McKinsey&Company

Corrado Bordonali,
Simone Ferraresi,
and Wolf Richter

Shifting gears in cybersecurity for connected cars

Automotive & Assembly April 2017

To secure products across the supply chain, the automotive sector must develop new ways to collaborate.

Although connectivity has the power to enrich societies, economies, industries, and companies, it is not without its risks. Particularly in the automotive sector, cybersecurity threats are real, and for several basic reasons. Products are becoming more complex, with an increasing number of electronic control units and lines of code. Connectivity is burgeoning, with dangers at every turn. The supply chain is fragmented, so policing security is hard. And the integration of automotive systems can compromise any specific countermeasure.

We believe that the sector needs a holistic, two-front approach to cybersecurity. On the first front, solutions ought to address the design of the product, the way it's developed, and the maintenance-and-response architecture. On the second, OEMs should focus more effectively on the automotive environment at the sector level (for instance, by cooperating among themselves), on the concerns of regulatory bodies, and on the mind-sets of final users, who must actively protect their cars.[1] An OEM's chosen approach should always preserve innovation, the user experience, and cost competitiveness.

Products can be secure only if they are designed with security in mind. Quick fixes may add costs, much more complexity, and sometimes weight. They could also be relatively easy to circumvent because they may not solve the vulnerability challenge structurally—the architectural issues, for example. Penetration tests are at best a temporary solution. Other sectors (such as aviation, trains, and critical infrastructure) have adopted a variety of approaches to design, not just technologies, because no one "silver bullet" can eliminate cybersecurity issues. What's clear is that future automotive designs have to be "cybersecurity natives," integrating these concerns into the earliest stages of development.

A secure design, while necessary, won't guarantee full security over time. Solutions are effective only if they are implemented consistently, and high-quality components—software and hardware alike—implement the design. This requirement calls for a sound and managed development process, including reinforced collaboration between product-security teams and corporate IT-security teams. OEMs must thus create and enforce strict guidelines to minimize the chances of bugs and software-security gaps and to make modifying or patching systems easier.

[1] For example, by updating the software.

That's why over-the-air (OTA) updates—which have recently become available for some cars, though often for limited parts of the software—are clearly essential for connected systems: they help OEMs to counter attacks quickly and to eliminate specific vulnerabilities before malefactors can exploit them. These benefits have a price, however: implementing support for OTA updates is quite complex and expensive, both for cars and the back-end infrastructure. OEMs must therefore trade off the desired level of effectiveness (and the systems that can be updated) against the costs. That calls for a deep understanding of the architectures and peculiarities of these systems.

OEMs, which exclusively control the relationship with customers and are usually the final system integrators, bear the ultimate responsibility for integration risk and for ensuring that secure stand-alone systems aren't vulnerable when connected. These companies must ascertain that security practices have been implemented consistently throughout the full value chain, including suppliers. Procurement executives must therefore learn to negotiate over the cybersecurity features of components as rigorously as they do anything else. OEMs should also play an active role in shaping the sector's future standards—both regulations and best-practice guidelines.

In many sectors, including oil and gas, financial services, and aviation, alliances help companies to deal with regulators and to share intelligence on threats and vulnerabilities, both internally (among OEMs and suppliers) and externally (with regulatory bodies and the media). Such alliances also facilitate prompt responses to novel threats. Some automotive companies are already creating alliances; other OEMs and suppliers should consider joining them.

But the OEMs' best efforts will succeed only if car drivers understand the importance of cybersecurity, play their role in realizing it, and avoid anything that could facilitate threats. Unfortunately, recent research shows that despite this issue's resonance in the automotive community, car drivers largely ignore the problem.[2] OEMs must consider tools to increase their awareness by cultivating a culture of cybersecurity (through in-car screen guidance and functional inhibitors, for example) or by pushing for the introduction of cybersecurity questions in license exams.

As for regulators, though an increasing number of them have started focusing on cybersecurity in the automotive sector, the definition of formal rules is still at a preliminary stage. Since OEMs and relevant suppliers have a mutual interest in effective and realistic security guidelines, they should continue their collaborative discussions with regulators (for instance, by leveraging industry alliances). Who knows what might happen if, for example, scary but ill-informed newspaper headlines inspired new cybersecurity rules. OEMs and their suppliers should therefore help regulators to understand the actual risks and the countermeasures already in place to deal with them.

[2] Andy Greenberg, "Only one in 4 Americans remembers last year's epic Jeep hack," *Wired*, March 8, 2016, wired.com.

Finally, to make products secure while minimizing wasted investments and hastening time to market, OEMs should follow a holistic process to select and implement cybersecurity solutions for every subsystem of every vehicle:

- Assess the acceptable risk profile—the components and areas (such as autonomous- or assisted-driving systems and infotainment gear) that customers, companies, or regulators would regard as vulnerable to cyberthreats.
- Understand the exposure to cyberrisks from a product-resiliency standpoint; in a given vehicle, infotainment, for example, might be extremely safe but an autonomous-driving system could be easy to hack—a critical departure from the acceptable risk profile.
- Identify the cybersecurity solutions, making all necessary trade-offs among costs, time to market, the user experience, and product innovation.
- Define the implementation strategy and key enablers (designing the road map, sourcing capabilities, and managing relationships with key stakeholders).

Automotive OEMs face a unique challenge, so they must complement their own efforts to develop security strategies by taking action on a higher level: the sector as a whole must secure its products across the entire supply chain by developing new ways to collaborate and interact. If it doesn't, cybersecurity problems could irritate customers or even generate regulatory burdens that might well upend the cars of the future before they hit the road. □

Corrado Bordonali is a consultant and **Simone Ferraresi** is an associate partner in McKinsey's Rome office; **Wolf Richter** is a partner in the Berlin office.

The authors wish to thank Garrett Bray, Marc Sorel, and Dominik Wee for their contributions to this article.