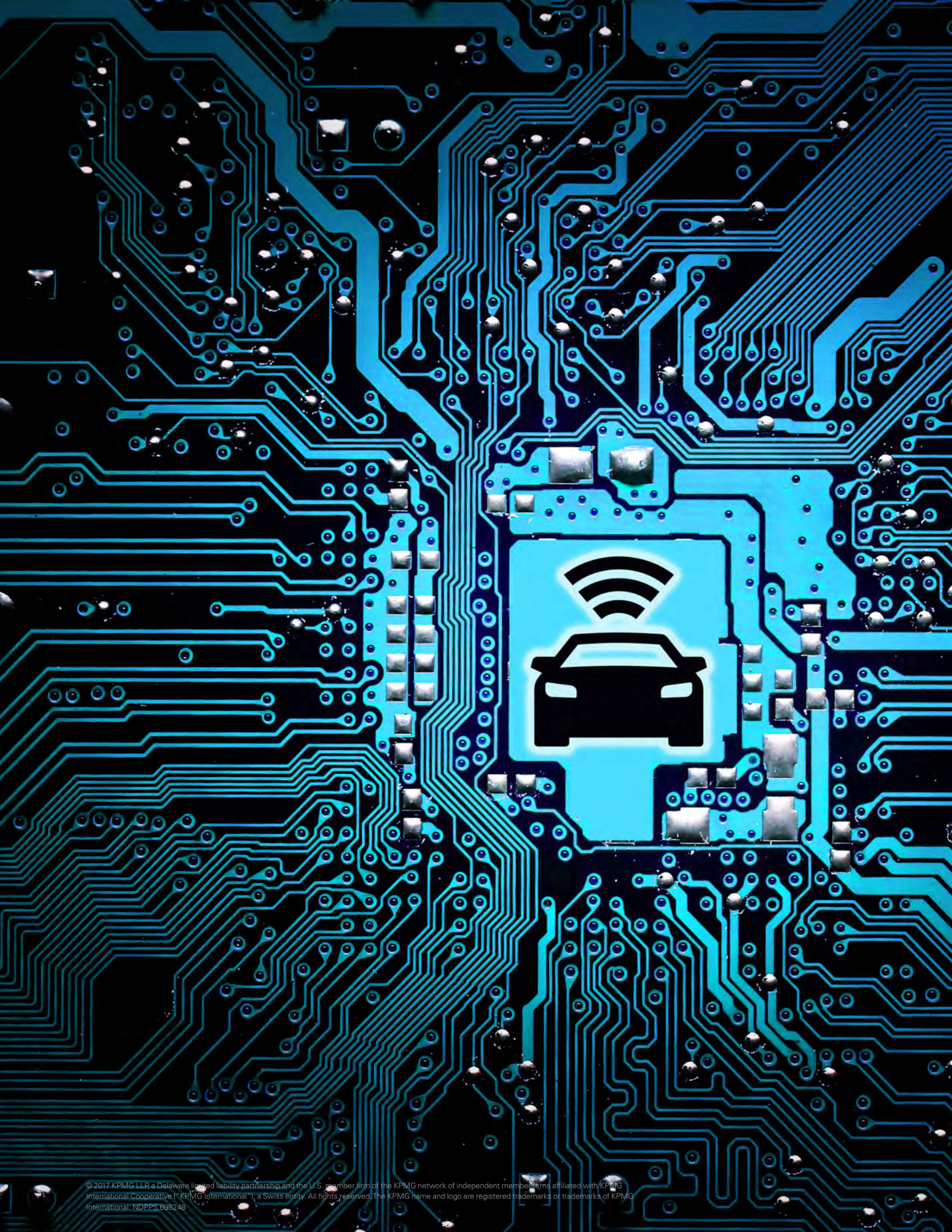
KPMG

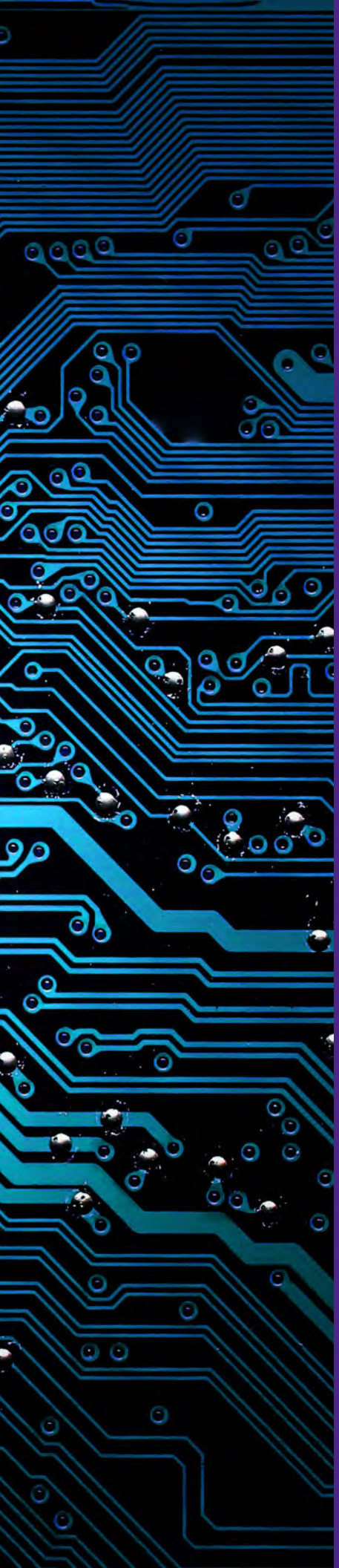
Protecting the fleet... and the car business

Today's cyber-physical threats disrupt automotive operating models

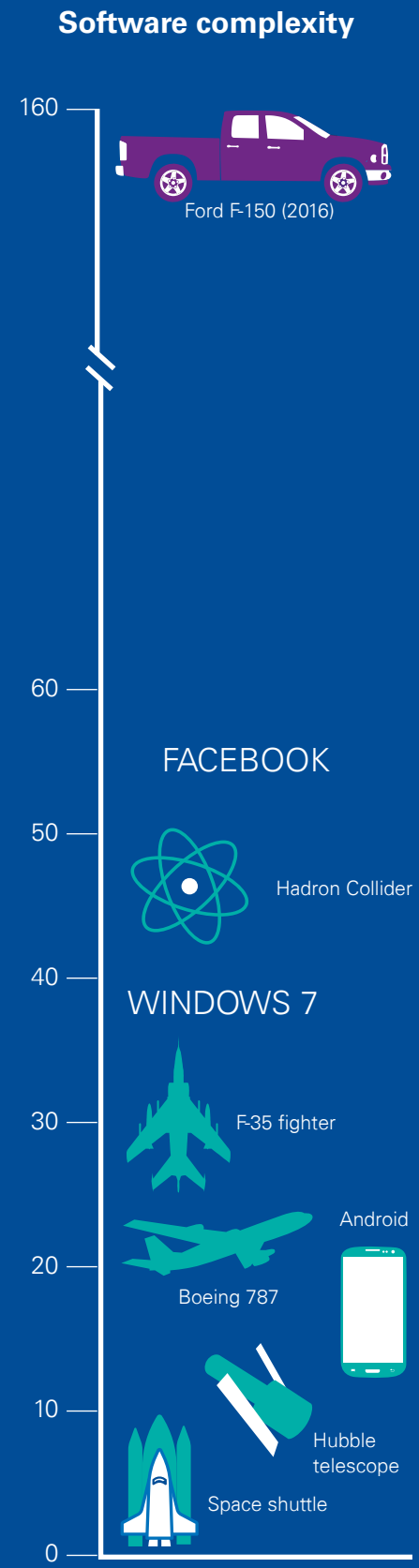
Sponsored by KPMG's U.S. Manufacturing Institute Automotive Center

www.kpmg.com/us/automotive





Contents



Ready for a car hack... times one million?

Modern vehicles are marvels of innovation. Even today's most popular models are chock full of technology and connectivity. The average car contains more than 150 million lines of code, plus multiple individual computers and a vast number of wireless connections to internal and external communication channels[1]. It can stream music, send texts, offer real-time traffic information and personalized roadside assistance, detect nearby activity through sensors, and even drive autonomously in controlled situations.[2] This immense amount of on-vehicle technology has created automobiles that have more lines of code than a 2016 Ford F-150, an F-35 fighter, and a Boeing 787.[1]

Moreover, vehicles and their users are data hungry. By the end of 2017, North American users will consume an average of 6.9 gigabytes each month. Five years from now, that number is expected to more than triple.[3] When you couple these figures with the rollout of 5G by the cell carriers in all major metropolitan areas—which will enable the data speeds necessary for additional vehicle innovation and autonomy—it is clear that the "Internet of Cars" (IoC) is already here.

The increasing complexity of vehicle technology has countless benefits, but at the same time, it creates a real risk of cyber attack—a risk we fear many companies in the automotive industry may be underestimating.

Vehicle hacking incidents have been well-documented over the past several years, drawing attention to the issue within the industry. According to the KPMG 2017 U.S. CEO Outlook Survey, 85 percent of automotive executives say their organizations will increase cyber security spending in the next three years, and 56 percent expect "significant investments"—more than all other industries surveyed.[4] Many manufacturers have made huge strides in addressing cyber security issues within their vehicles, taking various approaches to the challenge even as the threat landscape continues to evolve and solutions continue to emerge and mature.

Finding and fixing vulnerabilities in the hardware and software embedded inside individual cars will continue to persist as a key issue for automakers. However, we think there is an additional risk that automakers need to address—a risk that goes far beyond the traditional cyber threat of singular vehicle attacks, which has been the focus of much of the cyber security conversation in the industry.

That risk is the potential hacking of entire fleets of cars (see sidebar on page 3). Due to the potential platformwide impact of a cyber attack on a fleet of connected vehicles that share common operating systems, software, or

[1] "Vetronics, Software and Cybersecurity" (Wind River, AeroAuto Conference, May 4, 2017)
[2] "Auto industry diverges on timeline for self-driving cars" (*Automotive News*, March 16, 2017)
[3] "We'll all be crazy data hogs by 2022" (CNET, June 13, 2017)
[4] KPMG 2017 U.S. CEO Outlook Survey (KPMG LLP, 2017)

hardware, we believe that fleetwide attacks represent the next big disruptive threat to the automotive industry. In fact, we submit that all future cyber attacks may be fleetwide attacks.

Tesla chief executive officer and world-renowned innovator Elon Musk seems to agree with KPMG's assessment. "My top concern from a security standpoint [is]...making sure that a fleet-wide hack or any vehicle-specific hack can't occur," Musk stated in July 2017.[5]

Although many companies are beginning to focus on preventing intrusions of their corporate networks and building cyber security into the design of individual cars, few are prepared for the business, technological, privacy, and operational challenges of managing a cyber attack on a connected vehicle fleet, potentially impacting millions of cars both in production and deployed on the road. Most carmakers did not consider the economics of managing a fleetwide cyber attack when they initially started embedding so much technology and connectivity into their fleets. Today we are seeing opportunities for after-market solutions to mitigate fleetwide cyber risks by providing bolt-on security controls. But even now—when malware and ransomware commonly affect millions of computers all at once—today's fleetwide cyber risks are not addressed in the current automotive operating models.

KPMG has proudly served as an automotive industry thought leader on this topic (see next page). Our forward-looking insights on the convergence of the automotive and technology sectors help clients prepare for disruption, pivot smartly, and come out ahead.

Now, we are focusing our attention on the current cyber and physical risks facing modern connected car fleets, with the aim of helping automotive companies take the right steps to protect the drivers and users of their fleets, their fleets of vehicles themselves, and their businesses.

Read this paper for an inside look at how fleetwide cyber threats:

— Could play out on a small and large scale

— Will change automotive operating models

— Can be managed with the right risk mitigation strategies and innovative technology.

[5] "Elon Musk's top cybersecurity concern: Preventing a fleet-wide hack of Teslas" (CSOonline.com, July 17, 2017)

How does KPMG define a vehicle fleet?

In this piece of thought leadership, we define a fleet as a group of individual vehicles that connects to a common technology platform through shared operating systems, software, or hardware. A fleet might include all the vehicles created by a single manufacturer, or vehicles from different manufacturers that use the same parts suppliers. We believe exploiting vulnerabilities in the common technologies shared by the vehicles in a fleet will become increasingly attractive to cyber attackers, given the potential platformwide impact.

Automotive investments in cyber security in the next three years

56% **Significant** investment

29% **Incremental** investment

15% **No new** investment

0% **Decrease** investment

KPMG 2017 U.S. CEO Outlook Survey

“As vehicle connectivity continues to rapidly increase, so does the volume of data cars churn out. Data is created, processed, and transmitted both within and around the vehicle where the integrated cloud to fog policy-based systems determine which data is wirelessly sent into the cloud. Securing this growing communication ‘fog’ is paramount in the connected car era.”

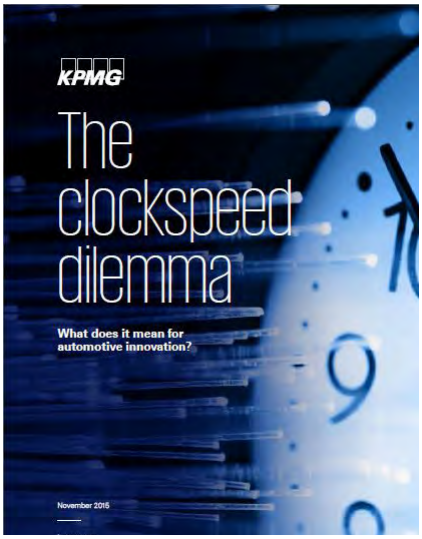
Maciej Kranz, Vice President of Strategic Innovation at Cisco

“Our study of automotive industry and cyber security trends indicates that singular vehicle attacks may soon be a thing of the past. Fleetwide attacks—which will have a much more significant scope and impact and a much greater potential payoff for cyber attackers—threaten to disrupt not only automotive security but also many other aspects of the automotive business and operating model. The time is now for companies to take notice and evolve.”

Gary Silberg, National Automotive Leader, KPMG

Read more KPMG insights on the future of the automotive industry

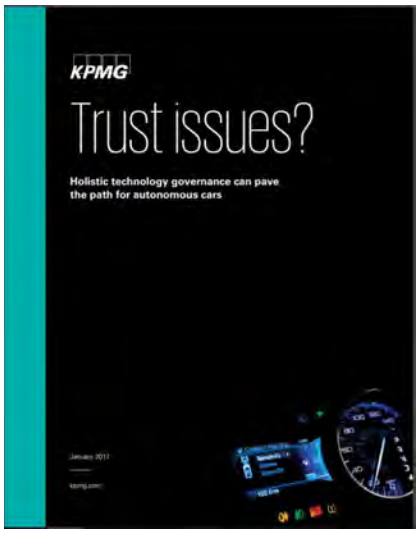
The clockspeed dilemma: What does it mean for automotive innovation?



Your connected car is talking. Who’s listening?

Test-driving vehicle cybersecurity … as regulators help define the rules of the road

Trust issues? Holistic technology governance can pave the path for autonomous cars



What is hiding in the wireless communication fog?

A white hat researcher takes control of an SUV's steering wheel and brakes while it speeds down a highway.[6] Thieves exchange crowbars for laptops to hack vehicle electronics and steal parked cars.[7, 8] Law enforcement eavesdrops on conversations inside cars by "bugging" the dashboard computer.[9]

Prior vehicle cyber incidents have been well publicized. And they have been pretty frightening. But this may be just the beginning of what is to come.

As cars become more connected and complex, this leads to greater cyber security risk and privacy exposure and potential for failure. The growing number of remote communication devices and platforms in connected cars has created a wireless communication "fog" engulfing the vehicle that is dense with hidden cyber risks.[10] There is a steady stream of chatter and noise radiating from the car and colliding with the "fogs" of the other cars it encounters, increasing the amount of attack opportunities. A car fitted with vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), cellular, Bluetooth, and Wi-Fi connections, for example, has a much greater attack surface than a car with only a single, isolated computer system. In fact, recently, a malware attack was identified that could put 5.3 billion devices with Bluetooth signals at risk.[11]

Moreover, the fog will densen as the majority of the cars manufactured in the next few years will be connected—not just the newest models or the premium brands. According to BI Intelligence, the connected car market is growing 10 times as fast as the overall car market. They estimate that by 2020, 75 percent of cars shipped globally will be connected, equaling 220 million connected cars on worldwide roads.[12]

[6] "Remote Exploitation of an Unaltered Passenger Vehicle" (illmatics.com, Dr. Charlie Miller and Chris Valasek, August 10, 2015)

[7] "Car hacking: Thieves armed with laptops are stealing cars" (CSOonline.com, July 7, 2016)

[8] "Thieves Go High-Tech to Steal Cars" (*Wall Street Journal*, July 5, 2016)

[9] "Cartapping: How Feds Have Spied On Connected Cars For 15 Years" (Forbes, January 15, 2017)

[10] According to Webopedia, "fog computing" is an industry term used among information technology companies. Initially created by Cisco, it refers to extending cloud computing to the edge of an enterprise's network.

[11] "Billions of Bluetooth devices could get hit by this attack" (CNET, September 12, 2017)

[12] "The Connected Car Report: Forecasts, competing technologies, and leading manufacturers" (BI Intelligence, April 29, 2016)

“It is clear that the Internet of Cars (IoC) is already here.”

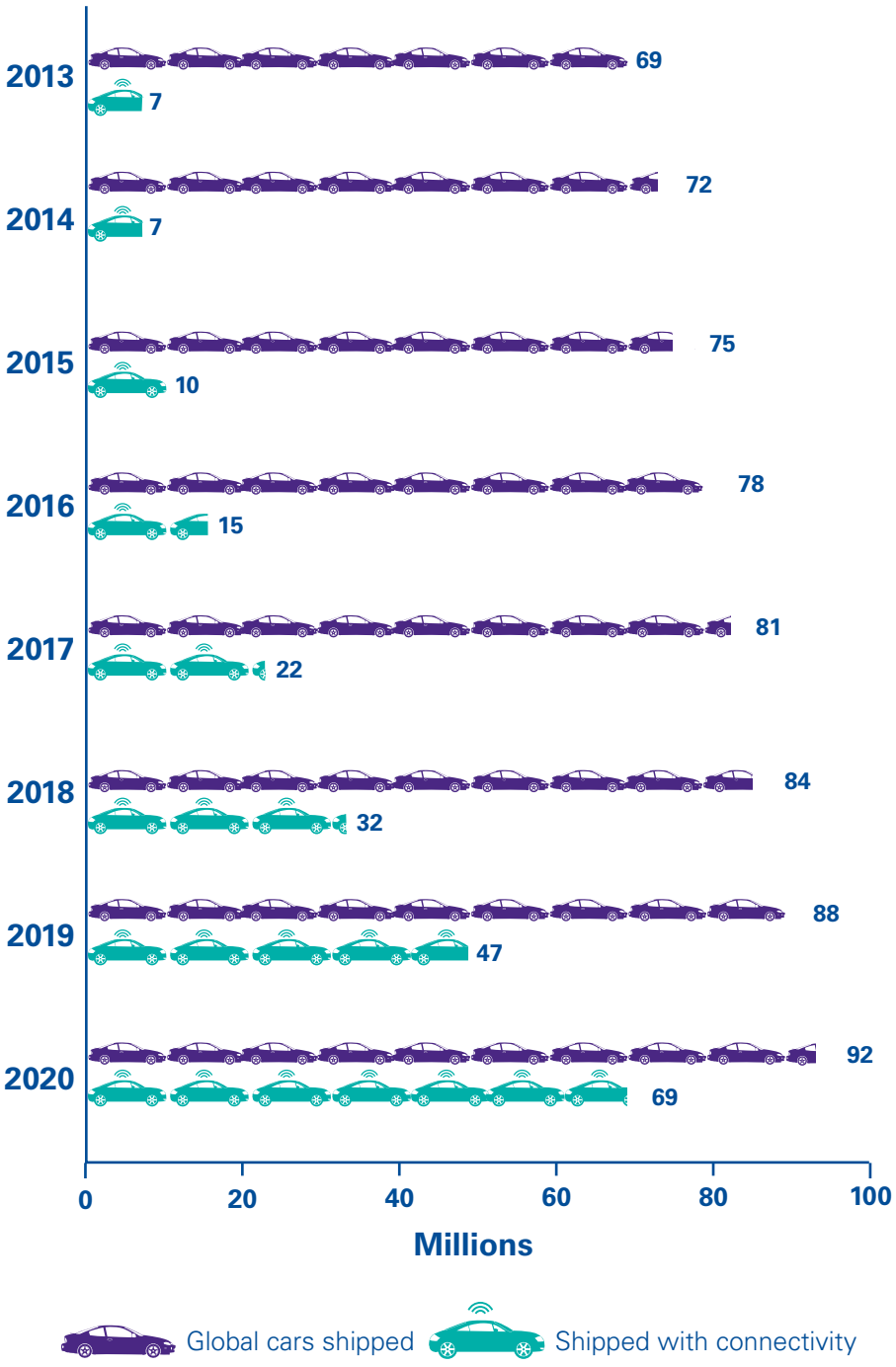
Michael Krajecki, Director, KPMG Emerging Technology Risk Services

“The massive complexity of the connected car ecosystem makes it vulnerable to cyber attack. Each vehicle’s connection to the external environment, including other vehicles, could potentially be exploited to breach the systems of entire fleets of vehicles.”

Ron Plesco, Principal, KPMG Cyber Security Services

Connected car shipments forecast (Global)

Five-year (2015–2020) CAGR 45%



BI Intelligence, 2017

Sporting navigation, infotainment, roadside assistance, and other high-tech features, the typical car today is part of the IoC, an internet-connected network. That means even if the car's own code and software are super secure, it is still vulnerable to cyber attacks. Lurkers in the bushes, a crowded mall, or a foreign country can all potentially penetrate the car, largely unseen, by taking advantage of weaknesses in the security of a wireless, internet-connected cloud—think Bluetooth and near field communication (NFC)—that is constantly talking and listening.

Or even more likely, an entire fleet.

Consider—from a hacker's perspective—the potential payoff of cyber-attacking not one car, but 100, 1,000, or 1 million. With the connectivity that is out there today, every single car in the fleet constantly has an always-listening, open "ear" to the external environment, eager to get its next command. And because of the broadcast reach of the internet, the same over-the-air (OTA) attack technique that works on a single car can be applied toward all the cars connected to it with relative ease.[13] For approximately the same cost and effort, a fleet attack can potentially have a much greater impact. The question boils down to what the threat actor is after—easy money by stealing and selling the users' personally identifiable information (PII), or ransom attacks?

This changing value proposition may attract a new type of threat actor, such as state-sponsored hackers. And most importantly it may mean isolated incidents may soon be a thing of the past, giving way to an influx of fleetwide cyber attacks. That is bad news for the automotive industry—unless the players change their approach.

The first step is an understanding of the governing of risks. As such, we have identified some of the major emerging cyber threats with real-world privacy impact that carmakers must be prepared for. On the following pages, we have highlighted some progressively serious cyber risks that could happen not just to an individual car, but to entire fleets of cars.

[13] "Remote Exploitation of an Unaltered Passenger Vehicle" (illmatics.com, Dr. Charlie Miller and Chris Valasek, August 10, 2015)

Want to unplug your car? Good luck.

The connected car is here and it is here to stay. Not only are most cars online, but if you try to take them offline, you are also likely to run into some problems.

That is what happened to a security researcher last year when he tried to disable the always-on connected system in his car. The researcher could not do it himself. Not only were the circuit board and other components of the device embedded deep in the dashboard, but he also found out that removing the system would actually void his warranty. The employees at the carmaker's dealership were at a loss. Even the corporate offices could not help. They told him removing the system was impossible, and even if it could be done, it may interfere with some safety features. Ultimately, the only solution—eventually proffered by the carmaker—was to have dealership mechanics put the vehicle in "flight mode," which severs the connection of the car to the cellular network.

Adding to the problem is that most manufacturers do not make it easy to take a lesser step toward data privacy—wiping personal data from a car's onboard computer. That means vehicles that have been rented or sold could unwittingly pass sensitive information—such as calendars, contacts, and phone records—on to the new owner.

Taking out a fleet before it is on the road

The infamous "WannaCry" virus that hit global companies in spring 2017 demonstrates the potential enterprise impact of a cyber attack, as manufacturers continue to add more connectivity and technology to their factories. Honda was forced to shut down production at a plant in Japan after the company discovered that ransomware had made its way through the company's computer networks. Renault and Nissan also had factories infected by WannaCry.

"Honda Shut Down Plant Impacted by WannaCry" (ThreatPost, June 21, 2017)

"To hackers, data is like gold. And as cars become centers of consumers' connected lives, their networks are overflowing with it: location data, credit card information, contacts and emails, and much more."

Doron Rotman, Managing Director, KPMG IT Audit and Assurance

Vehicle thefts

Attack once. Steal many. That is the reality of car theft today.

Cyber criminals have already succeeded at intercepting keyless entry commands in parking lots and even home garages, allowing them to simply drive off with the car whenever they would like.[14] That same theft technique could potentially be applied on a much larger scale. For example, an attacker could plant a tiny device in a restaurant valet stand that captures the wireless unlock codes for dozens or even hundreds of vehicles. All diners would finish their meals satisfied, only to realize they are all victims of a massive car theft.

Or, cyber criminals could mastermind an even bigger loot—and present a real safety risk to boot. Consider that many cars today are equipped with expansive remote command features that are processed through a cloud-based application. Using those commands to do things like unlock the car or press the ignition does not even require proximity to the vehicle. For example, one of the authors of this paper uses this command every day to start his car and prechill the environment. As such, an attacker could potentially send remote unlock commands to an entire fleet of cars at once and drive away with them one by one.

Consumer data breaches

Cars have become the centers of consumers' connected lives, controlling volumes of valuable sensitive data and PII—a person's location, credit card information, e-mails and phone calls, travel history, and much more. What better incentive for a hacker to break into a car's network? This information has a real-world darknet street value. It is no wonder cyber criminals have invented ways to remotely wiretap into vehicles through on-board assistance features as well as capture information from the broadcast signals cars send out.

But it is one thing to access the private data of one individual. It is quite another to get it from 500,000 people to use over time on the sly. To organized criminals, the street value of all of that data is immense, making car fleets a highly attractive target for cyber attack.

Clever hackers could use the data in other sinister ways, too. For example, hackers could use it to profile different types of victims based on a number of attributes, such as specific locations, time of day, vehicle cost, etc. Consider the personal privacy impact and overall damage that could be done if a hacker breaches the vehicle network of a corporate after-market fleet, such as an enterprise's black car service for executive travel or a package delivery service, such as an armored car fleet. With sensitive routing data and mapping data at their fingertips, hackers would have the opportunity to locate a company's valuables (both physical and digital).

Physical safety

Physical safety has been the hallmark of the automotive industry for years. Passengers feel safe because of all of the redundant technology built into the car. However, core aspects of the connected car ecosystem potentially create a tremendous amount of risk to drivers and passengers.

[14] "Vulnerability In Car Keyless Entry Systems Allows Anyone To Open And Steal Your Vehicle" (Forbes, May 12, 2015)

For one, the expanded network controlling the car goes into the internet to unseen places around the world, meaning attacks can originate from anywhere, including criminal attacks from hackers or terrorists. Attackers can also target third parties and other intermediaries in the ecosystem to gain access to vehicle users' data and/or the car. And when you consider the interconnected nature of the automotive supply chain, the risk expands further. With many manufacturers sharing common suppliers of hardware and software components and common clouds, a cyber breach to a key supplier of safety-critical parts, such as chip sets that control braking mechanisms, could easily ripple across the entire industry.

Secondly, errors or technical failures in the network can occur. Vehicle mechanical components are increasingly controlled by technology, which means a cyber breach can put drivers and passengers in physical danger. In fact, white hat security researchers have successfully sent remote commands to moving vehicles, impacting speed, steering, and braking systems.

Vulnerabilities in the connected car ecosystem mean that a hacked car could suddenly jeopardize physical safety. For example, a hacked car could automatically brake or accelerate to 120 miles per hour all by itself and swerve across a couple of lanes of traffic. This potential was demonstrated by security researchers in 2015.[15] And it might not just happen to a single car, but to thousands of other cars connected to the first car's ecosystem.

It is not hard to imagine what is at stake from a fleetwide cyber attack. While there are many potential mass-attack scenarios, the worst of all might be the idea of a cyber criminal turning a whole fleet of cars into remote-controlled weapons of terrorism. A cyber attacker could conceivably remotely start an entire garage of cars—similar to the keyless entry relay attack—and weaponize a whole convoy of cars. Or, hackers may be able to attack the sophisticated battery control systems that keep explosive materials inside cars from overheating. Some cars contain explosive components such as 1,000 pound battery packs or compressed gas.

"With the ability for thieves to cyber attack many cars at once, 'attack once, steal many' is the best characterization of today's grand theft auto threat."

Danny Le,
Principal and Automotive Leader,
KPMG Cyber Security Services

"To organized criminals, the street value of vehicle data is potentially immense, making car fleets a highly attractive target for cyber attack."

Ron Plesco, Principal,
KPMG Cyber Security Services

[15] "Remote Exploitation of an Unaltered Passenger Vehicle" (illmatics.com, Dr. Charlie Miller and Chris Valasek, August 19, 2015)

Cyber disruption will transform automotive businesses

Fleetwide cyber attacks are not just scary from the consumer security and privacy perspective. As a completely new threat to automotive companies, they promise to significantly change both the cost and the method of doing business.

As we predicted in our 2016 thought leadership paper on autonomous driving, *I see. I think. I drive. (I learn.)*, we have entered a new era in the automotive industry, propelled by massive technological and business model change. In the near future, most car companies will not simply be automakers anymore. Rather, they will enter a major new market for mobility services related to autonomy, mobility, and connectivity.

Already, many leading automotive companies recognize that providing mobility services is a much more lucrative business model than the traditional approach to automotive sales. For example, when Jim Hackett took over as Ford's CEO—he previously led the company's smart mobility group—he announced the company's new direction, including a deeper focus on connected cars and specifically big data, artificial intelligence (AI), and robotics.[16] More recently, Hackett said Ford will work to drive more revenue through nontraditional mobility businesses, including potentially partnering with disruptive car sharing, ride hailing, or parking start-ups.[17]

The traditional automotive business model relies heavily on one-time sales of vehicles that take 7–10 years to come to market and lose value as soon as the purchaser drives off the lot. By contrast, the mobility market—which KPMG's

[16] "Ford names Jim Hackett CEO to take its connected car plans up a gear" (Techcrunch.com, May 22, 2017)

[17] "Ford CEO Jim Hackett Is Putting Together a 100-Day Plan. Here's a Peek." (*Fortune*, August 17, 2017)

What does a cyber misstep cost?
According to KPMG's Consumer Loss Barometer report, automotive customers are extremely sensitive about cyber security as it relates to their cars. Our research shows cyber security issues will cause some consumers to even abandon a brand—forever.

If your car was hacked, how would that change your perception of that particular automaker?

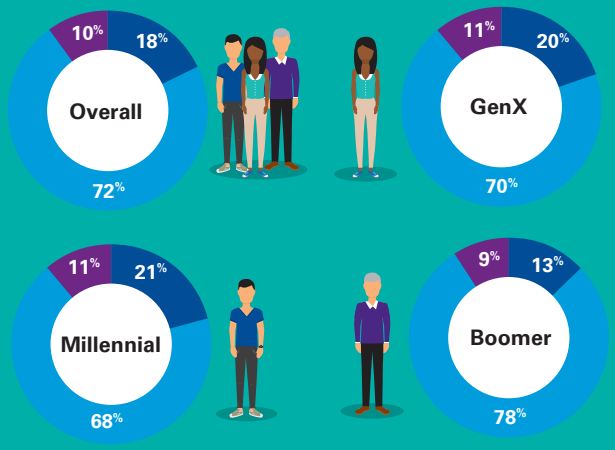
Your brand is at risk

- Huge negative impact
- Negative impact (but still loyal to that automaker)
- Moderate negative impact
- No impact

Consumer Loss Barometer (KPMG LLP, 2016)

If a particular vehicle brand was hacked, how would that impact your consideration to purchase from that particular automaker?

Your sales are at risk



- No impact
- Greater wariness of buying from that automaker
- I would not buy (ever) from that automaker

Automotive practice anticipates will be worth more than $1 trillion by 2030—will create profit potential across the entire life cycle of the car, while also driving massive growth in miles traveled.

To participate in the mobility ecosystem, automakers will have to recognize and embrace the power of the fleet. Even now, what matters most to an individual car's performance is often the ability to interact with the larger fleet and the ecosystem in which it drives. Connectivity to the network is essential for many of the core product functions automotive customers demand, including infotainment, mapping, routing, and advanced driver assistance systems (ADAS). And looking to the not-so-distant future, constant interaction with the fleet will be required to build real-world driving datasets to train self-driving algorithms to eventually power fully autonomous commercial vehicles.

That is where cyber security comes in.

Protecting the fleet will require carmakers to actively maintain connectivity and provide real-time security support to embedded software on millions of vehicles that have already been sold and deployed. That is a significant shift in the traditional automotive operating model, in which fleet problems are dealt with using recalls, and dealer networks and body shops do most of the heavy lifting.

While the industry may not be prepared to secure connected fleets today, it is important to note that the responsibility may not ultimately fall under the manufacturer's purview. It may reside with another player in the ecosystem—a supplier, a third-party service provider, a technology platform, or even a government regulator. Still, numerous industy wide disruptive impacts will follow from the fleetwide cyber threat:

— **Cyber security and privacy will likely become integral to brand value:** Car manufacturers will soon fight for consumer brand loyalty not only through quality, safety, and innovation, but also through establishing a relationship founded on maintaining customer privacy through digital trust. According to KPMG's Consumer Loss Barometer, 82 percent of consumers would be wary or never buy from an automaker if that brand experienced a car hack.[18] The new cyber landscape demands automotive companies think of security and privacy enhancements as competitive differentiators—right alongside quality, safety, and reliability—and manage their reputations accordingly.

"Today, new technologies and changing customer needs are helping us transform personal mobility and deliver new transportation solutions that are safer, more sustainable and better than ever. We believe one of the best ways to deliver these solutions is through greater access to self-driving electric vehicles deployed in sharing networks."

Mary Barra, General Motors Chairman and CEO, to the Orion Assembly, on June 13, 2017

"I believe there is a really big business in autonomous vehicles. I wouldn't be going after it if I didn't think that."

Jim Hackett, Ford CEO, to the *Detroit Free Press,* on June 17, 2017

[18] Consumer Loss Barometer (KPMG LLP, 2016)

> **We will auto-update our cars the same way we auto-update our computers.**

Jono Anderson, Principal, KPMG Strategy

> **Safety and security are the top priorities in developing any type of autonomous vehicle. To protect these connected vehicles, we are bringing proven technologies that are deployed in the datacenter—such as encryption, authentication and virtualization—and bringing them into the vehicle. In addition we are creating an entirely new computing architecture that leverages AI and deep learning to thwart cyber security attacks both in the cloud and in the car.**

Danny Shapiro, Senior Director, Automotive at NVIDIA

— **The rise of OTA service models:** Software is not like hardware; it needs to be patched much more frequently. As such, in the near future, recalls might get pushed aside and replaced by OTA updates—a major technological challenge. In fact, Tesla has already introduced this service model, putting pressure on its competitors. As they follow suit, they may find that service networks become more risky than helpful, as it is very challenging to ensure software and firmware updates do not cause inadvertent issues on vehicles. We expect all cars to receive OTA updates via home Wi-Fi or cellular connectivity, similar to how we enable our computer, TV, iPad, or other devices to auto-update.

— **Emphasis on "the nervous system":** Automakers will need to consider security throughout the design, development, and manufacturing of the connected car "nervous system"—the computer brain that processes data from sensors and cameras and communicates with the external environment. The data and operations centers in the cloud, from which companies manage, monitor and service their fleets, also need to be protected. This means leveraging a "security by design" and "privacy by design" approach, which we describe in further detail in the next section.

— **Changing expectations for suppliers:** Automotive suppliers that are responsible for major hardware and software components in the car will also be impacted, in both what they deliver and how they deliver it. They will need to show their products are as impenetrable as possible, that they embed state-of-the-art security into them, and that they are integrated with the Original Equipment Manufacturer (OEM) security control system. Suppliers will also need to show their own monitoring operations are prepared to respond at speed and scale should an attack occur. They will need an auditable trail all the way back to the raw materials provider to maintain the integrity of the hardware and code.

— **Significant shifts in the auto insurance market:** The emerging cyber security threats to the car and its ecosystem are set against a backdrop of declining vehicle ownership and improved road safety, brought about by greater connectivity, mobility, and autonomy. As such, even the service providers around the car—such as personal automotive insurers—will need to change how they do business. Car insurers will need to innovate new methods of pricing policies and determining coverage(s) aligned to the changing risk landscape, in which roads are safer and therefore both policy sales and premium rates are likely to drop off. While auto insurers may find a profit stream in the newly emerging cyber insurance market, industry trends indicate OEMs will ultimately pressure insurers by considering insurance as a product warranty issue and including coverage of software, hardware, and engineering vulnerabilities—including cyber vulnerabilities—right into the sale price of the car. Consider that if a single car hack happens, automakers could conceivably cover the losses for that specific driver or situation, but if the loss is platformwide, the impact and liability may be larger and more centralized to the OEM.

Clearly, managing the risk of a fleetwide cyber attack will demand that companies all throughout the automotive ecosystem take a new approach, especially with regulators, customers, and suppliers expecting car brands to maintain responsibility for both quality and safety, as has historically been the case. The industry will need to transform many aspects of the business, including how companies develop, service, and support vehicle networks and the assets, capabilities, people, and relationships they prioritize.

Blockchain for automotive cyber security

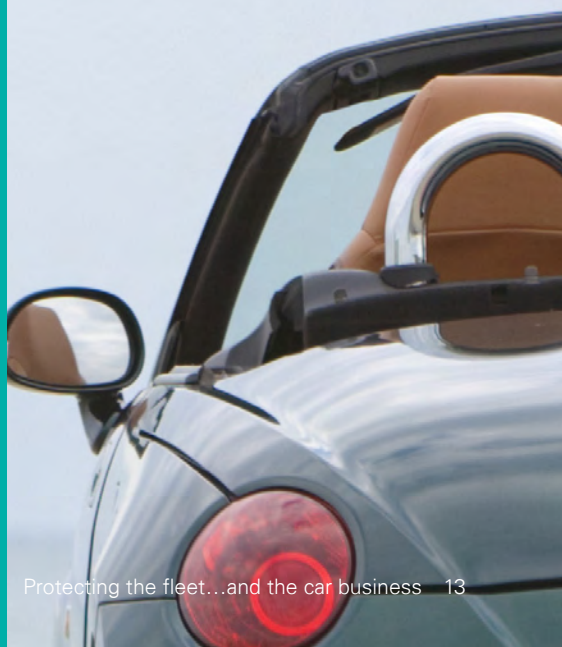
Automotive companies are racing to embrace one of the hottest new technologies to emerge in recent years: blockchain. Blockchain is a distributed ledger file system that keeps records of digital transactions that are maintained by the participants in the blockchain. The files within the blockchain are composed of blocks. Each block includes a cryptographic signature of the previous block, creating an ultrasecure record that cannot be altered and is transparent.

Blockchain has a number of potential cyber security-related applications in the automotive industry. Automotive companies are considering deploying it—or in some case, have already deployed it—to enhance cyber security:

— **Manufacturing, supply chain, and logistics:** Blockchain technology can be used to register and secure any data that is important for managing the supply chain. The ledger would make it possible to trace back all parts to every supplier—even to the raw materials. For example, think of every part having its own encrypted and identifiable digital identity in the blocks, thereby enabling the instant identification of fraudulent parts. Toyota recently partnered with MIT to form a consortium of manufacturers focused on applying blockchain to improve data sharing between cars, rideshare transactions, and usage-based insurance offerings.

— **Sales, operation, and service:** There are various types of data involved in vehicle operations in this era of connected cars, and soon, autonomous cars. There's customer data for purchase and finance, service, and infotainment. There's vehicle data related to telematics, parts, warranties, and service. There's shared data related to V2V communication. Blockchain technology can be used to keep that data secure.

"Toyota pushes into blockchain tech to enable the next generation of cars" *(Techcrunch.com, May 22, 2017)*



Steering the way to more secure fleets

Cyber security can no longer be viewed as a corporate challenge. It is a much broader and more complex engineering, production, and operational challenge—and it requires a new approach.

To combat against the infiltration of software, electronics, computing platforms, communication networks, and data across the connected automotive ecosystem, carmakers will need to develop robust and multidimensional security programs that encompass the individual vehicle, the connected fleet, the automotive business, and the wide-ranging supply chain.

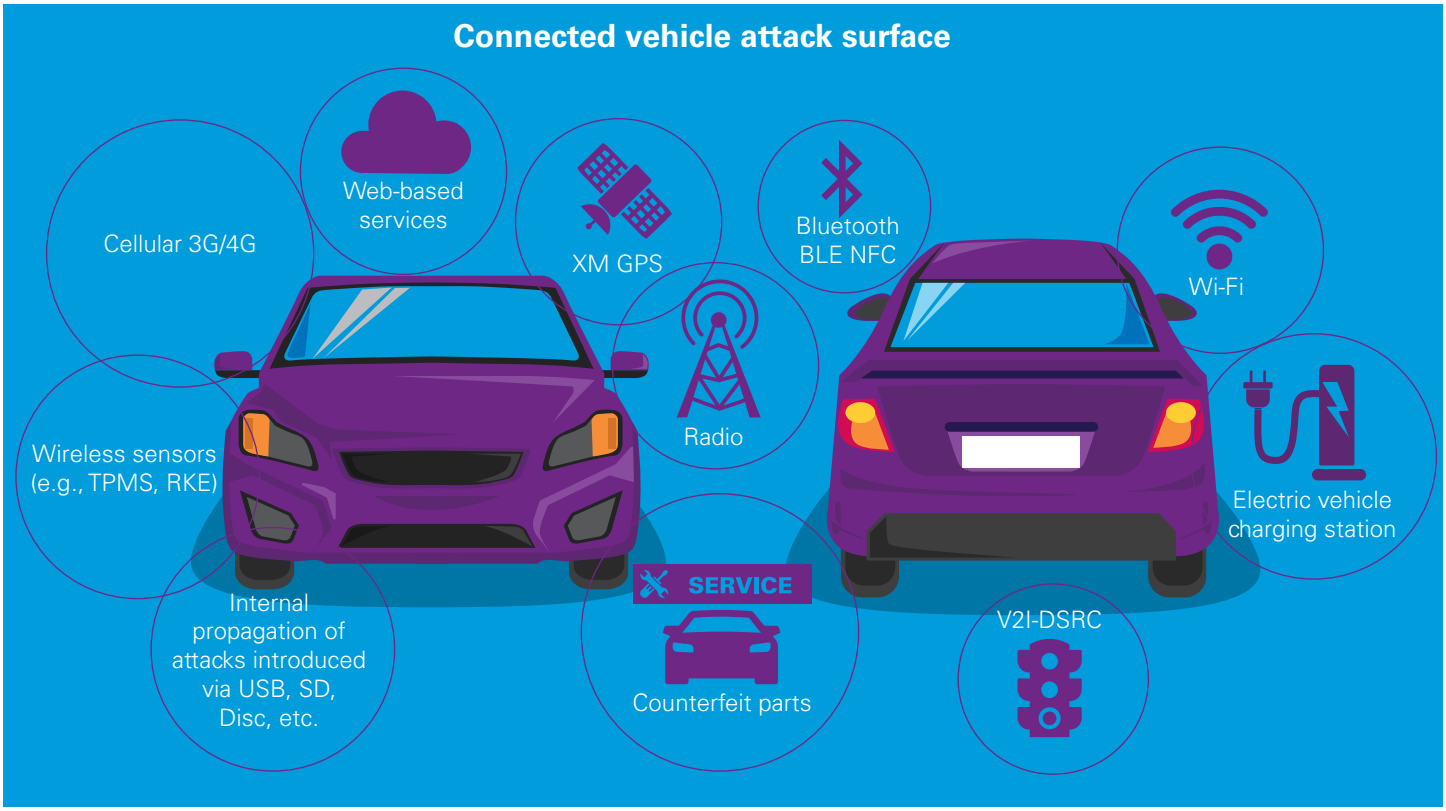
While creating a 100 percent secure vehicle network may not yet be feasible, there are numerous ways carmakers can make fleets safer and more secure while staking a leading position in the future automotive industry.

Below, we have outlined eight key recommendations, based on our deep knowledge and experience with automotive security and innovation. Some recommendations are critical security practices that should be deployed today. And some are untapped opportunities to harness the historic innovative power of the automotive industry to turn fleet security into a competitive advantage.

Minimize the attack surface

In the connected age, a weakness on one vehicle could expose all the rest. The growing "fog" of communications within and around the vehicle creates multiple attack vectors that could potentially expose critical vehicle systems across the entire fleet.

To cope, automotive manufacturers need "fog lights" to see through the risks and perform threat modeling exercises to identify all potential remote points of entry, and focus on consolidating remote entry points to shrink



the attack surface. While consolidating remote entry points may seem counterintuitive in an era where everything is becoming increasingly wireless, the "behind the scenes" vehicle communication and authentication channels should not be unique for each vehicle feature and service. It is more efficient, cost effective, and practical to secure and protect fewer entry points than manage multiple remote attack vectors.

Embrace "security by design"

"Security by design" is a well-known concept in software engineering circles, but it is still in the process of being adopted widely in the automotive industry. It is urgent to put the pedal down.

To address access, control, and privacy issues on today's high-tech connected car fleets, automakers will need to rethink how vehicles are designed and built. Security cannot be an afterthought. Patchwork security of individual technology components is not sufficient to prevent breaches of the open, internet-connected networks behind today's vehicle fleets.

Rather, a secure architecture requires that cyber security be integrated into every step of the development process. Establishing a multilayered security model, including the cloud, telematics, and on-vehicle layers, will be the key to successful implementation of vehicle cyber security.

Engineering teams and suppliers should build cyber security requirements into the design specifications for all software and hardware components. Security testing practices, such as penetration testing and design verifications, should be performed prior to finalizing components. And the Privacy Office should be involved to review key decisions around data collection, transmission, usage, sharing practices, compliance, and local data sovereignty laws. It is imperative that these measures are taken not only for the on-vehicle components, but also the supporting telematics and cloud infrastructure.

Embrace "privacy by design"

Similar to security, a "privacy by design" approach should be adopted by the automotive ecosystem. When companies want to add new functionality or collect additional information, they should first perform privacy impact assessments on the system applications, etc., that will contain customer content data or PII.

These assessments should consider key privacy-related areas, such as:

— What information is being collected?

— What is the basis for collecting and processing the data?

— How are privacy practices communicated?

— What choices do individuals have about how their data is collected and used?

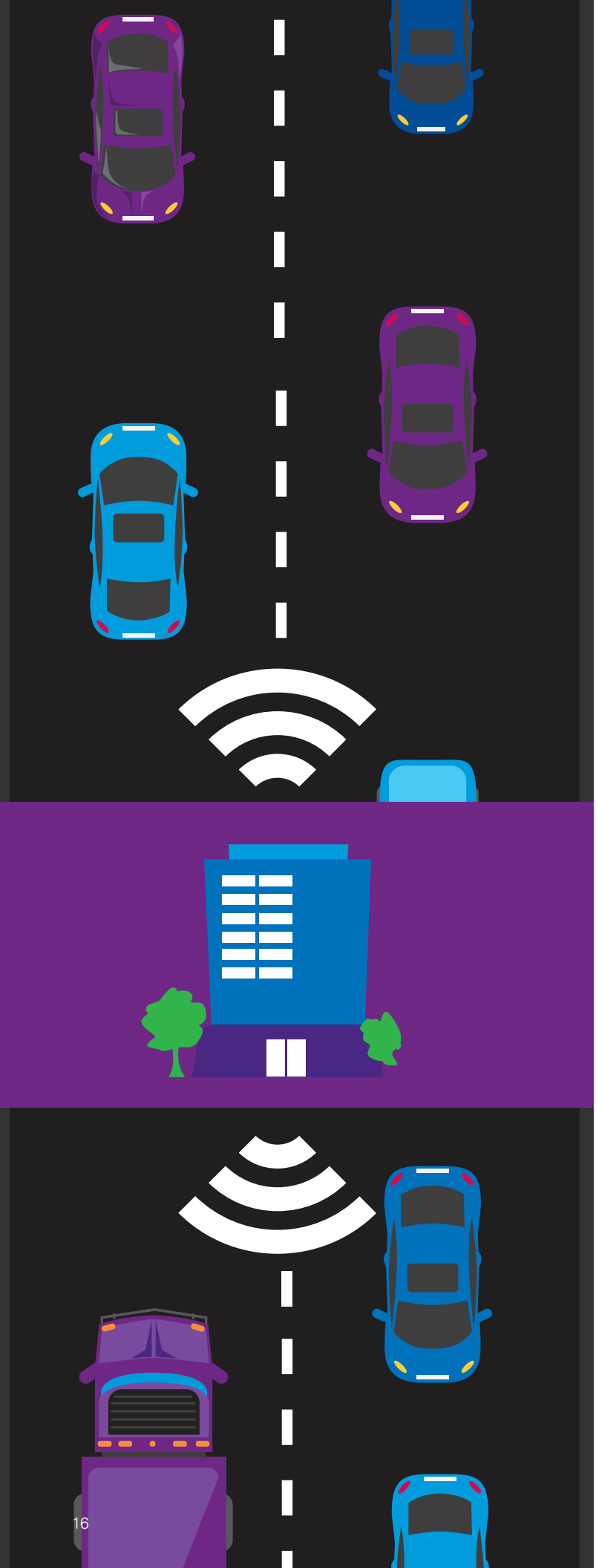
Furthermore, as cars are sold in multiple jurisdictions, companies should integrate local data privacy regulatory requirements into the development process and establish a risk-based approach to addressing those requirements.

Build out your cyber organization

Traditionally, engineers possess significant control over many aspects of vehicle manufacturing. However, security by design requires that IT security be part of the core team. They should have a much more prominent seat at the table in the future automotive organization.

Cyber security professionals will have an integral role to play in managing secure and remote fleets, including securing vehicle design and development processes and monitoring the integrity of the software, electronics, and data of the fleet at all times. From an organizational standpoint, this is likely to require a different organizational hierarchy—one in which IT security holds an elevated status and has arms across a wider scope of the business, including the groups involved in overall vehicle operational safety. It also might require automakers to hire new cyber security talent.

We suggest automakers take a look at organizational design from aerospace and defense organizations, which are responsible for designing, operating, and securing major satellite systems. In these organizations—which must ensure that globally critical, billion-dollar hardware out in space cannot be tampered with—cyber security is typically prominent, with IT security having an equal voice to engineers.



Establish a vehicle operations center

Automotive competitive advantage may soon go to the company that does two things effectively:

— Maintains the integrity of the vehicle fleet by checking the identification, configuration, and behavior of each vehicle every time it comes online

— Manages and leverages the enormous volumes of data and information created by the fleet to protect and defend it, while protecting the privacy of the individuals who interact with the fleet.

As more automakers enter the real-time service and operations business, we recommend establishing a vehicle operations center to integrate, analyze, and use the information coming in from the extended fleet network. Several industry leaders are already establishing such capabilities.

The vehicle operations center will have skills and resources to monitor in real-time the health and performance of the fleet and the technology, apps, and platforms inside it. This will enable fleet operators to identify potential threats and vulnerabilities before it is too late.

The center will also provide a streamlined, cost-effective operating model to mitigate the impact of a cyber breach. It will be designed to isolate issues as they occur, broadcast OTA software patches and fixes, and identify forensic evidence of why, how, and by whom the attack was perpetrated.

Finally, the center—with its analytical edge—has numerous valuable applications that go beyond cyber security. For example, it can help manage fuel levels, gas mileage, and maintenance concerns and deliver additional services to enhance customer experience and confidence.

Merging cyber and physical security in the auto industry

When General Motors (GM) hired its chief cyber security officer to oversee global vehicle safety, it was a clear sign that cyber security can no longer be separated from the overall culture of safety and quality that has long been the hallmark of the automotive industry. "In today's connected world, combating cyber security threats have become an integral part of our continued company commitment to quickly identifying and resolving product safety issues of all kinds, so it's a natural extension for us to combine these two roles into one," GM CEO Mary Barra said in a statement.

"GM cyber security chief to head global vehicle safety" (*Automotive News*, August 18, 2017)

Create fail-safe protocols

Fail-safe is not just a mechanical issue anymore.

Many of today's connected vehicles have "drive-by-wire" accelerators, meaning the physical input of pushing down on the gas pedal triggers the digital action to speed up the vehicle. And some of the highest-tech models have drive-by-wire capabilities applied to other vehicle operations as well, such as electronic steering systems that can help you park and even collision avoidance systems that can apply the brakes and swerve around an obstacle—not to mention the beta autopilot functionality in recent Teslas where the whole car drives itself.

When a vehicle is hacked, drive-by-wire capabilities can create huge risks. For example, if the software systems performing the digital actions become compromised, they could potentially ignore physical inputs. Alternatively, data from different sensors—the radar versus the camera, for example—could conflict with each other, requiring a decision to be made on which sensor data is more reliable or trusted.

For all these reasons, establishing level-of-trust and priority protocols—rules for how the vehicle will handle inaccurate, missing, or conflicting inputs—is critical to protecting the fleet. Also important is designing cars with different trust zones based on data sensitivity and criticality. This is similar to how airplanes segment information through different antennas, bandwidths, and communications systems that require lesser levels of trust (i.e., internet entertainment consoles) from safety-critical information (i.e., real-time commands from the flight management software).

> **"[We must] make super sure that a fleetwide hack is basically impossible and that if people are in the car, that they have override authority on whatever the car is doing. So, if the car is doing something wacky, you can press a button that no amount of software can override—that will ensure that you gain control of the vehicle and cut the link to the servers."**

Elon Musk, Tesla CEO, at the National Governors Association summer meeting, 2017

Racing ahead of regulation

The automotive industry is prime for a regulatory standard or common security framework that encourages OEMs to implement standardized cyber security controls and best practices. The digital disruption in the industry has so far outpaced traditional automotive safety and quality regulations—and regulators and standard setters are playing catch-up. They are especially sharpening their focus on the issues of vehicle cyber security and data privacy, asking what additional measures should be added to current practice to protect the interests of consumers and manufacturers and comply with regional and national data sovereignty laws.

For KPMG's thorough update and perspective on the automotive regulatory environment, read our recent white paper:

Test-driving vehicle cybersecurity

> **Analyzing the entire fleet-level data offers full visibility into the fleet's security posture. By understanding the complete picture, normal car and driver behavior can be monitored effectively and attacks can be prevented before they reach the network and cause harm.**
>
> Yoav Levy, Cofounder and CEO, Upstream Security

Collaborate on cyber security solutions

Automakers should have a strong voice in establishing industry standards and leading practices on vehicle cyber security, as well as shaping the regulatory environment. For this, collaboration among industry peers, researchers, government agencies, external consultants, and even adjacent industries is imperative.

That may seem like an obvious point, but in practice, true teamwork on cyber security is a significant challenge. Most companies in the automotive ecosystem are not used to open information exchange. In fact, there are legal, regulatory, and competitive barriers to sharing knowledge and ideas.

Further complicating matters is the unsolved question of who is liable for a cyber breach—the driver, the insurer, the manufacturer, the technology supplier, etc. That issue impacts how much each party is willing to work together on common cyber security solutions.

Still, there are numerous efforts to create collaboration on vehicle cyber security, such as the Automotive Information Sharing and Analysis Center.[19] Nonprofit groups like this could go a long way toward reducing industry-wide cyber risk.

Reduce third-party risk

Third-party risk has been one of the most focused risks for almost all companies in all industries. We believe the automotive industry can develop leading practices for other industries in addressing third-party risk.

The supply chain—especially electronics and software manufacturers—poses an increased risk to OEMs in light of today's cyber-physical challenges. Imagine if a software company inserted nefarious wireless code into a software product that goes into a vehicle fleet, enabling the software supplier to access and control the vehicles within that fleet.

And third-party risk is not just limited to the supply chain. In operating connected car fleets—and ultimately, autonomous car fleets—OEMs may establish relationships with premium service providers (car sharing, mapping, infrastructure, parking, infotainment, etc.). Such relationships will require OEMs to maintain a higher level of security, as weaknesses in third parties can also be exploited by cyber attackers. For example, academic researchers recently put stickers on street signs to trick the vision systems inside self-driving cars, causing the car's algorithms to misread the signs.[20]

Because their brands are the ones most at stake from a cyber security failure, automakers will need to take measures to protect against such scenarios. That means enhancing both supply chain and other third-party certification and transparency. By setting standards and requirements for suppliers regarding cyber security, and by requiring greater visibility into what suppliers are designing and programming, OEMs can close vulnerabilities in the supplier base and third-party relationships—and reduce their own organizational risk posture.

[19] www.automotiveisac.com

[20] "Researchers hack a self-driving car by putting stickers on street signs" (Autoblog, August 4, 2017)

Making the right turns ahead

While automotive businesses are still in the early phases of vehicle cyber security, it has been a clear industry focus as cars integrate more and more electronic, hardware, and software components. Many carmakers are establishing dedicated functions to identify and manage cyber security risks. Others are investing in next-generation security techniques or bringing cyber experts onboard from outside the industry.

But when it comes to securing the fleet, start to finish is a long distance to travel. Cruising forward on cyber security and privacy protection will not be enough to compete in the very near future. The automotive business is likely to experience huge changes as companies prepare to manage the potential risks of a fleetwide cyber attack. This newly emerging cyber risk will likely even disrupt how automakers currently design, produce, sell, and support fleets.

There are many different strategies about how best to address fleet security, but one thing is clear: Cyber must be addressed. Automotive manufacturers must decide very soon how they will enter the fleet security business to enhance the value of their brand. We believe that OEMs can use vehicle cyber security as a marketplace advantage, viewing cyber security similar to vehicle safety as a competitive differentiator to customers and investors. We hope this paper helps them make the right turns today to race ahead tomorrow.

How KPMG can help

KPMG's automotive cyber security services are directly aligned to the four key pillars of the automotive business environment—vehicle strategy, design, delivery, and operations—with the goal of embedding security throughout.

KPMG can help automotive companies in the areas of:

Secure strategy and governance: Investing strategically in vehicle cyber security, based on the client's unique goals, capabilities, and risk appetite.

Secure design: Securing cars—and their software and hardware components as well as online and OTA services—from the ground up.

Secure production: Managing cyber risk across the entire vehicle production process, including materials demand planning, the global supply chain, and plant operations.

Secure operations: Ensuring the ongoing security and performance of vehicles on the network as well as the new and growing aftersales service opportunities.

Contact us to learn more about how KPMG is distinctly positioned to help automotive companies seize the opportunities of technological disruption—while making the road safer for everyone.

Secure design

- Principles-based security architecture
- Security requirements governance
- Software assurance
- Penetration testing
- Security controls and fail safes
- Data privacy design

Secure production

- Production processes
- Supply chain risk management
- Digital manufacturing
- Vendor security risk and compliance management

Secure strategy and governance

- Risk profile and risk management
- Planning security investments
- Long-term security program roadmaps
- Formal vehicle governance to promote consistency and efficiency

Secure operations

- Security monitoring
- Intrusion detection
- Security patching
- Network operation centers
- Regulatory compliance

About the authors

Gary Silberg is the national automotive leader at KPMG, as well as the global lead partner for Delphi Corporation and Ford Motor Company. With more than 25 years of business experience, including more than 14 years in the automotive industry, he is a leading voice in the media on global trends in the automotive industry. Gary advises numerous domestic and multinational companies in areas of strategy, mergers, acquisitions, divestitures, and joint ventures. For the past five years, he has focused on the intersection of technology and the automotive industry, with groundbreaking research on self-driving cars, connectivity, and mobility-on-demand services.

Jono Anderson is a principal in KPMG's Strategy practice. Specializing in growth and innovation strategy, he has more than 20 years of experience in product and technology strategy. He currently serves the automotive and aerospace industries. Prior to joining KPMG, Jono was a research scientist and mathematician working extensively with unmanned and autonomous systems and the underlying mapping, guidance, sensors and high performance computing capabilities..

Andi Baritchi is a director in KPMG's Advisory practice with more than 15 years of experience in cyber security, technology, and business strategy. Prior to joining KPMG, he was global managing principal in charge of a leading cyber security practice. Andi contributes regularly to industry mindshare on the critical link between cyber security and business risk via published research, speaking engagements, and executive briefings. His research interests include cloud security, connected cars, and securing the Internet of Things.

Danny Le is a principal in KPMG's Cyber Security Practice leading the Automotive and New Mobility agenda. He is one of the founding partners of KPMG's Cyber practice in the US. Danny previously spent 10 years in China building KPMG China's Consulting business as well as serving as the head of KPMG China's Automotive practice and a member of KPMG's Global Automotive Steering Committee. He brings current and specific experience in helping automotive companies develop and implement new mobility services and move traditional businesses on-line. Danny has been contributing thought leadership in KPMG's Automotive practice for numerous years.

Ron Plesco is a principal in the Cyber Security practice. He and his team focus on cyber threat assessments, intelligence and breach investigations. He is an internationally known information security and privacy attorney with 18 years of experience in cyber investigations, information security, privacy, identity management, computer crime and emerging cyber threats, and technology solutions. Concentrating on the automotive industry, Ron regularly presents on vehicle hacking and the cyber security concerns regarding interconnected vehicles. Prior to joining KPMG, Ron was CEO of the National Cyber Forensics and Training Alliance, where he managed the development of intelligence that led to more than 400 worldwide cyber crime arrests in four years and prevented more than $2 billion in fraud.

Mike is a Director in KPMG's Emerging Technology Risk Services practice. He has over ten years of experience helping organizations balance the risk vs. reward equation of disruptive technologies, including leading the development of KPMG's Internet of Things (IoT) Risk and Governance service offering and supporting framework. Mike has executed extensive engagements helping organizations identify, assess, and manage risks related to connected, digital products and devices. His IoT delivery experience has been focused on use cases within automotive, public transit, consumer products, medical devices, and industrial IoT (i.e., Industry 4.0).

Sponsored by KPMG's U.S. Manufacturing Institute Automotive Center

The KPMG U.S. Manufacturing Institute's Automotive Center is an open forum where industry specialists share knowledge, gain insights, and collaborate on timely and relevant issues facing the automotive market. KPMG recognizes that success in business is not a result of random inspiration, but rather of focused, strategic adaptations to ever-changing conditions. And with the unprecedented amount of change happening in business today, KPMG inspires automotive companies to confidently empower their organizations to evolve rapidly and to capture value in emerging opportunities. For more information on the Automotive Center, please visit www.kpmg.com/us/automotive.

Contact us

Gary Silberg
Partner and National Automotive Leader
T: 312-665-1916
E: gsilberg@kpmg.com

Jono Anderson
Principal, KPMG Strategy
T: 858-750-7330
E: jonoanderson@kpmg.com

Andi Baritchi
Director, KPMG Cyber Security Services
T: 972-489-4289
E: abaritchi@kpmg.com

Danny Le
Principal and Automotive Leader, KPMG Cyber Security Services
T: 213-430-2139
E: dqle@kpmg.com

Ron Plesco
Principal, KPMG Cyber Security Services
T: 717-260-4602
E: rplesco@kpmg.com

Michael Krajecki
Director, KPMG Emerging Technology Risk Services
T: 312-665-2919
E: mkrajecki@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia