KILL SWITCH

WHY CONNECTED CARS CAN BE KILLING MACHINES AND HOW TO TURN THEM OFF

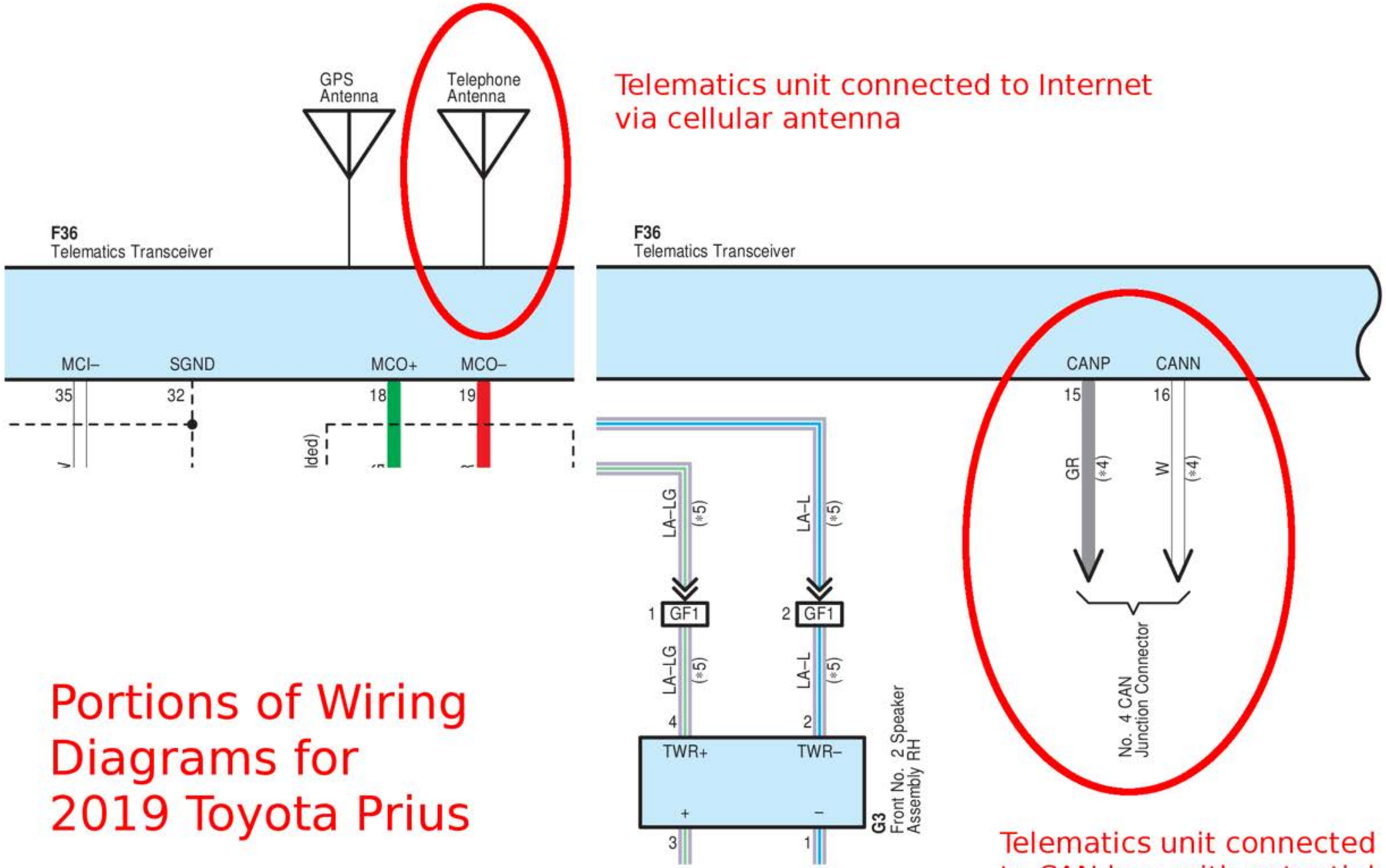
Consumer Watchdog

Figure I: Top Selling U.S. Carmakers' Connected Car Goals [4] [5] [6] [7] [8] [9]

Top-selling Makes in U.S.	U.S. Market Share	New cars at risk due to connectivity
General Motors (Chevy, Buick, Cadillac, etc.)	17.02%	All new vehicles today
Toyota	14.63%	All by 2020
Ford	14.44%	All by 2020
Fiat-Chrysler	12.98%	Next generation platform providing connectivity in all cars by 2022
Renault-Nissan-Mitsubishi	9.35%	90% of new cars by 2022
Honda	9.10%	Unknown
Hyundai/Kia	7.42%	Unknown
Subaru	3.94%	Unknown
Volkswagen	3.69%	Unknown
Daimler	2.06%	Unknown

Figure II: Vulnerable Connectivity Features in Top Models

Vehicle	Commercial Name(s)	Models
Toyota Camry	Remote Connect, Safety Connect	*** All Models ***
Lexus ES	Enform	*** All Models ***
Honda Civic	HondaLink	All hatchbacks; coupes and sedans "Sport" model and above
Mercedes C-Class	me connect	*** All Models***
Subaru Outback	STARLINK	*** All Models ***
Tesla Model 3	*N/A -- connectivity is an integral feature in all Tesla vehicles*	*** All Models ***
Ford F-150	SYNC Connect	All but the lowest-end models
BMW 5-series	ConnectedDrive	*** All Models***



Telematics unit connected to Internet via cellular antenna

Portions of Wiring Diagrams for 2019 Toyota Prius

Telematics unit connected to CAN bus, with potential access to all critical systems

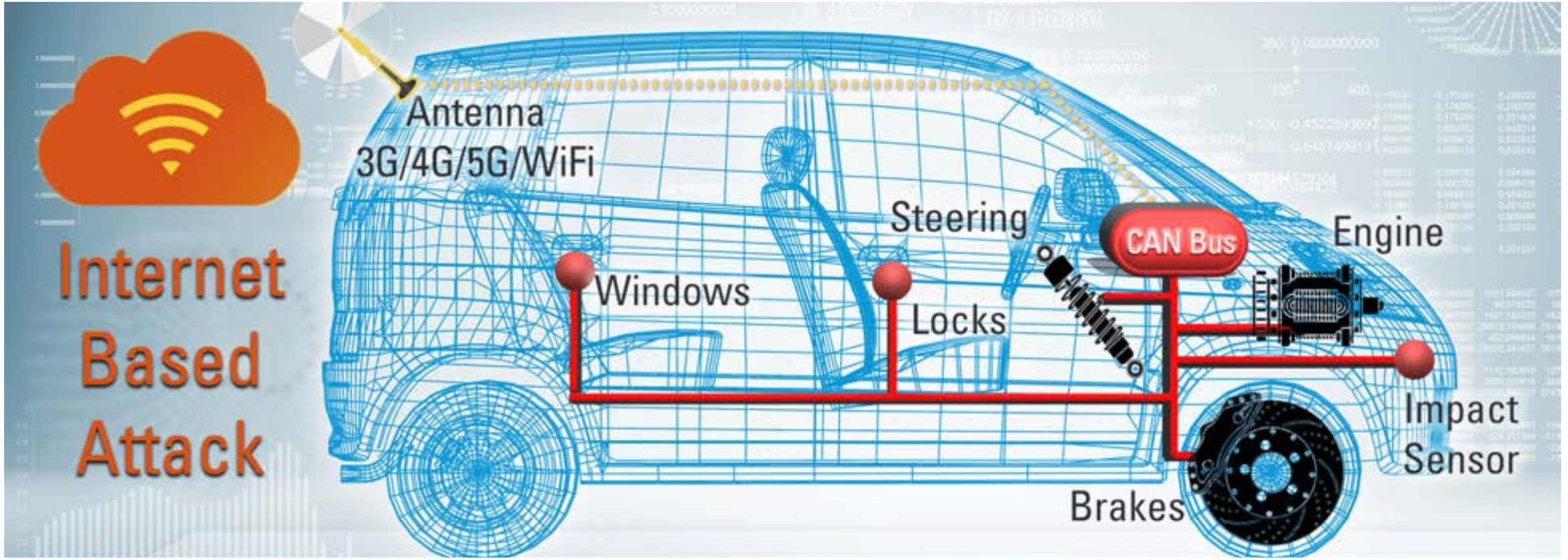
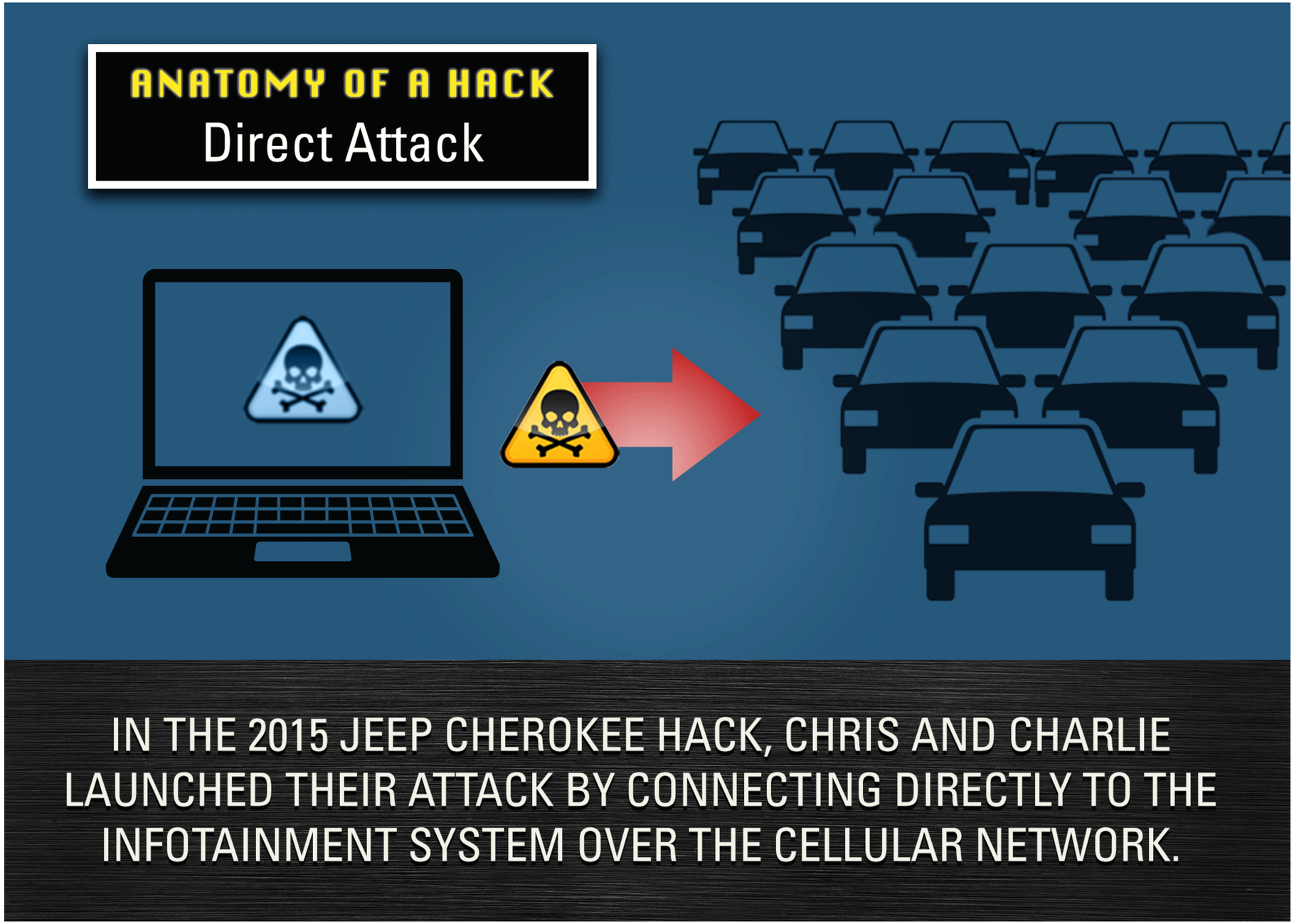

Internet
Based
Attack
Antenna
3G/4G/5G/WiFi
Windows
Steering
Locks
CAN Bus
Engine
Impact
Sensor
Brakes

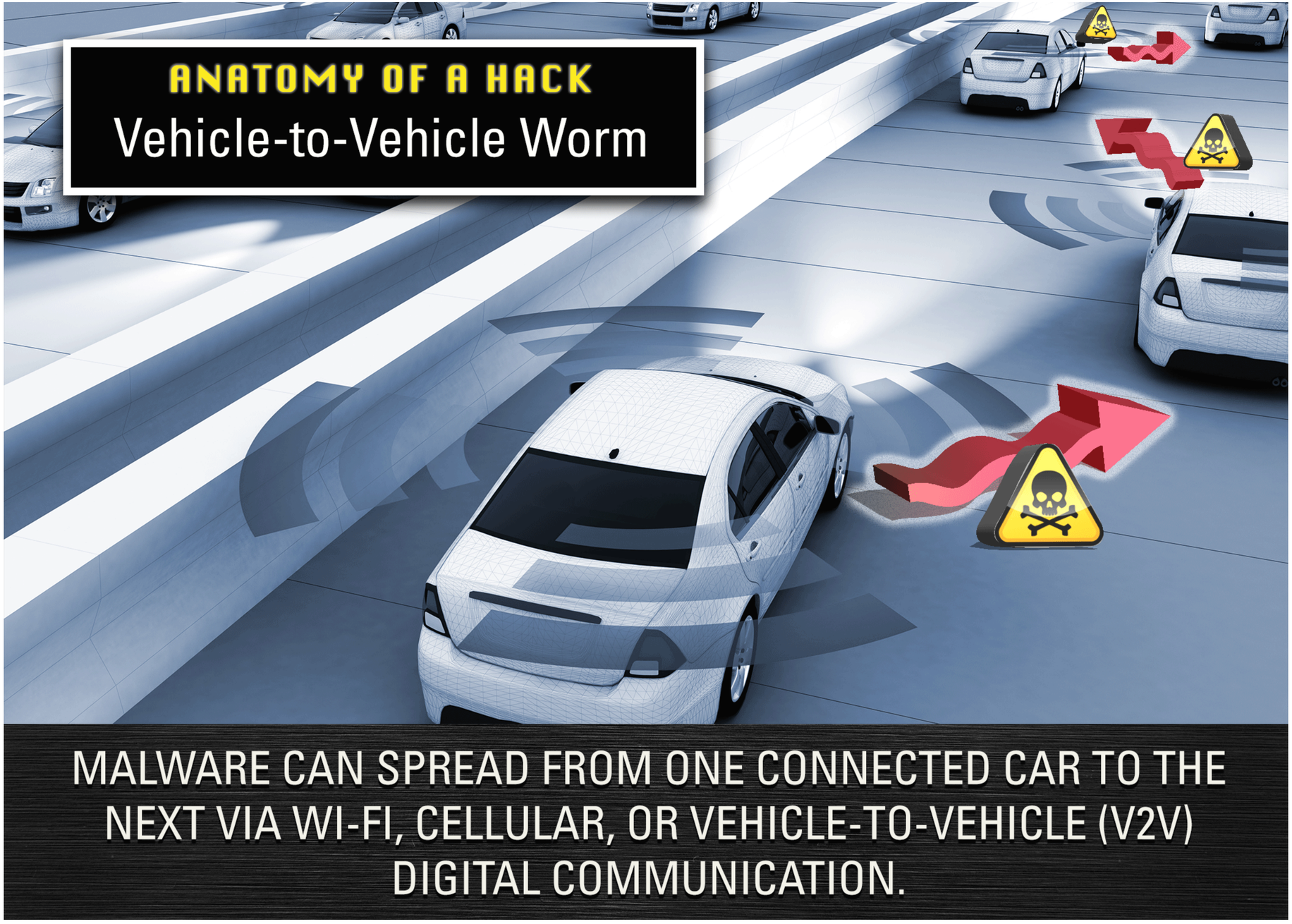
Figure IV: Known Current and Future Open Source Operating Systems

Linux	Tesla, Audi, Mercedes-Benz, Hyundai, Toyota, BMW, Chevrolet, Honda
Android	Fiat-Chrysler, Volvo, Renault, Nissan, Mitsubishi
FreeRTOS	Tesla

Figure V: List of Bug Bounties

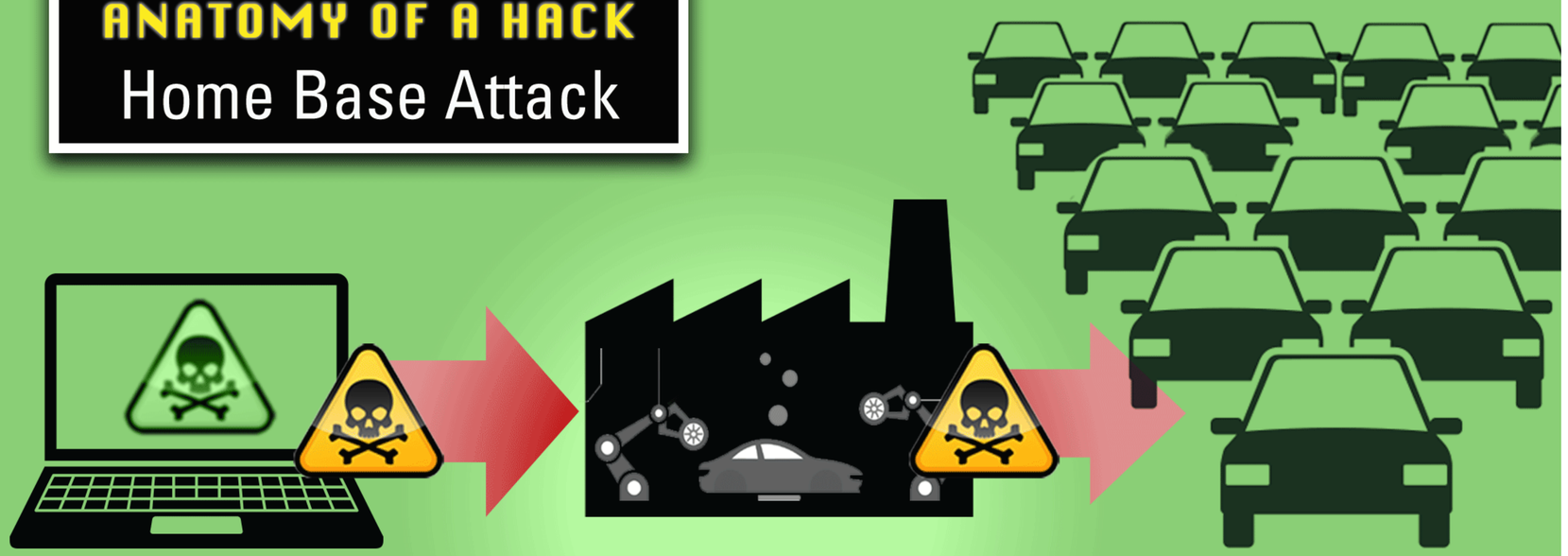
Fiat-Chrysler	• 93 vulnerabilities rewarded • 300+ "hall-of-famers" who reported vulnerabilites • $4,760 payout per bug on average over the last 3 months • Disclosing details of the vulnerability to the public explicitly prohibited	https://bugcrowd.com/fca
Tesla	• 348 vulnerabilities rewarded • 426 "hall-of-famers" • $2k average payout	https://www.tesla.com/about/security https://bugcrowd.com/tesla https://techcrunch.com/2018/09/06/teslas-new-bug-bounty-protects-hackers-and-your-warranty/
BMW	Note: does not appear to offer any reward Note: no statistics available	https://www.bmwgroup.com/en/general/Security.html


ANATOMY OF A HACK
Direct Attack
IN THE 2015 JEEP CHEROKEE HACK, CHRIS AND CHARLIE LAUNCHED THEIR ATTACK BY CONNECTING DIRECTLY TO THE INFOTAINMENT SYSTEM OVER THE CELLULAR NETWORK.

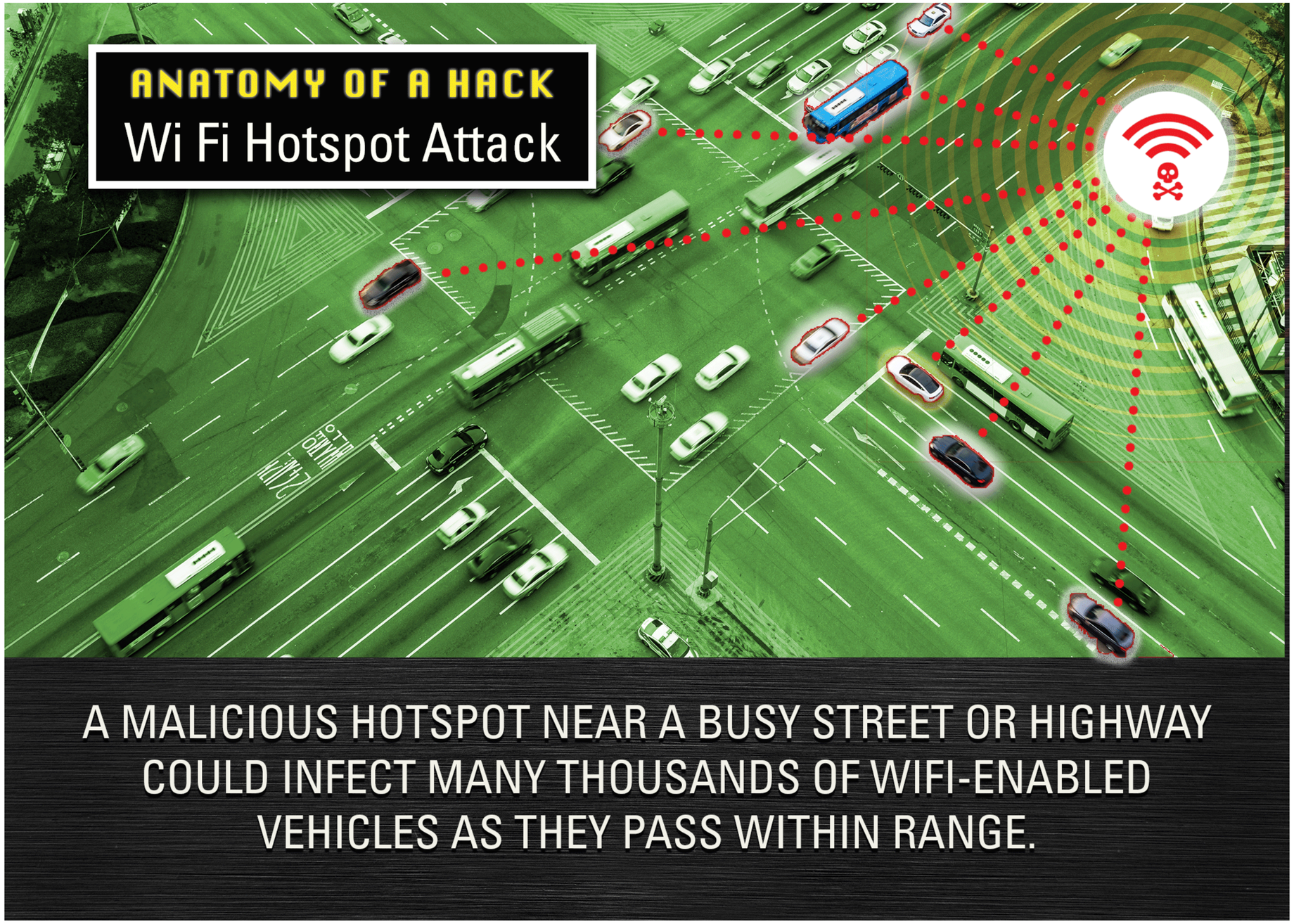

ANATOMY OF A HACK
Vehicle-to-Vehicle Worm
MALWARE CAN SPREAD FROM ONE CONNECTED CAR TO THE NEXT VIA WI-FI, CELLULAR, OR VEHICLE-TO-VEHICLE (V2V) DIGITAL COMMUNICATION.

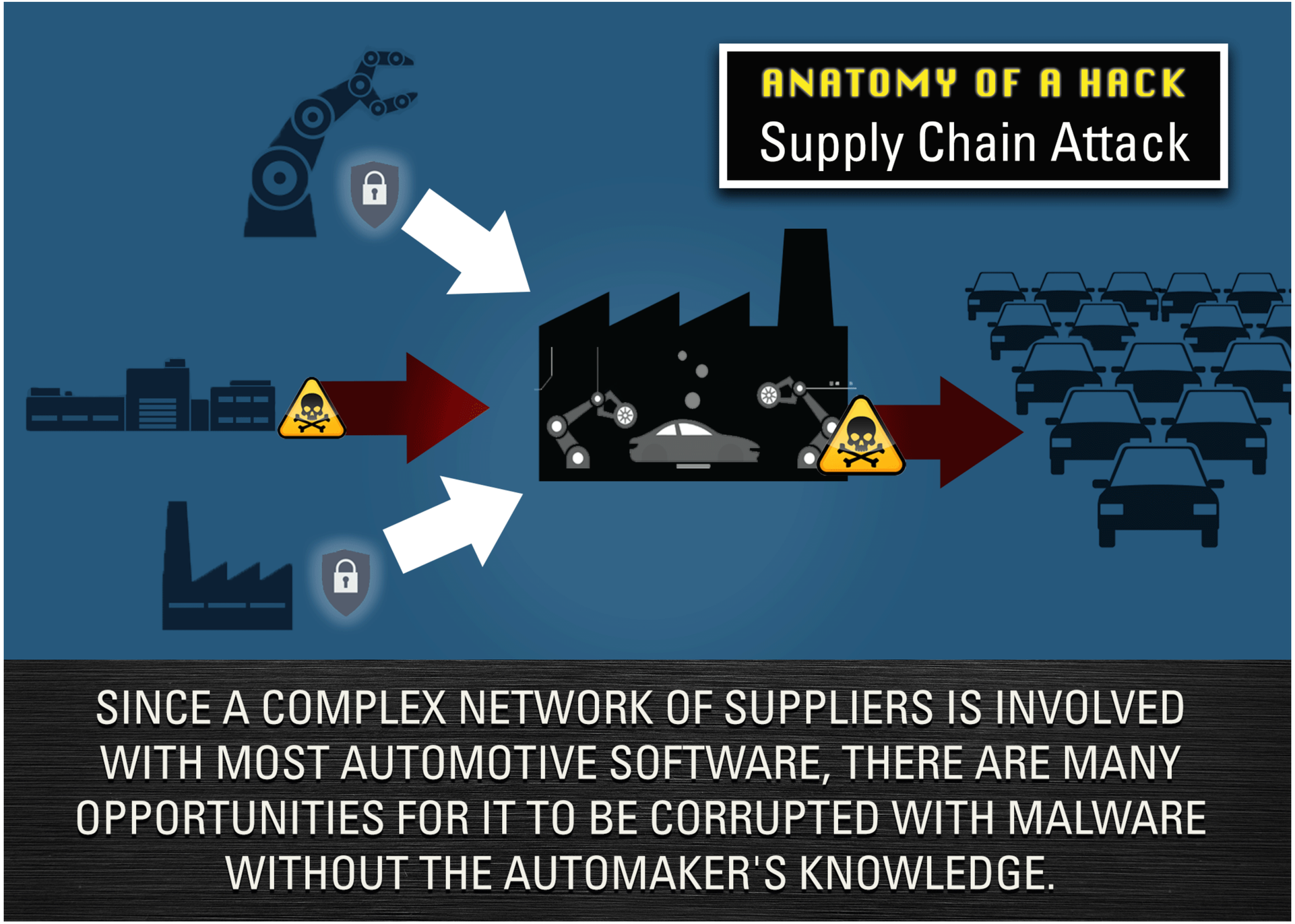
ANATOMY OF A HACK

Home Base Attack

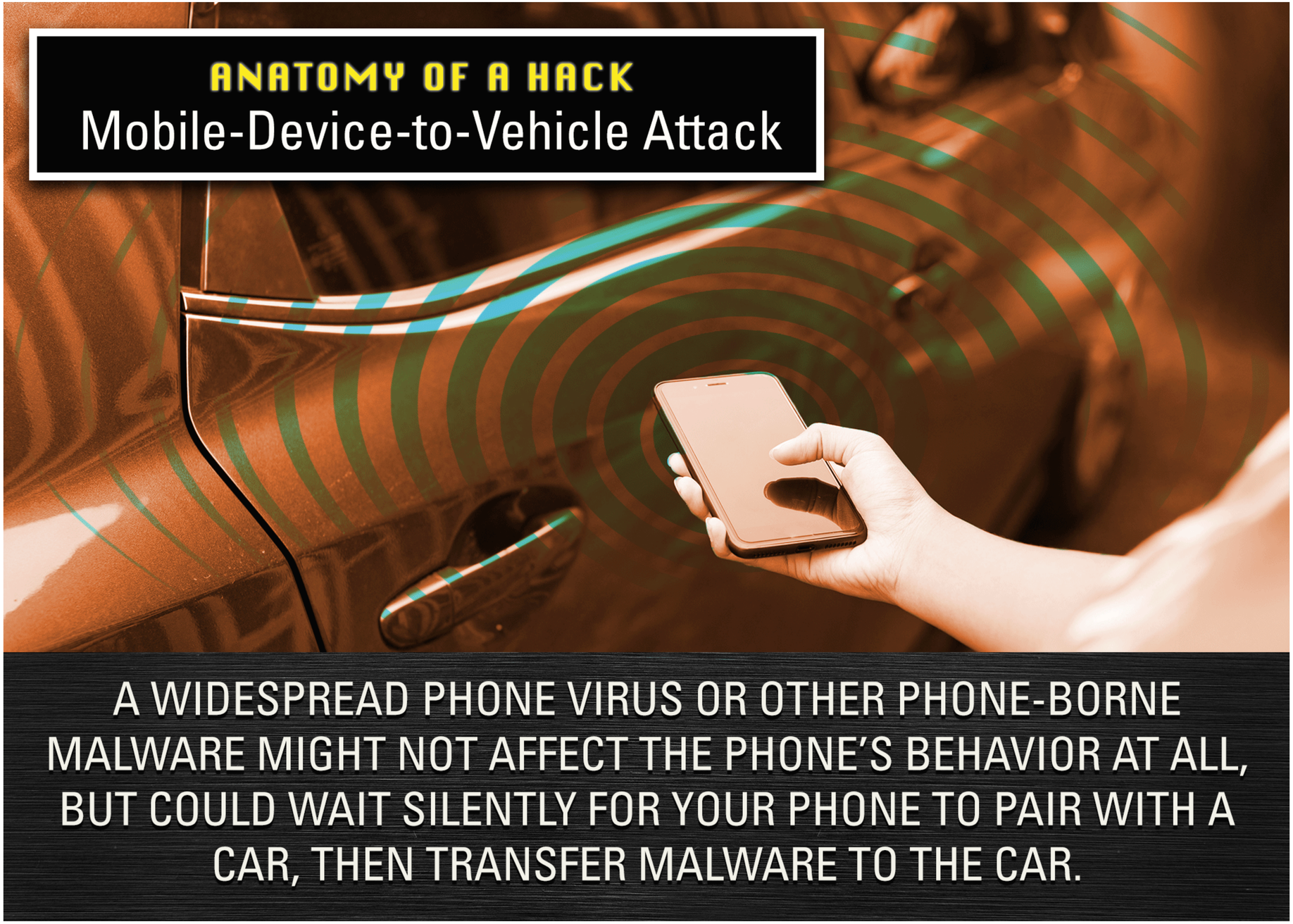


BECAUSE CONNECTED VEHICLES COMMUNICATE WITH THE MANUFACTURER, A HACKER OR SABOTEUR WHO PENETRATES THE CORPORATE NETWORK CAN POTENTIALLY SPREAD MALWARE TO MILLIONS OF CONNECTED VEHICLES, FOR EXAMPLE, BY CORRUPTING OVER-THE-AIR UPDATES.


ANATOMY OF A HACK
Wi Fi Hotspot Attack
A MALICIOUS HOTSPOT NEAR A BUSY STREET OR HIGHWAY COULD INFECT MANY THOUSANDS OF WIFI-ENABLED VEHICLES AS THEY PASS WITHIN RANGE.


ANATOMY OF A HACK
Supply Chain Attack
SINCE A COMPLEX NETWORK OF SUPPLIERS IS INVOLVED WITH MOST AUTOMOTIVE SOFTWARE, THERE ARE MANY OPPORTUNITIES FOR IT TO BE CORRUPTED WITH MALWARE WITHOUT THE AUTOMAKER'S KNOWLEDGE.


ANATOMY OF A HACK
Digital Application Attack
ANY DIGITAL “APP” YOU INSTALL ON YOUR CAR IS A POTENTIAL VECTOR FOR MALWARE. SECURITY HOLES IN THE APP —WHETHER ACCIDENTAL OR MALICIOUS—COULD GIVE ATTACKERS REMOTE ACCESS TO YOUR CAR'S STEERING, BRAKING, AND ACCELERATION.


ANATOMY OF A HACK
Mobile-Device-to-Vehicle Attack
A WIDESPREAD PHONE VIRUS OR OTHER PHONE-BORNE MALWARE MIGHT NOT AFFECT THE PHONE'S BEHAVIOR AT ALL, BUT COULD WAIT SILENTLY FOR YOUR PHONE TO PAIR WITH A CAR, THEN TRANSFER MALWARE TO THE CAR.

19 million
Number of vehicles on the road at rush hour in U.S.

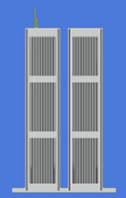
3.75 million
Potential number infected by fleet-wide hack

262,500
Drivers of infected cars would be on the road at rush hour

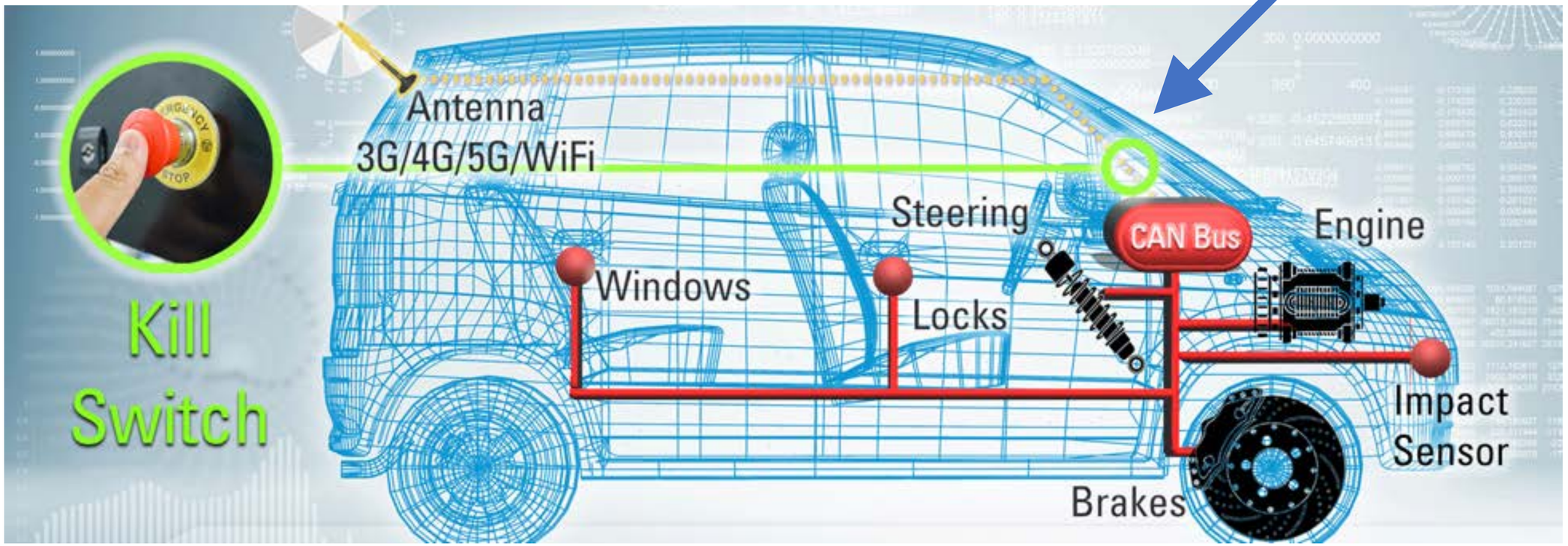
134,400
Projected injuries from a fleet-wide attack

3,000
Estimated number of fatalities nationwide

2,996
Deaths on 9/11



Proposed Kill Switch



Investor Disclosures Acknowledge Hacking Risks

Tesla

2019 SEC 10-K

"We have designed, implemented and tested security measures intended to prevent unauthorized access to our information technology networks, our products and their systems…**there can be no assurance that vulnerabilities will not be exploited in the future before they can be identified, or that our remediation efforts are or will be successful."**

Investor Disclosures Acknowledge Hacking Risks

Daimler Chrysler

2018 Annual Report

"Due in particular to the changed risk situation relating to cybercrime and hacker attacks, the possible impact of information-technology risks has increased compared with the previous year from Medium to High."

Investor Disclosures Acknowledge Hacking Risks

Ford

2018 SEC 10-K

"Such cyber incidents could materially disrupt operational systems; result in loss of trade secrets or other proprietary or competitively sensitive information; compromise the privacy of personal information of customers, employees, or others; jeopardize the security of our facilities; **affect the performance of in-vehicle systems; and/or impact the safety of our vehicles. A cyber incident could be caused by malicious third parties using sophisticated, targeted methods to circumvent firewalls, encryption, and other security defenses, including hacking, fraud, trickery, or other forms of deception. We, our suppliers, and our dealers have been the target of these types of attacks in the past and such attacks are likely to occur in the future. The techniques used for attacks by third parties change frequently and may become more sophisticated, which may cause cyber incidents to be difficult to detect for long periods of time**. Our networks and in-vehicle systems may also be affected by computer viruses or breaches due to the negligence or misconduct of employees, contractors, and/or others who have access to our networks and systems**."**

Investor Disclosures Acknowledge Hacking Risks

General Motors

2018 Annual Report

"Security breaches and other disruptions of our in-vehicle systems could impact the safety of our customers and reduce confidence in GM and our products. Our vehicles contain complex information technology systems. These systems control various vehicle functions including engine, transmission, safety, steering, navigation, acceleration, braking, window and door lock functions. We have designed, implemented and tested security measures intended to prevent unauthorized access to these systems. However, hackers have reportedly attempted, and may attempt in the future, to gain unauthorized access to modify, alter and use such systems to gain control of, or to change, our vehicles' functionality, user interface and performance characteristics, or to gain access to data stored in or generated by the vehicle."

Investor Disclosures Acknowledge Hacking Risks

General Motors

2018 Annual Report

"If risks relating to information security, data protection and IT were to materialize, they could have a high earnings impact over the two- year assessment period. **Despite extensive security measures, the risks in this area are classified as high**."

Shi Tie
IES PLAYOFFS - D3