Grant Thornton

#GTBharat
SHAPING A VIBRANT INDIA

Auto Bytes

August 2022

Automotive cyber security: Building safer ecosystems

With the number of connected cars set to increase to **352 mn** by 2023, compared with **119.4 mn** in 2021, there has been an astronomical increase in the data privy to cyber crimes[1]. A connected car is expected to generate approximately 25 GB of data per hour by 2025, whereas a fully autonomous vehicle is likely to produce data as high as 500 GB an hour. The new wave of connected mobility will only increase reliance on cyber security tools. Currently, software-enabled cars use **100 mn** lines of code, which could rise to **300 mn** by 2030.

The frequency of cyberattacks on cars has increased by 225% from 2018 to 2021. With over 84.5%[2] of automotive incidents being carried out remotely, today, hackers can access vehicles in more ways than one, such as manipulating the car's internal code, distributed denial of service (DDoS) attacks, spoofing and phishing attacks, embedding viruses in communication media, etc. Automotive cybersecurity entails securing communication networks, electronic systems, software and data collected by the new wave of connected mobility.

Top cyber automotive attacks in 2021[3]

Data/privacy breach
38%

Car/theft break-ins
27%

Control systems
20%

Cybersecurity vulnerabilities can be grouped under three umbrellas.

Vehicle

The Electronic Control Units (ECUs) in a connected car can send data through air transmission or via physical media, which can be exploited by attackers.

Communications layer

Vehicle data in transit paves way for data breaches such as DDoS attacks, spoofing and phishing.

Application layer

The stakeholders/ultimate data users, such as navigation and entertainment providers, fleet owners and city authorities, must ensure data privacy and protection against malicious attacks.

[1] Capgemini report
[2] Upstream's 2022 Global Automotive Cybersecurity report
[3] Upstream's 2022 Global Automotive Cybersecurity report

How secure is your vehicle

Secure vehicle architecture ultimately means mitigating risk for public and creating safer roads for all. To ensure this, manufacturers/suppliers prefer working with companies which follow set industry standards for reliable exchange of information throughout the production and supply chain.

For Indian automotive market, cybersecurity entails highly recognised security standards.

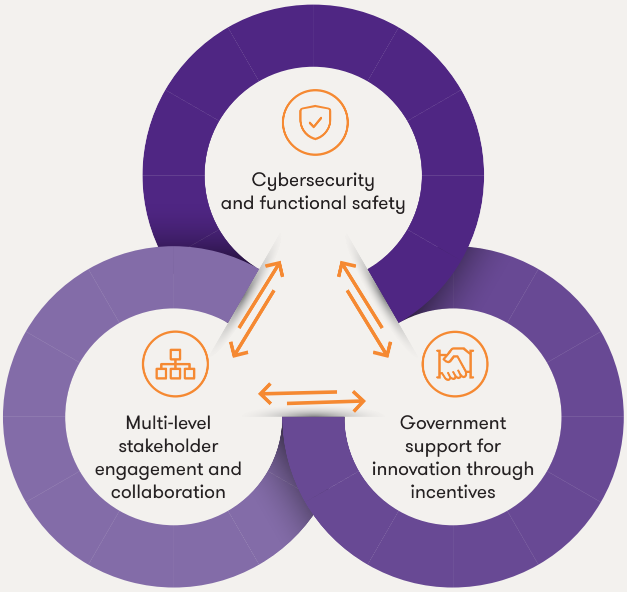
- **ISO/SAE 21434 road vehicles:** Developed by the International Organisation for Standardisation (ISO) and the Society of Automotive Engineering (SAE), this cybersecurity engineering standard[4] guides the automakers towards compliance with WP.29 automotive cybersecurity regulation and ISO 21434 suppliers and manufacturers to prioritise cybersecurity throughout the vehicle lifecycle, from ideation to retirement of a vehicle.

- In June 2020, United Nations Economic Commission for Europe (UNECE) WP.29 officially rolled out two new regulations focusing on vehicles' cybersecurity and software updates[5]. These regulations will be applicable to passenger cars, vans, trucks and buses.
  - Cybersecurity and Cybersecurity Management Systems (CSMS)
  - Software Update and Software Update Management Systems (SUMS)

- **TISAX (Trusted Information Security Assessment Exchange):** It is an exclusive certificate primarily for the automotive industry (although it can be introduced in other industries as well), which enables secure communication between clients and suppliers and protects intellectual property, i.e., prototype[6].TISAX covers a wide range of security methods and layers, including dual-factor authentication, key performance indicator (KPI) monitoring and database encryption to ensure the highest level of protection, making security a priority.

- The European Unioun (EU) has adapted to the WP.29 regulations, making them mandatory for all vehicle types in the EU from July 2022. South Korea and Japan have also committed to the regulations. **With the connected car market on a cusp of growth in India (with only 2% connected cars in 2020, to most leading vehicle manufactures developing connected cars, growth in demand is visible), ensuring effective automotive cybersecurity is the need of the hour.**
The country requisites to pivot and factor cyber security within its automotive ecosystem – from product engineering to the end-user.

[4] https://www.iso.org/standard/70918.html
[5] https://unece.org/wp29-introduction
[6] https://enx.com/en-US/TISAX/


Cybersecurity and functional safety
Multi-level stakeholder engagement and collaboration
Government support for innovation through incentives

Cybersecurity is one of the three-pillars to boost auto sector in the Indian market

The ISO 26262[7] serves as a guide to keep up with the increased software complexities while ensuring functional and software safety encompassing Advanced Driver Assistance Systems (ADAS), passive and active systems, by-wire systems and electronic stability control of the vehicle.

This functional safety must be backed with software-security at all levels, enabling a holistic approach towards gaining customer's trust.

> To stay ahead of the curve and grow towards the future of mobility, robust cybersecurity and functional safety are one of the pivotal pillars, among multi-level stakeholder engagement and government support

An ideal cybersecurity ecosystem should identify areas of risk for various stakeholders and provide risk mitigation solution for each silos, as well as overall data ecosystem. Various standards (such as ISO/IEC 27001) not only provide a blueprint to ensure effective data security but also enhance productivity and profitability by reducing duplication of operational steps. Additionally, the government of India has attempted to introduce techno-legal legislations to regulate advancements in automotive and mobility technology. However, it is still in the nascent stages of development and has not been brought under the law. Such legislation includes the Geospatial Information Regulation Bill 2016, which proposes to regulate the acquisition, dissemination, publication and distribution of geospatial information.

Challenges ahead

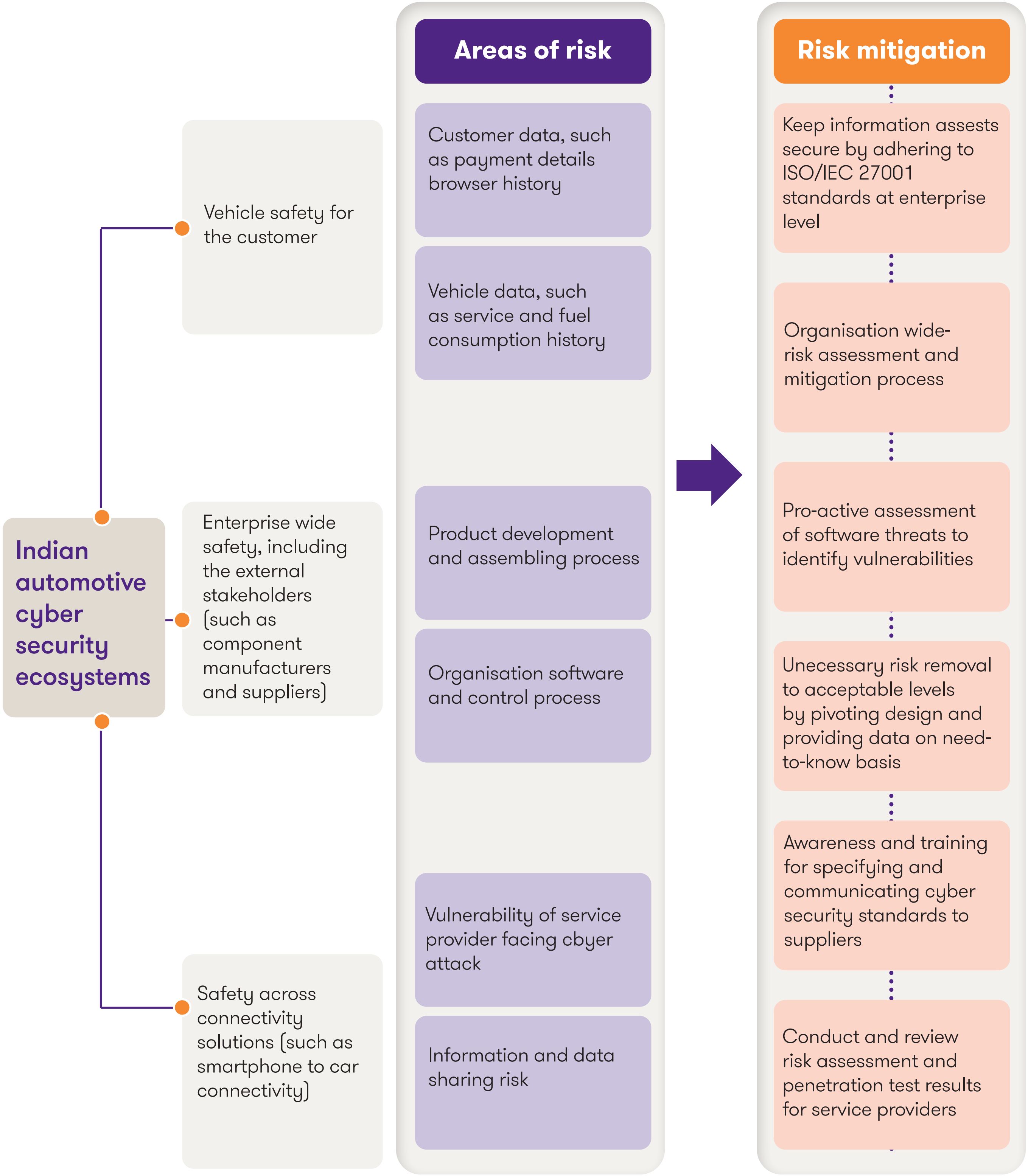
The first two months of 2022 reported more cyber crimes than the entire 2018, evidenced in the CERT-In data. With these statistics, the Indian carmakers need to go the extra mile to gain customer's trust and ensure vehicle safety. In a recent automotive customer study by IBM, 62% of consumers said they would consider the brand which has better security and privacy.

Additionally, with the technologies such as shared mobility, ADAS and safety systems being at the nascent stages in India, an augmented demand for connected systems is on the rise.

Major challenges in this regard are faced by EV start-ups, which are on the forefront of new technology adoption but lack sufficient resources and organisational structure to maintain and adhere to cybersecurity quality standards

[7] ISO 26262

Risk environment and mitigation



Indian automotive cyber security ecosystems

- Vehicle safety for the customer
- Enterprise wide safety, including the external stakeholders (such as component manufacturers and suppliers)
- Safety across connectivity solutions (such as smartphone to car connectivity)

Areas of risk

- Customer data, such as payment details browser history
- Vehicle data, such as service and fuel consumption history
- Product development and assembling process
- Organisation software and control process
- Vulnerability of service provider facing cbyer attack
- Information and data sharing risk

Risk mitigation

- Keep information assests secure by adhering to ISO/IEC 27001 standards at enterprise level
- Organisation wide-risk assessment and mitigation process
- Pro-active assessment of software threats to identify vulnerabilities
- Unecessary risk removal to acceptable levels by pivoting design and providing data on need-to-know basis
- Awareness and training for specifying and communicating cyber security standards to suppliers
- Conduct and review risk assessment and penetration test results for service providers

Best practices for automotive players

Allocation of a dedicated team focused on cybersecurity

To ensure timely and effective organisation-wide cybersecurity governance systems, there is a need to allocate dedicated resources proficient at mapping threats within each layer of the production, supply chain and distribution value chain. This will enable fostering a proactive cybersecurity culture within the organisation.

Perform gap-assessment

It is imperative to analyse if the best practices pertaining automotive security, such as incident response, collaboration and engagement with appropriate third parties, governance, risk assessment and management, awareness and training are being followed. Dedicated resources and pro-active intervention, wherever a gap is recognised can go miles.

Engage within the ecosystem

Auto-firms can tie-up with organisations, such as Car Connectivity Consortium (member companies include smartphones and vehicle manufacturers, automotive Tier-1 suppliers, silicon/chip vendors, security product suppliers and more) for a holistic perspective for building safer ecosystems.

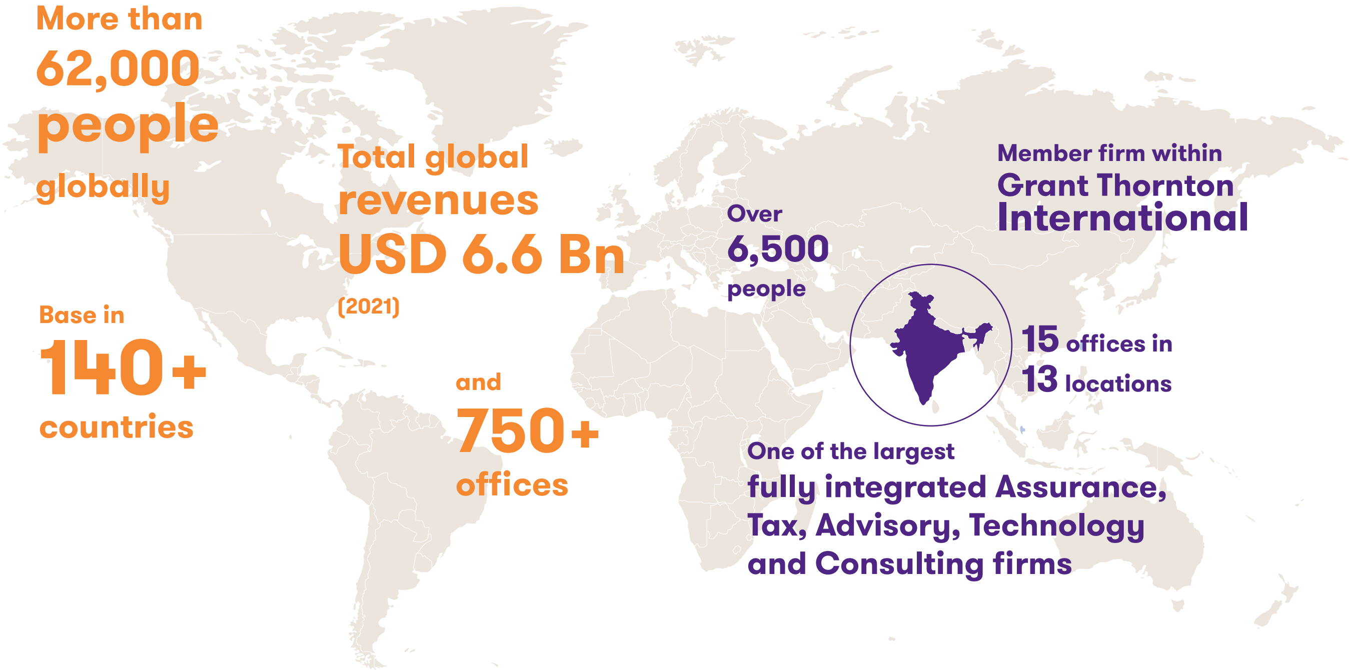
Are you future-ready?

With the estimated projection of automotive industry losing USD 505 billion by 2024 to cyberattacks, the industry needs to be proactive and vigilant in identification and prevention of malicious attacks and cyber criminals. Over the next decade, the global automotive cybersecurity market is expected to record an annual growth rate of 21.7%[8]. A majority of OEMs are acknowledging the needs of connectivity and introduction of new technologies to foster mobility. This signals a huge growth opportunity for market players. Additionally, this trend highlights that the automotive organisations that take cybersecurity most seriously are best placed to lead the market from the front in the coming decade. Indian OEMs need to start preparing for a full-fledged cybersecurity management system. The years 2022 to 2024 would be the foundation for Indian OEMs to lay structural blueprint and map requirements for organisational cybersecurity.

Sources

[8] Globe NewsWire Report: Cybersecurity Market

About Grant Thornton Bharat



More than **62,000 people** globally

Total global **revenues USD 6.6 Bn** (2021)

Base in **140+ countries**

and **750+ offices**

Over **6,500** people

Member firm within **Grant Thornton International**

15 offices in **13** locations

One of the largest **fully integrated Assurance, Tax, Advisory, Technology and Consulting firms**

6 compelling reasons to consider Grant Thornton

01 A truly global organisation

02 Proven global credentials

03 A single global audit approach

04 A different way of doing business

05 Deep expertise in non-audit services

06 Strong local expertise

Acknowledgements

For further queries, write to:

Saket Mehra
Partner and Auto Sector Leader
E: saket.mehra@in.gt.com

Akshay Garkel
Partner and Cyber Leader
E: akshay.garkel@in.gt.com

Sindhu Vethody
Director
E: sindhu.vethody@in.gt.com

Astha Malik
Manager
E: astha.malik@in.gt.com

For media queries, contact media@in.gt.com

Contact us

To know more, please visit www.grantthornton.in or contact any of our offices as mentioned below:

NEW DELHI
National Office,
Outer Circle, L 41,
Connaught Circus,
New Delhi - 110001
T +91 11 4278 7070

NEW DELHI
6th Floor, Worldmark 2,
Aerocity,
New Delhi - 110037
T +91 11 4952 7400

AHMEDABAD
Unit No - 603 B, 6th Floor,
Brigade International
Financial Center,
GIFT City Gandhinagar,
Ahmedabad - 382355
T +91 79 6900 2600

BENGALURU
5th Floor, 65/2, Block A,
Bagmane Tridib, Bagmane
Tech Park, CV Raman Nagar,
Bengaluru - 560093
T+91 80 4243 0700

CHANDIGARH
B-406A, 4th Floor,
L&T Elante Office Building,
Industrial Area Phase I,
Chandigarh - 160002
T +91 172 4338 000

CHENNAI
9th floor, A wing, Prestige
Polygon, 471 Anna Salai,
Mylapore Division, Teynampet,
Chennai - 600035
T +91 44 4294 0000

DEHRADUN
Suite No 2211, 2nd Floor,
Building 2000, Michigan Avenue,
Doon Express Business Park,
Subhash Nagar,
Dehradun - 248002
T +91 135 2646 500

GURGAON
21st Floor, DLF Square,
Jacaranda Marg,
DLF Phase II,
Gurgaon - 122002
T +91 124 462 8000

HYDERABAD
Unit No - 1, 10th Floor,
My Home Twitza, APIIC,
Hyderabad Knowledge City,
Hyderabad - 500081
T +91 40 6630 8200

KOCHI
6th Floor, Modayil Centre Point,
Warriam Road Junction,
MG Road
Kochi - 682016
T +91 484 406 4541

KOLKATA
10C Hungerford Street,
5th Floor,
Kolkata - 700017
T +91 33 4050 8000

MUMBAI
11th Floor, Tower II,
One International Center,
SB Marg Prabhadevi (W),
Mumbai - 400013
T +91 22 6626 2600

MUMBAI
Kaledonia, 1st Floor, C Wing,
(Opposite J&J Office),
Sahar Road, Andheri East,
Mumbai - 400069

NOIDA
Plot No 19A, 2nd Floor,
Sector - 16A,
Noida - 201301
T +91 120 485 5900

PUNE
3rd Floor, Unit No 310-312,
West Wing, Nyati Unitree,
Nagar Road, Yerwada
Pune - 411006
T +91 20 6744 8800

For more information or for any queries, write to us at GTBharat@in.gt.com

Follow us @GrantThorntonIN

©2022 Grant Thornton Bharat LLP. All rights reserved.

"Grant Thornton Bharat" means Grant Thornton Advisory Private Limited, the sole member firm of Grant Thornton International Limited (UK) in India, and those legal entities which are its related parties as defined by the Companies Act, 2013, including Grant Thornton Bharat LLP.

Grant Thornton Bharat LLP, formerly Grant Thornton India LLP, is registered with limited liability with identity number AAA-7677 and has its registered office at L-41 Connaught Circus, New Delhi, 110001.

References to Grant Thornton are to Grant Thornton International Ltd. (Grant Thornton International) or its member firms. Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered independently by the member firms.