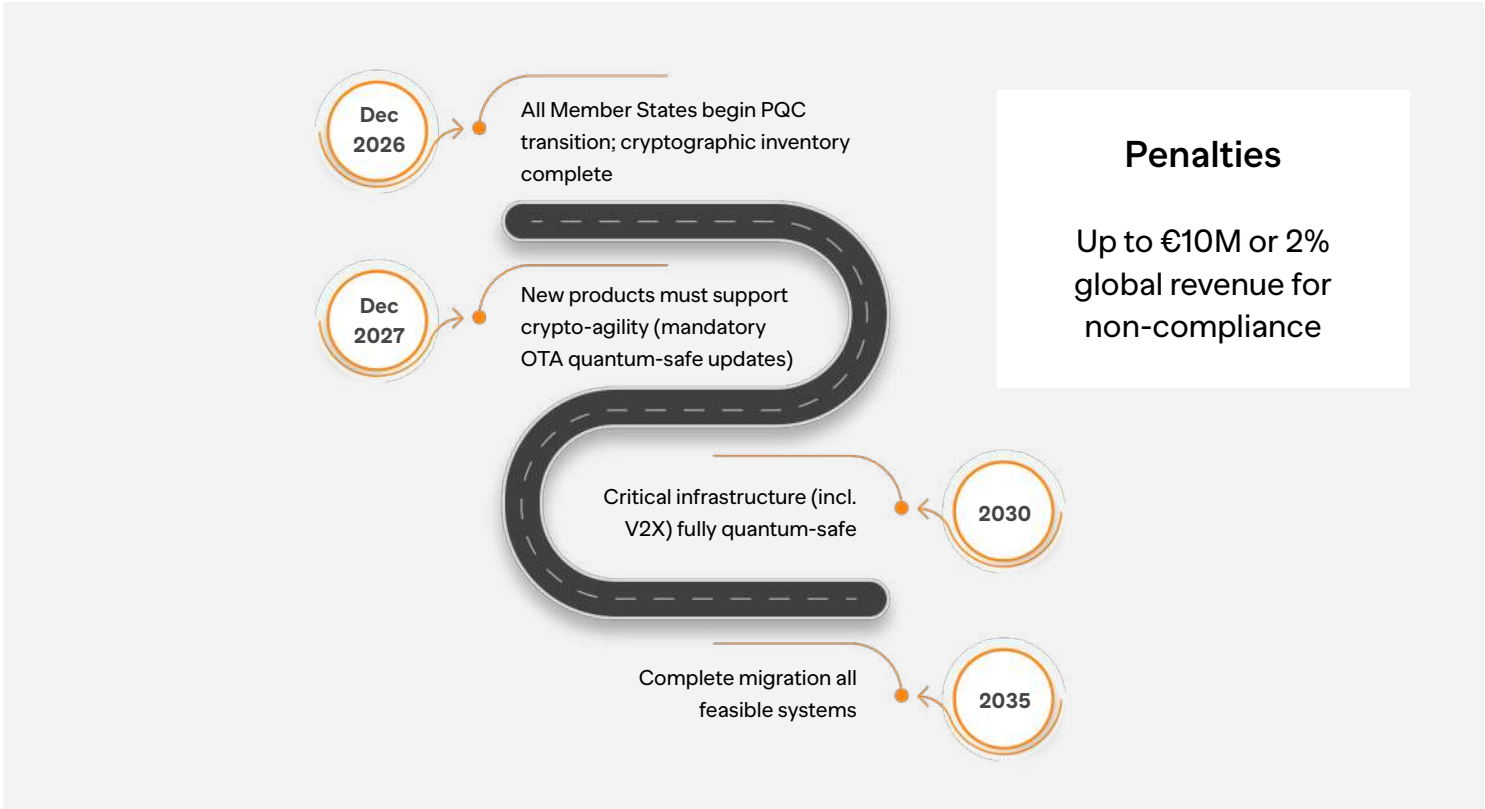
GLOBAL REGULATORY MANDATES & TIMELINES

1.1 | EUROPEAN UNION



- NIS2 Directive + Cyber Resilience Act
- Automotive-Specific

NIS2 Directive + Cyber Resilience Act:



Automotive-Specific:

EU General Safety Regulation II Cybersecurity mandatory for type approval	V2X Communications Must be quantum-safe by 2030	OTA Updates Quantum-safe signatures required Dec 2027
---	---	---

(Source: <https://digital-strategy.ec.europa.eu>)

1.2 | UNITED STATES



- Federal Mandates
- NIST Standards (Aug 2024)

Federal Mandates:

- **NSM-10**
All agencies mitigate quantum risk by 2035
- **OMB M-23-02**
Annual quantum-vulnerable system inventories through 2035
- **Quantum Preparedness Act**
Mandatory PQC migration for federal contractors (includes automotive suppliers)
- **EO 14144 (Jan 2025)**
TLS 1.3 quantum-safe by Jan 2, 2030; CISA/NSA product categories by Dec 1, 2025
- **NSA CNSA 2.0**
New National Security Systems acquisitions PQC-compliant by Jan 1, 2027; full compliance 2033

NIST Standards (Aug 2024):

FIPS 203
ML-KEM (CRYSTALS-Kyber)

Key encapsulation

FIPS 204
ML-DSA (CRYSTALS-Dilithium)

Digital signatures

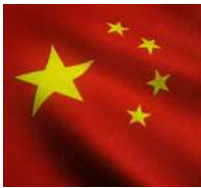
FIPS 205
SLH-DSA (SPHINCS+)

Hash-based signatures

FIPS 206
FN-DSA (FALCON)

Lattice signatures (pending)

1.3 | OTHER MAJOR MARKETS



CHINA

Mandating quantum-safe connected vehicles
2026-2027; 2,000km quantum network operational



JAPAN

\$7.4B quantum investment; Toyota/Honda PQC
integration targeting 2028



UK

NCSC clear roadmap; critical automotive
infrastructure PQC by 2030



INDIA

₹6,003.65 crore National Quantum Mission; indigenous
development focus 2025-2030

(Source: <https://www.safelogic.com/compliance/pqc-standards>)

THREAT LANDSCAPE & ATTACK VECTORS

2.1 | CRYPTOGRAPHIC VULNERABILITIES

Protocol	Usage	Quantum Attack	Risk
RSA-2048	V2V comms, sessions	Shor's algorithm	CRITICAL
ECC	Chip PKI, certificates	Shor's algorithm	CRITICAL
AES-128/256	Data encryption	Grover's algorithm	HIGH
TLS/SSL	Internet connectivity	Both algorithms	CRITICAL
PKI	Certificate authority	Both algorithms	CRITICAL

Breakthrough

RSA-2048 breakable with only 372 physical qubits (Source: arXiv:2212.12372) - significantly
accelerates threat timeline.

2.2 | CRITICAL ATTACK VECTORS

A | V2X Communication Compromise

- **Scale**
400M+ connected vehicles
- **Impact**
Traffic manipulation, collision induction, mass disruption
- **Safety**
ISO 26262 functional safety compromised

B | OTA Update Hijacking

- **Method**
Quantum breaks update authentication
- **Impact**
Malicious firmware injection at fleet scale

Example

Tesla 4M+ annual OTA updates - all vulnerable

C | ECU Exploitation

- **Targets**
70-100 ECUs per vehicle (braking, steering, acceleration, ADAS)
- **Result**
Life-threatening physical manipulation
- **Regulation**
UN R155/R156 insufficient for quantum threats

D | Autonomous Vehicle AI Theft

- **Data**
25 GB/hour autonomous vehicle generation
- **Value**
\$1B+ investment per manufacturer
- **Impact**
Instant competitive technology parity

E | Supply Chain Intelligence

- **Targets**
Battery tech, powertrain, manufacturing processes
- **Exposure**
Tier 1-3 supplier networks vulnerable

2.3 | "HARVEST NOW, DECRYPT LATER" ACTIVE THREATS

Currently Being Collected:

- ✓

Encrypted vehicle telemetry (location, driving behavior)
- ✓

OTA update packages (firmware, patches)
- ✓

Proprietary R&D communications
- ✓

Manufacturing process data
- ✓

Infotainment personal data

Future Impact (Post-Quantum 2026-2031):

- ✓

10-15 years historical data exposed
- ✓

Individual privacy catastrophically violated
- ✓

Complete vehicle design specifications revealed
- ✓

Safety vulnerabilities systematically identified

Attribution

China PLA Cyberspace Force, Russia state actors, North Korea cybercrime, corporate espionage

(Source: <https://vicone.com/blog/quantum-computing-in-the-automotive-industry-looming-risks-to-cybersecurity>)

QUANTUM COMPUTING TIMELINE & CAPABILITIES

3.1 | CURRENT STATE (October 2025)

IBM

Quantum System Two
- 1,121 qubits

Google

Willow chip
computational advantage

IonQ

64-qubit commercial
systems

China

Massive quantum
research investment

3.2 | PROJECTED CRQC TIMELINE

Year	Capability	Automotive Impact
2026	500-1,000 qubits	Early V2X vulnerabilities
2027-2028	1,000-2,000 qubits	OTA update compromise possible
2029-2030	2,000-5,000 qubits	Fleet-wide exposure
2031+	5,000+ qubits	Complete security failure

MITIGATION STRATEGIES & ACTION PLAN

4.1 | IMMEDIATE (Q4 2025 - Q1 2026)

A | Cryptographic Inventory - Complete by Q1 2026:

- Map all encryption
ECUs, protocols, supplier dependencies
- Use Cryptographic Bill of Materials (CBOM)

C | OTA Enhancement:

- Ensure crypto-agility for algorithm updates
- Test quantum-safe signature verification
- Mandatory
EU Cyber Resilience Act Dec 2027

B | Risk Assessment (Mosca's Theorem):

- Automotive
(15yr lifecycle + 3yr migration) > 5yrs =
SEVERE RISK

D | Supply Chain Audit:

- Establish contractual PQC requirements
- Create vendor scorecards
- Required
EU NIS2 Directive

4.2 | SHORT-TERM (2026-2027)

A | Hybrid Cryptography:

- Deploy classical + quantum-resistant (FIPS 140-3 compliant)
- Performance impact
10-30% latency increase

B | NIST PQC Integration:



C | V2X Updates:

- Ensure crypto-agility for algorithm updates
- Test quantum-safe signature verification

4.3 | MEDIUM-TERM (2027-2030)

A | Fleet-wide Rollout:

- OTA deployment

100M+ vehicles per major OEM
- Dealership updates for non-connected vehicles

C | Supplier Ecosystem:

- Mandate quantum-safe components
- Industry-wide certification (AIAG, JASPAR, VDA)

D | HSM Upgrades:

- Deploy Quantum Random Number Generators (QRNG)
- ISO/SAE 21434 compliance

B | New Production Standards:

- All new models quantum-safe by default
- Type approval requirements updated

D | Autonomous Protection:

- Quantum-safe AI training data
- Secure vehicle-to-cloud

ISO 26262 + quantum integration

FINANCIAL ANALYSIS & ROI

5.1 | INVESTMENT REQUIREMENTS (Per Major OEM)

Category	Cost (5 Years)
R&D	\$500M – \$1B
Infrastructure	\$1B – \$2B
Fleet Updates	\$5B – \$10B
Supplier Programs	\$500M – \$1B
TOTAL PER OEM	\$7B – \$14B

5.2 | COST OF INACTION

Risk	Exposure
IP Theft	\$10B – \$50B per manufacturer
Safety Recalls	\$50B – \$150B
Litigation	\$5B – \$20B
Brand Damage	Immeasurable
Market Share Loss	10-30% potential
TOTAL BREACH COST	\$65B – \$220B+

ROI CALCULATION



Investment
\$7B - \$14B



Breach Cost Avoided
\$65B - \$220B+



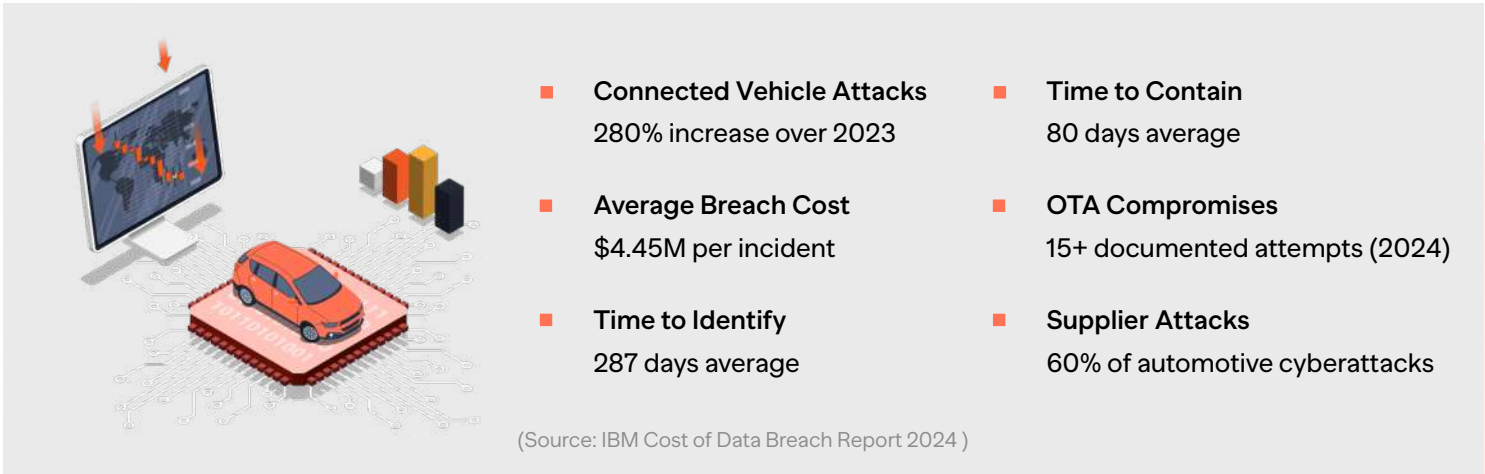
Net Benefit
\$51B - \$206B+



ROI
450% - 1,500%

INDUSTRY STATISTICS & THREAT INTELLIGENCE

6.1 | 2024 AUTOMOTIVE CYBERSECURITY DATA



6.2 | THREAT ACTOR CAPABILITIES

Nation-State:



China PLA
Targeting EV tech,
autonomous driving; HNDL
active since 2020+



Russia
Manufacturing intelligence,
supply chain disruption



North Korea
Ransomware funding,
cryptocurrency theft

Corporate Espionage:

- R&D theft

Battery tech, autonomous systems, ADAS
- Market strategy

— Production plans, pricing, launches

Organized Crime:

- Preparation for quantum-enabled ransomware
- Connected vehicle IoT botnets
- Payment system vulnerabilities

CONCLUSION: STRATEGIC IMPERATIVES

FIVE CRITICAL ACTIONS:

- 01

ACT IMMEDIATELY

Window closing: quantum computers expected 2026-2031
- 02

COMPLY GLOBALLY

Meet EU 2030, US 2027 mandates proactively
- 03

PROTECT FLEETS

Ensure OTA quantum-safe capability ALL vehicles
- 04

SECURE SUPPLY CHAINS

Mandate PQC entire ecosystem
- 05

COLLABORATE INDUSTRY-WIDE

Coordinate via Auto-ISAC, standards bodies



CONSEQUENCES OF DELAY

- ⊗

Regulatory non-compliance → Market exclusion
- ⊗

IP theft → Competitive disadvantage
- ⊗

Safety liability → Massive recalls (\$150B+)
- ⊗

Brand destruction → Consumer trust loss



BENEFITS OF ACTION NOW

- ✔

Competitive differentiation & market leadership
- ✔

Regulatory compliance & market access
- ✔

IP protection & innovation preservation
- ✔

Customer trust & brand strengthening

THE QUANTUM THREAT IS NOT "IF" BUT "WHEN."
ACT NOW.



KEY SOURCES

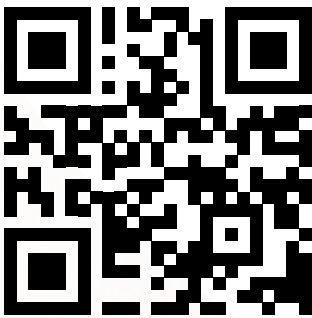
- **EU Digital Strategy**
<https://digital-strategy.ec.europa.eu>
- **SafeLogic PQC Standards**
<https://www.safelogic.com/compliance/pqc-standards>
- **VicOne Automotive Security**
<https://vicone.com/blog/quantum-computing-in-the-automotive-industry>
- **NIST PQC Standards**
<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>
- **US DIA Threat Assessment**
https://armedservices.house.gov/uploadedfiles/2025_dia_statement_for_the_record.pdf
- **McKinsey Quantum Report**
<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights>



[Blogs →](#)

[Whitepaper →](#)

Tomorrow's Quantum Security, Today.



Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary
Building, 2nd Floor, East Wing, #28 MG Road
Bengaluru - 560025

CIN: U72900KA2016PTC096629

India

USA

Australia

Global