TRUSTONIC

2023 in review

and our automotive industry predictions for 2024

Towards the end of 2022, we at Trustonic compiled a list of our key automotive predictions for the year ahead. With 2023 drawing to a close, now is the perfect time to look back on the year, and assess how accurate our forecast has proven to be.

Furthermore, with 2024 on the horizon, we are taking this opportunity to put forward our predictions for the industry developments we expect to see in the automotive industry over the next 12 months.

Right on target

In an industry as fluid and prone to change as automotive, the odds of accurately predicting the future are certainly stacked against you. As such, some of our 2023 predictions haven't panned out as we expected them to, while some have at least been partially correct, if not exactly how we envisaged. Other predictions we made, however, have proven to be correct.

For example, we rightly predicted that the reality of WP.29 – regulations providing automakers with clearly defined performance and audit requirements in key areas like cybersecurity – would set in with one year to ensure compliance. With the July 2024 deadline looming when all new vehicles must abide by the guidelines, OEMs have been busy taking action to prepare, with many already having Vehicle Security Operation Centres (VSOC) in place. There has also been a marked increase in the breadth of cyber security requirements in RFQ/Is as well as a requirement for their supply chain to provide detailed Threat Assessment Risk Assessment (TARA) inputs and to be ISO 21434 compliant.

After all, ensuring they are compliant is entirely in the best interests of manufacturers, given that failure to do so would result in severe penalties being levied against them. OEMs have certainly shown all the right signs of preparing for WP.29, but to what extent they're truly ready remains to be seen. It will be interesting to watch how the United Nations body responsible for introducing and enforcing the regulations responds to OEMs' efforts to ensure compliance once the official deadline has passed.

Another prediction that proved to be accurate was that the importance of the connected used car market would begin to be realised. Although the new car market performed better than we and many others in the industry had forecast – with sales up by 20.2% on the previous year – used cars also grew considerably. Used connected cars – specifically battery electric vehicles [BEVs] – experienced the biggest growth in this segment by far, with sales soaring by 99.9%, according to figures published by the Society of Motor Manufacturers and Traders [SMMT].

In fact, the price of used cars in many markets experienced an uplift during 2023. As more and more connected vehicles join the world's used car stock, sales of such vehicles will continue to grow, and vendors will increasingly realise the benefits of selling them on second hand to customers.

We also anticipated that Hollywood would continue to ramp up the fear factor surrounding the hacking of connected vehicles throughout 2023. With the release of big blockbuster movies like *Fast X* and *Mission: Impossible – Dead Reckoning Part One* – both of which prominently featured hacking – this has certainly turned out to be true. However, it should be reiterated that much of what we've seen play out on the big screen with regards to hacking should be taken with a hefty pinch of salt. Unfortunately, however, as moviemakers continue to use hacking as a device to tell their stories, consumer perception of vehicle cybersecurity will continue to erode, much to the chagrin of OEMs.

Additionally, we predicted that, over the course of 2023, we would increasingly see automakers coming together to tackle the security challenges that they collectively face. Although OEMs are, of course, in competition with one another, its undeniable that cyberattacks pose a very real threat to the continued prosperity of all manufacturers. As such, it's in the best interest of OEMs to share whatever knowledge they can to better protect the industry from such risks. Many automakers have recognised this, which helped lead to the formation of the Automotive Information Sharing Analysis Center [Auto-ISAC] in 2015.

Established by manufacturers to form a global information sharing community, this helps to cast a spotlight on the need to address vehicle cybersecurity risks, and has brought more and more OEMs to this cause. Auto-ISAC also contributed to the formation of GlobalPlatform's Automotive Task Force initiative this year, which has brought together key automakers to facilitate cross-industry collaboration on security standardisation. By opening up such forums for debate and co-operative work, OEMs will better prepare themselves for the cybersecurity challenges that inevitably lie ahead of them.

AUTO-ISAC
Automotive Information Sharing and Analysis Center

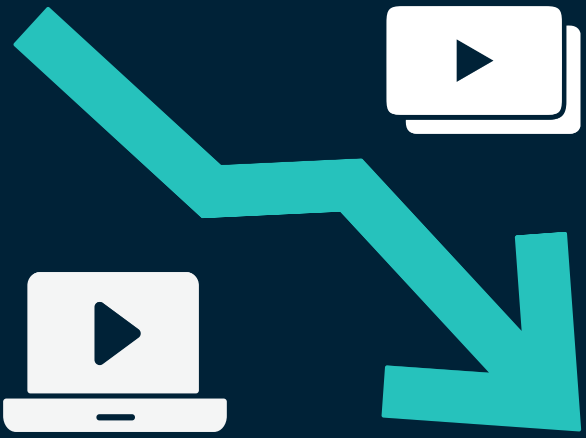
Hitting the crossbar

Some of the predictions that we made for 2023 largely came true, but with some important caveats. For example, we expected automotive bug bounty programs to properly take off at long last. These initiatives see OEMs publicly inviting ethical hackers to access vehicle systems to detect vulnerabilities that they can then report in exchange for a reward. Despite these programs having been poorly promoted in the past, some manufacturers have made a more concerted effort to incentivise hackers to get involved this year. This included Porsche, which launched a brand-new bug bounty programme in October 2023 to further improve the security of its products and digital services. While certain OEMs have succeeded in promoting their bug bounty schemes, many others continue not to place much focus on them. As such, while it’s fair to say that some bug bounty activity has taken place, it wouldn’t be accurate to say that action has been widespread.

We also thought that we would see a growth in direct-to-consumer [DTC] leasing packages this year. Whereas the traditional leasing model is marred by unnecessary obstacles for motorists, the DTC approach focuses on benefitting the consumer, rather than the dealer themselves. This is because the vehicle is sold directly to the buyer rather than through a third party, meaning they can get access to the financing and vehicle options that they need with as little hassle as possible. While some OEMs, such as Volvo and Audi, have rolled out their own DTC programs this year, this approach hasn’t been pushed as aggressively as we’d anticipated across the board. It’s likely that the ongoing cost-of-living crisis – which has helped bring about the aforementioned boom in the second-hand market – coupled with the conflict in Ukraine, have contributed to the lack of activity around alternative leasing in 2023. For the sake of consumers, we’re hopeful that more leasing options will be rolled out in 2024.

Wide of the mark

Other predictions we made were probably curtailed by the cost-of-living crisis, including that 2023 would become the year of Level 3. The third of six levels of driving automation defined by the Society of Automotive Engineers [SAE], Level 3 stands as an important step towards the future of driverless cars. It pairs assorted driver-assistance systems with Artificial Intelligence [AI] to handle complex situations on the road, such as automatically navigating around traffic, detecting weather conditions, and merging when lanes of traffic end. While some automakers have taken strides towards implementing Level 3 capabilities to their vehicles in previous years, we thought many more OEMs would incorporate Level 3 during 2023 than they actually did. The year started well, with Mercedes-Benz announcing support of Level 3 technology in its new S-Class model. We also saw Tesla, GM and Ford all offering hands-free Freeway driving in the US, but none of these systems have yet been certified as Level 3. This slower than expected progress is likely due to economic factors like the cost-of-living crisis, which presented a timing challenge to manufacturers given the extra costs associated with Level 3 technology. Hence it is our view that many decided to pull back on promotion efforts as a result.



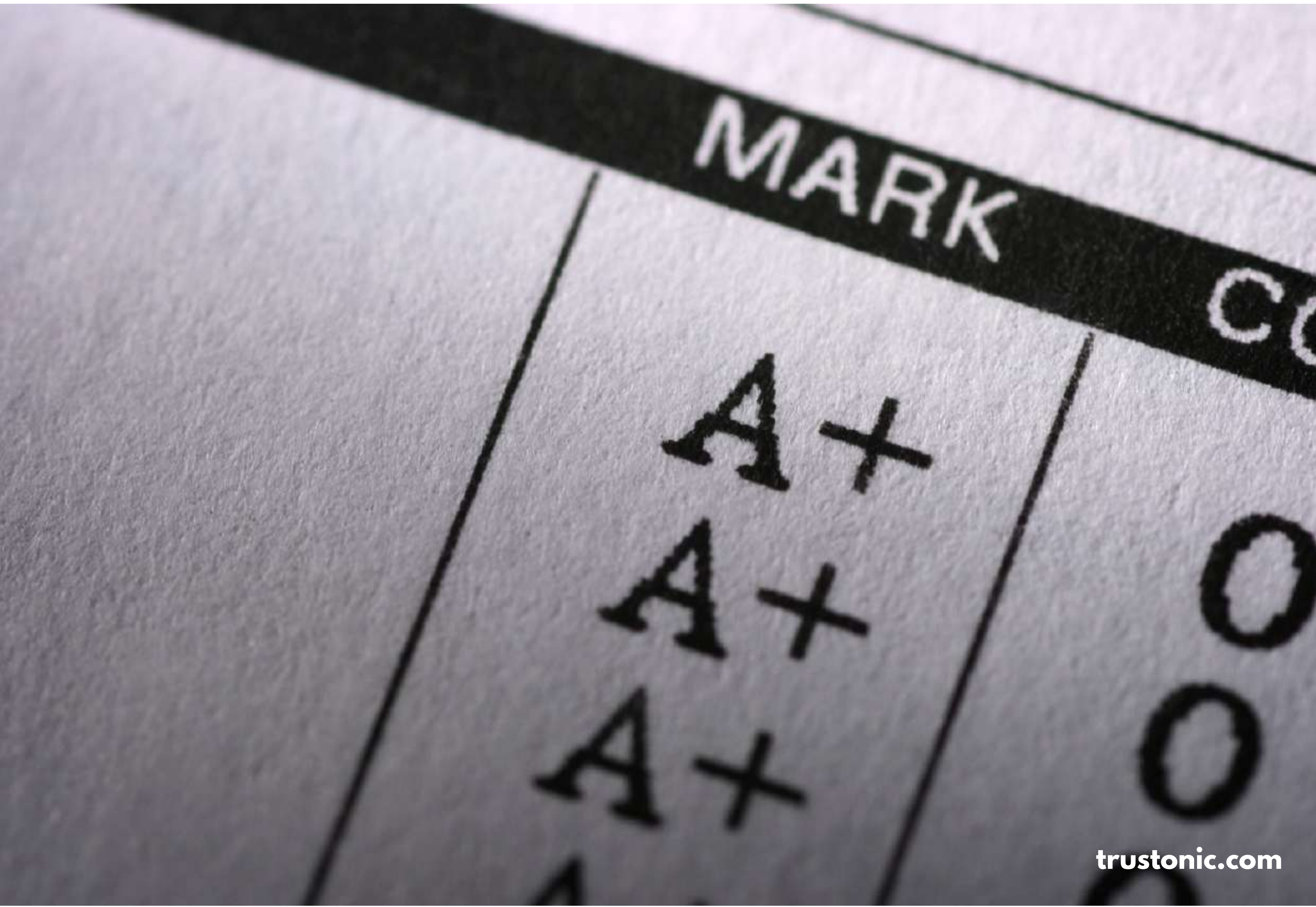
We also believed that at least one of the major streaming platforms would start to promote in-vehicle services as a means of offsetting their declining subscriber numbers. Again, however, the cost-of-living crisis is likely to have dissuaded consumers from adding new paid-for streaming services, and even prompted some to cancel those that they already subscribed to.

This is reflected in declining subscriber numbers for platforms like Netflix and Amazon Prime Video, both of which experienced a drop in household subscriptions during the second quarter of 2023. However, Netflix has likely succeeded in mitigating the losses its incurred as a result of the cost-of-living crisis by cracking down on password sharing, which has prompted new subscribers to sign up. With the crisis expected to persist throughout 2024, however, it's unlikely that we will see any of the streaming giants aggressively pushing in-vehicle services over the next 12 months either.

Marking the report card

Overall, we feel that we did well with our 2023 predictions, especially given how fluid the industry is at the best of times, let alone amid a cost-of-living crisis. Some of what we predicted has played out over the course of the past 12 months, and this is testament to how closely we, as a leading cybersecurity provider, follow the latest trends in the automotive industry. With regards to other predictions, we were wide of the mark, but this in some cases was due to unforeseen circumstances that many others besides us would have failed to forecast. However, in almost all cases, there was at least an element of truth to the predictions we made, even if everything that we expected to happen didn't actually come to pass. All in all, we're happy with the success of our 2023 predictions.

On that note, our top predictions for the year ahead are below. As with our 2023 predictions, we're not afraid to take risks by making statements that later turns out be inaccurate if it means those that we do get right are more impactful. Because we stand side by side with our OEM partners, it is our hope that this new set of predictions will help them to prepare for what may happen throughout 2024 and beyond.

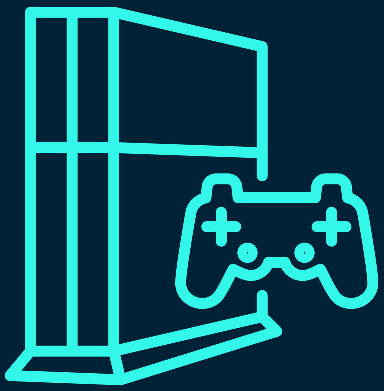


1. The industry starts to explore gaming as the potential next big digital service

For many years now, the video games industry has been a multi-billion-dollar business, having generated an estimated 347 billion dollars in revenue in 2022. Of this number, approximately 248 billion dollars came from the mobile games market, amplifying the huge appetite there is for ‘gaming on the go’ among players. With so much of our lives spent travelling – often long distances – games can serve as a welcome distraction from the journey, and an enjoyable way to while away the hours. Yes, radios and built-in DVD players have long served this function in vehicles, but there’s arguably no substitute for the level of immersion that gaming can offer, and this is something that automakers are increasingly recognising.

Portable systems like the Nintendo Switch, PlayStation Portable [PSP] and Game Boy have all served gamers on the go for years, but automakers are now exploring new ways how cars can become games consoles themselves. BMW, for example, announced a partnership in 2022 with AirConsole to provide ‘casual gaming’ in new vehicles from 2023. Using their smartphones as controllers, this enables passengers to play a varied selection of titles together via the BMW’s Curved Display. This means people no longer have to bring their handheld systems with them on long journeys because all their gaming needs have effectively been built into the vehicle’s design.

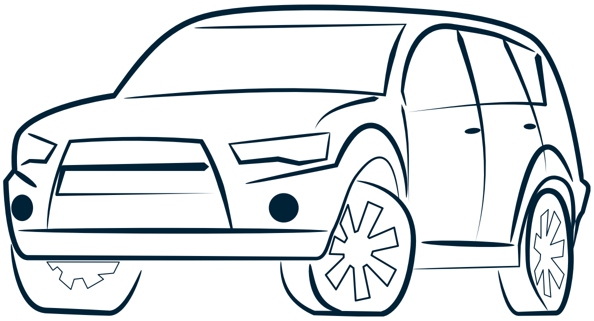
Automakers have only scratched the surface of what’s possible when it comes to in-vehicle gaming so far, but we expect to see many more exploring how they can move into this space throughout 2024. While gaming won’t explode onto the market this year, or even next year, it’s likely that it will start to appear more prominently in requests for quotation [RfQs] for vehicles launching in three to four years’ time from now. Over the next 12 months, we expect that OEMs will consider their viable options for incorporating gaming into vehicle design in the years ahead and, importantly, what the real use cases are that will entice vehicle users to pay for such services.



This could see many deciding to embed an existing console – such as the PlayStation 5 or Xbox Series X – into a car, much like they would with a high-quality audio system. As a result, passengers will have a huge range of games at their fingertips; a benefit for automakers, considering no developer is likely to make a game specifically for one manufacturer’s vehicles.

However, this approach would constitute a massive increase in power consumption, which is why some OEMs might decide that focusing on integration of a specific game engine to existing IVI platforms or cloud gaming are more logical options for them to take. In the case of cloud-based gaming, not only would hosting games via remote servers and streams reduce the level of power required to play, but it would also allow manufacturers to link up with popular cloud gaming services like Amazon Luna with their cross-platform support capabilities. Additionally, by baking in cloud gaming, automakers would be able to incorporate 5G networks into their vehicles, helping to further encourage data sharing among consumers. This could support OEMs' efforts to collect customer data for use in improving key areas of their services.

Whichever way OEMs choose to implement gaming, it's inevitable that the number of potential cybersecurity vulnerabilities present in vehicles will grow as a result. As such, it is vital that automakers have robust security measures in place to ensure that they provide the most seamless and secure gaming experiences for players.



2. Automotive begins thinking about the role of 'offensive' AI tech, and how security responds to the emerging threat

Until recently, AI was merely the stuff of science fiction to many people; a nebulous vision of some far-off future where flying cars soared through the skies and people used teleportation machines to go about their daily business. Now, what once seemed like fiction has become a fact of everyday life. In 2023, we use AI as smart assistants in our homes, as the providers of answers to complex questions, and even in our cars.

Although the use of AI isn't necessarily a new phenomenon in vehicles – its roots can be traced back to early applications like anti-lock braking systems [ABS] and electronic stability control [ESC] – its prominence has certainly grown exponentially in recent years. AI-enabled personal digital assistance has become a vital part of user experience [UX], with automakers harnessing the technology to allow drivers to more seamlessly carry out a number of functions. Everything from making calls, adjusting the temperature, and changing radio stations has become easier than ever, with users simply needing to instruct their on-board AI to perform these tasks for them. While this has made for a much more convenient driving experience – and given automakers access to vital consumer data – the unfortunate reality is that it has also brought new vulnerabilities to vehicles, which attackers have wasted no time in exploiting.

According to a report published in 2021, remote attacks against vehicles have consistently outnumbered physical attacks since 2010, accounting for 79% of all attacks between that point and 2020. As the integration of AI has accelerated in recent years, the number of remote attacks has grown further, with 77.8% of all attacks in 2020 alone having been carried out in this way.

What's more, AI doesn't only present a vulnerability to vehicle security, but also serves as a potential weapon in an attacker's arsenal. This is because the technology can be used to scope out vulnerable applications, devices, and networks with considerable ease, and even identify opportunities to access sensitive data on a vehicle-by-vehicle basis.

It’s clear that, while the rise of AI brings a raft of benefits to user experiences, it isn’t without its significant setbacks as well. Not only does AI create new vulnerabilities, but it can also be used as a way of attacking vehicles.

However, automakers do not have to merely accept that they are at the mercy of attackers as they continue to roll out AI across their cars. In fact, the technology can simultaneously function as a means of taking the fight back to cybercriminals, and this is an area of research that we are likely to see develop over 2024. OEMs will begin to think more about how AI can itself form a vital part of a vehicle’s security infrastructure, marking a move from ingress detection to ‘behaviour detection’. In this way, AI can help security become more predictive and preventative than reactive, identifying potential threats as soon as possible and taking swift action to eliminate them.

3. As the focus remains on Chinese OEMs expanding globally, the nation's tier one and silicon vendors seek to gain a foothold in the West

Historically speaking, China probably isn't one of the first countries that springs to people's minds when they think about vehicle production. Looking back to the mid-1980s, China was only making a few thousand cars per year. Since then, the Chinese automotive industry has practically exploded, boosted by important partnerships with major foreign manufacturers like Volkswagen, GM, and Honda. Now, the country is set to become the world's second largest exporter of passenger vehicles, surpassing even the likes of South Korea and the United States. In fact, forecasters are expecting Chinese OEMs to capture as much as 33% of global new vehicle sales by 2030, exemplifying just how far the nation's car market has come over the last 40 years.

Despite Chinese automotive having expanded overseas, this expansion has been primarily focused on developing markets, with the developed West proving a tougher nut to crack. According to a survey conducted by market research firm Jato Dynamics, this has largely been due to a negative perception of Chinese vehicles among Western consumers, with 62% of those surveyed favouring cars produced in the West. While this perception of inferiority may persist among a large percentage of consumers, the reality is that many Chinese vehicles are actually of a higher quality than their Western counterparts. Manufacturers in China have worked hard to improve the safety and quality of their products, to the point where many of the country's OEMs now regularly achieve five-star Euro NCAP ratings, placing them alongside Europe's finest automakers. In fact, some of the big-name Europeans OEMs have been handed zero-star scores for safety in recent years, having removed vital safety equipment from their vehicles in an effort to cut costs.

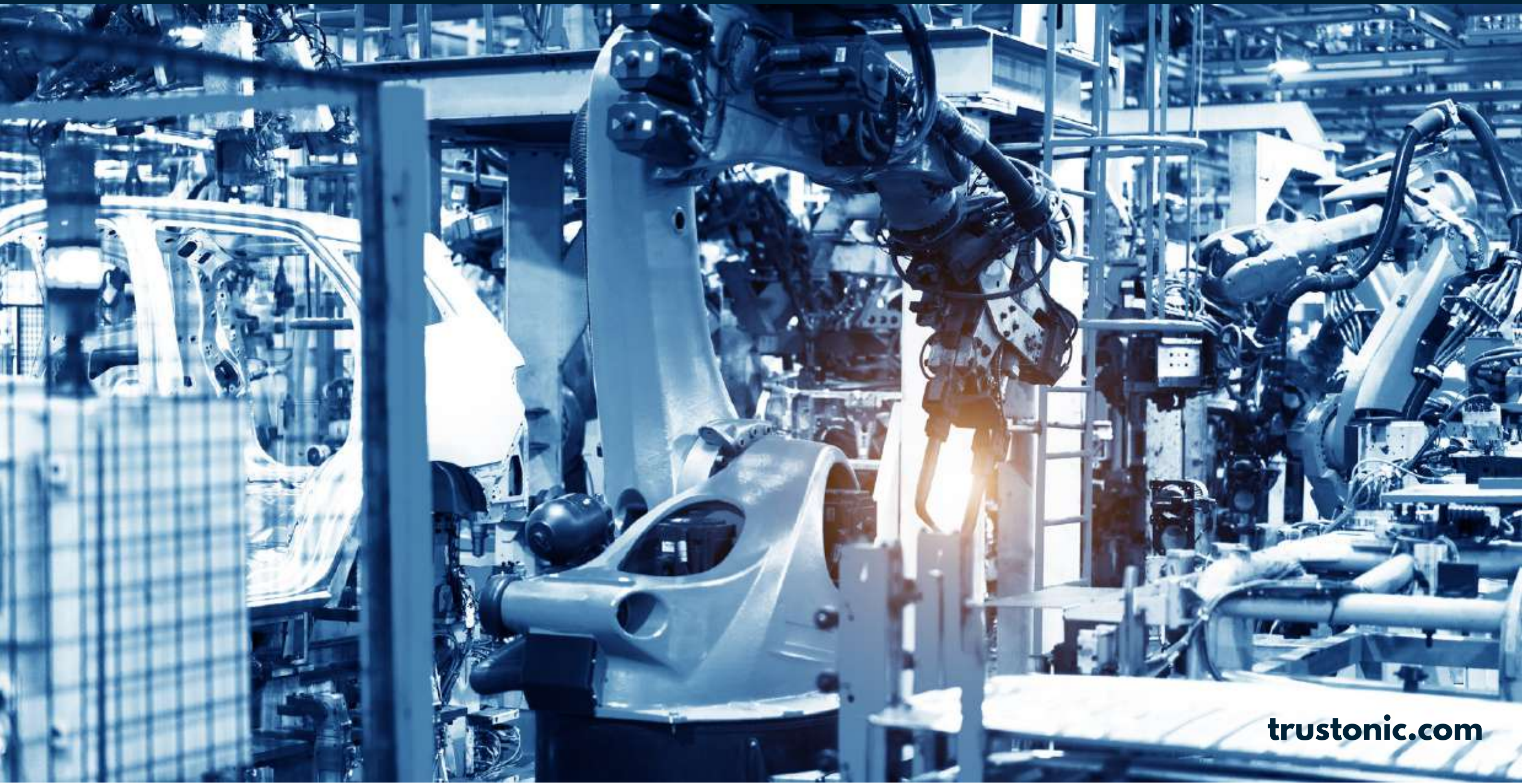
As China continues to focus on improving quality instead of cutting corners, we anticipate that 2024 will be the year that Western markets finally wake up to the fit and finish quality of Chinese vehicles. This will help manufacturers from China to establish a stronger foothold in Western markets, and open up more plants across Europe and North America. In turn, this will encourage the nation's tier one and silicon vendors to expand their operations across the West, emboldened by the newfound perception of Chinese quality around the world. With vendors investing increasingly in electrification tech as this segment of the market continues to grow substantially, breaking through to the West will be key to China's prosperity in the electric vehicle [EV] revolution that lies ahead.

4. Western consumers views towards Chinese OEMs brands starts to change

The fact that China features so prominently in our predictions for 2024 illustrates just how dominant the country has become in the industry over recent years. As already referred to, many Chinese vehicles are now considered to be among the best that the world has to offer in terms of quality and safety. But this high standard of safety is not merely limited to physical safety in the event of a crash; it also extends to vehicle cybersecurity.

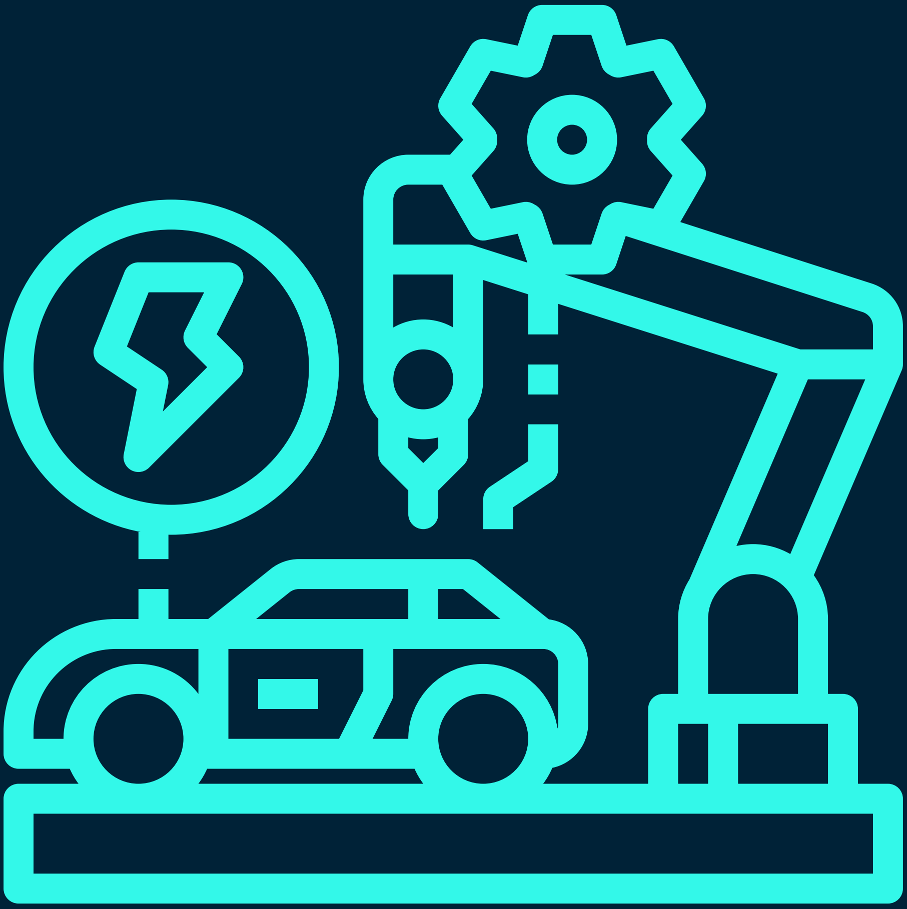
To many people, this may come as a surprise. After all, China is often depicted as a ‘surveillance state’ among many Western countries, and an ever-present threat to personal privacies. With so much of the technology that we buy coming from China, many people are made to live in constant fear that their home appliances are subtly spying on their every move, often with the backing of the Chinese government.

The reality, however, is that many major tech companies and governments around the world are collecting large amounts of consumer data. For people in the West, however, China makes for a convenient bogeyman; an embodiment of the clandestine practices carried out by manufacturers around the world.



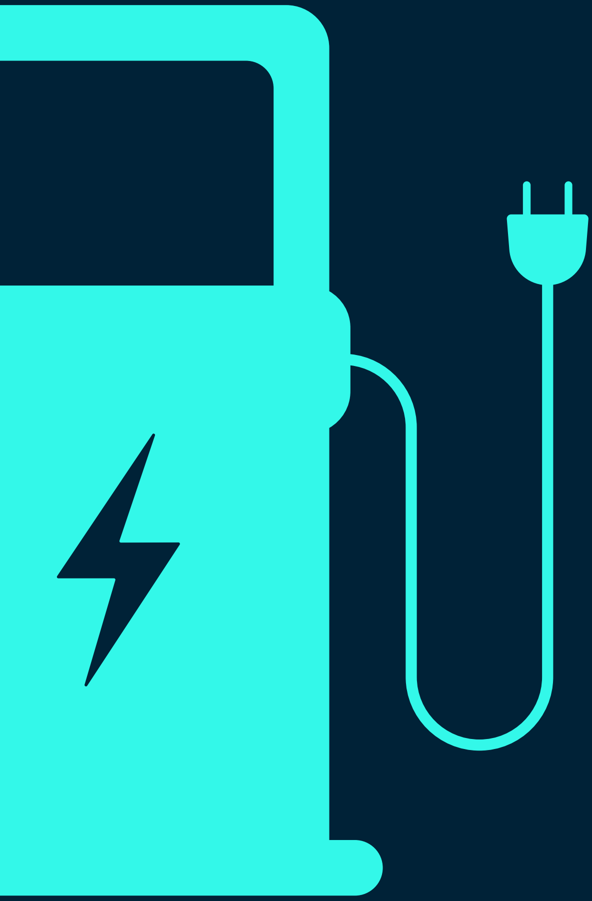
The conversation around surveillance is much more nuanced than that though, and the Chinese state is progressively increasing its investment in cybersecurity. This is largely in an effort to change negative perceptions among Western markets, but also to consolidate China's position as a leading provider of 'gold standard' security solutions. Government investment has enabled OEMs like Nio to flourish overseas, despite the manufacturer effectively positioning itself as a startup. Because Western governments aren't allowed to invest in OEMs in this way, it could be argued that the fight for cybersecurity supremacy isn't a fair one for European and North American manufacturers. Regardless, one thing is for certain: Chinese vehicle cybersecurity will continue to improve, and we believe that, over the next 12 months, China's OEMs will begin to be seen in a more positive light by Western consumers. Indeed, many of the nation's manufacturers appear to be taking cybersecurity more seriously than Western tech vendors, and this is something that customers increasingly appear to be discovering for themselves.

If Chinese OEMs can translate this into positive marketing messages this will help companies like Nio to grow their market share considerably, especially as cybersecurity becomes an ever more important consideration for consumers. No longer will vehicles be seen as a threat to motorists' privacy simply because they were produced in China – after all, any car that passes Type Approval in a Western market should be considered trustworthy, given the level of documentation and evidence that's needed. But if Western OEMs don't want to be left in the dust, they need to be making cybersecurity a key priority now to avoid losing consumers en masse to their Chinese competitors.



5. One of the world's top five OEMs will start a new company to innovate faster

In recent years, relatively new market entrants like Tesla and Nio have taken the automotive industry by storm, particularly in future-thinking areas like electric and autonomous vehicles. With EV sales in the US having recently hit a record high – as customers move away from petrol and diesel cars ahead of the 2035 ban – Tesla still accounts for 50% of the market. Although this share is falling quarter on quarter as new startups continue to enter the space in their droves, it's unmistakable that the industry's more traditional players are lagging behind in electrification. In fact, analysis conducted in 2022 by campaign group InfluenceMap found that just two of the world's largest carmakers are on the trajectory needed to hit the international target of limiting global heating to 1.5ºc. This is because, despite the growing shift towards EVs, plenty of OEMs are still focusing on selling petrol and diesel vehicles, which tend to be more lucrative than their electric counterparts. When it comes to autonomous vehicles, meanwhile, established manufacturers have been quicker off the mark, but still trail behind new entities like Waymo – also known as the Google Self-Driving Car Project. In fact, according to a report by investment bank UBS, Waymo is on track to capture 60% of the driverless market by 2030. It's clear, therefore, that despite the efforts of industry stalwarts to innovate at pace, growing competitiveness in areas like electrification and autonomous vehicles are making it tougher for them to cut through the noise, and reaffirm their dominance.



This is why we're predicting that at least one of the world's top five OEMs will start an entirely new company this year focused on EVs or autonomous vehicles. With new entrants to the market maintaining such a solid lead in these areas, the industry's old heads will need to take a bold and well-publicised move to shake the market up, giving those who would seek to take them on pause for thought. Electrification and autonomous vehicles are unquestionably the new frontiers upon which the automotive industry will do battle, so the faster that manufacturers can innovate in these areas now, the more prosperous they will be in the long run. Setting up a new company would allow the big OEMs to achieve this objective, and prevent themselves from being consigned to the scrapheap of history.

6. The focus of ransomware attacks expands to vehicles

Ransomware attacks have long plagued the automotive industry. Indeed, in a 2021 survey of 35 industries, automotive ranked eighth for reported ransomware attacks, and as the highest targeted manufacturing sub-sector, accounting for roughly a third of total attacks in all manufacturing disciplines. Typically carried out by criminal organisations, this type of malware-based attack involves the encryption of important files and data, with perpetrators then demanding a ransom from their victims – i.e., OEMs, suppliers, third parties, etc. – in exchange for the decryption key. Besides the obvious financial impact that such attacks can have on OEMs, they can also inflict severe reputational damage as well. After all, if customers can't trust that manufacturers can keep their sensitive data safe from criminals, they're likely to switch their allegiances to a competitor who they believe will do a better job.

The risk of ransomware attacks has been compounded by the fact that many OEMs still treat cybersecurity as a mere afterthought, rather than an intrinsic part of their operations. While many manufacturers have moved to digitalising their facilities, not nearly enough attention is paid to ensuring that systems are kept secure. This is why it's estimated that about half of the top 100 OEMs continue to be heavily impacted by ransomware attacks.

And to worsen the situation for those companies not taking their cybersecurity responsibilities seriously, new vulnerabilities are presenting themselves all the time. As the technology that cybercriminals use grows more sophisticated, new ways of committing attacks are constantly becoming open to them, and this is something that we are beginning to see play out. For example, many fleet management companies have fallen victim to ransomware attacks over the course of 2023, with criminals specifically targeting fleets themselves.

This has been different from the traditional approaches to committing attacks, which have typically focused on targeting organisation's core systems rather than their fleets. But with each vehicle now posing a potentially catastrophic vulnerability to an entire fleet due to the technology present within, carrying out an attack in this way is becoming an increasingly viable option for hackers.

As such, it's highly probable that, this year, we will start to see ransomware attackers expanding their focus from OEMs, suppliers and third parties to consumers and their vehicles. For example, due to the embedded connectivity of modern cars, it's entirely possible that criminals will begin hacking on-board systems, rendering vehicles undrivable for their owners. Extortionists could then demand a ransom from motorists in exchange for the restored use of their car. But with the vehicle's systems clearly compromised, victims would have little recourse in preventing subsequent attacks from taking place against them. This would add further reputational damage to OEMs who've already been targeted by ransomware attackers and should be working hard to build trust with consumers as a result. To prevent this from happening, manufacturers need to give the cyber security of their vehicles the highest level of priority, not only as a means of protecting their own systems, but also to keep customers out on the road safe from the scourge of cybercriminals as well.

7. The insurance industry's rebellion against EVs gathers pace

In September 2023, John Lewis Financial Services stopped providing car insurance to new and existing customers who own electric cars. This, its underwriter Covéa explained, was due to the analysed expenses associated with repairing EVs, especially damaged batteries, which can cost upwards of £10,000 to replace. While the John Lewis announcement received much media attention at the time, it wasn't the first insurer to have made such a move. Earlier in the year, Aviva U-turned on its decision to provide insurance for the Tesla Model Y, declaring that it was 'no longer able to offer a policy at renewal'. While most major insurers continue to provide cover for the Model Y and many other electric cars besides, it's clear that John Lewis and Aviva's decision forms part of a wider, worrying trend away from insuring EVs and towards other, more lucrative markets. As insurance costs and premiums for electric vehicles continue to remain so much higher than those of their fossil-fuel based counterparts, it's highly likely that we'll see more insurers moving away from providing EV products in 2024, or significantly ramping up the excess amounts borne by the vehicle owner. Not only will this come as huge blow to existing electric car owners – many of whom may be forced to bear the cost of repairs themselves – but will also create a barrier to consumers keen to move towards greener options in the run up to the 2035 ban on new diesel and petrol cars.

News that insurers are removing coverage for EVs will likely cause many of these customers to think twice before making the switch to electric, risking the ban being pushed back even further than it already has been – creating further uncertainties around OEMs' future supply chain and manufacturing investments. This makes the need for OEMs to implement more robust cybersecurity measures into their EVs all the greater, given that cyberattacks and hacker-based thefts form a substantial part of the risk assessment surrounding the insurance of electric cars.

As cyberattacks and thefts committed against EVs grow more prevalent and sophisticated, OEMs must give insurers the confidence they need to provide coverage, safe in the knowledge that the manufacturer has taken every precaution to minimise the risk. Doing so would not only be in the best interests of OEMs and insurers alike, but would also be far cheaper that having to constantly second guess when and how the phase out of ICE engines will happen. It would also reassure motorists, who would gain ready access to the products they need to justify purchasing an electric vehicle.

Conclusion

As 2023 draws to a close, it looks increasingly likely that 2024 will be another momentous year for the automotive industry. While China is set to solidify its dominance in the industry ever further over the next 12 months, OEMs will continue to explore emerging areas like electrification, automation, and in-vehicle gaming, offering exciting new experiences to drivers and passengers alike.

Amid the innovations that the industry is making, however, cybersecurity concerns will inevitably persist. Ransomware and other forms of attacks will become increasingly commonplace as the tools available to cybercriminals grow more sophisticated and dangerous in nature. OEMs must work hard to protect both themselves and their consumers if they are to fully embrace the opportunities presented by new segments of the market, and truly secure the industry’s sustainable, autonomous future.