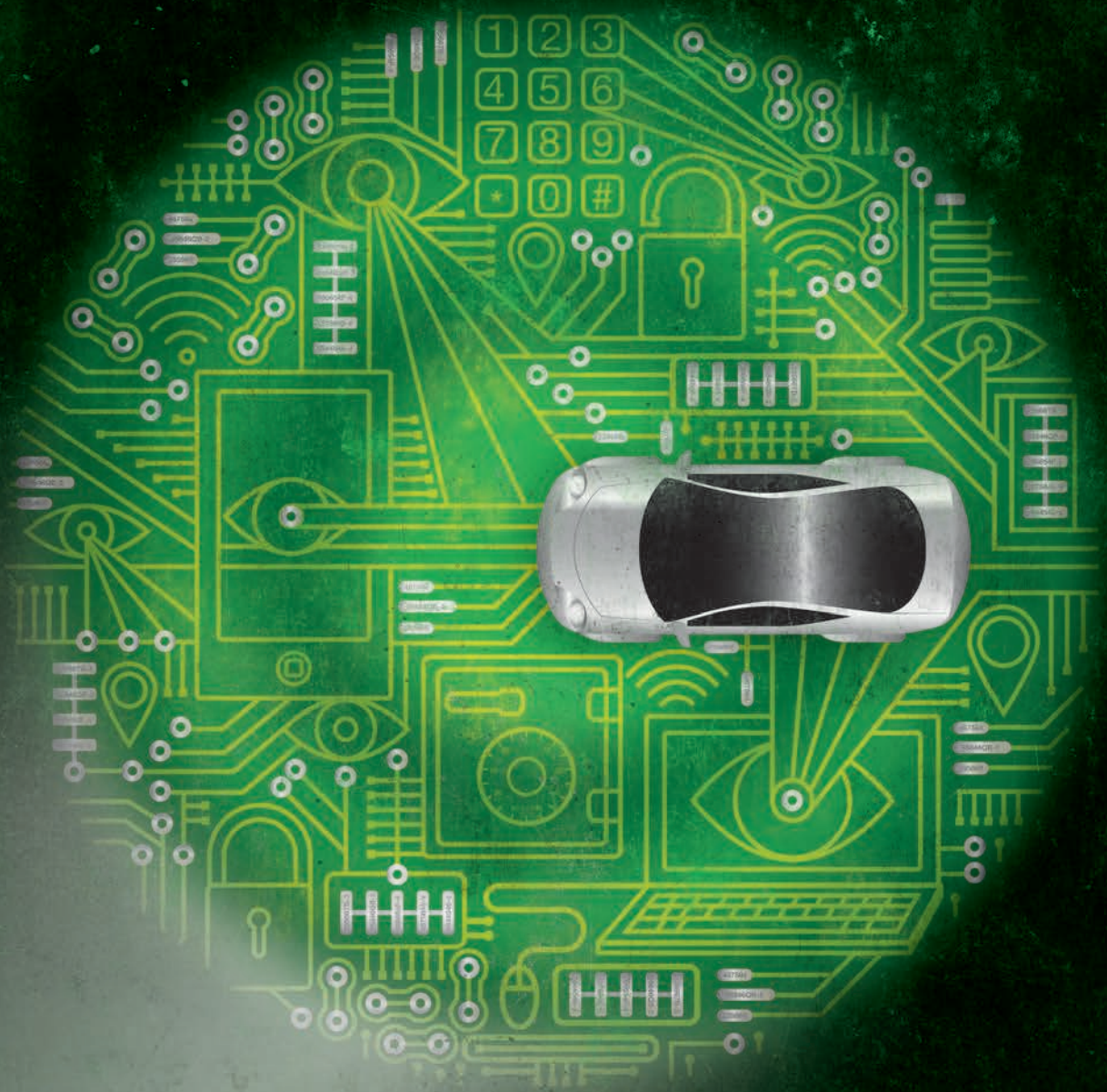
Part of a Deloitte series on the future of mobility™

Deloitte.
University Press



Securing the future of mobility

Addressing cyber risk in self-driving cars and beyond

Deloitte's Center for Integrated Research focuses on developing fresh perspectives on critical business issues that cut across industry and function, from the rapid change of emerging technologies to the consistent factor of human behavior. We uncover deep, rigorously justified insights and look at transformative topics in new ways, delivering new thinking in a variety of formats, such as research articles, short videos, or in-person workshops.

COVER IMAGE BY: TRACI DABERKO

CONTENTS

Introduction

An unwelcome passenger

CLIMBING into a car has long been among the riskier things that people do—famously, the least safe part of an airplane trip is the drive to the airport.[1] So it's likely no surprise that self-driving cars' safety is one of their most often cited benefits. Indeed, many expect the emerging mobility ecosystem,[2] with increasing shared access to transportation as well as autonomous technology, to all but eradicate routine accidents.

> The very innovations that aim to enhance the way we move from place to place entail first-order cybersecurity challenges.

But as the future of mobility offers potential growth and new sources of value creation, it presents new types of risk. The very innovations that aim to enhance the way we move from place to place entail first-order cybersecurity challenges. And the dangers that promptly come to mind—such as hacked autonomous vehicles crashing[3]—only begin to scratch the surface; indeed, they may not even represent the most likely or high-stakes threats. Shared vehicles could hold data from hundreds of unique users, making them a ripe target for digital thieves. Connected and increasingly autonomous vehicles may provide new opportunities for malicious ransomware. And as mobility managers take the hassle out of travel by managing end-to-end trip planning, they could gain an increasingly holistic view of people's lives, including where they go, when, and for what purpose, accumulating data and raising the stakes even further.

The path forward should incorporate a comprehensive approach to cybersecurity that makes connected vehicles and the associated ecosystems secure, vigilant, and resilient. This likely involves a radical change to how organizations address cybersecurity:

Secure. Establish risk-focused controls around the most sensitive assets, balancing the need to reduce risk, while also enabling productivity, business growth, and cost optimization.

Vigilant. Develop monitoring solutions focused on critical business processes. By integrating threat data, IT data, and business data, companies can equip themselves with context-rich alerts to help prioritize incident handling and streamline incident investigation.

Resilient. Rapidly adapt and respond to internal or external changes—opportunities, demands, disruptions, or threats—and continue operations with limited impact to the business.

Cyber risk poses perhaps the greatest threat to the future of mobility, and data governance, privacy, and protection will likely be of paramount importance as individuals and organizations move to make it a reality. Just as collision warning systems and antilock brakes haven't eliminated all road mishaps, a world of shared and autonomous vehicles can never be risk-free. A key challenge for players in the mobility ecosystem lies in making the *degree* of risk acceptable to both consumers and regulators. As automakers, technology companies, governments, and others place bets on how and when the future of mobility may unfold, those moves could be for naught without a broad understanding of the myriad cyber threats likely to emerge—and a concrete plan to address them.

Where could the risks lie?

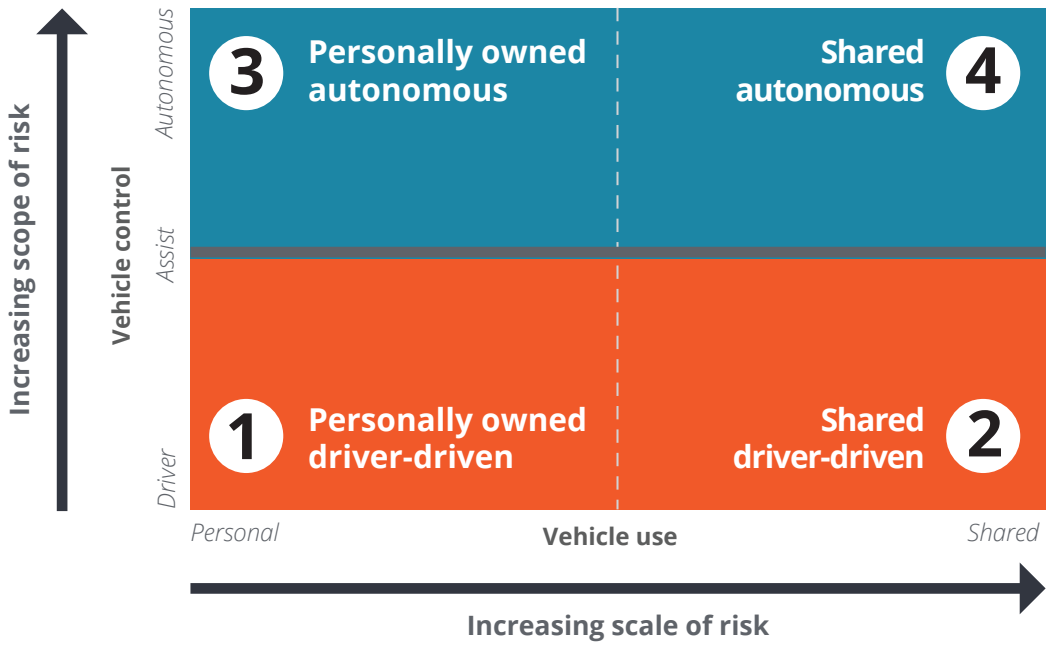
AFTER a century of addressing mainly problems with engineering, automakers are facing a new set of challenges. Other industries are also dealing with cybersecurity issues, and players in the mobility ecosystem can look to others for similar solutions, although the specific implementation of those solutions would need to be carefully shaped to fit the auto industry's unique needs.

What steps companies take also likely depend on which ecosystem roles they intend to play. In *The future of mobility,* we envisioned four co-existing future states of mobility: some quite similar to today's landscape and others that posit more ambitious vehicle sharing and autonomous driving possibilities (see figure 1).[4]

Each of the four future states of mobility brings a unique set of data-related risks and, consequently, a unique set of challenges and required solutions.

Future state 1: This is the most conservative vision of the future, in which vehicles would remain individually owned and operated, much as most are today. Yet even here, vehicles are expected to become increasingly connected and data-centric (creation, consumption, analysis, etc.) and to employ advanced driver-assist technologies (stopping short of full autonomy). As vehicle designs advance, their security capabilities should evolve too. Enhanced security features will likely be based on in-vehicle technology and features already present in today's cars. This enhanced security would need to secure current technology and features while continuing to evolve to protect the incremental changes that we expect providers to develop in future state 1.

Figure 1. The future states of mobility



Source: Deloitte analysis.

INSIDER THREATS

The future of mobility, even in the most incremental vision, will likely introduce a new kind of infrastructure, one based on bits and bandwidth more than bridges and boulevards.[5] As vehicles communicate with other vehicles and their surroundings, V2X networks will likely emerge to help with everything from rerouting emergency vehicles to easing traffic congestion to facilitating parking and electric vehicle charging.

As with smartphone development today, it is likely that hardware and software vendors will collaborate in the design and production of future vehicles and other mobility infrastructure. Consider a hypothetical software developer partnering with a V2X device manufacturer that ships and configures devices that enable connected infrastructure. When the developer's lead engineer leaves the company, he takes with him critical trade secrets and knowledge of a backdoor into the root of the V2X system. Perhaps because of discontent with his former employer, he leaks information about the security bypass, making vulnerable hundreds of thousands of installed and active devices. The attacks could begin as irksome pranks but soon escalate: Targeting one city, hackers could manipulate information to tell traffic apps and rideshare vehicles that there is construction on every street, causing accidents and delays in emergency service response. Next, they could remotely quadruple the amperage of electric vehicle charging stations and begin starting fires.

Of course, companies work to maintain safeguards against single bad actors causing such widespread harm, but plenty can sneak through. In a recent survey conducted by the Manufacturers Alliance for Productivity and Innovation and Deloitte, manufacturing executives traced 42 percent of cyber incidents to "insider threats."[6]

The extended automotive industry could take cues from how organizations such as the North American Electric Reliability Corp. (NERC) have created standards and practices that guide the secure development of critical electric power systems. Led by a standards committee and aided by drafting teams comprising industry volunteers and their staff, NERC develops guidelines based on a set of principles that emphasizes reliability and market impact—principles that could readily be adapted to mobility-focused systems.[7] As vehicles and transportation infrastructure begin to integrate with their surroundings and other systems, governments and developers should consider protecting that infrastructure like any other essential public service.

Such a standard-setting effort could build off the Nation Institute of Standards and Technology's Generally Accepted Principles and Practices for Securing Information Technology Systems.[8] Similar to how secure content providers protect publicly accessible devices with encryption and authentication, critical infrastructure protection typically requires the addition of secure software development as well as physical and public safety measures. This is because regulating bodies and organizations, such as the US Department of Transportation and the National Highway Traffic Safety Administration, have recognized that the assets they oversee are exposed to an increasing number of threats as they become more complex and open to remote operation. The same level of attention would need to be paid to connected vehicles and associated devices that make up the new mobility ecosystem's critical infrastructure.

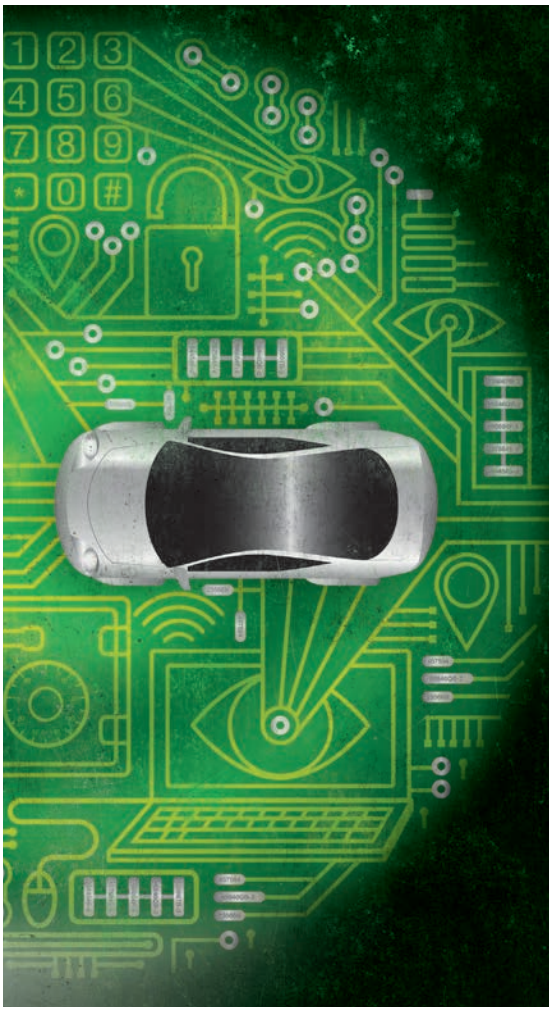
The NHTSA looks to be laying down some of the first concrete steps down this path. In October 2016, the agency offered a series of recommendations to the automotive industry aimed at improving cybersecurity safety, focusing on "layered solutions to ensure vehicle systems are designed to take appropriate and safe actions, even when an attack is successful."[9]

Even today, many vehicles rely heavily on proprietary software that may already have numerous vulnerabilities. The average new vehicle relies on computer systems that utilize more than 100 million lines of software code,[10] leading to cars that are increasingly sophisticated and connected—but also increasingly exposed (see sidebar, "Insider threats"). And it isn't only the quantity of code that drives risk—it's the quality. As companies accelerate change and innovation to differentiate themselves, it can be easy to sacrifice the rigor of end-to-end development and testing to beat competitors to the market. This shortsighted approach could increase the chance of system errors or security vulnerabilities, leading to potential recalls and reputational damage. New features will almost inevitably bring more integrated code from multiple sources and the potential for more vulnerabilities, with a corresponding need for vehicle manufacturers and software providers to redouble their focus on the integration, securing, and testing of components throughout the vehicle.[11]

Regulators, too, could be challenged as vehicle shortcomings increasingly arise from flawed code rather than faulty components. Some have already recognized the difficulty. National Highway Traffic Safety Administration (NHTSA) administrator Mark Rosekind put it succinctly: "How many times have we talked about . . . millions of lines of code? There's no way we'll have the resources to look at that."[12]

Future state 2: With the rise of the "sharing economy" and the growth of ridesharing and carsharing companies, a second potential future state sees the possibility of continued expansion of shared mobility, even as vehicles remain human-controlled.

We see glimpses of this future state today, providing a window into the potential cybersecurity challenges, but accelerating adoption could dramatically increase the scope, magnitude, and complexity of these threats. With the proliferation of social media, ridesharing, and other mobile applications, access to a consumer's smart device can expose her to additional risks.



In particular, protecting the personal information of both drivers and riders becomes a high priority. Some nefarious parties would find this information valuable, and ridesharing and carsharing companies present an attractive target. Payment systems can expose credit and banking information to potential theft. Navigation and location information can compromise customer privacy, requiring providers to keep onboard communications secure.

As automotive companies and technology firms consider expanding their services to include shared mobility,[13] they should consider the unique risks and cyber threats that accompany this business model.

DUMPSTER DIVING FOR DATA

Just as flight data recorders collect information about what happens in a cockpit, connected vehicles absorb details about what their owners and passengers do once they climb in. But vehicle-based technology can also compile and analyze data to generate less obvious insights: For instance, devices can be taught to differentiate between a set of users based solely on brake pedal input.[14] In-depth data collection will likely become increasingly common with shared vehicles, as customers come to expect seamless integration with the rest of their digital lives. Many parties eagerly await unrestricted access to these data, including standard players such as data brokers and insurance carriers, but pairings are forming to monetize the data in new ways. Some rideshare providers already offer the ability to sync a passenger's streaming audio service with the vehicle while she rides.[15]

Now, imagine a scrapper picking over parts in a junkyard. She skips the fenders, doors, and air bags. The real money could be in the CPU modules—not for use in repairs or as replacements but, rather, for their data. Each module might contain a wealth of valuable information—for instance, a data recorder from a rideshare vehicle may well contain a list of the previous owners' linked smart devices, with addresses and ID numbers, along with a full history of everywhere the donor vehicle went in the year before the accident that wrecked it, as well as hundreds of account numbers and logs that can be used to link passengers to phone numbers, addresses, and payment histories. A good set of data might fetch a much higher price online than individual resale of replacement parts.

Tomorrow's vehicles are expected to know much about their owners and users—and for many, this is a growing concern. Would the manufacturer of the vehicle own those data? What about the person who bought, borrowed, or is simply a passenger in that vehicle? How might our legal systems consistently define ownership? What would happen when the vehicle crosses boundaries of jurisdiction? How would a police agency handle logs from a connected vehicle involved in an accident? At the end of their lives, who would be responsible for wiping clean obsolete data recorders?

For a path ahead, automakers and shared mobility providers might look to enterprise IT. Many companies that issue electronic devices to their employees have wiping procedures for laptops and mobile devices upon end of lease or separation, which includes encryption, factory resets, or other data erasure procedures. In one survey, more than half of respondents indicated their company had a formal secure IT asset disposition policy.[16] Similar procedures could be adopted upon change of ownership or at the end of a vehicle's useful life.

Future state 3: This future state envisions the adoption of personally owned, fully self-driving cars. While much of the core autonomous functionality may be self-contained within the vehicle (making it relatively less vulnerable to attackers), self-driving vehicles would need to communicate with the outside world through sensors, vehicle-to-everything (V2X) capabilities, GPS software, and other systems. As with future state 1, when working as intended, these connected cars may have the potential to help improve the passenger experience, but they also likely open up new vulnerabilities. Last year, security researchers were able to use a flaw found in an OEM-provided application to run down an electric vehicle's battery, potentially stranding the vehicle owner.[17] While this flaw was addressed, this example highlights an escalating threat landscape caused by increased connectivity. And in an autonomous vehicle, where the car's systems would be fully in control of the vehicle, the potential damage caused by an intrusion or flaw could be fatal.

Autonomous vehicle developers currently protect their prototypes from these issues by having a human operator who takes control in the case of failure or fault, but this approach is not expected to be extended to consumer-owned vehicles. In particular, the Department of Transportation Automated Vehicles guidelines specify that, "fall back strategies should take into account that . . . human drivers may be inattentive, under the influence of

HACKING INTO MANUFACTURER-TO-VEHICLE COMMUNICATIONS

While runaway autonomous cars might capture the imagination, the possibility of more conventional threats loom just as large. Today, many automakers install software-related recalls and patches in person, one car at a time, at the dealership. It can be challenging to get car owners to respond to these service requirements, especially when the vehicle seems to be operating normally.

With far more onboard software needing regular security and navigational updates, autonomous vehicles in the new mobility ecosystem will likely have dedicated communication lines back to the manufacturer for instant transmission of software-related recalls and patches. Updates to vehicle systems would be handled in a similar way as with smart devices and computers today, with patches downloaded wirelessly and applied when the device in question is not being used.

In the near future, a self-driving car might require a minor update to its telematics unit. The device that receives and applies this patch could be connected directly to the vehicle network and allow the existing hardware to initiate the process once the car is parked. Imagine one of these receiving devices sharing a processor with a common smart device that ambitious hackers could compromise and unlock, meaning that this device—in nearly any vehicle with that device—can be exploited to replace manufacturer updates with user-generated updates. A skilled attacker could even install ransomware on thousands of vehicles, granting the ability to lock out users or freeze vehicles in place unless owners pay a fee. Manufacturers, with their proprietary channel blocked, would struggle to counter the attack, and owners could not even direct the vehicles to a service bay. This would be especially challenging, as a cornerstone of the automobile industry has traditionally included the aftermarket ecosystem, allowing owners to alter and customize vehicles to enhance their performance and capabilities. With ever more accessories being online and connected, a vehicle owner may unintentionally introduce vulnerabilities.

With each new connected feature creating a new attack surface, how to maintain security? Automakers and software developers can learn from the approach that content delivery services have taken to prevent tampering. Satellite and cable media providers address this by including digital relays, fault recorders, equipment diagnostic packages, automation equipment, computers, programmable logic controllers, and communication interfaces.[18] But this process has been uneven and often ad hoc. Content providers are limited by the capabilities of end users' technology. In the past, devices such as satellite receivers were barely able to authenticate subscribers over the air without compromising the content's quality, just as vehicle networks today strain to secure communications between modules in a given vehicle. Security was layered on incrementally as the receivers became more powerful, but content thieves and disruptors were able to use the same technology in the receivers to circumvent security.

A similar process will likely play out in the connected and autonomous vehicle space unless automotive technology suppliers take steps to implement the lessons learned from secure content providers in other sectors. Secure content delivery today is encrypted and authenticated at both ends, with rotating security keys that are impractical to crack within the designated response window. Access to the automated systems that facilitate these actions are often limited and routinely checked for exploits and remote tampering.

alcohol or other substances, drowsy, or physically impaired in some other manner."[19] Additionally, autonomous vehicles may operate in a mode where no human driver is present to take over in the case of failure—for example, if a self-driving car "delivers" itself to the shop for maintenance. The policy does not specify how autonomous vehicles should behave in these circumstances, and autonomous vehicle developers and researchers will have to work to ensure they develop a safe approach.

For some consumers, putting their safety into the hands of an automated vehicle would require a new level of trust in the security, integrity, and

functionality of vehicle and infrastructure technologies. Autonomous cars are expected to have numerous onboard attack vectors, including radar, cameras, GPS, ultrasonic sensors, V2X, and other networking capabilities, not to mention the related infrastructure components and technologies on which these sensors may depend. The architectural and operational (think monitoring, vulnerability management, security operations, etc.) requirements for fully automated vehicles are considerably higher than for partially automated or assisted driving vehicles. Stout vehicle technology to support cybersecurity and individual privacy must be a primary concern.

Future state 4: Finally, an increase in car- and ride-sharing and the maturation of vehicle automation could converge at a point of "accessible autonomy," in which many individuals can reach destinations by simply requesting rides from nearby autonomous

HIJACKING VEHICLE CONTROLS AND SENSORS

Ideally, for users, an app on a smart device could seamlessly control ridesharing and access to other modes of transport. When everything is synced properly, you would be able to easily order, unlock, direct, and pay for a communal autonomous vehicle. The car itself would accept signals from cellular and satellite networks in addition to Wi-Fi and shorter-range communications; a paying customer would simply approach a vehicle and sync up with it as with a portable speaker or smart television.

Seamless hardly means risk-free, though. Beforehand, an attacker might conceivably have surreptitiously installed a surveillance device, leaving a transceiver to extract customer data or inject malicious data into the vehicle network. Subsequent customers would unknowingly broadcast everything from personal information to payment details to the attacker. Worse, a hacker might flood the vehicle network with bad sensor and navigation data, making the car swerve to avoid imaginary obstacles or take passengers to the wrong destination.

Initiating a vehicle network open to communications from smart devices can create new attack surfaces and increase the risk for data loss. The intersection of critical and noncritical vehicle busses can allow a message injector to pass unwanted data to devices in the vehicle. Nominally, the devices that control cabin lighting and playing music should be unable to communicate with systems that perform critical tasks such as braking and acceleration. Currently, these vehicle networks are physically connected at the telematics or body controller units, allowing propagation of data between networks.

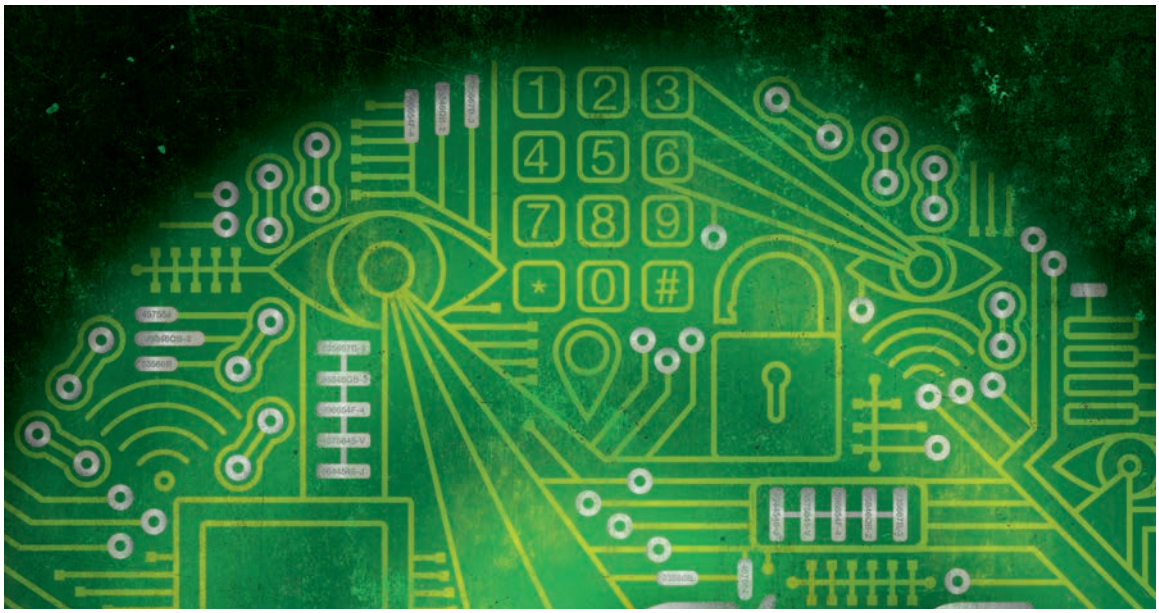
The cybersecurity domain strives to tackle these issues. To protect cardholder data, payment card processors today follow established data security standards (DSS) that aim to guard the devices that handle data as well.[20] The DSS—in common use, though not mandated by a government body—provide high-level guidance such as, "Do not use vendor-supplied defaults for system passwords and other security parameters" and, "Encrypt transmission of cardholder data across open, public networks." Organizations in the payment card industry opt in and become compliant at will, but if a company wishes to accept payment cards, it must enter a contractual agreement and become DSS-compliant. Noncompliance can lead to fines, increased transaction fees, or termination of service.

Establishing and implementing security standards in the extended auto industry could fall along the lines of a DSS-like ruleset applied to suppliers of vehicle electronics or infrastructure devices. This could also be applied to the ways in which connected vehicles store and communicate data themselves. Most current vehicle network architecture is unequipped to deal with intrusion detection or threat monitoring, let alone authentication or encryption. A modern attacker with physical access to a vehicle is typically capable of sending or extracting any information he pleases from the vehicle network, as long as he knows what kind of communication the vehicle expects. This problem may only get worse as automakers add features, increasing vehicle capabilities but broadening the vehicles' attack surface in the process. In past eras of automotive technology, the simplistic and less powerful vehicle electronics were nearly impenetrable to attackers.

fleets. This future state is most likely to begin with urban commuters in large cities but could quickly spread as capabilities and consumer willingness expands. The adoption of these technologies could spur the emergence of an integrated intermodal mobility ecosystem that offers safer, cleaner, cheaper, and more convenient transportation.

This future state includes the same security vulnerabilities and personal data theft as other future states—and would present a problem of another order of magnitude, since a hacker breaching "smart" infrastructure or a large fleet of shared autonomous vehicles could inflict dramatically greater damage.[21]

In every future state, cars and their occupants will likely need to place additional trust in onboard technology, raising the stakes for vehicle cybersecurity. Security researchers have highlighted vehicle vulnerabilities, engaging the interest (and possibly the imagination) of the public, regulators, elected officials, and many others. Successfully addressing those risks is expected to require both consensus on the overall standards to be met and a broad effort to make the future of mobility secure, vigilant, and resilient.



A path forward

The big picture: Reaching consensus

While the possible advances that comprise the future of mobility bring with them significant new potential threats, the dangers are hardly insurmountable, partly due to a growing awareness of the importance of cybersecurity among the general public, federal, state, and local governments, as well as regulatory and standards bodies. One example: In 2016, the FBI and the NHTSA issued a warning to the general public and manufacturers of vehicles, vehicle components, and aftermarket devices to "maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles."[22] The NHTSA also convened a public roundtable in January 2016 to facilitate a diverse stakeholder discussion on vehicle cybersecurity topics. Attendees included representatives of 17 automotive OEMs, 25 government entities, and 13 industry associations.[23]

This increase in awareness comes at an opportune time. As the private sector and governments work to make the future of mobility a reality, the extended global auto industry faces what most consider an urgent need to establish cybersecurity standards to create current baselines for today's needs—as well as to prepare for future software development and distribution. Thankfully, early efforts are already under way. In 2015, the Automotive Information Sharing and Analysis Center formed to enhance cybersecurity awareness, share information about threats, and improve coordination across the global auto industry.[24] The Alliance of Automobile Manufacturers and the Association of Global Automakers also developed a "Framework for Automotive Cybersecurity Best Practices."[25]

While these are important early steps, more can be done. The current efforts are voluntary, and the organizing groups' memberships are limited to auto OEMs and major suppliers—a narrow focus considering that the future mobility ecosystem is expected to cut across traditional industry lines and include players from technology, telecom, media, insurance, finance, and beyond. A much more diverse consortium of actors would be needed to effectively set standards that can bridge tomorrow's diverse mobility options. Indeed, given that this new wave of technology is still in its infancy, current technology vendors seem well positioned to shape the relevant standards.

A much more diverse consortium of actors would be needed to effectively set standards that can bridge tomorrow's diverse mobility options.

The technology industry has shown the path forward on many occasions in the past. One of the better examples is how the then-players in the communications industry came together and formed the Bluetooth Special Interest Group (SIG). The Bluetooth SIG—a not-for-profit, non-stock corporation—oversees the development of Bluetooth standards and the licensing of Bluetooth technologies and trademarks to manufacturers.[26] Now, any company incorporating Bluetooth wireless technology into its products must become a member.

What makes the Bluetooth SIG so effective is its control of the specifications for the technology, requiring that members certify their products as compliant

with the standards. SIG members declare their compliance with both the Bluetooth Patent/Copyright License Agreement and Bluetooth Trademark License Agreement.[27] The enforcement program helps to protect all SIG members by confirming that all Bluetooth products are properly qualified, declared, and branded. The enforcement program monitors the market and performs monthly audits to ensure that members are using trademarks in accordance with the Bluetooth brand guide and selling goods and services that have successfully completed both the Bluetooth qualification and declaration process.[28]

The enforcement program helps to protect all SIG members by confirming that all Bluetooth products are properly qualified, declared, and branded.

Granted, creating a similar entity for connected and autonomous vehicles would be no small feat—it would require the myriad groups independently developing self-driving systems to come together and agree on certain baseline features. But the advantages could be significant—not least, helping to assure a possibly skittish public that developers are adopting a rigorous and tightly controlled process for establishing the safety and integrity of autonomous vehicle systems.

The details: Building in safeguards

Standards alone likely aren't enough to protect the future of mobility: Automakers and other manufacturers will still need to build secure components and provide for their safe interactions. The industry standard has been to bench-test vehicle components on a per-component basis, assessing vulnerabilities in software and firmware, over-the-air updates, and communications channels. Often, individual modules are farmed out to specialists familiar with that particular component, bringing in multiple partners for the different components. Integrating these independently developed components together as one product can present multiple challenges. First, communication between components could reveal attack vectors that are not present when tested independently. For example, a module may fail if sent messages are invalid or malformed. Second, unexpected communication could open up a manufacturer or their partners' intellectual property to malicious attacks. Failing to securely integrate these component parts could expose an easy attack vector.

Figure 2 is a representation of the complete connected vehicle, showing how the individual components interact with one another. A failure in one component often results in a cascading effect, putting both the driver and others in the vehicle's path in a precarious situation.

Integrating these independently developed components together as one product can present multiple challenges.

As an example, if the vehicle communication busses break down, then the real-time vehicle systems would not be able to transmit vital situational awareness to the advanced vehicle systems. If the advanced vehicle systems do not receive the information, then the integrated vehicle security systems that control physical components such as braking, acceleration/deceleration, and crash avoidance would fail to react.

Below is a summary description of the components in the wheel to provide a full perspective of each component's key functions and the associated risks.

Figure 2. Assessing the connected vehicle

Source: Deloitte analysis.

- **Vehicle communication busses.** Providers should rigorously test Controller Area Network, Internet Protocol, 2Wire, Ethernet, and other vendor-specific communication bus systems to identify security vulnerabilities impacting communications between software and hardware components.
- **Mobile applications.** Vehicle remote applications on handheld devices and the onboard dash applications that interact with them should be assessed to verify end-to-end security. With the proliferation of mobile apps and the integration with advanced vehicular systems, this risk continues to escalate.
- **Connected vehicle services.** Enterprise services, sensor communications, over-the-air firmware updates, V2V, and V2X communications provide potential attack surfaces that providers should review for end-to-end security weaknesses. Other common attack vectors include vehicle locator, remote unlocking and starting, and fleet health monitoring.
- **Integrated vehicle security.** Providers and automakers should consider ways to block attacks on the vehicle's physical security systems, such as the immobilizer, alarm systems, and unlocking systems. Additionally, attacks over radio frequency, such as replay and denial of service

for key-fob messages, should be considered and mitigated.

- **Infotainment systems.** The vehicle's head unit, navigation system, USB, CD/DVD, and other physical interfaces are easily accessible and offer a potential foothold for hackers to enter the system with direct access to onboard components and firmware.
- **Wireless communications.** Wi-Fi, Bluetooth, Near Field Communication, and mobile Internet technologies provide many additional possible paths into the connected vehicle and should be examined for weaknesses and vulnerabilities.
- **Advanced/autonomous vehicle systems (including semi- and fully autonomous driving capabilities).** Advanced connected vehicle systems, such as radar, cameras, driving and parking assistance systems, and collision prevention systems, offer attackers a connection that bridges the gap from a cyber attack to a physical one. Under hacker control, these systems can be used to undermine fundamental vehicle safety. This makes confirming their integrity paramount to the vehicle's overall safety.
- **Firmware.** Hackers can extract and analyze Electronic Control Unit firmware. This allows for the discovery of possible vulnerabilities built into the firmware, as well as the extraction of sensitive data, such as encryption keys. Ensuring that these files are protected and tamper-resistant is critical to overall system security.

Throughout the development process, companies should strive to achieve three cardinal virtues of cyber risk management: becoming *secure*, *vigilant*, and *resilient*.

Throughout the development process, companies should strive to achieve three cardinal virtues of cyber risk management: becoming *secure, vigilant*, and *resilient*. In the spirit of "prevention" being worth more than a "cure," effective risk management begins with securing critical components and preventing system breaches or compromises. Making a system secure is not typically a once-and-for-all proposition. Hardware and software degrade over time, and both the nature and intensity of attacks can change. Consequently, providers should complement security with vigilance—monitoring to determine whether a system is still secure or has been compromised. Finally, when a breach occurs, limiting the damage and reestablishing normal operations are much more easily and effectively achieved when there are processes in place to promptly neutralize threats, prevent further spread, and recover.[29]

Conclusion

SECURING the new mobility ecosystem is a daunting challenge, and the stakes are high. In a swiftly changing world, the future of mobility continues to become more complex, leaving many questions unanswered and many more unasked. As many automakers and technology companies push rapidly toward a world of shared autonomous vehicles, consumers are approaching the prospect of self-driving cars with caution.[30] Without assurances that vehicles will function safely and securely, those investments could be for naught.

Thankfully, many of the cyber risks posed by the future of mobility have been confronted before.

Thankfully, many of the cyber risks posed by the future of mobility have been confronted before. By taking the hard-earned lessons learned from other industries, the extended auto industry can keep itself ahead of hackers and other adversaries. A few of the steps to take:

- Leverage enterprise IT processes for data privacy and data decommissioning
- Implement encryption and code signing to protect the integrity of system software
- Develop standards of practice for secure development of critical vehicle systems
- Enforce developed standards on their suppliers, similar to payment card processors

By taking these cues from others that have grappled with securing critical digital infrastructure—including current efforts to protect connected cars—the extended global auto industry can help make hopping into a shared driverless car as blasé as getting behind the wheel is today.

ENDNOTES

1. Aurelio Locsin, "Is air travel safer than car travel?," *USA Today*, http://traveltips.usatoday.com/air-travel-safer-car-travel-1581.html.
2. See Scott Corwin, Nick Jameson, Derek M. Pankratz, and Philipp Willigmann, *The future of mobility: What's next?*, Deloitte University Press, September 14, 2016, http://dupress.deloitte.com/dup-us-en/focus/future-of-mobility/roadmap-for-future-of-urban-mobility.html; and Scott Corwin, Joe Vitale, Eamonn Kelly, and Elizabeth Cathles, *The future of mobility*, Deloitte University Press, September 24, 2015, http://dupress.com/articles/future-of-mobility-transportation-technology/.
3. Lorenzo Franceschi-Bicchierai, "Car hacking looks much cooler in 'Fate of the Furious' than it does IRL," *Motherboard*, March 9, 2017, https://motherboard.vice.com/en_us/article/fast-and-furious-8s-car-hacking-might-be-the-most-credible-stunt-in-the-movie.
4. Corwin et al., *The future of mobility*.
5. Simon Ninan, Bharath Gangula, Matthias von Alten, and Brenna Sniderman, *Who owns the road? The IoT-connected car of today—and tomorrow*, Deloitte University Press, August 18, 2015, https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-automotive-industry.html.
6. Carol Mangis, "How to recycle old electronics," *Consumer Reports*, April 22, 2016, www.consumerreports.org/electronics-computers/how-to-recycle-old-electronics/.
7. North American Electric Reliability Corp., "Standards," accessed October 26, 2016, www.nerc.com/pa/stand/Pages/default.aspx.
8. Marianne Swanson and Barbara Guttman, "Generally accepted principles and practices for securing information technology systems," National Institute of Standards and Technology, September 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.
9. National Highway Traffic Safety Administration, "U.S. DOT issues federal guidance to the automotive industry for improving motor vehicle cybersecurity," October 24, 2016, www.nhtsa.gov/press-releases/us-dot-issues-federal-guidance-automotive-industry-improving-motor-vehicle.
10. David Gelles, Hiroko Tabuchi, and Matthew Dolan, "Complex car software becomes the weak spot under the hood," *New York Times*, September 27, 2015, https://nyti.ms/2mF6Teu.
11. Kenneth van Wyk, "The true root causes of software security failures," *Computer World*, May 21, 2013, www.computerworld.com/article/2497957/security0/the-true-root-causes-of-software-security-failures.html.
12. Pete Bigelow, "NHTSA mulls role of car-hacking researchers, but time's ticking," *AutoBlog*, October 10, 2015, www.autoblog.com/2015/10/10/nhtsa-car-hacking-researchers/.
13. Joshua Jamerson, "Verizon to buy Fleetmatics for $2.4 billion," *Wall Street Journal*, August 1, 2016, www.wsj.com/articles/verizon-to-buy-fleetmatics-for-2-4-billion-1470055429.
14. Miro Enev et al., "Automobile driver fingerprinting," *Proceedings on Privacy Enhancing Technologies*, 2016 (1), pp. 34–51, www.autosec.org/pubs/fingerprint.pdf.
15. Uber, "Uber & Spotify = Music for your ride," November 17, 2014, https://newsroom.uber.com/uber-spotify-music-for-your-ride/.

16. Iron Mountain, "Enterprises have room for improvement in secure IT asset disposition," May 8, 2014, www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/Sponsored/Enterprises-Have-Room-for-Improvement-in-Secure-IT-Asset-Disposition.aspx.

17. Troy Hunt, "Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs," February 24, 2016, www.troyhunt.com/controlling-vehicle-features-of-nissan/.

18. Global Information Assurance Certification, "A content delivery case study," June 23, 2003, www.giac.org/paper/gsec/3503/content-delivery-case-study/105714.

19. National Highway Traffic Safety Administration, *Federal Automated Vehicles Policy*, September 2016, www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.

20. Victor Oluwajuwon Badejo, "Case study: Payment card industry—data security standards (PCI–DSS)," March 11, 2016, www.slideshare.net/VictorOluwajuwonBade/case-study-on-pci-dss.

21. North American Electric Reliability Corp., "Standards."

22. David Shepardson, "FBI warns automakers, owners about vehicle hacking risks," *Reuters*, March 17, 2016, www.reuters.com/article/us-fbi-autos-cyber-idUSKCN0WK0BB.

23. Ryan Beene, "NHTSA chief vows action this year on cybersecurity," *Automotive News*, January 19, 2016, www.autonews.com/article/20160119/OEM06/160119727/nhtsa-chief-vows-action-this-year-on-cybersecurity.

24. Automotive Information Sharing and Analysis Center, www.automotiveisac.com/, accessed March 27, 2017.

25. Auto Alliance, "Framework for automotive cybersecurity practices," January 14, 2016, https://autoalliance.org/wp-content/uploads/2017/01/Framework.AutoCyberBestPractices.14Jan2016.pdf

26. Bluetooth, "Membership agreements," www.bluetooth.com/membership-working-groups/membership-types-levels/membership-agreements, accessed March 27, 2017.

27. Ibid.

28. Bluetooth, "Qualification enforcement program," www.bluetooth.com/develop-with-bluetooth/qualification-listing/qualification-enforcement-program, accessed March 27, 2017.

29. Irfan Saif, Sean Peasley, and Arun Perinkolam, "Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age," *Deloitte Review* 17, July 27, 2015, https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html.

30. Craig Giffi, Joe Vitale, Ryan Robinson, and Gina Pingitore, "The race to autonomous driving: Winning American consumers' trust," *Deloitte Review* 20, https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-20/winning-consumer-trust-future-of-automotive-technology.html, accessed January 24, 2017.

ABOUT THE AUTHORS

LEON NASH

Leon Nash is a principal in Deloitte & Touche LLP's Cyber Risk Services practice, with nearly two decades of helping his clients be secure, vigilant, and resilient in the face of an ever-growing cyber threat. Nash has served his clients by establishing cyber security programs, developing robust security architectures, delivering enterprisewide security implementations (identity and access management, enterprise resource planning security, etc.) using industry-grade technologies to solve critical business problems across a multitude of disciplines and industries. While he serves clients in a number of industries, Nash has spent the past seven years focused on cybersecurity in the automotive sector.

GREG BOEHMER

Greg Boehmer is a senior manager in Deloitte & Touche LLP's Cyber Risk Services practice, specializing in cyber security for the automotive industry and public utilities. He has more than a dozen years of risk management consulting and auditing experience, including work on three continents. His experience focuses on SAP security, controls, and governance, risk, and compliance, and he has researched and published additional articles related to cybersecurity and the future of mobility. Boehmer holds 10 professional certifications. He can be found on LinkedIn.

MARK WIREMAN

Mark Wireman is an IT practitioner and an educator in Deloitte & Touche LLP with 17 years in the industry, specializing in software engineer, application security, and information security within the automobile, retail, manufacturing, defense, finance, oil and gas, and health industries. Wireman has performed software development and integration, application security assessments, third party software risk, and secure software and product dlc assessments and integrations. Wireman is recognized as a technical specialist for his ability to combine practitioner and management views to create a comprehensive solution for his clients.

ALLEN HILLAKER

Allen Hillaker is a consultant in Deloitte & Touche LLP's Cyber Risk Services practice, specializing in automotive cybersecurity. He has three years of automotive cybersecurity testing and research experience, with work for both domestic and foreign automotive companies. Additionally, he has experience with critical infrastructure security, including execution of practical attacks on transportation networks and traffic management equipment.

ACKNOWLEDGEMENTS

The authors would like to thank the following advisers who helped shape the perspectives in this article: **Scott Corwin**, **Irfan Saif**, and **Derek Pankratz**. Special thanks to **Vikram Salgaonkar** and **Robert Carton** for their significant contributions to the development of this article. Thanks to **Matthew Budman** for his editorial guidance and reviews of the article at multiple stages. **Joe Kwederis** and **Jeff Buccola** provided additional research and review support.

CONTACTS

Leon Nash
Principal
Deloitte & Touche LLP
+1 714 436 7879
leonnash@deloitte.com

Greg Boehmer
Senior manager
Deloitte & Touche LLP
+1 313 394 5524
gboehmer@deloitte.com

Scott Corwin
Future of Mobility practice leader
Managing Director
Deloitte Consulting LLP
+1 212 653 4075
scottcorwin@deloitte.com

Philipp Willigmann
Senior manager
Strategy
Monitor Deloitte
Deloitte Consulting LLP
+1 347 549 2804
phwilligmann@deloitte.com

Joe Kwederis
Principal
Deloitte & Touche LLP
+1 313 396 3813
jkwederis@deloitte.com

Mark Wireman
Senior manager
Deloitte & Touche LLP
+1 704 887 1609
mwireman@deloitte.com

Allen Hillaker
Consultant
Deloitte & Touche LLP
+1 313 806 5837
ahillaker@deloitte.com

 Follow @DU_Press

Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

About Deloitte