Within the next few years, virtually all new cars will be connected to the internet. That will give drivers and passengers even greater access to the kinds of digital services, such as streaming media and e-commerce, that have helped make smartphones so indispensable. Yet, it will also likely usher in a pressing new challenge for automakers: **how to keep the connected car safe from cyberattacks.**

**A smarter car thief?** Car thieves tampering with remote keyless entry systems account for most of today’s automotive hacks. Researchers have demonstrated, however, that it’s possible to wreak much more havoc by penetrating the connected car’s electronic brain. In 2015, a pair of cybersecurity experts grabbed headlines by remotely disabling the engine of a car driving down an interstate highway at 70 m.p.h.¹ The following year, researchers from a security company identified a weakness in a vehicle entertainment system that could lead to a ransomware attack.² And last summer, the Department of Homeland Security warned several automakers that their cars’ telematic control units, which enable tracking of—and communication with—the vehicle, could be vulnerable to denial-of-service attacks.³

The dangers posed by these kinds of digital intrusions will likely only deepen as autonomous-driving technology advances. While cars are far from becoming driverless living rooms on wheels—PwC estimates fully autonomous vehicles won’t enter the mainstream until 2027 at the earliest—the onus is on automakers to not only address vulnerabilities that have already surfaced, but also to safeguard against future threats.

**Cybersecurity needs to take a front seat** To stay ahead, automakers should start thinking about cybersecurity at the very beginning of a new vehicle’s development. Once a car leaves the factory, it can become difficult to add new security features or bolster existing ones. That means any potential weaknesses need to be dealt with before vehicles enter production. Early testing may catch most problems, but since most cars have a three- to five-year development cycle, one or two rounds of tests won’t be enough. Taking an iterative approach to cybersecurity testing may slow down the process of getting a new car to market, but it’s cheaper and easier to prevent problems then to fix them later. In the long run, secure design will limit recalls, reduce liability risk, and help prevent embarrassing intrusions by hackers.

Of course, cybersecurity isn’t only the car manufacturer’s responsibility. It’s important that third-party suppliers share a focus on preventing attacks, since they provide the majority of sophisticated components in the connected car. Nonetheless, automakers, not their supply-chain vendors, will bear the reputational risk if a vehicle’s digital defenses are breached. That’s why the responsibility is on car makers to develop cybersecurity requirements and make sure suppliers meet them. They also need to be open about vulnerabilities discovered in testing, so they can be addressed by the vendor that built the deficient part.

This would all be easier if the automotive industry had clearer cybersecurity standards. No such common playbook yet exists, although a set of best practices for connected vehicles released by the Automotive Information Sharing and Analysis Center (Auto-ISAC) is a step in the right direction. The Auto-ISAC serves as a repository of intelligence on cyber threats to help automakers and their suppliers prepare for, and respond to, vehicle cybersecurity risks. Strengthening Auto-ISAC by being diligent in sharing threat information and analysis should be a priority for every automotive company.

**Digital threats extend beyond cars** The impact of advanced technologies isn’t limited to the car itself. The factories that produce them are more connected than ever, too. While robots have been a mainstay of automotive production lines for decades, the advances in artificial intelligence and other digital technologies have made it possible to automate an ever-increasing share of the manufacturing process. And advanced materials and improving 3D printing has revolutionized the way prototypes and, increasingly, production components are made. But as the factory becomes “smarter,” it also becomes more vulnerable to cyberattack.

Fortunately, there are a few steps automakers can take to protect themselves. First and foremost, a successful defense against online threats begins at the top. The CEO and board of directors should make cybersecurity a priority and ensure that it’s woven into company culture.

---

Next, it’s important to take an inventory of what’s at risk of attack and by whom. Since it’s too expensive to protect all assets, automotive companies should determine which are their most valuable and focus aggressively on protecting them. Companies also need to categorize and prioritize the kinds of threats they are facing, now and in the next few years, as well as the perpetrators most likely to do damage.

To best respond to an incident, automakers should think about who will respond and how before something goes wrong. Manufacturers should develop a matrix that can be used to situate attacks on a graduated scale of potential impact based on brand, financial, or operational damage, the number and type of systems compromised, and plans for notifying stakeholders. A working group including representatives from the IT, legal, and corporate communications departments can implement the response and help minimize confusion and delay.

Automakers should take the lead in making sure suppliers are abiding by the cybersecurity plans they develop for their operations, just as they should for their cars. Smaller vendors present special risks, since they tend to have less stringent security protocols, so contracts should include audit clauses and mandated testing procedures.

**Fighting fire with fire** Automakers need the right processes to fight cyberattacks. But proper planning isn’t enough. Advanced technological defenses coordinated across all production platforms and throughout the supply chain need to be built. Careful control of sensitive data must be maintained even as it’s shared between factories, among suppliers, and with other key stakeholders. Cloud-based services provide real-time updates that aggregate information and keep defenses fresh and dynamic, making them a solid choice. But it’s equally important to deploy and configure tools that meet each organization’s specific operating circumstances.

Taking an enterprise-wide view is critical. Compared to other types of fraud, cybercrime was rated as twice as likely to have a potential impact on organizations over the next two years, according to PwC’s most recent Global Economic Crime and Fraud Survey. And it’s the most common form of fraud faced by U.S. companies, with phishing and malware making up the majority of attacks.

Cybersecurity is likely to remain a core concern for both legacy automakers, who have valuable brands and customer relationships to maintain, as well as for disruptive new entrants, who are still building trust and seeking mainstream adoption of their vehicles. Keeping hackers from penetrating vehicles and the factories where they’re built could require manufacturers to think differently about how cars are designed, tested, and made. And it could mean enhanced oversight and closer partnership with suppliers. These changes may not always be easy, but they’re necessary to keep the automotive industry (safely) on the road to the future.

Read PwC’s full Cyber Readiness report for the automotive industry at [www.pwc.com/mobility](http://www.pwc.com/mobility)