Cyber security in mobility

Shifting the focus from mobility safety towards mobility security

Technological breakthroughs are affecting the mobility ecosystem at a rapid pace. The continuing developments within the mobility sector raise questions about data sharing, data privacy, and cyber security from a mobility perspective. It is of vital importance that we think carefully about how we can best prepare for the future, how we can organize our systems and which parties we work with, and how we work with them. Especially considering that the aspects of cyber are changing and the boundaries between physical and digital are becoming increasingly blurred.

Ronald Heil MSc GICSP CISSP CISA
is a partner at KPMG Cyber.
heil.ronald@kpmg.nl

Marnix Bel MSc
is a consultant at KPMG Cyber.
bel.marnix@kpmg.nl

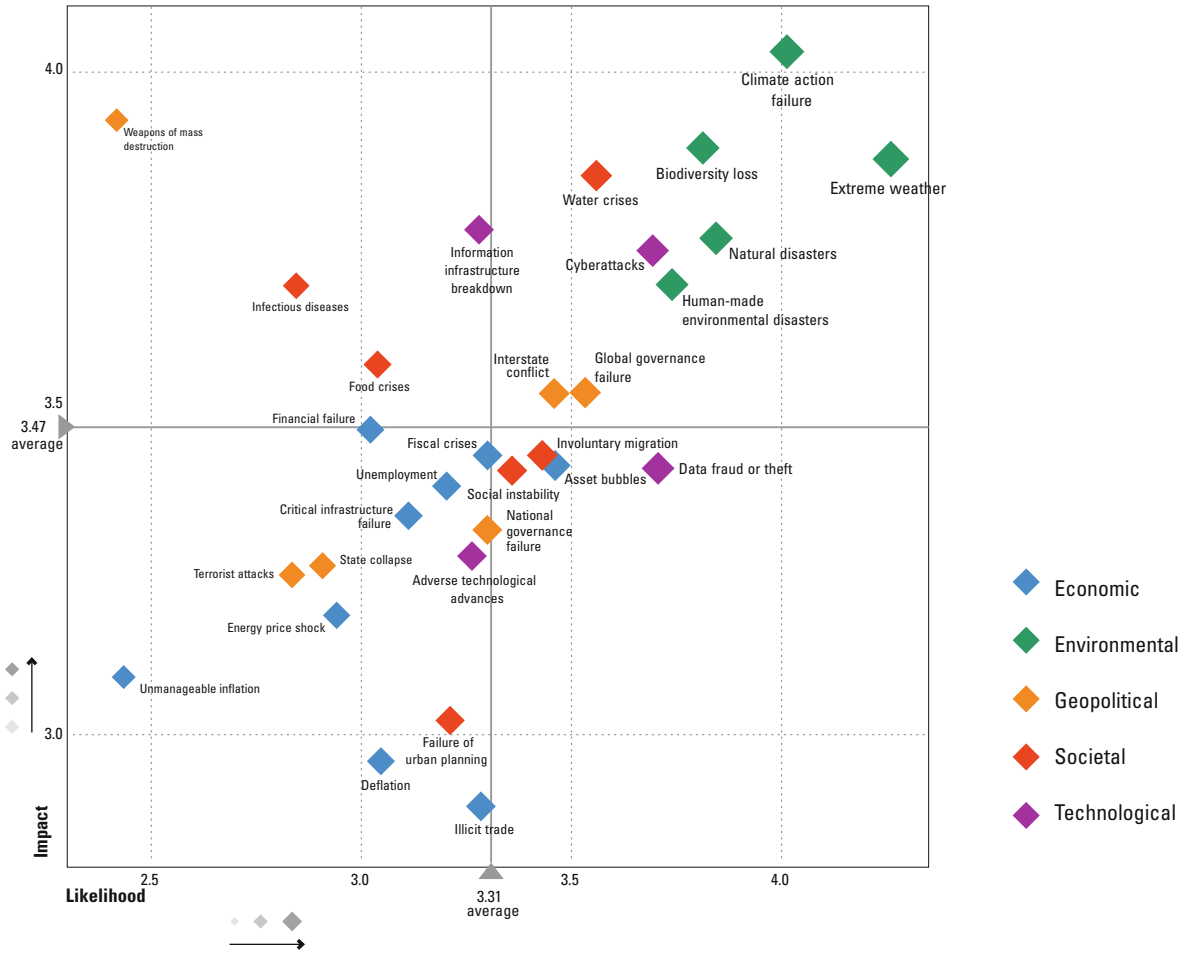

Figure 1. WEF – Global Risk Report 2020.

INTRODUCTION

We are on the verge of major and global changes. Technological breakthroughs from the so-called "fourth industrial revolution" are affecting our daily lives. These disruptive technologies and trends – such as the Internet of Things, automation, robotics, virtual reality and artificial intelligence – are changing the way we live and work. It is of vital importance that we think carefully about how we can best prepare for the future, organize our systems and which parties we work with ([Dams19]). This is, unsurprisingly, also the case for the mobility ecosystem.

Imagine a world where travelers move seamlessly from place to place. Where they stipulate their journey and travel preferences on an app, computer or kiosk, and are presented with journey choices according to their preferences with the best price/quality for their travel plan. Where public and private transport modes are fully integrated, where logistics and transportation providers co-operate to perform as efficiently as possible and where trucks don't drive back to the distribution center without cargo. Where algorithms guide our decisions. Where payment happens automatically, using a processing method of choice. Where the transition from one mode of transport to another is straightforward, perfectly timed and effortless. Where there are plenty of on-demand travel options, and users have ready access to real-time journey information and an integrated journey planning platform providing on-the-go notifications, alerts and alternatives for unexpected events ([Thom17]). Where the future of mobility will contribute to the safety, accessibility and sustainability of mobility.

Sounds very promising. Where can I sign up? However, whereas the future of mobility offers us many advantages, it also raises questions. What about companies sharing my data to facilitate my journey (data privacy)? Can I fully trust the software that controls the steering of my car without a physical backup (cyber security)? Historically, technology has always had two faces. One is the perspective of progress and innovation. The other: a potential shift of vulnerabilities which may lead to disruption of the "steady, comfortable equilibrium/normal". The World Economic Forum identified current trends and risks in their 2020 Global Risk Report. We couldn't agree more on some of the top risks, such as: data fraud, information infrastructure breakdown and, last

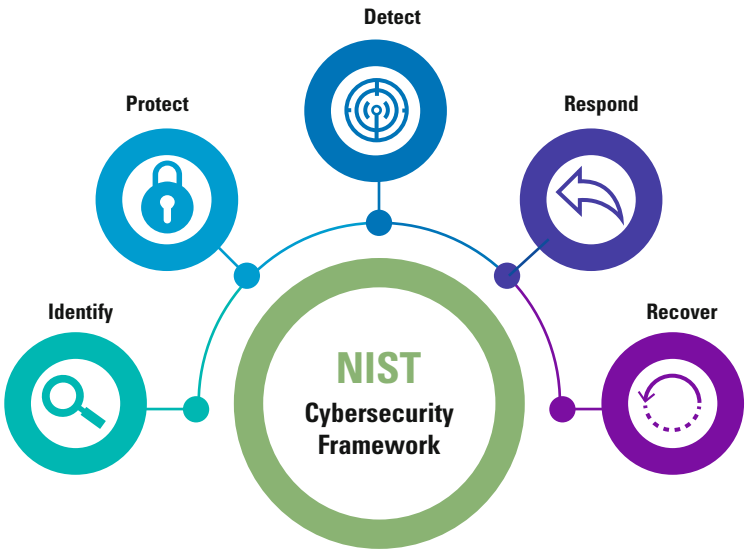

Figure 2. NIST CSF.

but not least – cyber-attacks ([WEF20]). Looking back at the previous revolutions in mobility, when the first cars started rolling from the assembly lines 100+ years ago, mobility in its "modern day form" became available for the masses. Nobody could truly foresee its benefits, or the potential issues such as traffic jams, parking permits and CO_2 pollution. And here we are, on the verge of the next revolution; industry 4.0 meets the mobility ecosystem.

How do we plan for security with fast-paced digitalization, hyper connectivity and automation of mobility? And how do we manage trust in this complicated sector that – upon disruption – may lead to social, economic and physical disturbances?

LET'S EXPLORE THE SECURITY CHALLENGES IN THE MOBILITY ECOSYSTEM

We have taken the first three elements of the NIST cyber security framework to analyze the mobility ecosystem ([NIST20]):

- Identify: know yourself, but especially know who is interested in you.
- Protect: protect your critical services against anyone.
- Detect: spot the "enemy" when they actually bypass the protective measures.

The framework also includes guidelines on how to respond and recover from an attack. We will not cover these topics in this article, but we will in a subsequent article:

- Respond: how to react when the "enemy" bypasses protective and detective measures but gets noticed in time.
- Recover: return the business back to usual when "shit hits the fan and the enemy compromised the estate".

Identify: know yourself and know your enemy

Keeping that analysis in mind, we should start by determining the mobility "crown jewels", the threat actors and align our security strategy for the mobility ecosystem.

The Mobility Crown Jewels: identify what matters most

The most valuable data, core processes and critical services which form the heart of an organization's business function are commonly referred to as Crown Jewels. Organizations need to identify and protect these. Data streams running through and within the mobility ecosystem can be seen as a criticality for proper functioning. Another example: the electrification of the mobility fleet in the Netherlands inevitably introduces security and capacity problems to the electricity grid.

The Mobility Ecosystem: it is all about the weakest link

The mobility ecosystem is fundamentally changing and redefines the conventional mobility usage. Traditional market boundaries are being broken. The automotive sector, energy sector, public sector, transport and logistics sector – they all have to deal with these trends, but also with new business models and mobility concepts. Organizations today operate within connected ecosystems that includes their suppliers. If any part of the ecosystem is attacked, other members of the ecosystem are at risk, making the ecosystem as strong as its weakest link.

Knowing yourself is all about focusing on that what matters most, both to yourself and to others you depend on. In the protection thereof, it is essential to find the right balance in your security efforts.

Threat actors: know your enemy

It is important to know yourself, and keep the following in mind: "keep your friends close and your enemies even closer", it is also very important to know your "enemies". Do you really know who is interested in your business? Or who wants to disrupt it? Or who wants to steal that small – but relevant – piece of information that is called competitive advantage?

Threat actors in cyberspace, and similarly in the mobility ecosystem, can be roughly categorized in the following categories ([Dams19]). Most hackers are referred to as script kiddies (e.g., inexperienced, usually young adolescent individuals or journalists that are looking for a juicy story, using known exploits and vulnerabilities). The impact of their cyber-attacks is, however, not to be underestimated. This is perfectly illustrated through the

success of Mirai DDoS botnets which was the work of low-skilled script kiddies. The infamous Internet-of-Things botnet took down major websites via massive distributed Denial-of-Service using hundreds of thousands of compromised Internet-Of-Things devices ([Burs17]).

Another important digital threat actors category is called cyber-criminal gangs. These gangs mainly have a financial motivation. As always, Hollywood managed to blur the lines between imagination and potential real-life future scenarios with its blockbuster The *Fate of the Furious* from 2017, in which hackers used autonomous cars as attack vehicles. A little longer ago, the *The Italian Job*, released in 2003, showcased automotive hacking skills. Using and abusing the infrastructure to ensure a swift getaway of the famous Mini Coopers, loaded with millions worth of gold. It won't be the first time that Hollywood's sometimes wild and endless imagination predicted more or less the future... Actually, this is already happening today, as both carmakers and the cyber security industry have accepted that connected cars are as vulnerable to hacking as anything else linked to the internet ([Gree17]).

Last but not least, nation state actors have entered the cyber-crime arena. Ever since Edward Snowden, former NSA contractor, revealed the depth of techniques used by the United Sates, it has become clear how much nation state actors invest in dominating the digital world. The US Department of Homeland Security has been warning against cyber-attacks by groups such as Dragonfly for many years. This actor group targets networks in the EU/US belonging to businesses involved in critical national infrastructure as well as their suppliers. The targets range from small businesses to major corporations that are responsible for the generation, transport and distribution of electricity and have the potential to put a halt to the most important power sources of the mobility ecosystem, crippling society ([NCTV19]).

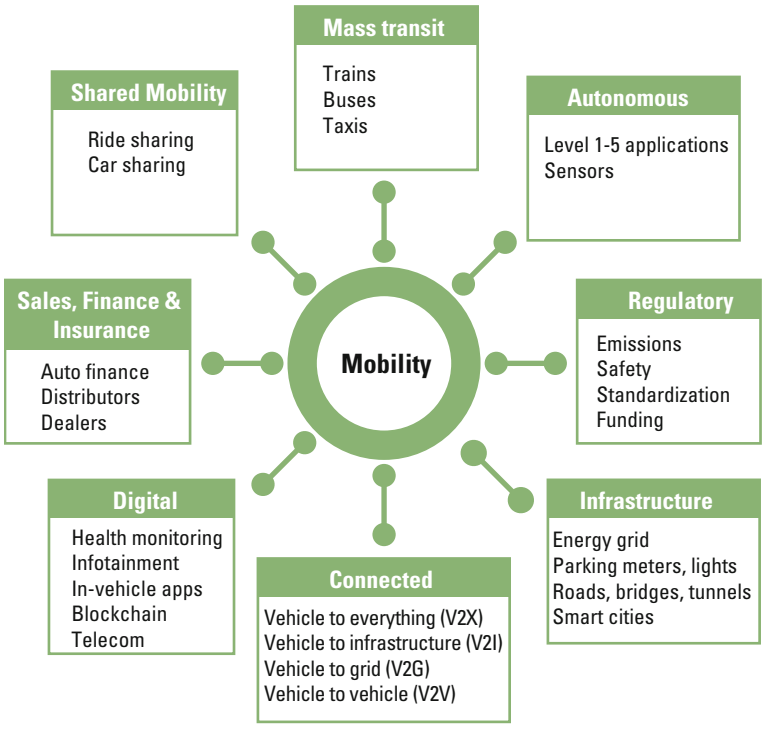

Figure 3. Mobility ecosystem.

The context of threat is emerging even faster

The threats the mobility sector is facing are changing, from "harmless" stealing of sensitive consumer data to impactful remote interference with the engine, steering and anti(block) braking systems. The risks linked to the modern forms of mobility are an unwanted side effect of the wireless connectivity with external networks, often through a mobile network connection (long-range wireless signal hacks) ([Youn16]). Similarly, passengers have the ability to connect a USB device or smartphone through the information port (wired and indirect physical hacks) and wireless devices via tethering or via onboard WiFi/Bluetooth systems (short-range hacks). All these connections increase the attack surface for malicious actors, and this is only accelerated further with the hyper connectivity in the mobility ecosystem.

With the increase of automation within the newly developed forms of mobility, the number of functions these devices run, increases as well. The functions vary from headlight control to critical systems such as brake control. Just like any other system, compromising one function, can endanger the entire system through the Controller Area Network (CAN) bus which links a car's various computers and information points together. Take the modern-day car for example: the mechanical linkage between the steering wheel and a car's front wheels is replaced by an electric power system, "drive by wire". After gaining access to the central bus, it becomes easy to control the car ([Cunn14]).

Policy makers and organizations must embrace a collaborative approach rather than pursuing fragmented or isolated developments of their own

Setting the standard for automotive cybersecurity

Traditional automotive safety and security standards have not sufficiently covered the topic of cybersecurity. The industry needed specific guidelines and standards for automotive cybersecurity. OEMs, ECU suppliers, cybersecurity vendors, governing organizations, and SME's joined forces to compose a deep and effective global standard for automotive cybersecurity. Using four main working groups focusing on 1) risk management, 2) product development, 3) production, operation, maintenance, and decommissioning, and 4) process overview, the ISO/SAE 21434 draft was born ([UPST20]). The standard formulated a common language between the automotive actors, criteria for effective automotive cybersecurity, accepted industry levels of cybersecurity assurance and regulatory enforced standardization.

Protect: making sure to keep the bad guys out

Secure by Design: secure from the start

In software engineering terms, "Secure by Design" means that software has been designed from the outset to be secure, thinking about security at the start of the project and throughout. A mindset that is much needed in critical sectors where human lives are on the line. Where safety and security are strongly related; it goes without saying that mobility that is not secure will ultimately not be safe.

Physical = Digital

"Mobility as a Service (MaaS) is the integration of various forms of transport services into a single mobility service accessible on demand" ([Tran19]).

Zero Day attacks are aimed at commonly used system. Zero Day is a computer software vulnerability that is generally unknown to those interested in mitigating the vulnerability. Zero Day attacks in the mobility market will not only have an economic and social impact, but physically endanger mankind and cascade effects to other industries.

Imagine a scenario where a cyber-criminal/ terrorist alleged group finds a Zero Day vulnerability that may affect tens of thousands of cars in Europe...

Organizations are beginning to compete and rush for a strong position in the mobility ecosystem to capture the greatest commercial value. However, for this to happen in a secure fashion, policy makers and organizations must embrace a collaborative approach rather than pursuing fragmented or isolated developments of their own ([KPMG19]). The "rush/time to market" to gain competitive advantage inherently causes more security related issues, where the "Secure by Design" mindset will lose focus and significance. Just to shed a light how detrimental this loss of focus can be; as was ruthlessly illustrated by the recently published investigation report by the House Committee on Transportation & Infrastructure on the two crashes that killed 346 people aboard Boeing's 737 Max ([Defa20]). The investigation outlined the "horrific culmination" of engineering flaws, mismanagement and a severe lack of federal oversight. The report, which condemns both Boeing and the Federal Aviation Administration for safety failures, emphasizing that Boeing prioritized profits over safety and that the agency granted the company too much sway over its own oversight ([Chok20]; [Levi20]).

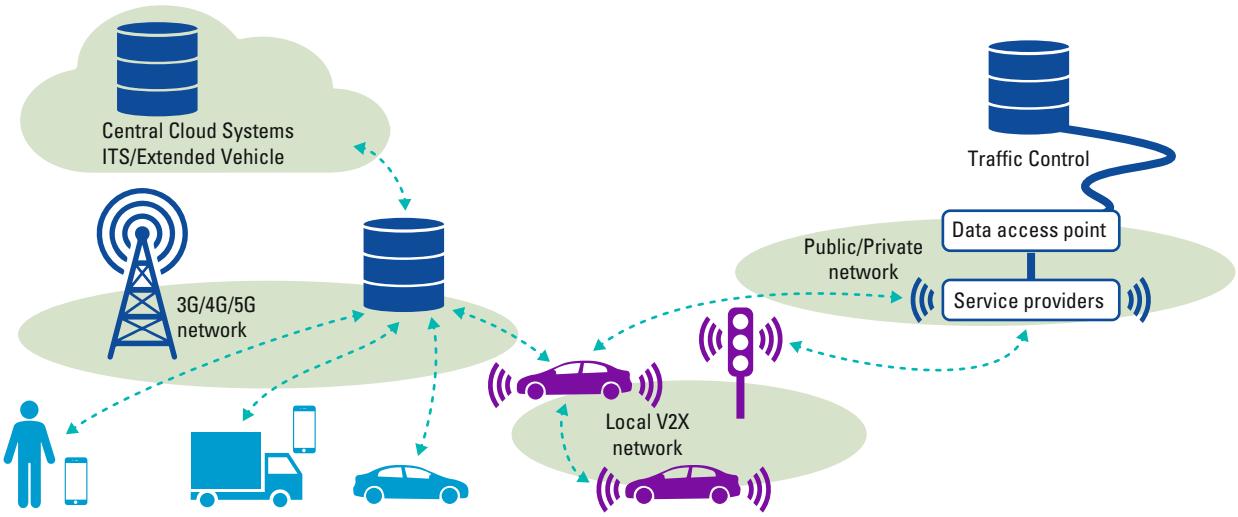

Figure 4. Overview of communication relationships between different actors in the mobility ecosystem ([KPMG19]).

Connecting the future of mobility: how do we keep the rapidly expanding need for data communication in the mobility ecosystem secure?
The (future) mobility world drives the ecosystem into a demand for real-time secure data flows, data availability and – of vital importance – data that can be trusted. As the ecosystem has yet to settle on common technologies and standards, the timing is right to introduce the principles of Secure by Design and Privacy by Design.

The automotive world is divided into two camps. NXP, among others, has put its cards on ITS-G5, a brother of WiFi, where the devices set up a direct link. Companies such as Qualcomm, on the other hand, see more in C-V2X (cellular v2x), a technology based on 4G where connections can run both directly and via a cell tower. The European Commission has committed to direct connections instead of cellular technology as a legal basis for communicating vehicles ([Edel18]).

"Hyper-connectivity"

Besides 3G/4G/5G connected mobility, other exciting ways of mobility communications are making their way in the mobility domain. These innovations have the potential to even bypass the telcos; namely LiFi (Light Fidelity) and car-to-car wireless mesh networks. LiFi is a technology based on communication using light as a medium. LiFi has evolved over the past years and has been proven to be secure, efficient and can send data at very high rates and might make its appearance in the mobility industry in the near future ([Haas18]). Car-to-car wireless mesh networks are basically a web of WiFi networks. It is made up of local networks to which cars and infrastructure are directly connected (also peer to peer).

Privacy by Design: what about data?
The continued increasing demand for data raises fundamental questions. Will anyone own data in the future? How can data be shared in a way that also respects the customer's privacy and does not breach their permissions? The success of a mobility ecosystem will depend heavily on the assurance that users and businesses are able to trust that their data is being used responsibly and appropriately. Legislation to this effect can be found in:

Article 10, Dutch constitution: right to respect privacy
Article 17 GDPR: Right to erasure ("right to be forgotten")
Delegated Regulation (EU) No 886/2013: "provision, where possible, of road safety-related minimum universal traffic information free of charge to users"

One of the distinguishing features of the mobility ecosystem will be the sheer amount of data it generates. Forecasts suggest that by 2025, the global datasphere will grow to 163ZB (i.e., a trillion gigabytes). That's ten times the 16.1ZB of data generated in 2016 ([Mell18]). Gartner analysts estimate around 80% of enterprise data today is unstructured, meaning not held in structured databases ([Rizk17]).

In a mobility ecosystem, data will inevitably flow between the different players so that the right services can be offered at the right time. This means that ownership, and especially responsibility of the data, will also change as it moves through the ecosystem ([KPMG18]).

Just like Secure by Design, we refer to Privacy by Design: the incorporation of privacy by default, embedded into every standard, protocol, process and carrying priority within the organization. Although we are seeing that privacy in the mobility ecosystem is receiving more and more attention, it is not yet on the level of Privacy by Design (just like Secure by Design is not).

The mobility ecosystem needs to develop innovative and collaborative data exchange platforms as soon as possible. The focus should be on incoming data that is cleansed and anonymized through a system of digital IDs. User information is tagged to a digital identity, which should not be accessible on a personal level. Under this model, data ownership would be shared between the participants across an ecosystem ([KPMG18]).

Fortunately, we see promising initiatives emerging, such as the National Data Warehouse for Traffic Information (NDW). This Dutch organization is known for its enormous database of both real-time and historic traffic data. The NDW has 19 public authorities working together on collecting, storing and distributing traffic data. Data is used to provide traffic information, to ensure effective traffic management, and to conduct accurate traffic analyses. The objective is a better accessibility and traffic flow ([NDW20]). Adding more actors that are active in the mobility ecosystems to the above-described independent data exchange platform(s) could potentially provide a very interesting combination as a start. Besides national initiatives, we also see some movement at European level. All European Transport Ministers, the European Commission and current industry partners joined forces and established the Data Task Force on Connected and Automated Driving. Their goal is to take the first steps towards data sharing for safety-related traffic Information in the European Union ([KPMG18]).

Detect: spot the "enemy" when they actually bypass the protective measures

Detect is about developing and implementing the right measures (governance, people, processes and technology) to identify the occurrence of the "enemy" bypassing the protective measures. In this article we only focus on the collective measures.

All of the stakeholders in the ecosystem have to work on their own detection measures. In the cyber security world "assume compromise" is a recognized concept and despite protection measures, one day ecosystem players will be hacked. Dutch companies might not even be well prepared to detect and respond to such attacks ([Dams19]).

Even more so, with the increased complexity, interconnectivity and dependency on each other (also in view of the weakest link in an ecosystem) it becomes very challenging – if not impossible – to implement adequate measures.

In order to overcome this, it is important that the stakeholders in the ecosystem are working together on cyber topics through a Mobility Information Sharing and Analysis Center (MISAC).

A MISAC is an excellent way to collaborate with other organizations within the same industry to increase the digital resilience of the organizations. The MISAC is used to share security expertise, share insights on incidents to prevent escalation in the ecosystem, incident response, and ideally provides the security eyes and ears of the mobility ecosystem.

To set up a MISAC, years of experience at the National Cyber Security Centre (NCSC) can be leveraged, which has already established many ISACs and used their developed roadmap to set up the (M)ISAC ([NCSC20]). Examples of industries that already implemented an ISAC are – not limited to; Airport, Chemistry/Oil, Energy, Financial Institutions, Legal and Nuclear.

Respond & Recover

As referenced in the introduction, this article focuses on the first three elements of the NIST cyber security framework: Identify, Protect and Detect. In the next edition we will revisit Detect in more detail and cover the Respond and Recover functions.

OUR VISION FOR THE MOBILITY ECOSYSTEM

We are on the verge of major and global changes. Technological breakthroughs from the fourth industrial revolution are affecting our daily lives. It could be said that we are not in an era of change, but in a change of era. It is of vital importance that we think carefully about how we can best prepare for the future, organize our systems and which parties to work with ([Dams19]).

Stakeholders in the mobility ecosystem should acknowledge the increasing complexity of the system (where working together is a must; and where there is full dependency on the weakest link – third party risk), the need for knowledge to be shared (from internal company-restricted to non-competitive sharing), and the need for a true Secure by Design and Privacy by Design approach.

The importance of independent consulting/knowledge firms and industry consortia will grow. They should grasp the opportunity and use their broad knowledge, experiences and expertise, which they accumulated by working in various industries, and transfer this into the mobility ecosystem.

From isolation to hyper connected ecosystems

Organizations in the mobility chain depend on each other's efforts to reduce risks to an acceptable level. To

this end, joint measures must be taken that are suitable for the entire chain. In essence, our vision for the future is a world in which:

- competitors work together to share data to mutual non-competitive advantage:
  - those organizations that attempt to keep data to themselves are unlikely to succeed – the network will simply be too big, too complex, and too open-sourced for this to be viable;
- we will need to see ecosystems, or "federations of competitors":
  - success will be about collaboration and cooperation – it will be about "co-opetition"!
  - joint effort in securing and monitoring the mobility ecosystem;
  - ensuring that interactions within the ecosystem stakeholders are valid, accurate and can be trusted;
- we will need to see the creation of independent data exchange platforms – shared platforms into which data would flow and:
  - incoming data is cleansed and anonymized through a system of digital IDs;
  - the protection measures are data oriented (not system, database or network oriented – the "zero trust" principle has to be applied);
  - access is regulated for each and every individual piece of data (based on identity, context, etc.);
- as said earlier, but worth repeating: a world in which Secure by Design and Data by Design are the "new normal".

References

[Burs17] Bursztein, E. (2017). Inside the infamous Mirai IoT Botnet: A Retrospective Analysis. Cloudflare. Retrieved from: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[Chok20] Chokshi, N. (2020, September 16). House Report Condemns Boeing and F.A.A. in 737 Max Disasters. Retrieved from: https://www.nytimes.com/2020/09/16/business/boeing-737-max-house-report.html

[Cunn14] Cunningham, W. (2014, February 11). Power steering shifts to electric. Retrieved from: https://www.cnet.com/roadshow/news/power-steering-shifts-to-electric/

[Dams19] Dams, T. et al. (2019). *Gaming the new security nexus.* Retrieved from: https://home.kpmg/content/dam/kpmg/nl/pdf/2019/advisory/gaming-the-new-security-nexus.pdf

[Defa20] Defazio, P. et al. (2020). *The design, development & certification of the Boeing 737 MAX.* Retrieved from: https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf

[Edel18] Edelman, P. (2020, October 22). EU kiest kant van NXP-kamp voor communicerende auto. Retrieved from: https://bits-chips.nl/artikel/eu-kiest-kant-van-nxp-kamp-voor-communicerende-auto/

[Gree17] Greenberg, A. (2017, August 16). A Deep Flaw in Your Car Lets Hackers Shut Down Safety Features. Retrieved from: https://www.wired.com/story/car-hack-shut-down-safety-features/

[Haas18] Haas, H. (2018). LiFi is a paradigm-shifting 5G technology. *Elsevier*, 2018(3), 26-31. Retrieved from: https://www.sciencedirect.com/science/article/pii/S2405428317300151

[KPMG18] KPMG (2018). *Mobility 2030 – Data rules.* Retrieved from: https://home.kpmg/content/dam/kpmg/xx/pdf/2018/10/mobility-2030-data-rules.pdf

[KPMG19] KPMG (2019, December). *Mobility 2030: Are you ready to rise to the challenge?* Retrieved from: https://assets.kpmg/content/dam/kpmg/nl/pdf/2019/advisory/mobility_report.pdf

[Levi20] Levin, A. (2020, September 16). Sweeping Failures and Insufficient Oversight Led to Boeing 737 Max Crashes, Scathing House Report Finds. Retrieved from: https://time.com/5889376/boeing-737-max-house-report/

[Mell18] Mellor, C. (2018, October 23). Igneous debuts DataThings for unstructured data management. Retrieved from: https://blocksandfiles.com/2018/10/23/igneous-introduces-datathings-for-unstructured-data-management/

[NCSC20] NCSC (2020). Samenwerking in een ISAC. Retrieved from: https://www.ncsc.nl/aan-de-slag/samenwerken/start-zelf-samenwerking/samenwerking-sector

[NCTV19] NCTV (2019). Cyber Security Assessment Netherlands. Retrieved from: https://www.thehaguesecuritydelta.com/media/com_hsd/report/255/document/CSBN2019-EN-def-Web-01-tcm32-405804.pdf

[NDW20] NDW (2020). National Road Traffic Portal. Retrieved from: https://ndw.nu/en/

[NIST20] NIST (2020). NIST Sybersecurity Framework. Retrieved from: https://www.nist.gov/cyberframework

[Rizk17] Rizkallah, J. (2017, June 5). The Big (Unstructured) Data Problem. Retrieved from: https://www.forbes.com/sites/forbestechcouncil/2017/06/05/the-big-unstructured-data-problem/#596b43d4493a

[Thom17] Thomas, E. et al. (2017). *Reimagine Places: Mobility as a Service.* Retrieved from: https://home.kpmg/content/dam/kpmg/uk/pdf/2017/08/reimagine_places_maas.pdf

[Tran19] Transit Protocol (2019, June 19). What is Mobility as a Service? Retrieved from: https://medium.com/@transitprotocol/what-is-mobility-as-a-service-672259066c87

[UPST20] Upstream (2020). ISO/SAE 21434: Setting the Standard for Automotive Cybersecurity. Retrieved from: https://upstream.auto/lp-setting-the-standard-for-automotive-cybersecurity/

[WEF20] World Economic Forum (2020). *The Global Risks Report.* Retrieved from: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

[Youn16] Young, M. (2016, December 12). The Big Problem with Connected Car Security That No One is Talking About. Retrieved from: https://www.pubnub.com/blog/the-big-problem-with-connected-car-security-that-no-one-is-talking-about/

About the authors

Ronald Heil MSc GICSP CISSP CISA is Cyber Security Partner at KPMG Advisory N.V. Over the last 18 years, he specialized in IT and OT Security, Cyber Defense/Resilience, Threat and Vulnerability Management, IT Auditing, and the security of Industrial Control Systems (ICS) and Industrial Internet of Things (IIoT).

Marnix Bel MSc is Cyber Security Consultant at KPMG Advisory N.V. Through his Master thesis, Marnix specialized in the field of Automotive Cyber Security and 5G and continued this during his time at KPMG. He also focuses on the Public Key Infrastructure (PKI) domain, providing independent assessments of the effectiveness of the architecture and security of PKI environments.