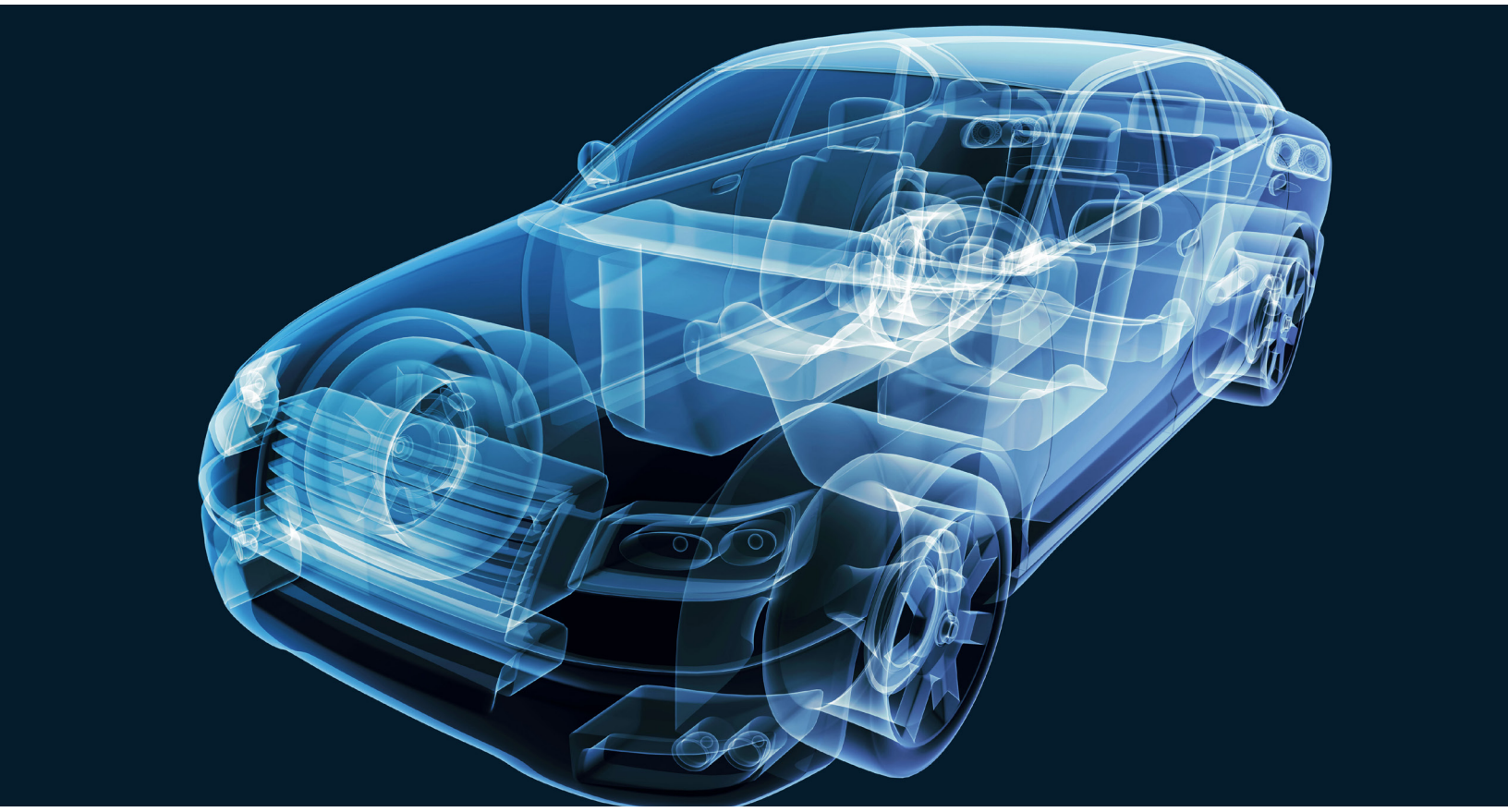
McKinsey & Company

McKinsey Center for Future Mobility

The race for cybersecurity: Protecting the connected car in the era of new regulation

The car industry's digital transformation exposes new cybersecurity threats. Learn what OEMs can do to protect their cars and customers from hackers.

by Johannes Deichmann, Benjamin Klein, Gundbert Scherf, and Rupert Stützle



October 2019

In the past, what happened in your car typically stayed in your car. That is no longer the case. The influx of digital innovations, from infotainment connectivity to over-the-air (OTA) software updates, is turning cars into information clearinghouses. While delivering significant customer value, these changes also expose vehicles to the seamier side of the digital revolution. Hackers and other black-hat intruders are attempting to gain access to critical in-vehicle electronic units and data, potentially compromising critical safety functions and customer privacy.

Cybersecurity becomes a core product and value-chain issue

Cybersecurity has risen in importance as the automotive industry undergoes a transformation driven by new personal-mobility concepts, autonomous driving, vehicle electrification, and car connectivity. In fact, it has become a core consideration, given the digitization of in-car systems, the propagation of software, and the creation of new, fully digital mobility services. These services include arrays of car apps, online offerings, vehicle features that customers can buy and unlock online, and charging stations for e-vehicles that "talk" to on-board electronics.

Today's cars have up to 150 electronic control units; by 2030, many observers expect them to have roughly 300 million lines of software code. By way of comparison, today's cars have about 100 million lines of code. To put that into perspective, a passenger aircraft has an estimated 15 million lines of code, a modern fighter jet about 25 million, and a mass-market PC operating system close to 40 million. This overabundance of complex software code results from both the legacy of designing electronics systems in specific ways for the past 35 years and the growing requirements and increasing complexity of systems in connected and autonomous cars. It generates ample opportunity for cyberattacks—not only in the car but also along the entire value chain (Exhibit 1).

The cybersecurity playing field tilts in favor of attackers

To be sure, the economics of car cybersecurity are inherently unfair: with the right state-of-the-art tools, attacks are relatively affordable, low-effort affairs. Mounting a coherent defense for the complex value chain and its products, on the other hand, requires increasingly higher effort and investment. So far, this reality tilts the playing field in favor of the attackers. Examples abound across the industry. For example, white-hat hackers took control of the infotainment system in an electric-vehicle model. They exploited a vulnerability in the in-car web browser during a hacking contest, causing the electric-vehicle maker to release a software update to mitigate the problem. In another white-hat hack, a Chinese security company found 14 vulnerabilities in the vehicles of a European premium-car maker in 2018. Another global automaker recalled approximately 1.4 million cars in 2015 in one of the first cases involving automotive cybersecurity risks. The impact of the recall was significant, with a potential cost for the OEM of almost $600 million, based on our calculations.

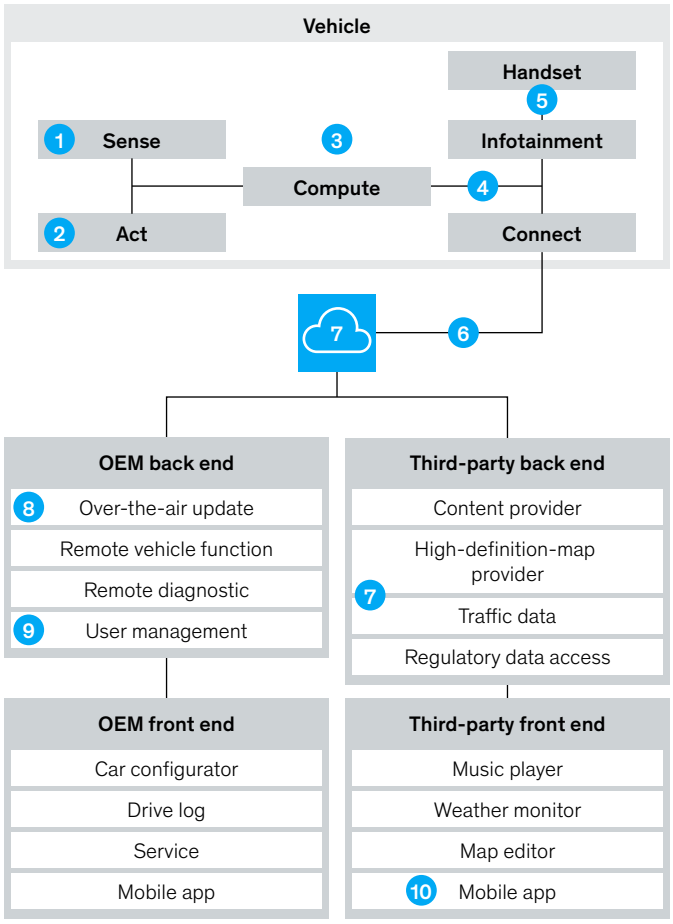
The automotive industry lacks a standard approach for dealing with cybersecurity

For an industry used to breaking down complex challenges and standardizing responses, cybersecurity remains an unstandardized anomaly. Thus far, automotive suppliers have a hard time dealing with the varying requirements of their OEM customers. Consequently, they try to balance the use of common security requirements that go into their core products against those via the software adjustments made for individual OEMs. However, current supplier relationships and contractual arrangements often do not allow OEMs to test the end-to-end cybersecurity of a vehicle platform or technology stack made up of parts sourced from various suppliers. That can make it difficult for both suppliers and OEMs to work together to achieve effective cybersecurity during automotive software development and testing.

Exhibit 1

The advancement of electrical and electronic architecture and digitalization of the car ecosystem increases attack surface and leads to increasing cyberrisk.

Vehicle ecosystem, illustrative



Emerging cyberrisks, not exhaustive

1. **Sensor spoofing:** Access autonomous-drive functions, engine, and brakes through vulnerability in sensors
2. **Take over:** Take over of safety-critical control units such as engine control or brakes
3. **Espionage:** Listen to voices in cars by misusing voice-recognition module
4. **Physical access:** Secure direct access to on-board diagnostics for manipulation of vehicle data, engine characteristics, and tuning chips
5. **Entertainment content:** Access infotainment system via Bluetooth, USB, or Wi-Fi
6. **Telematics:** Remotely unlock cargo doors through vulnerability in external connectivity modules
7. **Denial of service:** Stop cars that rely on back-end servers to provide data
8. **Over the air:** Access vehicle software though online updates
9. **Unauthorized access:** Access back-end vehicle services and user data
10. **Data theft:** Access car owner's private information via unsecure third party

Source: McKinsey analysis

Regulatory change in product cybersecurity is imminent

The difficulty is about to change. Regulators are preparing minimum standards for vehicle software and cybersecurity that will affect the entire value chain. Cybersecurity concerns now reach into every modern car in the form of demands made by regulators and type-approval authorities. For example, in April 2018, California's final regulations on autonomous-vehicle testing and deployment came into effect, requiring autonomous vehicles to meet appropriate industry standards for cybersecurity. While these regulations have an immediate impact on a limited fleet, the World Forum for Harmonization of Vehicle Regulations under the United Nations Economic Commission for Europe (UNECE) is expected in 2020 to finalize its regulation on cybersecurity and software updates. This will make cybersecurity a clear requirement for future vehicle sales; the associated regulations

will affect new vehicle-type approvals in more than 60 countries (Exhibit 2). Industry experts see the upcoming UNECE regulation only as the beginning of a new era of technical compliance regulation in the automotive sector addressing the increase and significance of software and connectivity within the industry.

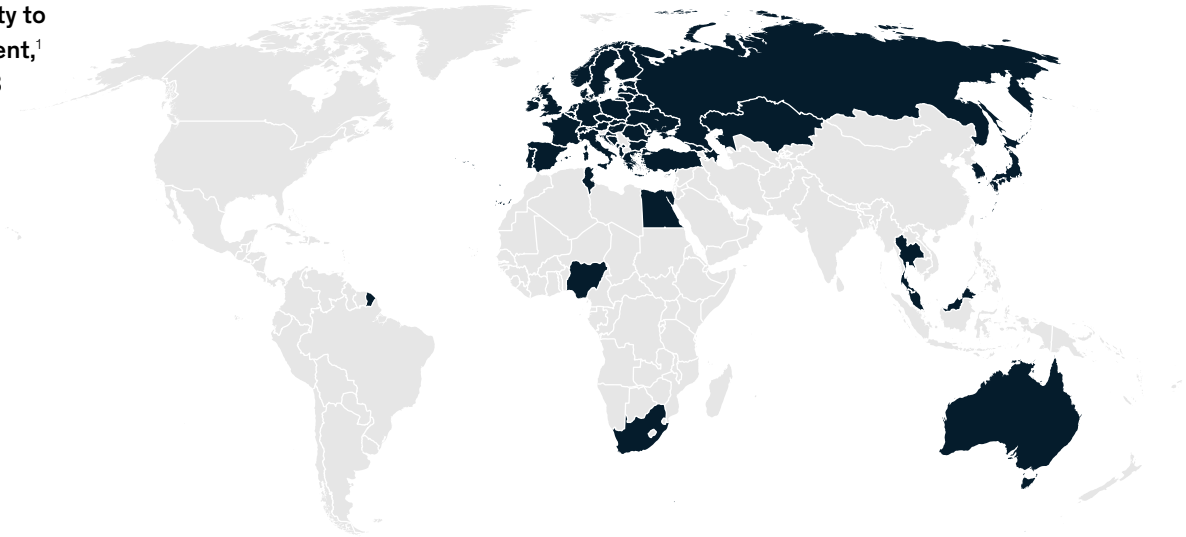
Shifting gears to make cybersecurity a core consideration

While still relatively new, the in-car cybersecurity threat will remain an ongoing concern. As such, automakers must now consider cybersecurity an integral part of their core business functions and development efforts.

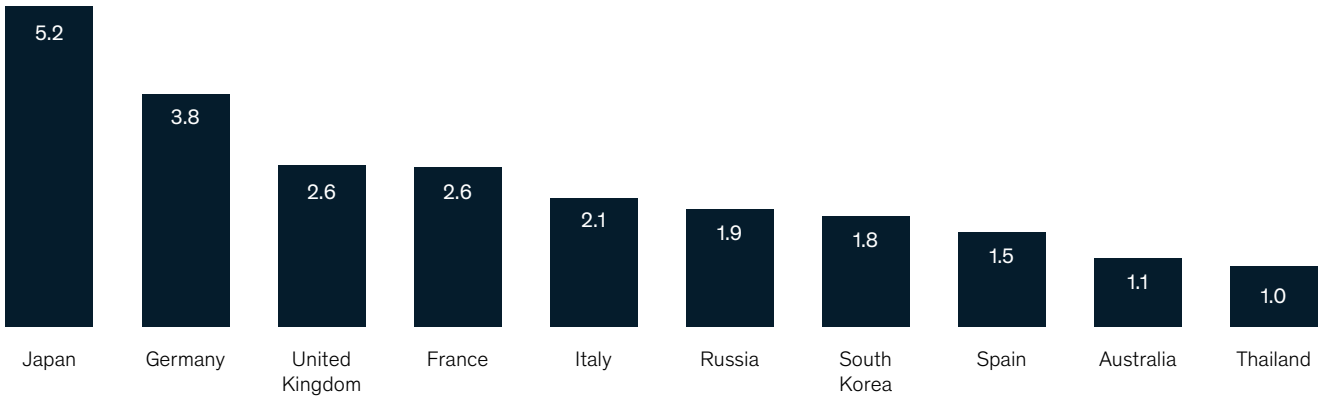
Exhibit 2

More than 24 million cars will be affected under the new World Forum for Harmonization of Vehicle Regulations on cybersecurity and software updates.

Countries party to 1958 Agreement,[1] as of Dec 2018



Top 10 countries party to 1958 Agreement by vehicle sales, 2019 estimate, million



[1] Agreement concerning Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations (original version adopted in Geneva on Mar 20, 1958).

Source: Automotive sales forecasts, IHS Markit, ihsmarkit.com; "ECE/TRANS/WP.29/343/Rev.27," United Nations Economic Commission for Europe, March 11, 2019, unece.org

What is more, the industry can no longer view cybersecurity as purely an IT topic. Instead, automakers need to assign ownership and responsibility for it along core value-chain activities (including among their numerous suppliers) and embrace a security culture among core teams. Likewise, suppliers in the automotive industry need to embrace OEM concerns on cybersecurity, develop capabilities to embed security best practices in their components, and collaborate effectively with OEMs on integration and verification of end-to-end cybersecurity solutions.

This requires the creation of a real, software-centric cybersecurity culture, given the pervasiveness of the cybersecurity threat along the entire value chain. Carmakers themselves have a strong record of establishing a culture of safety—but not yet in cybersecurity. Looking beyond automotive-industry borders, it becomes clear that many digital natives have demonstrated how to build strong security cultures in their engineering departments (not just in IT). At the best digital companies, everyone understands the importance of cybersecure coding practices, and the organizations maintain engineering-outreach and -education programs that train people in cybersecurity, enticing them to look below the surface and raise the cybersecurity bar constantly.

Including cybersecurity in design from the start

Carmakers must securely design vehicle platforms and related digital mobility services from the start. That is because the inherent complexity of vehicle platforms, with their long development cycles and complex supply chains, do not allow for late-stage architectural changes. Furthermore, regulators form strict requirements for OEMs to obtain type approvals for new vehicles (Exhibit 3).

Automotive players must consider cybersecurity over the entire product life cycle and not just up to when the car is sold to a customer, because new technical vulnerabilities can emerge at any time. These issues can have a direct impact on customers and cars already on the road, thus effectively requiring OEMs to provide security-related software patches well into the car's ownership life cycle.

High-tech companies, such as smartphone suppliers, currently deal with this issue by releasing software updates and security fixes for their products after the initial sales (in many cases, new operating-system fixes also support some older-generation products). However, this is typically limited to a period of two to three years, while vehicles have an average service life of a decade or even more. With the advent of OTA software upgrades, automakers could maintain the fleets on the road in a cost-effective way, in contrast with the current practice of costly reprogramming ("reflashing") of car electronic control units at the dealer.

The automotive industry must therefore develop common cybersecurity standards to keep development and maintenance costs under control. On this issue, OEMs and suppliers must speak one language to ensure manageable, end-to-end secure solutions.

Focusing on four core cybersecurity themes

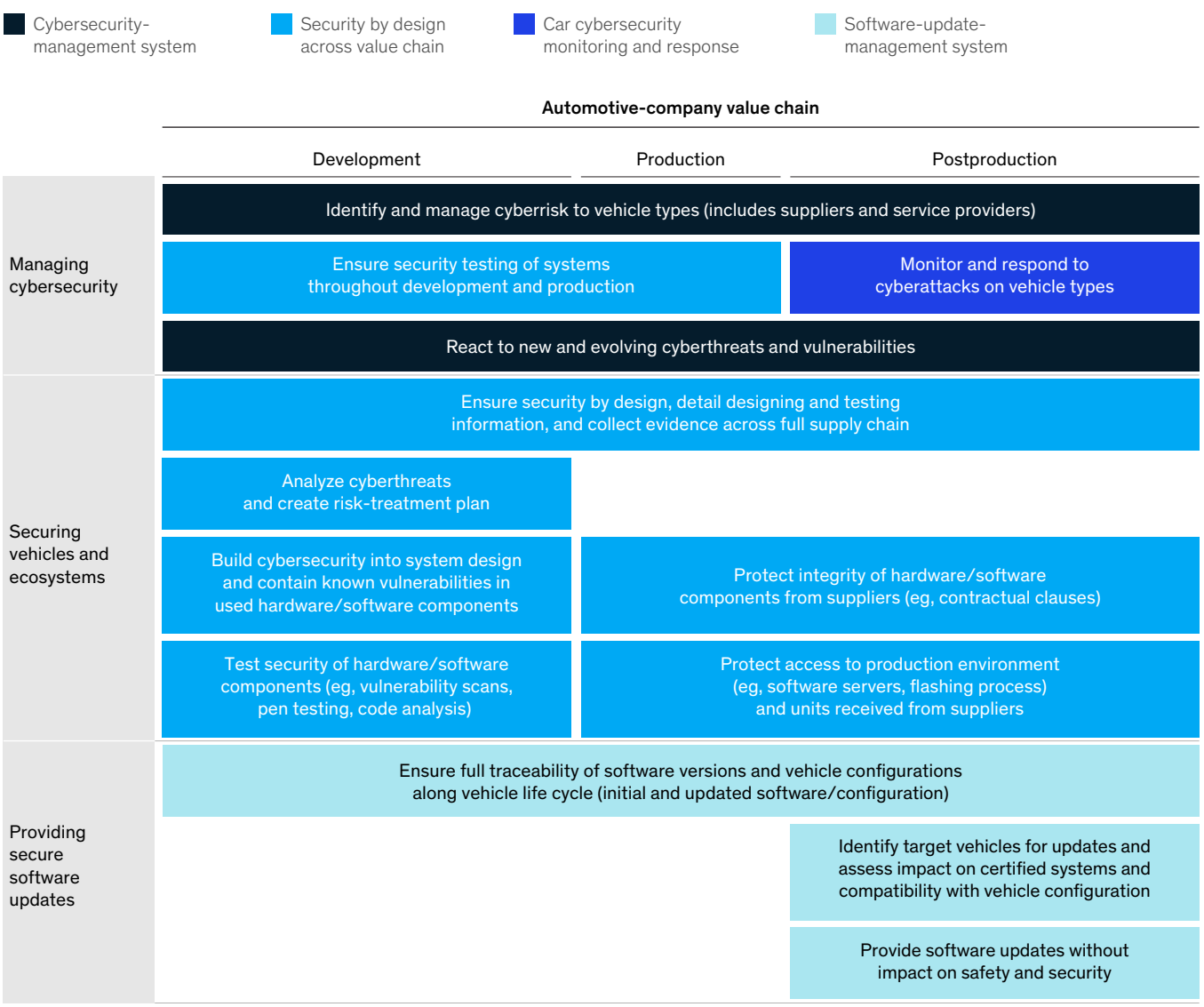
We believe automakers should attack the new cybersecurity and software-update challenges both along the value chain and across the digital life cycle of their cars. To do this, they should focus on four core themes:

1. Establish a clear baseline to execute against. The essence of a good baseline involves understanding requirements from relevant legislation in the OEM markets and leveraging existing international standards around cyber-security and software engineering. Doing so will enable OEMs to deliver cybersecurity practices as demanded by regulatory authorities and international standards and to develop and maintain secure software. A management system for cybersecurity (CSMS) can help ensuring a relentless application of cyber practices across cars and the digital-mobility ecosystem.

Exhibit 3

Upcoming regulations require automotive OEMs to step up cybersecurity activities along the entire value chain.

United Nations Economic Commission for Europe cybersecurity requirements



Source: "Draft recommendation on cybersecurity software updates of the task force on cybersecurity and over-the-air issues," ISO/SAE 21434:2018 Committee, United Nations Economic Commission for Europe, World Forum for Harmonization of Vehicle Regulations; McKinsey analysis

2. Create a true digital-security-by-design culture in engineering, quality assurance, and other core value-chain functions and promote car-software architectures with security built-in. This might require OEMs to overhaul their software engineering and software quality-assurance practices that oftentimes do not follow rigorous software-engineering processes as seen in software-native industries. This security-by-design culture should focus on secure development practices, enhanced software-testing processes, and new supplier-audit processes that include cyber issues. Other helpful elements include state-of-the

art supplier contracts that allow the testing of a component's cybersecurity, and cyber-awareness training for involved technical personnel and customer-facing staff.

3. Ramp up expertise and capabilities to monitor the cybersecurity of cars on the road. The focus should include fixing issues in a timely manner without costly product recalls and media scrutiny. That likely means fully managing the digital life cycle of cars and having full transparency over a vehicle's configuration (for example, using digital twins) and, ultimately, setting up a security-operations center for cars that receives data from the vehicles and the broader digital ecosystem—in line with data-privacy laws (for instance, back-end systems). The security-operations center would use correlation and artificial intelligence to detect adverse events and to launch clear incident-response activities, eventually leading to the provision of software updates to cars.

4. Adapt software-engineering practices that embrace function-based development, solid version control, and integration testing. This approach effectively allows an OEM to assess the potential impact of individual software updates to its vehicles and their relevant safety- and type-approval systems. Establishing such systems—version control for vehicle software, configuration management, and software-update management—thus helps to ensure operational safety when updating software in vehicles. The approach can also help when considering changes to a vehicle's configuration and assessing the impact on a car.

Sensing an opportunity, hackers have begun to focus more energy on compromising connected cars, posing a new challenge for automakers and suppliers alike. While consumers will largely take cybersecurity for granted until the first consequential breach, regulators will increase pressure on automakers and suppliers to ensure greater protection against attacks. The overall security of modern mobility services will depend on how well the industry addresses cyberrisks in and around connected cars, as well as on the strategic actions key players take today to prepare for future attacks.

Johannes Deichmann is an associate partner in McKinsey's Stuttgart office, and **Benjamin Klein** is a specialist in the Berlin office, where **Gundbert Scherf** and **Rupert Stützle** are both partners.

The authors wish to thank Georg Doll, Ralf Garrecht, and Wolf Richter for their contributions to this article.

Designed by Global Editorial Services