

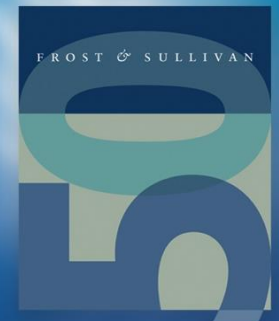
# Frost & Sullivan Cybersecurity Presentation

*2015 will be the Year of Security, Prognostics &  
Evolution of OEM Vehicle Automation Strategies*



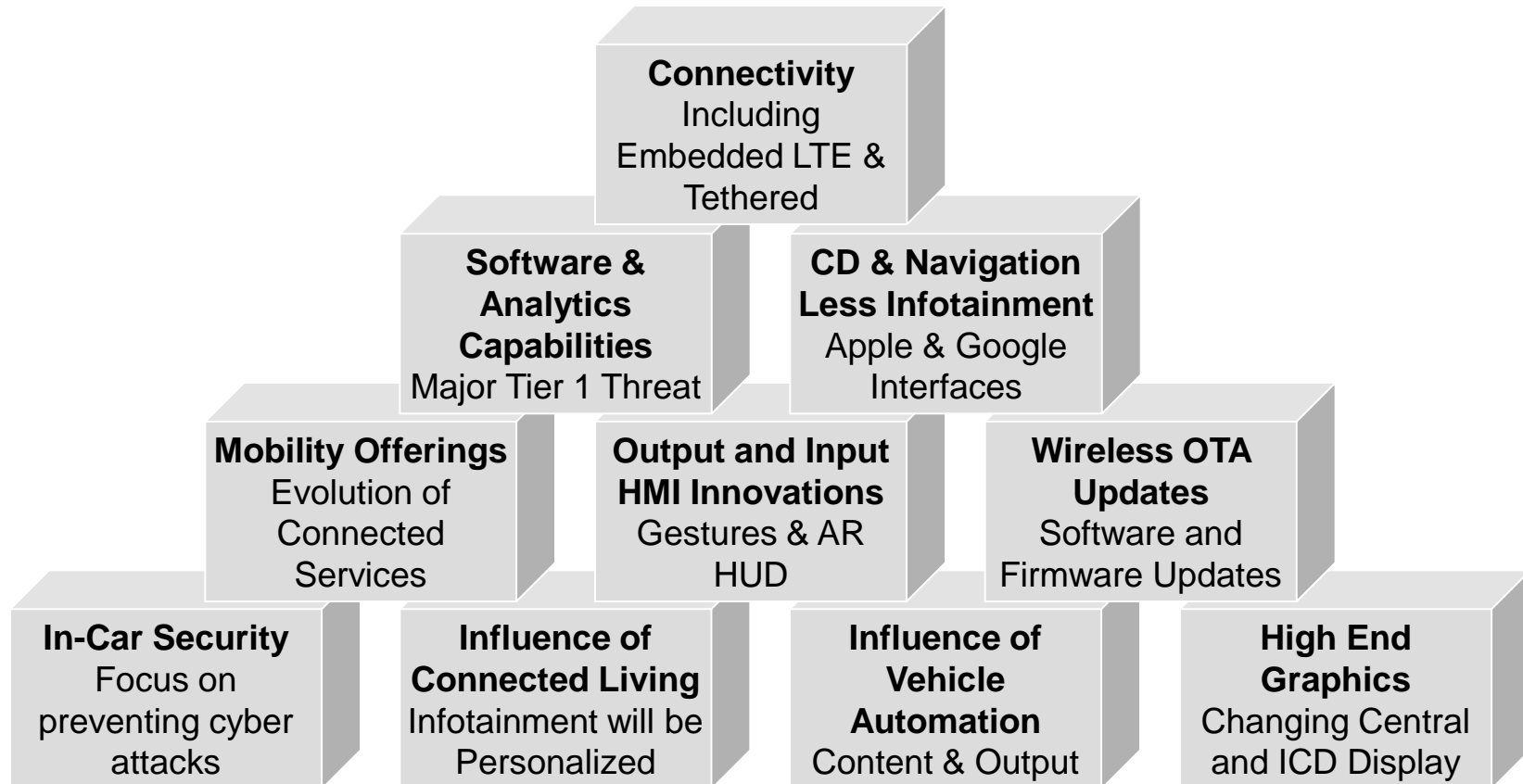
Praveen Narayanan  
Research Manager

Feb 2015



# Key Trends Impacting the Infotainment Market to 2020

Trends ranging from OTA updates to level 3 automation to predictive analytics all require a very high level of in-car and back end security



# OEM Activities in the Connected Space

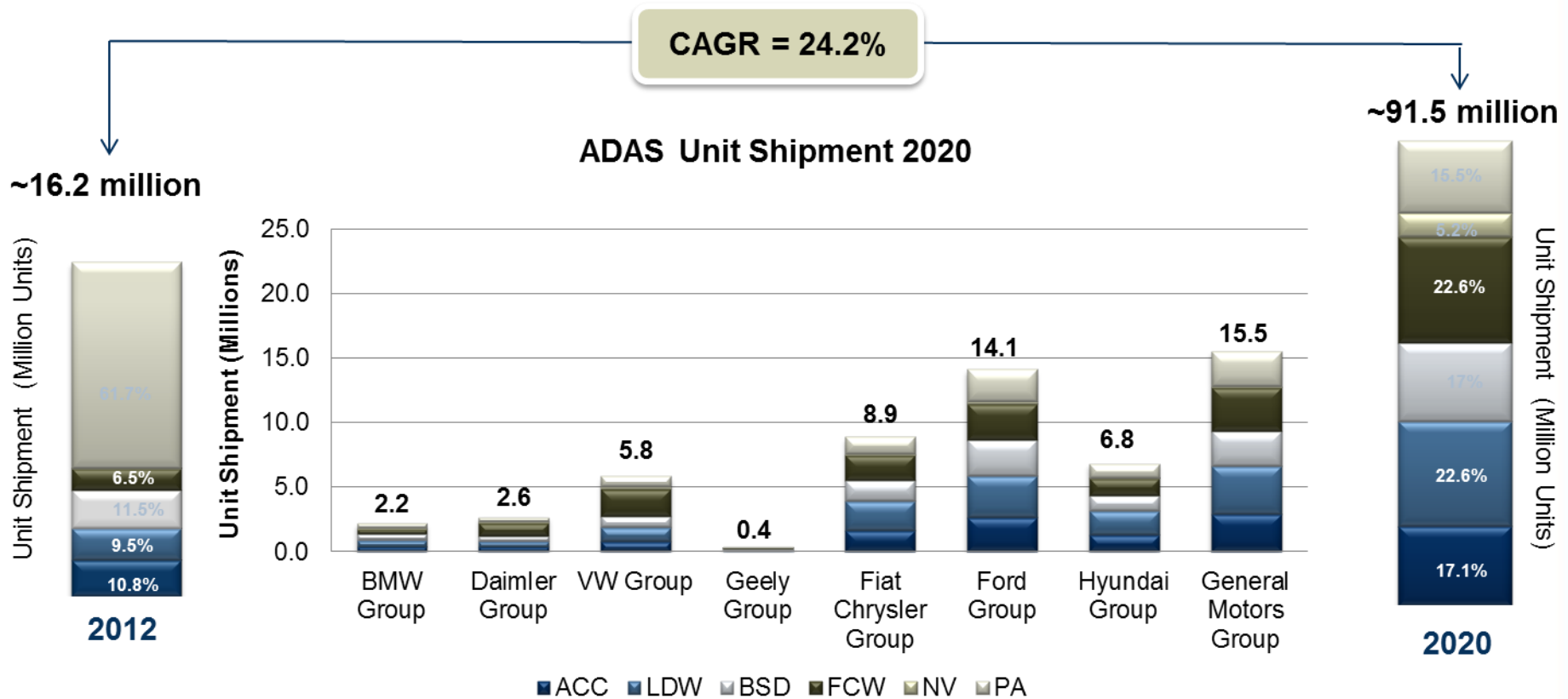
Almost every OEM in the US has a connected telematics service – another key area that is currently the first point of attack for hackers

OEM	Telematics Service	Connectivity	Free Trial Period	Features
General Motors	OnStar	Embedded LTE – AT&T	6-12 Months/5 Years	Safety, security, diagnostics, mileage-based insurance
Ford	SYNC	Tethered	3 Years	Vehicle health report, 911 Assist
Chrysler	UCONNECT Access	Embedded 3G – Sprint	6/12 Months	911 Assist, breakdown assistance, vehicle tracking, remote start/unlocking
Audi	Audi Connect	Embedded LTE – AT&T	6 Months	Google connected services, smart parking (no telematics)
BMW	Assist	Embedded 3G	10 Years	ACN, 911 Assist, breakdown assistance, condition-based maintenance alerts
VW	Car-Net	Embedded 2G - VZ Telematics	6 Months	Safety, security, diagnostics, vehicle health reports, maintenance alerts
Toyota	Safety Connect	Embedded 2G – Verizon	12 Months	Safety and Security – ACN, 911 Assist, breakdown assistance, vehicle tracking
Hyundai	Bluelink	Verizon	3 Years	ACN, 911 Assist, breakdown assistance, vehicle tracking, recall alerts, critical fault notification, maintenance alerts, in-vehicle service scheduling, etc.
Kia	UVO	Tethered	Lifetime	Vehicle health reports, maintenance alerts, critical fault notifications
Mercedes	Mbrace 2	VZ Telematics	3-6 Months	Traditional safety and security services
Volvo	On Call	Embedded 3G – AT&T	3 Years	Safety, security and remote link app
Nissan	Nissan Connect	Tethered	NA	Only connected apps such as a Pandora, etc.
Honda	HondaLink	Tethered	NA	911 Assist only
Tesla	NA	Embedded 3G- AT&T	3-12 Months	No core telematics feature

Source: Frost & Sullivan.

# ADAS Market Outlook to 2020 – Six Fold Growth

Growth in the market for ADAS by 2020 is backed largely by mass-market OEMs while innovation is expected to keep European OEMs ahead of the curve



Note: All figures are rounded. The base year is 2012. Source: Frost & Sullivan

# Requirements for Various Levels of Vehicle Automation

The leap from semi- to highly-automated is fairly easy to accomplish as driver override exists; the leap to fully-automated driving requires artificial intelligence to replace the human driver.

Level of Automation	Assistance	Semi-automated	Highly Automated	Fully Automated
Adaptive headlamp control	Optional	Optional	Imperative	Optional
Radar	Imperative	Imperative	Imperative	Imperative
Ultrasonic sensors	Optional	Imperative	Imperative	Imperative
Forward-looking camera	Imperative	Imperative	Imperative	Imperative
Rear-vision camera	Optional	Imperative	Imperative	Imperative
Surround-view camera	Optional	Imperative	Imperative	Imperative
Night vision	Optional	Optional	Imperative	Imperative
LIDAR	Optional	Optional	Imperative	Imperative
Map-supported ADAS	Optional	Optional	Imperative	Imperative
Steering and braking automation	Optional	Imperative	Imperative	Imperative
Artificial intelligence	Optional	Optional	Optional	Imperative
Multiple redundancies	Optional	Optional	Optional	Imperative
Self-Learning systems	Optional	Optional	Optional	Imperative

Source: Frost & Sullivan;

# Vehicle Design Changes due to Automation

Several of the factors that will change will require higher levels of security

**2003 VW Golf**



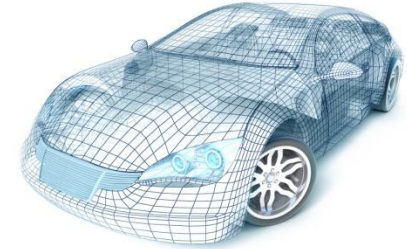
~35 ECUs  
~30 sensors  
<100 actuators

**2013 Ford Fusion**



~70 ECUs  
~75 sensors  
~150 actuators

**Automated car 2030**



~120 ECUs  
>100 sensors  
~200 actuators

Present	Parameter	Future
1-per safety-critical function	<b>Redundancies</b>	Several for each safety-critical function
Steering wheel, pedals, gearshift, etc.	<b>Vehicle Controls</b>	Buttons, navigation interface, touchscreens
Aesthetics, aerodynamics, ergonomics	<b>Design Criteria</b>	Aeodynamics, ergonomics
Primarily within the vehicle, with some telematics-based communication links	<b>Data Exchange</b>	High bandwidth data exchange for both inter- and intra-vehicular communication
All (or most) occupants face the road, partially reclining, fixed seats	<b>Seating</b>	Seating can be swivelled, fully-reclined, moved around to meet occupant's desires
Limited infotainment	<b>In-car experience</b>	Purpose built full-fledged infotainment

# Security the Big Picture

Over 50 vulnerable attack points exist in the modern day ECU driven smartphone on wheels and the concern is both in-car and back-end security

Remote Hacking  
Short Range (e.g. RFID)



Remote Lock/Unlock

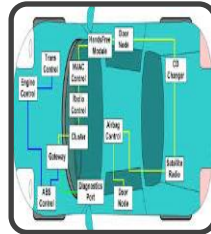


Manipulation



Vehicle Theft

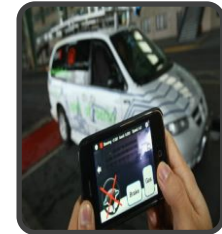
In-Car Hacking (e.g. USB)



Firmware  
Manipulation



Malware Injection



Feature Activation/  
Disabling

Remote Hacking  
Long Range (e.g. DSRC)



Copyrights



Valuable IP

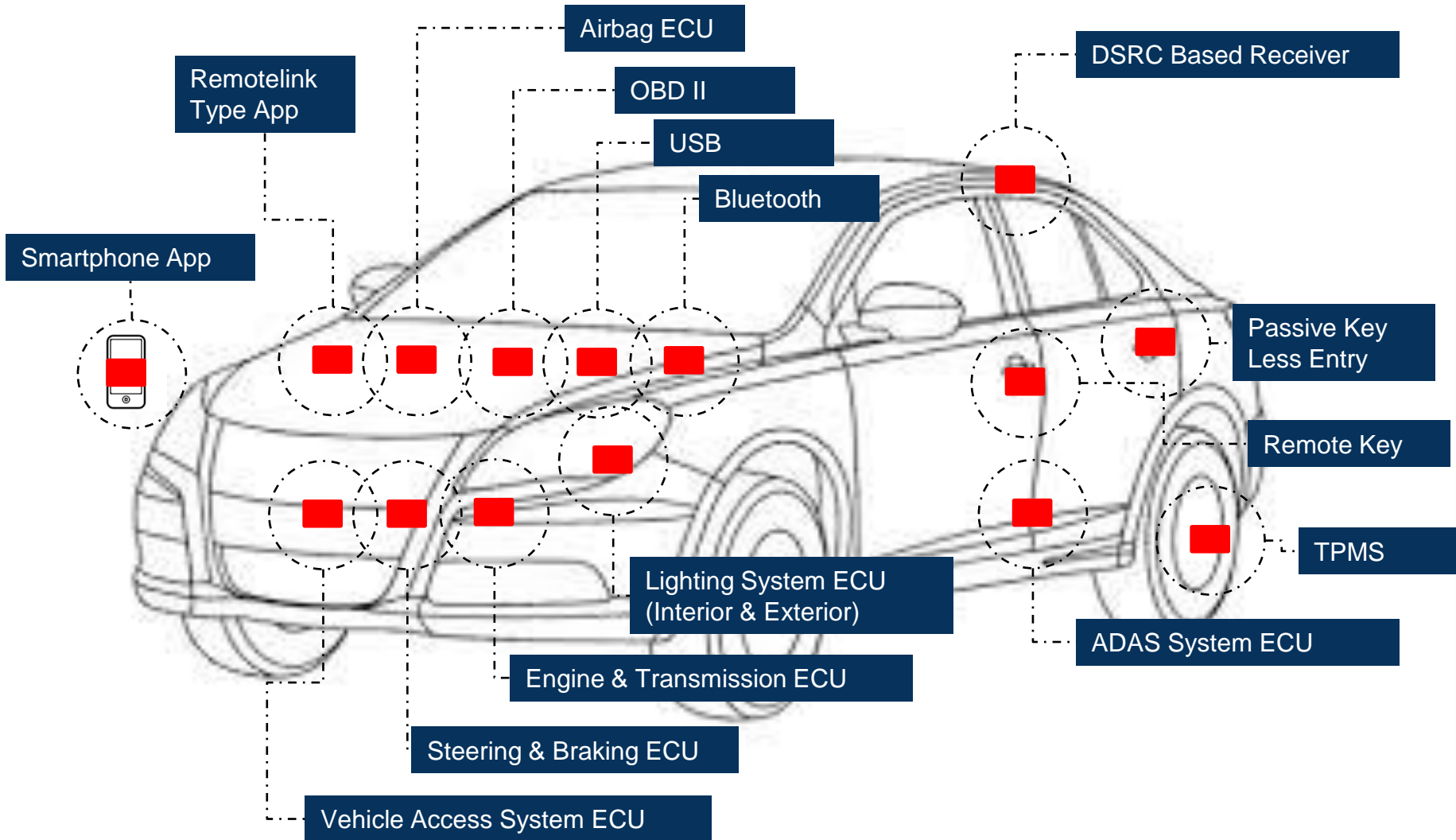


Licenses/Agreements



# The Current Day Focus

Almost 16 clear attack points exist in the moderate connected/safe car today

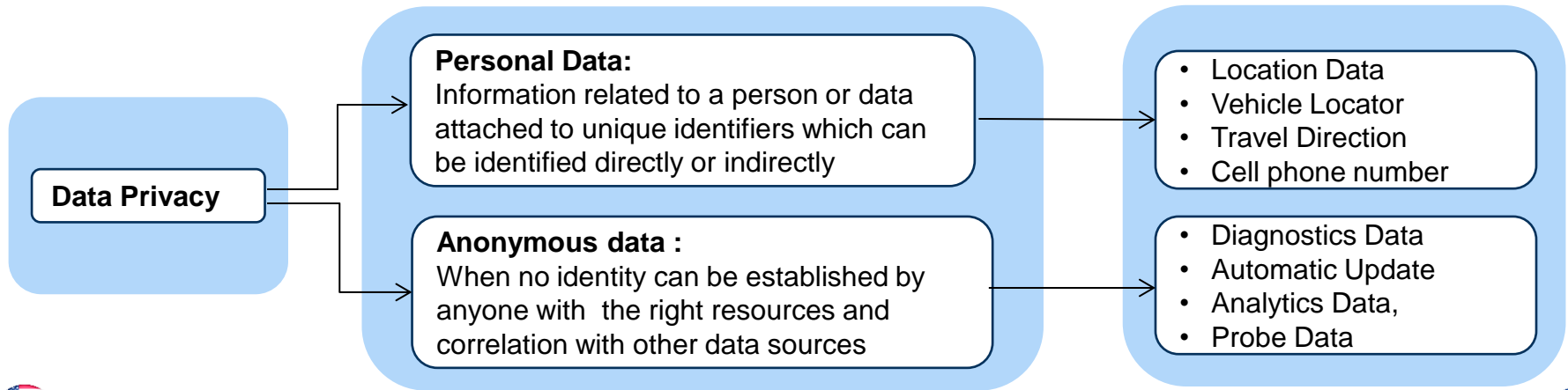




# Personal Identifiable Information (PII)

PII practices are key topic of discussion in North America and Europe as they try to establish norms on protecting consumer personal data.

## Cybersecurity Market: Personal Identifiable Information, Europe and North America, 2014



### US GAO's Recommended Practices

- Providing disclosure to consumers about data collection, use and sharing
- Obtaining consent and providing controls over location data
- Having data retention practices and safeguards
- Providing accountability for protecting consumers data

### EU Data Protection Elements

- Definition of personal data and understandable explanation
- Predefined purposes, time and volume limitation
- Balance of legitimate interest, consent and legal obligation
- Protect confidentiality and integrity
- Right to review, correct and object

Source: Frost & Sullivan

# How can Security be Improved

Most Important Action Item for OEMs currently is to create Virtualized Layers by which they can secure and stonewall mission critical vehicle systems

## Ways to Secure



**Firewalls Separating Critical Components**



**Secure/Hardened Operating System**



**Virtualization HW Partition Layers**



**Digital Certificates for Apps**



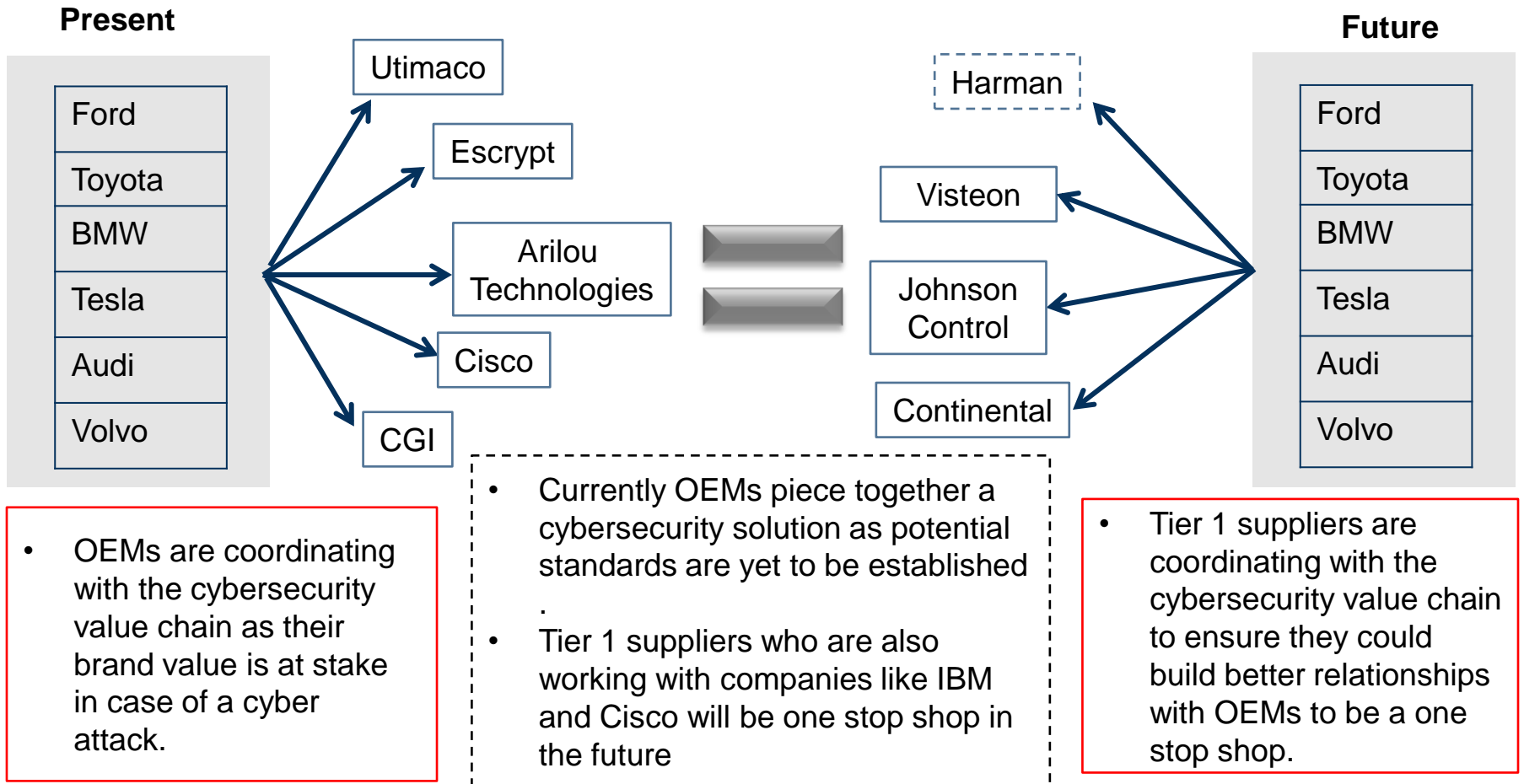
**Data Retention Policies**



**Data Ownership & Services for User**

# How is the Ecosystem Coordinated?

Specialist cybersecurity companies are working across the ecosystem to support security needs but the future might see a different scenario – e.g. Harman Acquiring Red Bend



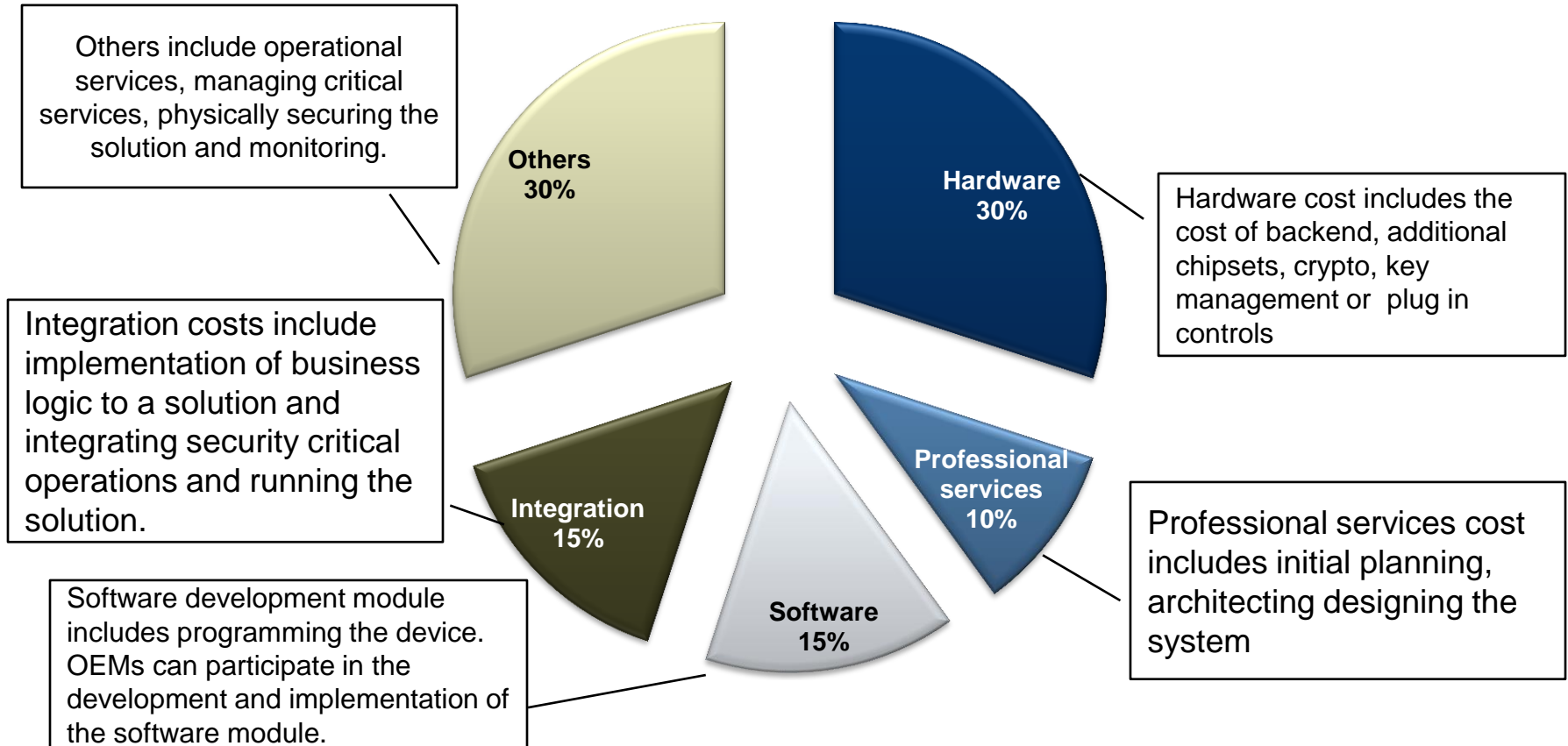
Source: Frost & Sullivan

# OEMs will be pushed towards Cybersecurity Solutions

Cybersecurity is a cost constraint to OEMs as it cannot be offered as a feature to the end consumer. OEMs today have to bare the cost of securing their cars.

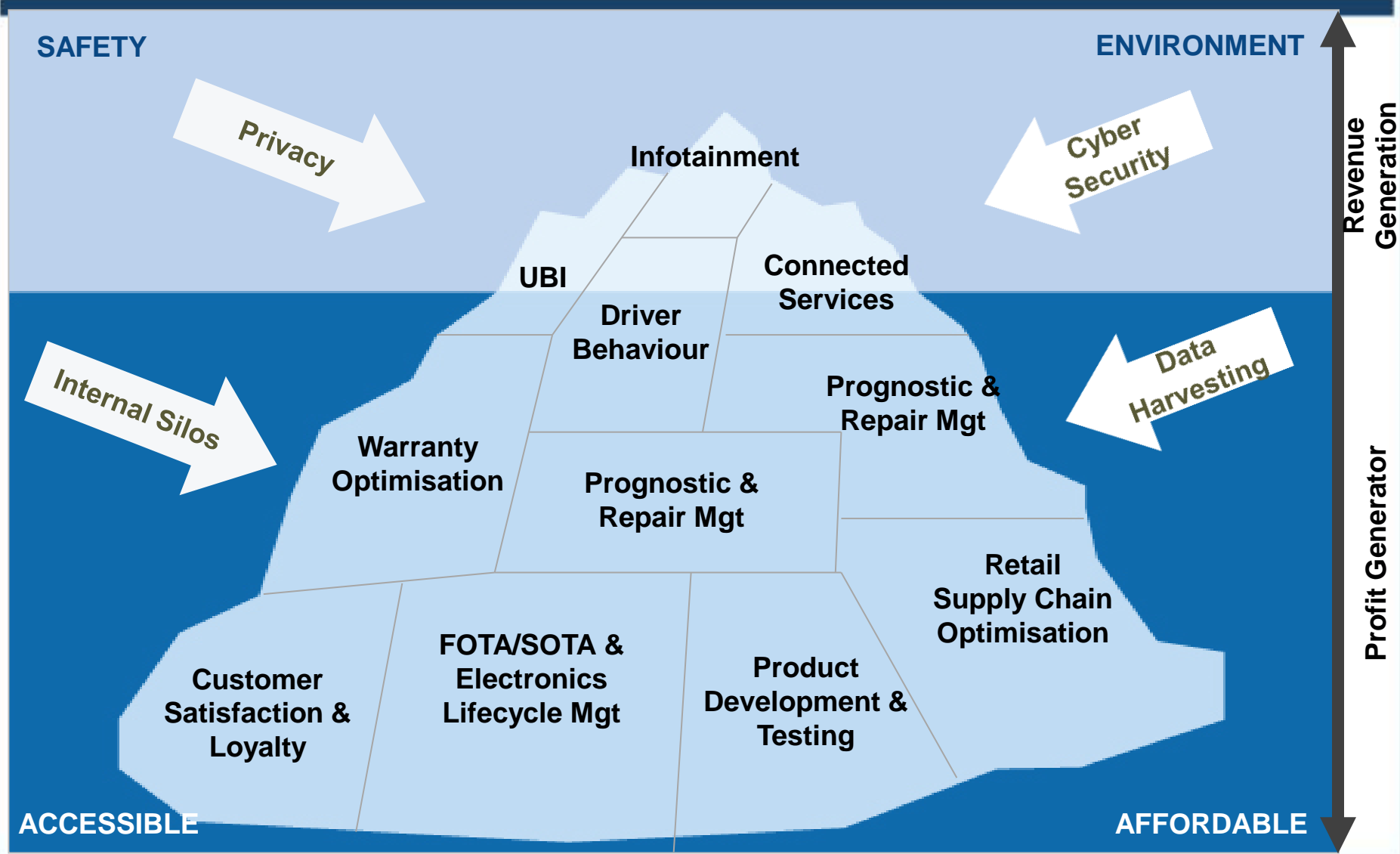
3-5%

## Cybersecurity of the cost of electronics



Source: Frost & Sullivan

# The Business Model of Connected car is like an “Iceberg” - The impact is significant, but the most important part is immersed !



# Thank You

---

FROST & SULLIVAN

**Praveen Narayanan**

Research Manager, Connected Cars  
Automotive & Transportation

P: 248.536.2008

M: 313.515.0614

[cpraveen@frost.com](mailto:cpraveen@frost.com)

