

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center



#RSAC

SESSION ID: MBS-T08

WITHIN 10 YEARS, AUTONOMOUS VEHICLES WILL CHANGE EVERY CISO'S JOB

Laura Koetzle

Vice President, Group Director.
Forrester Research
@lkoetzle



How many of you came to this session today because you wanted to see just how crazy this idea was?



“I think there is a world market for maybe five computers.”

--Thomas Watson, chairman of IBM, 1943









How do we define autonomy?

SAE's 6 Levels of Automation



SAE level	Name	Execution of Steering and Acceleration/Deceleration
<i>Human driver monitors the driving environment</i>		
0	No Automation	Human driver
1	Driver Assistance	Human driver and system
2	Partial Automation	System
<i>Automated driving system monitors the driving environment</i>		
3	Conditional Automation	System
4	High Automation	System
5	Full Automation	System

Source: SAE J3016, SAE International



#RSAC

Experts disagree about where the road leads.



Nirvana



Dystopia



#RSAC

So, which is it?



Neither.

Instead: Transformation.



Automotive



Logistics and shipping



Insurance and vehicle finance



Media and entertainment



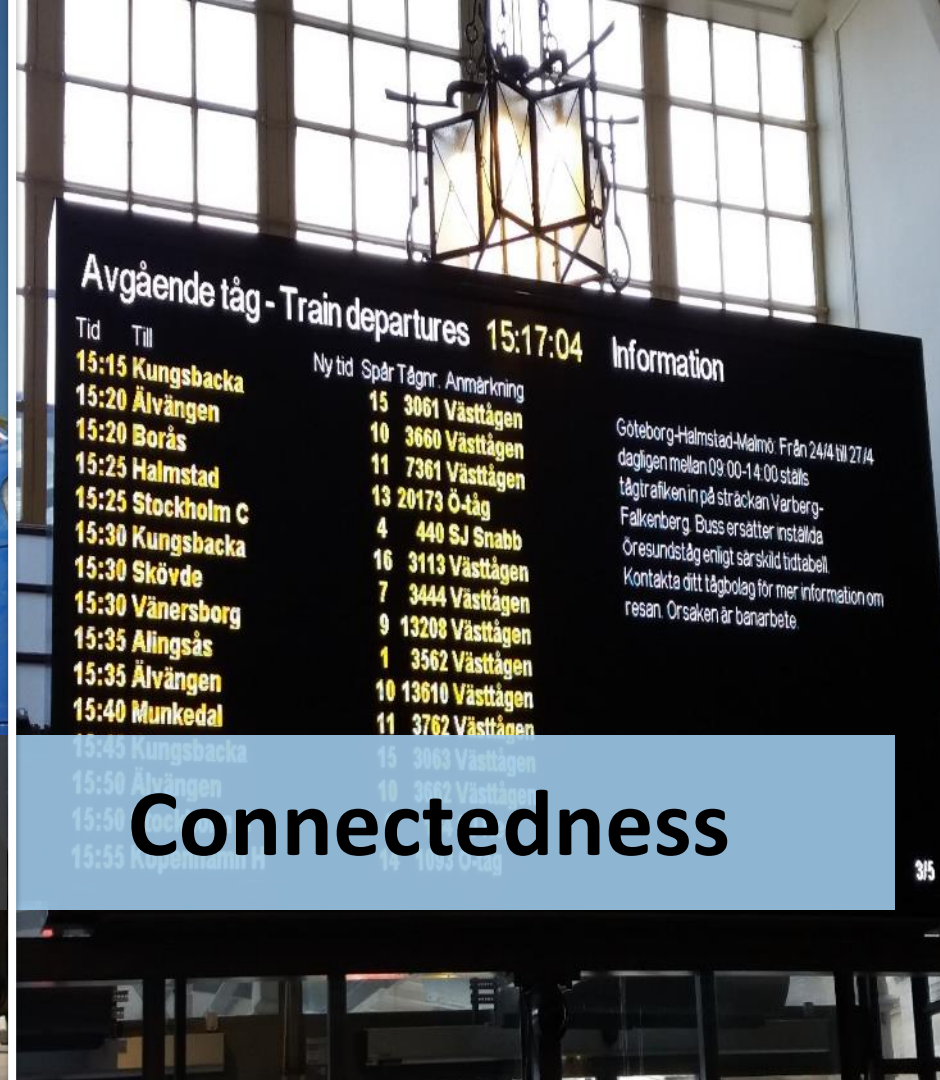
Public sector



**Information security and
privacy**



Autonomy



Connectedness

Automotive



Information security implications: Automotive



- Current model: “Vehicle only talks to the manufacturer’s back end.
Problem solved.”
- Over the air (OTA) vehicle system updates are tempting targets for introducing systemic vulnerabilities
- In-vehicle component architecture is segmented, and third parties can only get CAN-bus data from the OEM

Logistics and shipping



Information security implications: Logistics and shipping



- Current autonomous vehicle system design doesn't assume active sensor interference
- Current collision algorithms don't handle steep grades well, creating exploitable vulnerabilities
- Platooning will win over Level 3 autonomy

Insurance and vehicle finance



Information security implications: Insurance and vehicle finance



- Manufacturers, insurers, and public sector argue over ownership, use, and sharing of vehicle data
- Compromise solutions involve “neutral” servers to mirror OEM data and allow access to authorized third parties.
- Usage-based insurance (UBI) gives OEMs and insurers joint profit opportunities, but data output can drive controlling or discriminatory behavior

Media and entertainment



Information security implications: Media and entertainment



- Your firm needs ethical data usage guidelines on in-vehicle marketing and sponsored rides, too. Just because you *can*, doesn't mean you *should*.
- Autonomous vehicles drive finer-grained entitlements

Public sector

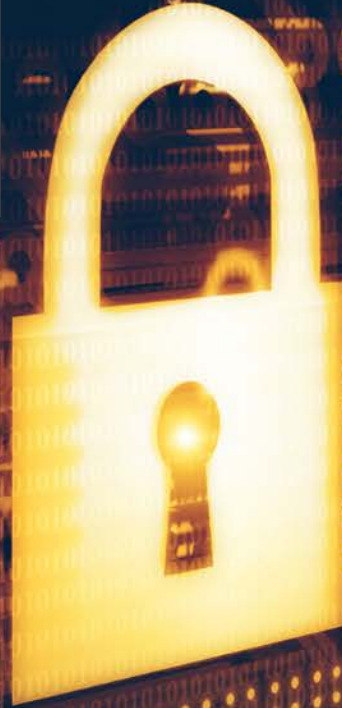


Information security implications: Public sector



- Vehicle to infrastructure (V2I) communication drives spoofing and poisoning attacks on public services (traffic, bridge closure updates, etc)
- City planners, infrastructure engineers, and transport policymakers need infosec help to play “what if” and incent useful behavior

Information security and privacy



Information security implications: Information security and privacy



- Autonomous vehicle security is indeed “just” an IoT security case. But each IoT security case is special.
- 10 years on, your firm will subsidize employees’ autonomous commutes; you will need to update employee relations and cyber-risk insurance policies to match



Three phases of transformation:

Three phases of transformation



Phase 1

2017 to 2020

- Warehouse automation
- Freight vehicle convoying/platooning
- Autonomous inland freight vessels and harbor convoys

Phase 2

2020 to 2025

- Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications
- Insurance rates rise
- Last mile autonomous drone deliveries
- Mobile parcel lockers

Phase 3

2025 and beyond

- All vehicles in Singapore and newly-built cities in China are autonomous
- Auto insurance rates fall
- Tesla no longer makes cars



**What does the threat model look like
in each of the three phases?**

Threat model: Phase one (2017-2020)



- Attacks on OTA updates of autonomous vehicle systems
- Companies transgress standards of ethical data usage, suffer losses of customer trust and fines (think EU GDPR enforcement)
- Third-party data sharing arrangements between OEMs, insurers, regulators, and service providers become prime targets

Threat model: Phase two (2020-2025)



- Attempted spoofing, poisoning, or disruption of V2V and V2I communications goes mainstream
- Sponsored rides and other in-vehicle advertising become targets; fraudsters get paid for spoofed eyeballs and deliberately flawed targeting

Threat model: Phase three (2025-beyond)



- Information security and safety concerns factor into “mandatory retirement” timelines for autonomous vehicles
- V2V and V2I communications decrease over time (vehicles become more “autonomous” in the true sense of the word) because they’ll always be more vulnerable to hacking



Further ripple effects





What to do next week



- Automotive, logistics and shipping, and transport:
 - Find your autonomous vehicle pilot groups, and start asking security questions
 - Pay particular attention to connections between vehicles, infrastructure, and people
- Insurance and vehicle financial services
 - Yours is mostly a conventional data security & privacy challenge, albeit bigger/faster/more
 - Boost the security of consortium and third-party data accessors; they're a softer target

What to do next week (II)



- Government
 - Offer your expertise to policy and regulatory working groups
- Media and entertainment
 - You may end up as the customer face of the autonomous vehicle, which makes you accountable for securing it
 - Understand your information security supply chain for these experiences

What to do in the next two years



- Discuss plans for autonomous commute support: Timelines, mechanisms supported, restrictions on employee usage planned
- Understand consumer and employee privacy expectations and regulatory requirements



“We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next 10.”

--Bill Gates, 1996

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: MBS-T08

THANK YOU



#RSAC

Laura Koetzle

+31.20.305.43.45

lkoetzle@forrester.com

@lkoetzle

For further reference:

Autonomous Vehicles Will Reshape The Global Economy