

# Deloitte.

Fasten your digital seatbelt

Securing today's automotive industry in Asia Pacific

**MAKING AN  
IMPACT THAT  
MATTERS**  
*since 1845*





# Introduction

The automotive industry is racing at full speed into the digital age. Cybersecurity is not always keeping pace, however. Motor vehicles and their factories, increasingly connected, are becoming more vulnerable to intruders.

A single breach could endanger people. It could delay or halt production, cost vast amounts of money, or harm the business overall.

Now may be the ideal time, while they are digitising, for automakers to introduce and refine security measures. We recommend focusing on three automotive domains: IT, vehicle, and manufacturing.

Each domain faces security challenges. But security also holds promise. It can help power the automotive industry into the digital age. The best route for digitising companies is one that secures these three domains all together.

Communication and collaboration are key to success. Functions and offices must work together. Global headquarters (GHQs) must share knowledge and resources with non-GHQs.

In this way, automotive companies can digitise as consumers now demand. And they can speed toward their goals with confidence that their data, people, and businesses are as safe and secure as can be.



# Every automotive domain has high inherent cyber risk, yet most are unprepared

In 2022, Deloitte conducted a research study with key automotive companies in the Asia Pacific region to examine the cybersecurity issues faced by the industry. One of the key findings was that while security management systems for digital processes which have long been in place were reasonably mature, security is most likely lagging behind where digitisation is more recent or ongoing.



Information technology (IT)



Vehicles



Factories

- **Information technology (IT)** systems, such as network devices and servers, tend to be better protected. IT professionals have been detecting and deflecting security incidents for years. Due to various types of security measures, well-established security products and services, and successful use cases in the IT domain, it is easier to address risks here as compared with other domains.

In addition, most IT teams in the automotive industry (more than 60%) report using threat intelligence sources to gather information on threats and vulnerabilities. There is a strong tendency to use such data as input for security measures at an early stage.

More than

**60%**

of IT teams in the automotive industry report using threat intelligence sources to gather information on threats and vulnerabilities.

- **Vehicles** are only recently becoming digital and connected devices, so security tends to fall behind. Regulators have become concerned about this lag.


Industry standards and regulations for the automotive sector continue to emerge. So far, these include the International Organization for Standardization's (ISO) [ISO/SAE 21434](#) and the United Nations' regulations [R155](#) and [R156](#).

UN R155, for instance, which is soon to take effect in a number of countries, requires auto manufacturers to have and operate vehicle cybersecurity management systems that protect against specific threats.<sup>1</sup> Based on findings in our research study, many automotive companies are still brushing up on their skills and knowledge of vehicle security.

Fortunately, developers are beginning to realise that security is important to their goals as well as to the business as a whole. To build secure products, however, they must start during the initial design phase. Frequent testing during and after launch is also critical to success.

But the need for speed may tempt developers to make light of security. DevSecOps, the practice of integrating security testing at every stage of software development, is designed to balance both, but many companies do not employ it.

#### Standards and regulations

**ISO/SAE  
21434** 

**R155** 

**R156** 

- **Factories** face the most difficult uphill climb. As they automate, they are adding robots, sensors, artificial intelligence (AI) and other technologies—and they are struggling to secure it all.

Embedded software, such as that used in Advanced Driver Assistance Systems, adds to the challenge. It may be difficult to find secure embedded software for this use.

Security management tools can be very effective but often automotive manufacturers cannot yet use them as their factories still have so many legacy systems. These security management tools include cloud access security brokers (CASB), identity and access management, and endpoint security.

Now, in the early stages of digitisation, is an optimal time to start using these and other security technologies. Meanwhile, factory heads may want to begin teaching workers about the importance of security.

1. <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-advisory-securing-the-vehicles-of-the-future-aoda.pdf>



# Threat intelligence is vital for staying in front of cybercrime

Modern technologies can give us much information about what cybercriminals are doing, how and when they are doing it, and even their likely motivations. Threat intelligence can also help us to accurately predict future threats and trends, better equipping us to stay a step ahead of malice.

For all its promise, however, threat intel may be the most underutilised tool in the automotive industry tool kit. While most GHQs use it to help secure their plant operations and systems technologies, only a few use threat intel to help them keep their vehicles secure.

Their cyber programs are often not properly organised with clearly established processes and a chain of command—crucial for putting to good use the information that threat intel provides.<sup>2</sup> For instance, threat intel data can help automotive security engineers design protection against known threats into their software.<sup>3</sup>

Threat intel data makes for better cyber decisions, but only if everyone knows who is responsible for making them, and how the process must work. GHQs should instil threat intel technologies and processes and educate their vehicle teams in how to use them effectively. They should also help their non-GHQ affiliates become more threat intel-savvy so that neither they nor their vehicles—nor their customers' safety—get left behind.

- <https://www2.deloitte.com/dk/da/pages/risk/cyber-risk/cyber-strategy-transformation/effective-cyber-risk-governance.html>
- [https://standards.ieee.org/wp-content/uploads/import/documents/other/e2e-presentations/feb-2021/04-Securing\\_Connected\\_Autonomous\\_Vehicles\\_as\\_an\\_Industry.pdf](https://standards.ieee.org/wp-content/uploads/import/documents/other/e2e-presentations/feb-2021/04-Securing_Connected_Autonomous_Vehicles_as_an_Industry.pdf)

# We are all connected, making security more important than ever

Factories are fast moving towards becoming 'cyber-physical systems' that run themselves almost without human intervention. Vehicles acquire new digital features every year, and the car that completely drives itself is closer to reality than ever before.

Machines, robots, sensors, people, software, hardware, firmware: Our era, in which nearly everything and everyone is digitally connected to something or someone else, truly is a digital age. But in the automotive industry, only the IT domain is closest to having adequate security in place to keep these connections unbroken by malicious forces.

Vehicles must have certain security features to comply with UN R155 and R156. These include secure over the air (OTA) programming by which software, firmware, and perhaps encryption keys get updated remotely, for instance. An unsecure vehicle poses risks to lives. Yet our research study found that the vast majority (80%) of original equipment manufacturers (OEMs) do not monitor their vehicles' security.

Factories, too, can be dangerous places for people if their machines, robots, sensors, and other connected devices get breached or tampered with. A cybersecurity incident can also shut down a factory, causing lost time and money. Yet, according to our research study, less than one-third (30%) of automotive factories monitor the ongoing security of their many connected devices.

Cybercriminals know this. They are stepping up their attacks in the vehicle and automotive factory domains. Losses and damages are scaling ever increasingly as a result, which is reason enough for continuous security monitoring to be put in place.

Laws and regulations are continuing to proliferate, too. Some are mandating cybersecurity measures in vehicles and at OEM plants.

Companies must become ever more vigilant against cyber threats to their systems, vehicles and factories, and use automated continuous monitoring to stay apprised of dangers before, and as, they arise.

---

## 80%

of original equipment manufacturers (OEMs) do not monitor their vehicles' security.

---

## 30%

Less than one-third (30%) of automotive factories monitor the ongoing security of their many connected devices.

---

# Computers that move need fast, nimble security

Increasingly, 'what's under the hood' refers less to the mechanics of a motor vehicle than to the software it uses. All vehicles will soon become 'software-first': computers on wheels.

Like all computers, 'software-defined' vehicles—those depending more on software than on hardware—are at risk of attack.<sup>4</sup> But the stakes are higher and the risks greater where today's (and tomorrow's) vehicles are concerned.

A corporate desktop computer or system, if breached, might cause the loss of data or a delay in a product's launch. A breached car, on the other hand, could cost a life, or several.

The likelihood that a modern-day Connected, Autonomous, Shared, Electric (CASE) vehicle will be tampered with is greater than ever before. According to one study, cyberattacks on vehicles rose 225 percent from 2018 to 2021 and nearly 85% of attacks on vehicles in 2021 were carried out remotely.<sup>5</sup> The study also states that losses to the automotive sector because of cyberattacks are expected to reach US\$505 million by 2024.<sup>6</sup>

Yet we are still seeing deficiencies across the board in Secure Software Development Life Cycle (SSDLC) software development processes. With SSDLC, developers should design security and privacy from the earliest planning stages. They should also continually test throughout the development process and for as long as the software is in use.

**Automotive companies can, and should, take steps to mitigate the risks to their technologies, and especially their vehicles and factories which are far behind in terms of secure software development. Our recommendations include:**



Assess the security of your third-party OEM suppliers. These are often software companies. They might provide global positioning systems (GPS), entertainment platforms, electrification, or autonomous driving capabilities, to name a few. How secure are their processes at each phase of the development cycle (planning, design, manufacturing, and testing)?



Assess your own software development processes. Your own developers too should apply SSDLC precepts. Doing so can help set your company apart from the competition. As CASE becomes the norm, vehicle security will come to matter more and more.

4. <https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/consumer-business/deloitte-cn-cb-software-defines-vehicles-en-210225.pdf>

5. <https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/>

6. Ibid.



# We are all in this together – company-wide and society-wide

As the entire enterprise goes digital, so does cybersecurity become a business-wide concern. Every business unit and subsidiary is now connected, and all are vulnerable. A single security flaw—a breach of just one device—could have disastrous effects throughout the enterprise and even around the world.

Working together as a single coordinated whole is the only way to secure our vehicles and our roadways.

Gone are the days when systems, networks, and data security were strictly an IT concern. Gone, too, is the individualised approach, with each subsidiary or function taking care of its own security and leaving the others to do the same. We are all in this together now.

Digitally mature OEMs have begun to recognise the interdependencies and are starting to manage security as a company-wide concern. Yet this 'all for one, and one for all' approach, as critical as it is, remains far from the norm in the automotive industry.

Every automotive company absolutely needs a department dedicated to cybersecurity across the enterprise—one that connects functions and business units among GHQs and subsidiaries.

Non-GHQs, in particular, have been slow to recognise the imperative of 'security for all' and to act on it. GHQs need to lead, showing non-GHQs the way forward and helping them to modernise their cybersecurity.



## The time to act is now

The automotive industry is particularly vulnerable to cybercrime in this moment. Cyber attacks are increasingly targeting various types of automobiles, enterprise systems, and factory facilities. In all three domains—IT, vehicles, and factories—automotive companies must do more to implement appropriate cybersecurity measures. They must make cybersecurity an enterprise-wide imperative now and in the future.

Cybercriminals, aware of the weaknesses, are stepping up their attacks on the industry. The consequences could be dire not only for the automotive sector but for drivers, passengers, and society as a whole.

Fortunately, some GHQs are already realising the importance of cyber maturity and making it a top priority. It is time, now, for all to do so, and for GHQs to pave the way for non-GHQs to follow suit. In this way, auto companies can not only support their own success but continue to foster a safer society for all.

# Authors and contributors

## **Hiroshi Hayashi**

**Asia Pacific Cyber Automotive leader**

hiroshi.hayashi@tohatsu.co.jp

## **Karen Grieve**

**Director**

kagrieve@deloitte.com.au

## **Eric Leo**

**Director**

eleo@deloitte.com.au

# Key contacts

## **Hiroshi Hayashi**

**Asia Pacific Cyber Automotive leader**

hiroshi.hayashi@tohatsu.co.jp

## **Ian Blatchford**

**Asia Pacific Cyber leader**

iblatchford@deloitte.com.au

## **China**

### **Boris Zhang**

**Partner**

zhzhang@deloitte.com.cn

## **South Asia**

### **Praveen Sasidharan**

**Partner**

psasidharan@deloitte.com

## **Japan**

### **Hiroshi Hayashi**

**Partner**

hiroshi.hayashi@tohatsu.co.jp

## **Southeast Asia**

### **Weng Yew Siah**

**Partner**

wysiah@deloitte.com





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2023. For information, contact Deloitte Asia Pacific Limited.  
Designed by CoRe Creative Services. RITM1403730



This is printed on environmentally friendly paper