international risk
governance center

WORKSHOP REPORT

Governing Cybersecurity Risks and Benefits of the Internet of Things: Connected Medical & Health Devices and Connected Vehicles

IRGC Expert Workshop
Swiss Re CGD, 15 – 16 November 2016

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

This report should be cited as: EPFL IRGC (2017). Governing cybersecurity risks and benefits of the Internet of Things: Connected medical & health devices and connected vehicles. Workshop report. Lausanne: EPFL International Risk Governance Center.

Available from: irgc.epfl.ch

For any questions, please contact: irgc@epfl.ch

Contents

Figures

Introduction

As part of an on-going workshop series and project work on cybersecurity and in line with its mission to bridge the gap between science and policy, IRGC organised a one-day expert workshop on Governing Cybersecurity Risks and Benefits in the Internet of Things (IoT), applied to connected vehicles and medical devices - Creating trust in connectivity: confidentiality, integrity and availability.

With the support of Swiss Re and AXA Technology Services, the invitation-only multidisciplinary workshop, held on 15 – 16 November 2016 at the Swiss Re Centre for Global Dialogue in Rüschlikon, Switzerland, brought together 30 experts from research, technology, industry, regulation, insurance and other stakeholder groups in an open, facilitated roundtable discussion under Chatham House Rule.

The workshop discussed cybersecurity challenges in the IoT, with a focus on two different sectors:

- Implantable and wearable medical devices (many of them are connected via unsecured communication)
- Connected vehicles (connectivity between vehicles and between vehicles and infrastructure is necessary for all levels of automation, up to driverless operation)

In those sectors, connectivity improves both safety and vulnerability, and cybersecurity failures can be life-critical or -threatening. The cyber vulnerability of connected cars and medical devices has drawn much media attention over the past year, emphasising the potential for severe accident and the lack of information about the probability of harm due to cybersecurity risk. However, it is important not to distract attention from the true benefits of connectivity, in particular with regards to safety and efficiency.

Workshop participants discussed technical cybersecurity solutions (very different between sectors, but similar in principles), risk management options (trade-offs between patients' or drivers' physical *safety*, *privacy* and data protection, other cybersecurity concerns, and *cost*), standards and certification, regulation, liability and insurability issues (insurance may be the final enabler in a regulated environment).

This document reports the discussions at the workshop, which were informed by the expertise of participants, as well as by information gathered from a literature review and industry reports and presented in a background paper used to inform the workshop discussions. Most of the information contained in the background paper is not repeated in this document. Readers are thus advised to consult the background paper available at http://irgc.epfl.ch/events/workshops/cybersecurityIoT-Nov2016.

This workshop report is composed of the following sections:

1. Highlights
2. Notes from discussions among participants, organised around key themes
3. Specific aspects discussed during breakout groups on networked medical devices
4. Specific aspects discussed during breakout groups on connected vehicles
5. An appendix: A focus on innovation, benefits and cybersecurity risks

1 Highlights

Dependence on network connected technologies has grown faster than the means to secure it. The balancing of risk and benefit is very complex.
"The growth of network-connected devices, systems, and services comprising the Internet of Things (IoT) creates immense opportunities and benefits for our society. IoT security, however, has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks."
- U.S. Department of Homeland Security (November 2016)[1]

Key points from the workshop discussions included:

1. **Cybersecurity risk poses a considerable challenge in both the automotive and the medical device sectors**. Failures ('risk of a really bad scenario') could certainly hinder innovation and development, especially as some companies may try to ignore the risk or fail to communicate about known risks. Technology is moving fast to keep up, yet it is not clear whether the industry applies the best techniques available (security by design and by default, encryption, integration of secure elements, software update, etc.). This is because of potential technical difficulties, the costs involved and the lack of incentives and requirements by standard setting organisations, regulators and insurers.
2. **The traditional way of increasing security by isolating systems is outdated**. Attempting to isolate a critical system, which must be protected from a potentially insecure external system, is probably no longer the most effective method of protection. Moreover, cybersecurity cannot be fixed just with a technical solution certified by an authority. Technical solutions are important, but cybersecurity must be dynamic and holistic; it is the outcome of continuous improvement within an ecosystem of collaborating actors.
3. **The benefit-risk balance is changing because the innovators are not those who take the risk**. The asymmetry of information is obvious and there is little transparency about this issue. Much of the attention is focused on comfort, convenience and performance. In the event of a failure, it is very difficult to identify who is responsible and therefore liable. Clear attribution of legal liability is absent and would be needed, notably in the case of software defects.
4. **In both sectors, if consumers (patients, drivers) have to choose, they choose physical safety (to avoid the risk of a health or car accident) over cybersecurity and privacy.** When prompted, or in an emergency situation, people are inclined to give up on privacy (they give access to their private data) in exchange for increased safety, comfort and convenience. When one looks at how people behave in reality, it is clear that the notion of privacy is changing. Prioritising physical safety over cybersecurity also implies that IoT connected devices may remain vulnerable entry points into interconnected networks (e.g. medical records in health care systems, location tracking in cars). Regulators are advised to consider customer behaviour when they regulate about cybersecurity and privacy. Moreover, trade-offs between privacy and security often have to be made at the individual level; but the choice that an individual

[1] Strategic Principles for Securing the Internet of Things (IoT). Available at: http://bit.ly/2eXOGzV

makes at any given moment may not be the best choice for society or for that individual later in life. Therefore, the development and use of methods that would enhance both privacy *and* security (such as with 'usable security' where the default option is both privacy and security and the consumer does not have to make a choice) should be encouraged.

5. **Collaboration between actors is still ill-developed.** Important actors in the dialogue to develop a common understanding of the cybersecurity challenge include governments and regulators, certification agencies, data protection agencies, industry (manufacturers), technology and security companies, service providers, telecom operators, insurance and user associations. Although compulsory incident reporting schemes in other sectors have demonstrated their effectiveness in contributing to raising awareness, thus encouraging the development of both technical and governance solutions, the medical and automotive industries are not keen on sharing information on cybersecurity incidents with others (whether regulators, insurers, the public, or even with those in the same industry). From 2018 data privacy breach reporting will become mandatory under the 2016 EU Global Data Protection Regulation (GDPR) and, for some sectors, the 2016 Network Information Security Directive (NISD). This reporting is primarily to regulators, but the GDPR also includes an obligation to notify affected individuals in certain cases. Cybersecurity may hence become a question of trust between manufacturers and their customer. Reputation matters.
6. **Cybersecurity is a challenge for standard-setting and certifying organisations, as well as public regulation**. Regulation has to adapt to a fast evolving field. If it is too strict it will hinder innovation and incentivise free riders. It may be that it is not possible to certify the cybersecurity of connected devices. Both standardisation and regulation may have to move towards recommending or requiring the adoption of certain principles and processes towards improvement, rather than a certain 'level' which manufacturers will aim to hit, but not exceed.
7. **The insurance of cybersecurity risk is a challenge**. Through interconnected supply chains and contracts, the risk of accumulation is considerable to insurers. However, if insurers cannot provide the necessary cover for cybersecurity risk, this will create gaps in the risk transfer chain, with threats to business and consumers. As insurance is a key actor to enable or constrain an innovation in coming to market in a regulated sector, their role in the IoT is critical. Cyber insurance for extraordinary events may eventually look like terrorism or natural catastrophe insurance, with governments providing coverage above a certain limit.
8. **Self-regulation by industry should not be neglected.** Public regulators are advised to create incentives for codes of conducts among manufacturers, thus fostering self-regulation and perhaps self-certification. Prior-approval types of regulation are not dynamic by default and do not allow the type of maintenance and updates that cybersecurity challenges require. Voluntary industry-level initiatives may provide a positive way forward if the industry can create and maintain trust with consumers and regulators. In this respect, it is up to industry to act. Self-regulation is accompanied by **liability regimes,** which are yet to be refined to address specific cybersecurity risks.

The IoT will continue to develop because many consumers, the industry and public institutions (e.g. in the health care sector or in public transport) are convinced that its benefits will exceed the cybersecurity risks. However, the possible occurrence of serious cybersecurity incidents may lead regulators to tighten product authorisation.

2 Key Themes

2.1 Cybersecurity risk in connected vehicles and medical devices

The purpose of connectivity is to bring benefit in the form of improved performance, convenience, comfort, efficiency or safety, and it is effective in achieving these goals. Technological innovation allows customers and users of services provided by the IoT to get access to cloud services and networks, allowing location-independent accessibility.

- IoT networks are complex. Connected devices are placed in an ecosystem of designers, manufacturers, service providers, customers and other actors. Each connected device can directly or indirectly interact with a large network of other devices and software, which raises issue of vulnerability to cyberattacks, especially when risks cascade from one network to another.
- Cybersecurity risks are relatively well known, but in reality these can be difficult to assess in both the type of threats and the extent of possible consequences beyond the well-documented individual cases.
- External or internal actors with the intention to cause harm can access an IoT device, manipulate the flow of information to and from that device or tamper with the device itself, prompting it to disrupt or disturb the services it is meant to deliver. The issue is particularly worrying if the services are critical to safety and health. The safety of patients who use a connected implantable or wearable medical device to monitor their health and deliver therapeutic treatment can be at risk. If a control unit of a connected car is hacked, the behaviour of the car can become unreliable or unsafe and cause an accident. In both cases, any device can be used as a virtual entry into interconnected systems, and the risk propagates.
- There is little information about the probability of harm due to cyber risk, which is probably statistically low, and we should be careful not to detract from the true benefits, in particular to physical safety and efficiency. At the same time, it is important to draw attention to these issues, because innovation is moving fast and innovation should take cybersecurity onboard, rather than ignoring it. Evaluating and managing the risk is complex and, in general, cybersecurity is not well integrated into organisations, whether in the automotive or the medical sectors. It is important to promote awareness and push the market toward better consideration of these issues and to generate confidence. In particular, regulators and insurers should be active participants and help design minimum requirements and principles or processes for improvement.
- Many aspects of protection need to be considered because each one can influence the risk. Beyond the well-known lack of cybersecurity measures such as authentication and encryption, other governance aspects are equally important, such as lack of user education, poorly-designed software, supply chains (where are the chips being manufactured), lack of concern by government and others with regards to use of open source software, weak and open access codes (login and passwords), and the fact that regulatory and certification agencies have not yet developed the necessary expertise or willingness to take responsibility for cyber risks.

2.1.1 Ransomware as the main motivation of hackers

The incentive for cybersecurity risk exploitation is primarily money (ransomware), where a hacker may raise the threat of physical harm in exchange for ransom. Ransomware demonstrates that the threat

is monetisable because individuals (patient, drivers and passengers of connected cars) are easy targets. Security researchers anticipate that attacks will soon be pre-packaged, as they have become in other sectors.

2.1.2 Low level of cyber risk awareness

The level of awareness about cybersecurity risk is generally low. One of the main problems is the discrepancy between the perceived risk and the perceived benefit of protection. Surveys among users of connected medical devices indicate that there is some general perception of the cyber risk but little concern about the fact that the risk may apply to their own devices.

2.1.3 Slow phasing out of legacy systems

There is a problem of legacy systems because of the co-existence of modern connectivity systems and devices with older devices, with low or insecure connectivity. This problem raises the question of maintenance and update, which can be a problematic issue for IoT software. If software updates are done during physical maintenance events, then this it is not sufficiently frequent. And if it is done over the air, it may be more difficult to guarantee security. Recalls are costly. Concepts such as 'end-of-life product' are not prevalent in both industries.[2]

2.1.4 Limitations of scanning for threat detection

The list of known threats, vulnerabilities and malicious software is continuously changing. Some platforms are resource or energy constrained, so they cannot run all the scans that would be needed. Even some antivirus software were found to have remote code exploitation, so they can become the source of the problem, not only the solution.

2.1.5 Basic recommendations

Operators of connected device networks are advised to work to understand the threats to their critical assets, assess and apply security measures, and collaborate to enhance cybersecurity. Promoting collaboration on cyber risk awareness, assessment and management is a key recommendation, which would help integrate cybersecurity into business processes, assist in developing products integrating cybersecurity with safety, and promoting a cybersecurity culture.

2.2 Driving the process of improving cybersecurity in the IoT through collaboration

Workshop participants emphasised the lack of, and the need for, more effective collaboration among IoT stakeholders. This report suggests that many of the challenges derive from a lack of effective collaboration and that potential solutions could stem from organised collaboration[3].

2.2.1 Who can drive the process?

To trigger a change, it may be useful to consider what the possible drivers are.

- Regarding cybersecurity of medical devices, the US regulator (FDA) has issued principles and recommendations, but it lets manufacturers work it out. FDA encourages manufacturers to work together, but collaboration is hindered because of the highly competitive environment

[2] See also sections 2.4.1 (the legacy problem) and 2.8 (software issues)

[3] For example, the National Telecommunications and Information Administration (NTIA) has convened a multi-stakeholder process concerning the “Internet of Things Upgradability and Patching” to bring stakeholders together to share the range of views on security upgradability and patching, and to establish more concrete goals for industry-wide adoption." Available at http://bit.ly/2mIzcc1.

and lack of maturity and capacity to address the cybersecurity issues collectively. Therefore, customers should probably contribute to driving the process in terms of what they require.

- For connected cars, industry is also driving the process, but insurers can contribute to promoting cybersecurity requirements. And this primarily because nothing will be done without insurance, as no car can get on the road without its driver or owner being insured. If insurance does not talk about cybersecurity, then the issue will not be taken seriously. Insurance must also design certain specific requirements. Regulators can also drive the process, including if there is unwillingness of industry to collaborate and exchange information on cybersecurity.

2.2.2 Defining what is meant by 'ensuring maximum safety and security'

To ensure maximum safety and security, stakeholders who want to collaborate could consider the following questions[4]:

- How safe and secure should connected vehicles and medical devices be *before* they are authorised and released to the market? This question implies that an authorisation system is put in place, which is the case for many medical devices, although not for some personal monitoring devices and wearables, and is not the case for connected vehicles. The main drivers should be *regulators* and *standard setting organisations*, which must clarify a minimum acceptable level of security, yet with a deliberate intention to improve continuously, adapt regulation and progressively clarify attribution of liability, possibly through litigation.
- How can a defined degree of safety and cybersecurity be reached as quickly as possible? It is primarily the role of *industry* and *customers* to drive the process here, to adopt self-regulation, good practices and above all, a culture of cybersecurity. IoT device manufacturers and service providers should care about customer data protection, not only where it is regulated but also because it is part of the trust relationship with customers. Customers can drive the process towards cybersecurity if they select devices and providers based on their confidence that the security issues are well managed, in addition to a selection based on convenience, comfort of use and price.
- How can we ensure that the most securely protected connected devices are those that customers purchase, once they reach an appropriate level of cybersecurity? The driver here might be *insurance* companies, which offer more attractive premiums to customers who opt for devices and software that are protected more securely.

2.3 Holistic cybersecurity

The challenge with cybersecurity is that all devices connected in the IoT environment are directly or indirectly possibly connected with each other. The risk is therefore 'the weakest link in the chain'. This link may be the device, the hardware, the software, the user, the network, a hacker, changes in regulations, or any individual, process or technology that comprises the chain. Often this is unknown.

[4] A slightly modified version of the questions were posed by Nidhi Kalra, Rand Corporation, in a presentation about " Informing regulations for autonomous vehicle technologies", at the IRGC conference on Planned Adaptive Regulation (London, January 2016)

- Cybersecurity is still predominantly approached restrictively. Most risk managers try to solve the problem from a traditional risk-constrained approach. But connected devices, whether medical or vehicles, are driven by demand from consumers. Neither regulators nor consumers have yet clearly formulated what their requirements or expectations are. Security by design is necessary but not sufficient[5].
- Risks in automated vehicles involve: the car does not do what the passengers (or driver in control) want it to do (for example, hitting a truck because the car does not understand that it is a truck, like in the Tesla case in 2016) or that private data from a passenger are at risk from an end-user perspective. In the latter case, this has nothing to do with the car itself, but with how the data is stored and accessed in the cloud, and how the car depends on surrounding infrastructure. The ecosystem of connected cars has to become trustworthy.
- Cybersecurity cannot be a checklist. Applying a standard does not mean that security is achieved, because security is applied by people who most often have no special training in cybersecurity. We need usable security that is seamless and that users can easily apply.

2.4 Dynamic cybersecurity

Security is and will never be complete and perfect. Hackers are always ahead of users.

2.4.1 The legacy problem

Both for connected vehicles and medical devices, replacing a device because it is not up to modern standards in terms of cybersecurity is not the norm.

- By the time a vehicle is designed and put on the market, the technology inside is already a few years old. Modern mobile technology that consumers use in the car is more advanced than the technology embedded in the cars currently on the road. The gap creates weak points and vulnerabilities.
- Software quality and security can always be improved, but it is not realistic to expect that any potential vulnerability is patched with updates that are delivered and installed on a real-time basis. Some regulatory guidance is needed as to where the priorities are.

2.4.2 The problem of prior-approval

It is impossible to guarantee that nothing bad will happen. Therefore, when it comes to cybersecurity, the limitations of 'prior approval' regulatory systems such as those for vehicles in Europe and medical devices in the US are obvious.

- The type-approval system that Europe has for vehicles is a one-step process and is valid until the car is removed from circulation. This no longer works because cybersecurity is an ongoing process that needs regular monitoring and potentially upgrading.
- Similarly, the US FDA prior approval system for medical devices is progressively moving towards a principle-based approach whereby FDA evaluates the willingness and capacity of a manufacturer to adopt a life-cycle approach. This approach should consider the next

[5] On 15 November 2016, the U.S. Department of Homeland Security published in "strategic principles for securing the IoT", which provides a list of suggested practices to incorporate security at the design phase. These include: enabling security by default, building devices using the most recent operating systems, using hardware that incorporates security features and design with system and operational disruption in mind. Available at: http://bit.ly/2eXOGzV

generation of devices, the process for threat and vulnerability assessment, the ongoing need to protect sensitive data and how the communication to the network is managed. This approach seems to have a positive effect on designers and engineers who develop the products, but it is too early to know whether it will really work or be an improvement, compared to the traditional approach of strict regulation and standards.

- Confronted with the dynamic cyber threat landscape, conformity assessment systems can no longer guarantee complete security protection. Regulation and incentives are needed to deal with the responsibility to constantly update cybersecurity.

2.5 Cost and value of cybersecurity

Cybersecurity is an asset and a cost. There is a potential bifurcation of interest: the manufacturer bears the cost, but the end user enjoys the asset. It is not clear who is willing to pay for updates. Cybersecurity costs money.

- All stakeholders are invited to work together to make the business case that security is worth the investment. Demonstrating the benefit-cost of cybersecurity will be needed, so that it can be priced upfront and thus be valued by customers.
- This may be particularly challenging in the medical sector, where the cost of cybersecurity may add significantly to the primary cost of the device, and obviously in other IoT sectors, such as home monitoring and surveillance, which use video cameras that are often sold at low prices.

2.6 Resilience

Resilience building strategies include the design of devices that would exhibit safe behaviour under any circumstances, including in the case of a total system failure and operational disruption. This requires understanding the consequences that could result from the failure of a device. IoT devices that control critical safety functions should be able to fail safely and securely, so that users and the system are not negatively affected.

- Hospitals are now routinely attacked through ransomware and are ill-prepared for this attack vector. Resilience strategies are being considered seriously. They are often based on 'pen and paper' so that the ‘health system’ still maintains a minimum ability to operate.
- In the automotive sector, it is advisable to build redundancy and two-way systems across the entire ecosystem to allow for fully automated driving to function safely, even if under attack. To avoid the risk of cascading failure if an incident or accident occurs, there should already be strategies in place to substitute the failing or deficient part that causes, relays or prevents notification of an accident.

2.7 Trade-offs

Effective cybersecurity requires, and results from, identifying and resolving the major trade-offs between potentially conflicting objectives, including physical safety, security (as confidentiality, integrity and availability), privacy and costs. In the medical and automotive sectors, regulators and managers are *not yet* routinely considering that attitudes, regulations and practices to ensure physical safety must *also* address concerns about cybersecurity.

- To illustrate this, here is the extract of a conversation between workshop participants about connected medical devices:
  "- Are we more concerned about security or about the confidentiality of our information?
  - It seems that for life-threatening application, where people are first concerned about physical safety, it is security that matters most. But for non-life-critical devices, it is the confidentiality of information that matters most.
  - When we speak security, are we talking security overall, or just patient's privacy?
  - What matters most for medical devices is integrity and availability
  - Interoperability and the number of technical interfaces increase vulnerability, although both can also increase ways to remedy to failures and deficiencies."

2.7.1 Physical safety versus cybersecurity (and privacy)

- Similar to the case of medical devices security and privacy dilemma, when passengers in connected vehicles are confronted with the risk of an accident, they prioritise their safety over data protection and privacy. Ideally, they should not be placed in the situation of having to choose. So techniques that can deal with both issues should be adopted.

2.7.2 Cybersecurity versus privacy

- The challenge is to ensure cybersecurity without communicating data that should be kept private. This is currently not feasible in the transportation sector because communication systems are interconnected. Most communications enable the tracking of vehicles, which is against privacy principles. See section 4.2.2 for more details.

2.7.3 Cybersecurity versus price and versus convenience / comfort / performance

- Cybersecurity has a cost and can make things less convenient. Customers can accept a certain level of inconvenience when they see improved benefits elsewhere. They choose the level of inconvenience based on their level of perception of risk.
  In the absence of the ability to deploy cybersecurity updates, manufacturers and customers are faced with the decision between costly recalls and leaving devices with known vulnerabilities in circulation.

2.8 Software issues

Software developers (often at the request of the market) keep adding to the list of what could be improved, but this cannot go on endless. Comfort, convenience and evolvability are not good companions with cybersecurity.

2.8.1 Software update

- The issue of cybersecurity is linked to that of software 'correctness'. The problem is that we do not know how to write (or prioritise) software that is 'correct'. Avionic is probably the best example of a critical system where software is almost perfect, but it is also very difficult to evolve. The downside of this is that there is very little innovation in that field, and when there is innovation, it is very slow. Although it is not safety critical, changing the flight entertainment system is very difficult, just because it is on an airplane.
- Beyond the issue of cost (and who pays for software updates), nobody is pleased with the idea that software regularly or continuously needs to be upgraded. Some regulation is needed to trigger the process and indicate priorities.

- Do we need an 'update warranty' or legal obligation, perhaps implied by statute, to ensure that software will be updated as needed? Is this realistic? Could this guarantee that only legitimate updates will be installed?

2.8.2 Software liability

The issue of liability in case of a software defect is complex. In general, product liability legislation was not written with software in mind, but there are initiatives in Europe to build a new role for software cybersecurity investigation, which might lead to some attribution of liability in case of software defects (see also section 2.12 on liability). When cybersecurity breaches occur, multiple failures at various levels are involved. Consequently, we may need to look at shared responsibility models between software developers and vendors in order to address the software liability issue.

2.9 Insurance

Covering the cybersecurity risk is problematic and complex.

First, insurers must determine what they insure under the term 'cybersecurity', which may or may not be subject to regulation: Is it data availability and integrity? Or privacy and confidentiality? Cybersecurity itself needs to be broken down. For medical devices as well as private cars, insurers are primarily involved in product liability (insuring manufacturers if their products do not function as can be expected and harm someone). Are there priorities? Is there a hierarchy of needs? The answers differ. In some countries, with strict data privacy laws, privacy will come first. So questions that insurers ask before making a cybersecurity insurance proposal include: "In which jurisdiction are you? Where are your cloud and data storage services located? Which law does apply? How is the liability attached?"

Eventually, estimating probability and expected loss may be done with standard probabilistic risk assessments for small and frequent events, but not for rare and large attacks.

2.9.1 Data collection

- As insurers need data to analyse the risk they insure, they collect as much data as possible. Vehicles themselves can generate data through 'black boxes' (equivalent to flight recording systems in airplanes), On-Board Diagnostic (OBD) devices (a class of devices that capture a car's computer sensor data using the OBD port) or through native connectivity. One objective is to improve the insurance pricing sophistication. For insurers, it is an opportunity to increase the frequency of interactions with customers and to become a partner in their mobility.
- Challenges include: collecting valuable data, being transparent about the collection, storage and further use, and undertaking these activities in a way that is legally correct, under data protection and privacy laws.

2.9.2 Quantification and pricing

- After they have collected data, insurers can begin to quantify the risk and calculate the resulting cost of an accident or cybersecurity incident.
- Cyber threats are increasing. They are getting increasingly sophisticated. It is a challenge to quantify the risk and to monitor cybersecurity exposure (silent and affirmative covers). Data from claims and from intangible assets valuation are used to better price and underwrite.

2.9.3 Inhibitor versus accelerator of innovation

- In these conditions, it is difficult for insurers to have a role in the development of connectivity in medical devices and cars until regulators and industry provide more clarity.
- However, especially when insurance is required by law, insurance can set standards, and thus drive the market. There could be a problem with lowest common denominators, when some insurers may propose insurance covers without requiring minimum cybersecurity requirements, so some standard and legal certification are needed to ensure that insurers do not insure below standards. Insurers can contribute to driving the market toward more cybersecurity, but they need clear regulation for that.

2.10 Standardisation

In general, standardisation is a way to meet requirements and acceptability relatively easily. However, the reality is complex and a cautious view on standardisation is needed.

- First, if we conclude that the cybersecurity challenge has become too complex for existing risk management tools, including regulation and standardisation, then many stakeholders would be concerned. In particular, insurers would lack the regulatory basis that they need.
- Second, standardisation is generally good, but for cybersecurity insurers it may cause other problems because of the risk of cascading failures to all devices that follow the same standards. It is, therefore, key that any cybersecurity standards does not focus on the use of certain technologies or even a level of performance, but rather on both design (e.g. security by design, privacy by default) and establishing processes for improvement.
- Focusing on 'security by design' should aim to produce a tool-supported comprehensive methodology and analysis techniques to allow a vehicle or a medical device designer to make well-informed decisions at an early stage of designing a product architecture. In the automotive sector, this would for example determine how security measures that isolate and segregate secure systems in cars are articulated vis-à-vis security measures that would be at the level of the whole vehicle-infrastructure. Similarly, this approach would apply to the respective need for passive and non-scalable security versus active or dynamic security.
- Besides the incorporation of cybersecurity at the design phase, other criteria for evaluating it in standards are those that ensure the development of an appropriate culture of cybersecurity improvement (in addition to a safety culture, which is already present in the medical and automotive sector). Example include: promoting cybersecurity updates and dynamic vulnerability management, sharing and building on successful industry practices, integrating cybersecurity in business processes, and promoting transparency across IoT.

2.11 Incident reporting and sharing

One critical factor for advancing cybersecurity is the reporting by manufacturers, immediately after an incident has occurred. The sharing of incident event data across industry, across the supply and liability chain, is considered as the first step towards collaboration to address the cybersecurity concerns. Regulators and insurers could have a positive role to play here, to provide the legal basis, impetus and business rationale.

- In the US, hospitals have to report incidents only when there is an adverse impact. Cybersecurity may often not be recognised as the cause of the adverse event. But even when cybersecurity is recognised as the cause, it is often not reported because of concerns about liability, reputation and the need to be open to audits.
- There is however an incentive to incident reporting: that regulators could give access to incident data reported to them. Data from post-market surveillance can and should be used to inform customers and the industry. Regulators could help white-hackers get access to devices. Some countries give legal protection to those who reverse engineer software. This could be extended to protect those who test IoT devices and other systems for security weaknesses, within reason.
- A statutory award system could be developed to provide a "bug bounty" incentive to people who report weaknesses in a responsible fashion. This would have a dual effect: (a) It will encourage people to report issues that they find responsibly, and (b) it will hamper the black market for exploitable security issues: the value of the exploit on the black market is diminished because any buyer might then report it and claim the "bug bounty".
- Standards for incident reporting are key to making reporting correct and useful and to understand the cause of the incident.
- The EU Directive on the security of network and information systems (the NIS Directive), adopted in July 2016[6] sets the legal basis for cyber incident reporting and sharing in certain critical infrastructure sectors, including transportation, healthcare and cloud computing services. It establishes the principles of Computer Security Incident Response Team (CSIRT), cooperation among member states on specific cybersecurity incidents, sharing information about risks (CSIRT network) and a culture of security across sectors.
- From 2018, data privacy breach reporting will become mandatory under the 2016 EU Global Data Protection Regulation.[7]
- The US department of Homeland Security (DHS) recommendation is to "develop a policy regarding the coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a Computer Security Incident Response Team (CSIRT). The US Computer Emergency Readiness Team (US-CERT) Industrial Control Systems (ICS)-CERT, and other CSIRTs provide regular technical alerts, including after major incidents, which provide information about vulnerabilities and mitigation."[8]

2.12 Liability

In the current environment, it is often unclear who bears responsibility in the case of a cybersecurity failure in a given product or system. In addition, the cost of cybersecurity failures or deficiencies is often not borne by those who create the risk or who are able to increase cybersecurity. There is no evidence or clarity regarding who should be responsible for cybersecurity and who should be liable for cybersecurity failures in the IoT continuum, between the designer or manufacturer of a device, the

[6] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[7] http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[8] http://bit.ly/2eXOGzV

developer and supplier of a piece of software, the network operator to which the device is connected and the final device provider.

- There are differences between the two industries. In the automotive industry, car manufacturers (OEMs) perceive themselves as those who take the biggest hit if things go wrong (such as in the 'Jeep Cherokee' attack), so they are taking it seriously, especially because insurance is compulsory. In the medical sector, manufacturers do not share the same type and level of concern and insurance is not a major actor.
- Liability in case of cybersecurity breaches in the IoT is highly complex and unclear, with an ongoing debate about possible software liability having a central role, insurers being in the front line, and regulators or litigation systems possibly having to make the final decision.
- In the EU, Directive 85/374/EEC on liability for defective products excludes, in most cases, the liability of software developers primarily for the reason that "the state of scientific or technical knowledge at the time the product was put into circulation could not detect the defect". But an ongoing evaluation of this Directive in view of concerns about how should strict liability for damages be allocated between the different participants in the Internet of Things or, in more general terms, in the case of connected objects relying on each other, indicates that a revision of the Directive might allow some software liability.[9]
- In the meantime, if new liability schemes develop, it will most probably be through court cases that attribute liability in case of an accident and in a specific contextualised case. All actors, from manufacturers, software industry, insurers and regulators, should prepare for this. At the same time, they should collaborate, perhaps by way of contracts, in the attribution of product responsibility and civil liability. This would support the creation of an appropriate regulatory and legal environment and incentivise efforts to enhance the cybersecurity of the IoT.

[9] http://bit.ly/2dNn6tU

3 Connected Medical Devices and Wearables

3.1 Medical and wearable devices

3.1.1 Connected medical devices

A connected medical device (CMD) is a device that communicates with a private network, public internet, or point-to-point connection (wired or wireless), or can be accessed in standalone mode via a user or machine interface. CMDs include drug infusion pumps, insulin pumps, cardio defibrillators and pacemakers. The ecosystem of CMDs comprises databases, capital equipment (such as scanners or IRMs) diagnostics, implantables, remote monitoring and mobile apps. There are many common and vulnerable components, such as device software with their remote support and maintenance, firmware and device hardware, removable media and network access / firewalls, physical access, operating systems, database and /or storage, ports / interface, and clinical applications (e.g. treatment planning software). The technology of medical devices has advanced dramatically in the past 50 years, to become increasingly connected. The technology for activity trackers ('wearables') for mobile health (mHealth) has also developed considerably towards connected environments and enhanced monitoring of health and activity. The number of these devices exposed to malicious threats increases, resulting in an elevated risk to both patient safety and information security.

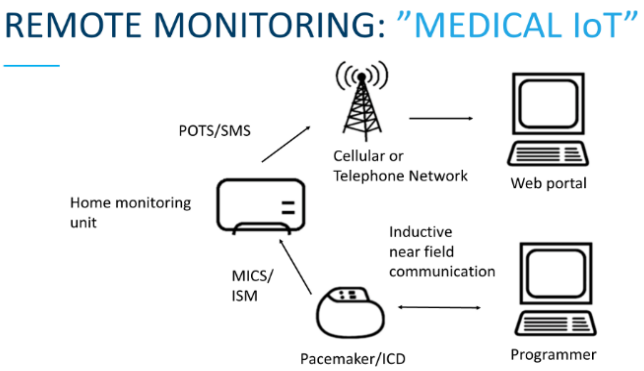

Figure 1: Remote monitoring medical IoT (Source: Marie Moe, SINTEF)

3.1.2 Wearable devices

Wearables, such as 'fitness trackers', collect data on individual behaviour and environment, satisfy the preference from consumers for mobile devices and enable easy interaction with computers, allowing analysts to recognise patterns in data (using artificial intelligence and predictive analytics). Technology becomes an integral part of people's life and arguably more than an extension of their life. Advances in wearables may change current business models in insurance, healthcare and other sectors. However, this raises a number of challenges, including the secure use of data (which current technology does not fully allow yet).

- Wearables per se would not have negative health outcomes (risk on physical safety) but their connectivity to open networks can lead to malicious intrusion and may generate a negative impact on privacy and data protection.
- Wearables can be useful to provide data to the insurance industry.

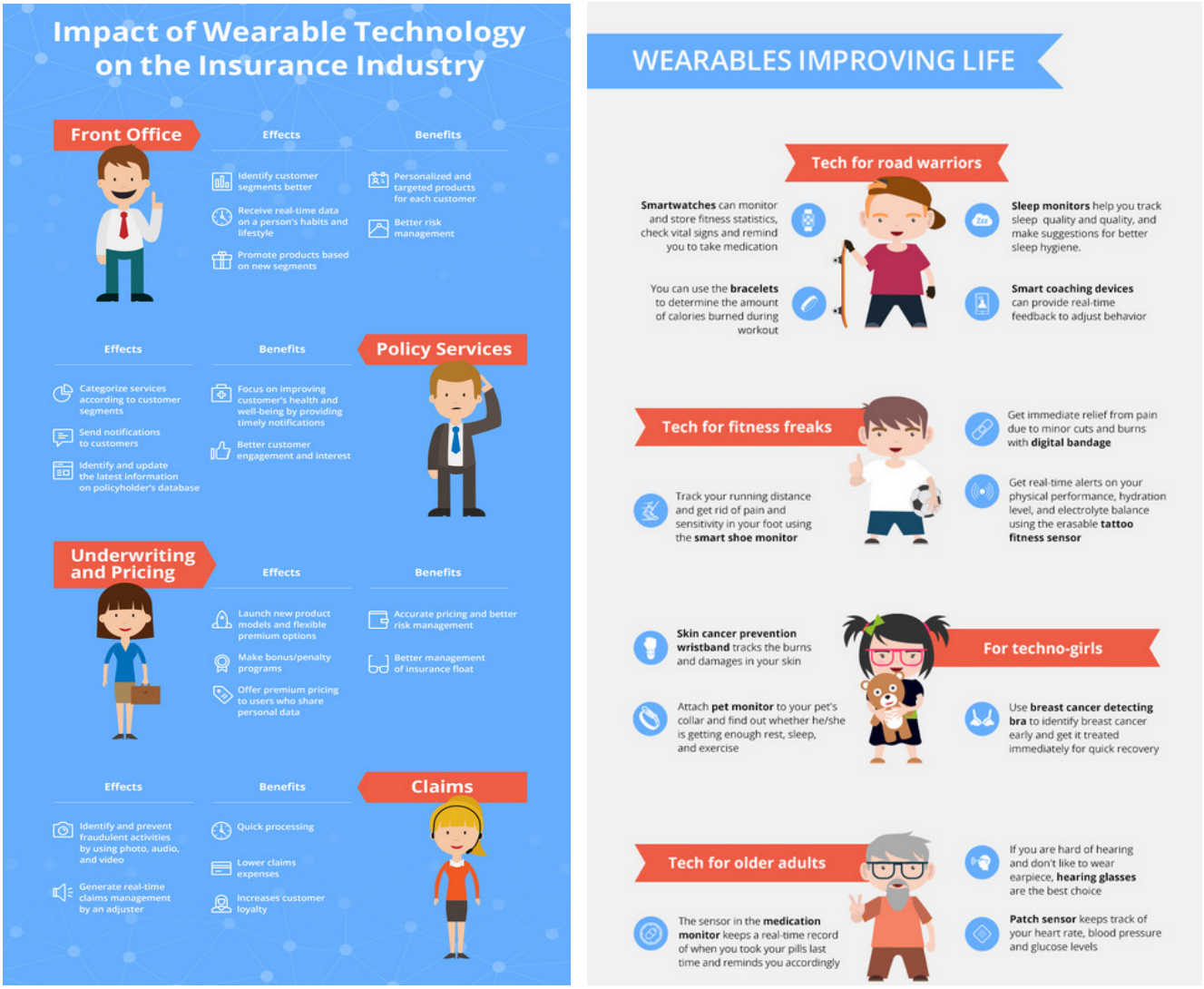

Figure 2: Infographic created by Life Insurance Post (https://lifeinsurancepost.com/) to illustrate how wearable technology is impacting the insurance industry including its effects and benefits for consumers

3.2 Cybersecurity issues: balancing risks and benefits

Cybersecurity vulnerabilities in medical devices develop as a multifaceted problem in a complex environment. For a range of reasons linked to regulation but also cost and resistance to change by medical professionals, the healthcare sector is slow to update technology and practice. This makes it unprepared for cyber attacks, because a cybersecurity attitude requires dynamic and fast-moving adaptation of technology and software.

- For example, can a pacemaker be hacked? Via remote monitoring (Medical IoT), pacemakers can send patient's data over the Internet, so security depends on how the data generated by the heart is secured for near field communication, or whether it is possible for someone with malicious intent to obtain access to an implanted device remotely via the communication interface. On January 9, 2017, the US FDA issued a Safety Communication [10] confirming vulnerabilities in St. Jude Medical's implantable cardiac devices and Merlin@home

[10] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

Transmitter. The FDA became aware of cybersecurity vulnerabilities in these devices after an independent research firm released information about these vulnerabilities.

- To understand why cybersecurity could become a serious issue in the field of connected implantable or wearable medical devices, it is useful to consider that: (a) we try to enforce cybersecurity on an environment that works on a basis of trust in the first place and; (b) much of what needs to be done for security does not fit into clinical workflow. Both aspects are valuable and must be protected: a patient can be treated regardless of whether a hospital has his health records and trust is a fundamental value. Therefore, these benefits must not be lost in the search for more cybersecurity protections.
- Looking at IoT, cybersecurity requirements must be balanced with the expected benefits. A checklist of measures may provide a feeling of security, but does not necessarily provide real protection and not always improved patient safety. For example, the transmission of heart rate from an IoT device may not have to be secured even if it is personal. Especially as the information must be available quickly in case of an emergency and therefore without strong authentication and encryption, which may impede interoperability. Cybersecurity costs money, speed of communication and computer power. Somehow, we have to make cybersecurity more feasible.

3.3 Regulation

3.3.1 Europe

- Medical devices are subject to stricter requirements than other types of equipment used in healthcare regarding product safety and quality management. Regulations are the same in all EC countries, Switzerland and Turkey. Medical devices have to bear the CE mark demonstrating compliance with the EC Directives 93/42/EEC (medical devices), 98/79/EC (In vitro diagnostic medical devices - IVD) or 90/385/EEC (active implantable medical devices). A medical device may only be placed on the market by a manufacturer or importer when the applicable conformity assessment procedure is successfully completed. For certain self-testing and active implants, a notified body (entity accredited by a Member State) assesses whether a product meets certain preordained standards and thus may be placed on the market.[11]
- Manufacturers must operate a product surveillance system and provide the following product-specific information to authorities: complaints, incidents, relevant experience concerning use and efficacy, reports from the specialised press, results of own investigations, corrective actions, device traceability. If an incident occurs with a medical device the manufacturer has to carry out the necessary in-house corrective actions and/or field safety corrective actions (FSCA) to reduce the risks to an acceptable level: recall, exchange, correction, destruction; software update; change of Instructions for use and/or labelling; send Field Safety Notice (FSN) to users; notify the national Competent Authorities concerning incidents and FSCAs.

3.3.2 USA

- Section 201(h) of the US Food, Drug and Cosmetic Act defines a medical device as any healthcare product that does not achieve its principal intended purposes by chemical action or by being metabolised.

[11] This is the case self-testing IVDs, List A IVDs, List B IVDs, active implants, and class Im, Is, IIa, IIb and III medical devices. Cf. http://www.ce-marking.com/medical-devices.html

- The FDA regulates manufacturers of any electronic product through the Electronic Product Radiation Control (EPRC) and medical device provisions of federal law. Through federal law, the FDA has formally recognised several standards related to radio frequency wireless medical devices. When manufacturers submit a pre-market notification to the FDA for device clearance or approval, declarations of conformity to these standards may eliminate the need for certain safety and effectiveness data.
- FDA prior-approval system does not fully embed the need for manufacturers to improve their products, as it may require a new approval. FDA allows a manufacturer to make a change if it is a patch that makes the device more secure, but new or additional functionality puts the device back at the beginning of the approval queue.
- Current approaches and recommendations need to be adaptive to the changing threat environment and potential vulnerabilities. The FDA's new approach (as of end 2016) aims to fill in the empty space with guidance, which is principle-based. They describe what they want to see in the application process, with regard to next-generation of the existing device. The application process takes time. It draws the attention of engineers who otherwise may not pay so much attention to these aspects at first, because the application is delayed until FDA gets satisfactory answers. Other questions from the FDA include: "how are you protecting sensitive data, how are you managing the communication between the device and the cloud, for the intended use and in the anticipated clinical environment?" This approach seems to have an effect, but it is too early to know whether it will be effective, rather than a more traditional approach using strict regulation and standards.
- On 27 December 27 2016[12], US FDA informed manufacturers of its new recommendations ('guidance') for the structured and comprehensive management of post-market cybersecurity vulnerabilities for marketed and distributed medical devices throughout the product lifecycle. US FDA reminds that:
    - Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. They are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.
    - Hospitals and health care facilities should evaluate their network security and protect their hospital systems.
    - FDA looks for, and encourages, reports of cybersecurity issues through surveillance of devices already on the market. Information regarding medical device cybersecurity vulnerabilities and threats can be shared with the NH-ISAC, MDISS and FDA.

[12] https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

4 Connected Vehicles

The development of automation and connectivity is driven by the prospect of increased road safety, as it is expected that the frequency or severity of accidents should decrease. However, other strong motivations highlight the improvements in traffic efficiency, air quality and more inclusive transportation models.[13] The wide range of expected benefits makes an increased exposure to cybersecurity risks *acceptable*, as they come along with increased connectivity.

- Connectivity between vehicles and with infrastructure is necessary to achieve full automation in driving. Connectivity develops in parallel to progress being made in assisted and automated driving, via various and combined types of sensors and software that analyse the signals received by the various central processing units.
- Proximity and GPS localisation are two of the basics of sensing technologies. Both functionalities can be compromised, which can pose serious challenges to transportation safety and security.

4.1 About car connectivity

Applications of car connectivity range from the provision of Internet access for passengers in vehicles (that wish to use various web content and streaming services) to improving driver assistance and traffic interference, which are crucial support for highly and fully automated driving. The inclusion of externally available (real-time) information about traffic conditions, obstacles and road hazards, etc. produces a more accurate and predictive image of the vehicle environment than the sole reliance on self-generated data generated by built-in vehicle sensors with limited coverage (such as cameras, radar and/or lidar systems). Data aggregation and refinement can be displaced in the infrastructure or in a distant cloud with the help of communication directly from the vehicle.

- A variety of different technologies (IEEE 802.11 OCB / ETSI ITS G5, UMTS, LTE, DAB, DVB-T etc.) exists today for wireless communication of vehicles with data and services-clouds, with infrastructure and with other vehicles or road users. However, the existing technologies will quickly reach their limits because of the huge number of new vehicles which require integration, the enormous volume of data which needs to be processed, and especially the high demands on latency and on reliability and security of communication.
- Requirements arising from expected future mobility applications must lead to the development of new technologies, such as the fifth generation of mobile communications (5G). However, today there is significant uncertainty about the functional scope of future technologies and whether different technologies will complement or replace each other.

4.2 Cybersecurity in connected vehicles

The automobile industry faces a massive cybersecurity problem. Intelligent public transport, as well as individual drivers and passengers exhibit low levels of awareness of cyber risk and poor behaviour to avoid the initial risk. For example, the use of non-secure 'infotainment' systems in cars that should be cyber-secure is a source of risk.

[13] Automated driving – consequences and impacts on transport policy. Report by the Swiss Federal Council in response to Leutenegger-Oberholzer postulate 14.4169 concerning automated mobility, Bern, 21.12.2016.

4.2.1 Holistic design approaches are needed

- Getting cybersecurity correct across the whole vehicle is vital. Barriers between the traditional vehicle subsystems are being eroded and the attack points are increasing. This has become very complex. One participant at the workshop said: "car manufacturers assemble cars but don't know what is in the car."
- In addition to securing vehicles, infrastructure must be secured as well. This includes traffic signals (and underground loop detectors), transportation systems, cloud storage and processing. Hacking one car can lead to scalable cascading hacking of infrastructure and other personal devices connected to that network.
- There is a legacy problem because of the co-existence of modern connectivity systems and connected vehicles with older vehicles, with no, low or insecure connectivity.

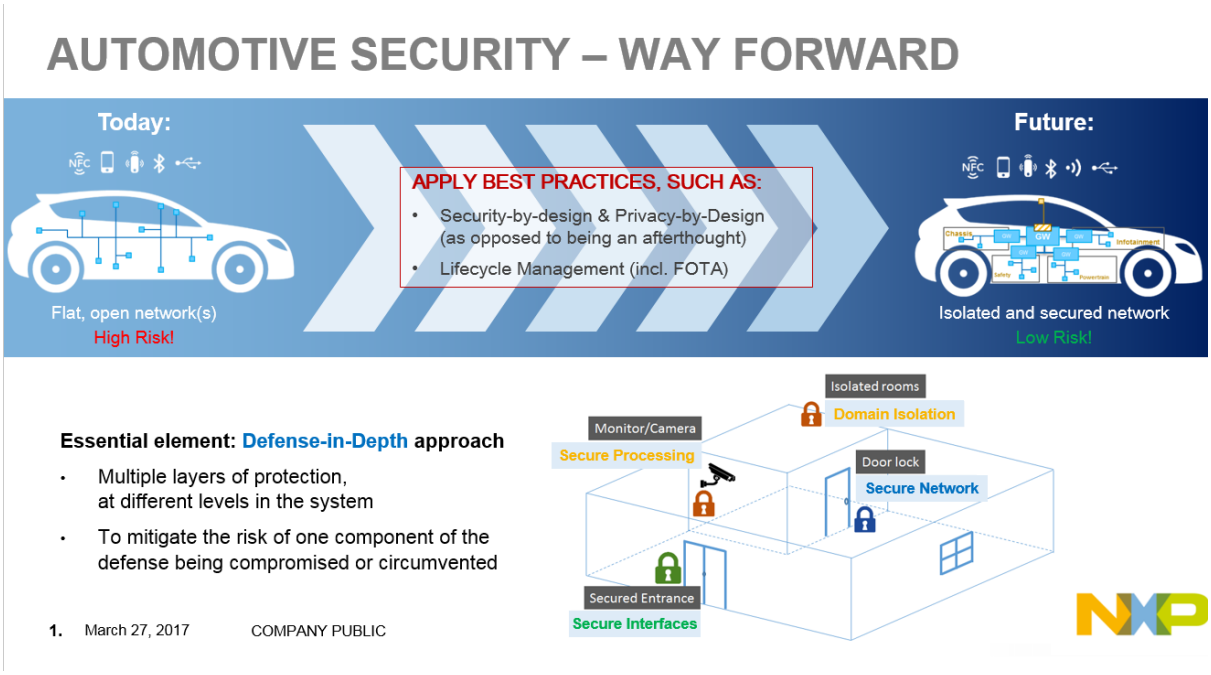

Figure 3: Automotive security – way forward (Source: NXP)

4.2.2 Connected cars must be secure, private and safe. This may involve trade-offs.

- With some variability across countries, large numbers of car users are aware of data privacy risks. This may have an impact on the adoption of connected cars.
- Combining cybersecurity and privacy can be at odds in vehicle-to-vehicle communications, so trade-offs are made currently. On the one hand, cybersecurity requirements involve the use of cryptographic tools for authentication to prevent attackers from disrupting traffic. On the other hand, privacy requirements imply that individual vehicles are not tracked. Using the same signing key to authenticate communications guarantees perfect privacy but very low cybersecurity in the case that the key is compromised. Vice-versa, using different signing keys in each vehicle implies high cybersecurity, but no privacy and vehicles are traceable by their

public keys. So new methods must be developed and implemented to preserve both security and privacy[14]

- There is also the need to combine cybersecurity/privacy and physical safety. Confronted with the risk of an accident, passengers would prioritise their own safety over the protection of their data and their privacy. Nevertheless, ideally they should not be placed in the situation of having to make a choice. Therefore, techniques to deal with both should be developed and used (considering constraints such as price).

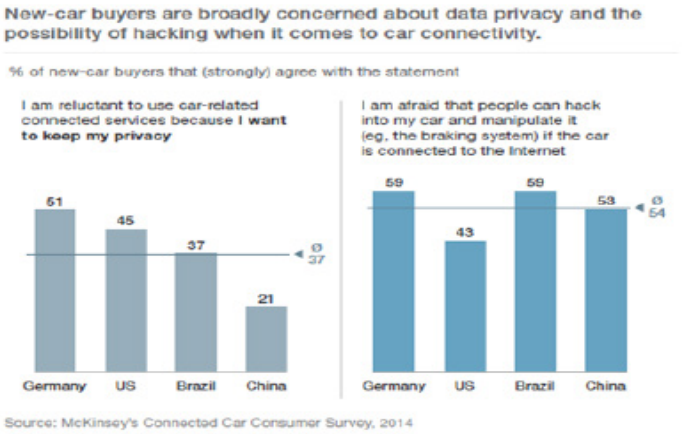

Figure 4: Connected Car Consumer Survey, 2014 (Source: McKinsey)

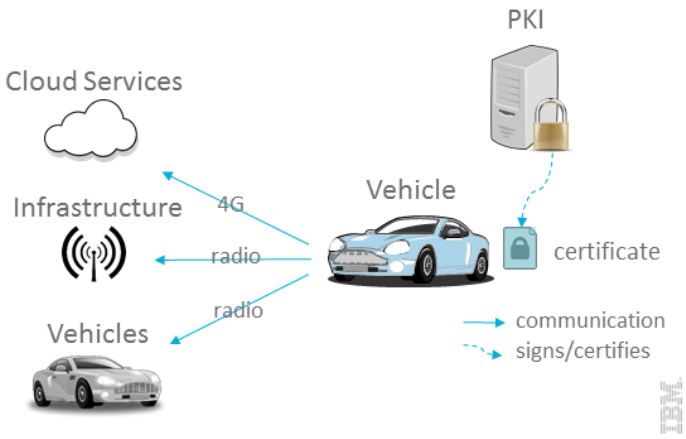

Figure 5: Connected vehicle (Source: Gregory Neven, IBM Research)

4.2.3 Standards, certification and testing will be important to create cybersecurity and trust

- As the automotive sector needs to create a secure environment for the future, it is critical that robust standards are developed, that derive from collaboration among actors and a holistic view of protection against cyber attacks across the ecosystem. The automotive industry is a massive, high-value, industrial sector, and routine collaboration to address cybersecurity is urgently needed.

[14] See for example work by Gregory Neven at IBM Research, Bryan Ford at EPFL or Patrick Pype at NXP.

- The automotive industry has a well-developed safety culture. National and international safety standards exist and protect customers in a good and dynamic manner by adapting continuously to new technologies. Consequently, it should be possible to elaborate from this safety culture to embrace a culture of cybersecurity. The automotive industry can take advantage of the well-developed MISRA[15] and ISO 26262[16] initiatives and integrate them into normal practice.
- In addition, as more systems interact and demonstrate interdependency, this means added complexity and increased difficulty in testing, assessing and validating. Hence, procedures for cybersecurity testing should be developed and systematised.
- Manufacturers need guidance. Organisations like ENISA can provide support to identify and promote good practice.[17] Together with stakeholders, the EU Commission is currently defining a common security and certificate policy for Europe for connectivity within its C-ITS platform.[18]

Figure 6: Taxonomy of threats to cyber security in connected vehicles (Source: ENISA Cyber Security and Resilience of Smart Cars, 2016)

[15] MISRA: Motor Industry Software Reliability Association https://www.misra.org.uk/
[16] *ISO 26262*: "Road vehicles – Functional safety", is an international standard for functional safety of electrical and/or electronic systems in production automobiles
[17] Cyber security and resilience of smart cars, ENISA, December 2016, doi: 10.2824/87614
[18] http://ec.europa.eu/transport/themes/its/c-its_en

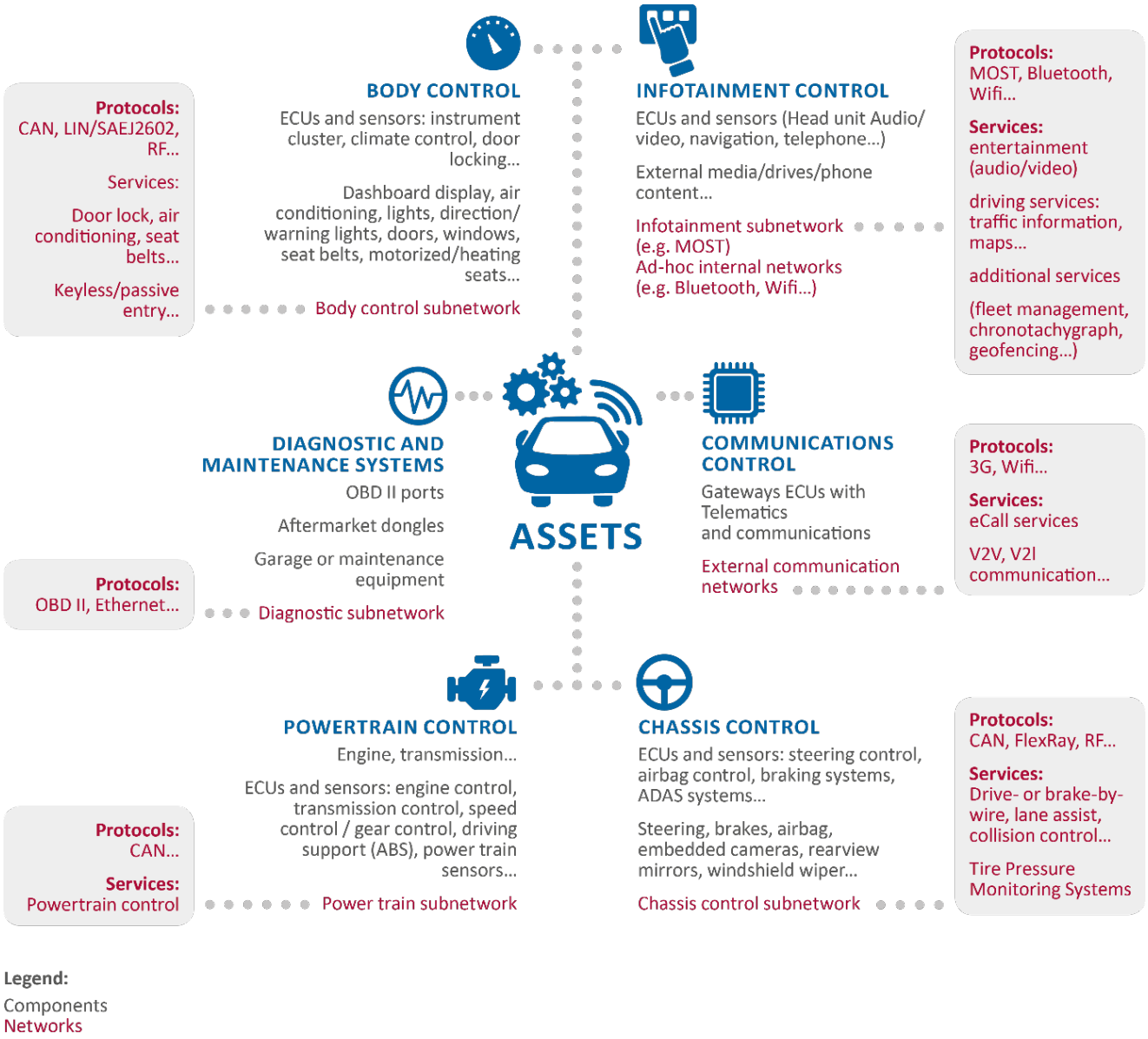

Figure 7: Smart car assets - components and networks (Source: ENISA Cyber Security and Resilience of Smart Cars, 2016)

Appendix: Innovation – Will the anticipated benefit of the IoT exceed the cybersecurity risks?

Innovation in the IoT is happening fast despite the fact that there are risks associated with it. This is because of the considerable benefits that the IoT brings to business and people. However, the innovators are not necessarily the people who take the risk, nor those who carry the risk. So a broader perspective is needed in order to evaluate innovation, benefits and risks.

At the beginning of the workshop, participants were invited to answer two questions:

1. To what extent do you think that cybersecurity challenges related to connected cars or implantable and wearable medical devices might hinder innovation and developments in those fields?

2. In your opinion and/or field of expertise, what is the most important thing to do in order to overcome hindering factors?

1. Answers to the first questions indicated balanced and nuanced views, with a group of participants who were of the opinion that "**innovation and development by responsible companies could be severely hindered by questions of security**", which "pose a tremendous challenge to connected vehicles" to the point that "innovators or deploying parties may face an unbearable liability level for potential damages", and that "ensuring security of connected cars and medical devices (wearable and implantable) is absolutely critical, as no customer would buy such technologies if they pose a threat to his or her life, which in turn would slow down progress in those fields". In that context, "if, in an early phase of the development of the value proposition a really bad scenario materialises, this could potentially bring down acceptance and developments to a standstill before they even have a chance to take off." The issue of technology acceptance was seen as important: "an even bigger the problem is the widespread implementation and acceptance of the technology".

Another set of views indicated though that, to date, cybersecurity risk "has not much hindered these industries as companies have mostly ignored the problems / taken minimal action. However, more recent events such as proven hacks on these products, or DDOS attacks supported by them means this can no longer be ignored".

Some participants emphasised the problem of inappropriate regulation. "Researchers and vendors will want to innovate and further develop functional improvements and ease of use for connected cars and connected medical devices – however, **if there are strict regulatory and compliance standards, this will slow down the approval process and hence hinder the pace of bringing innovations to the marketplace.** Heavy regulation will further drive up the cost of navigating through the approval process and hence will discourage innovation at the small business level". Thus "innovation might be hindered in so far as new potential entrants into the market may be discouraged to invest due to uncertainty about future requirements whereas existing market players may consider the cybersecurity challenge as one point to differentiate through innovation from competitors and protect from new market entrants."

Finally, some participants were of the opinion that cybersecurity challenges do not "hinder innovation at this stage" as "security is mainly in a 'catch up' mode", and can even be "an opportunity for innovation and developments in the field". "**When unaddressed, security and privacy issues are**

indeed potential showstoppers for connected cars and medical devices. At the same time, technology is capable of tackling both types of issues, so that innovation does not have to be hindered. "Innovation and development will take place although the challenges exist"

The conclusion was that "these concerns will clearly hinder innovation (at they should), but probably not to the extent of preventing development and deployment of these devices."

2. Answers to the second question highlighted the importance of three critical enablers to overcome hindering factors to the development of connected vehicles and medical devices: technology, regulation and collaboration.

On the technology side, 'security by design' and software came prominently, as well as the need for technical guidance.

Security by design: "Manufacturers will have to invest resources in secure product design, preferably by experts. Solutions must be designed with security and privacy in mind from the very beginning, ("as an integral part of the design process") not added as a fix or afterthought".

Software: "the quality of software needs to be improved, and more importantly, to be fully and competently applied in industry". Software updating must be improved as well.

Principles, guidance, standards, good practices are needed "that helps vendors develop better Security Architecture for their devices so that the devices are less vulnerable and easier to maintain through their lifecycle". "Create a set of open and usable standards for the IoT and discuss to what extent regulation makes sense or is necessary. Critical topics for standards include secure communication, software updates, and key management". "We need to re-think principles of communication and architecture and usage of data". "Security of the overall system must be an end-to-end responsibility between all the involved parties. Until today every involved part of the solution is made “secure” but it is not seen as the overarching system.

On the regulatory side, it is clear that "regulation might play a significant role here", notably to "build trust by establishing a global regulatory framework".

The question of liability is central: "in the end, it is a question of liability. If manufacturers are fully liable for “hacked” devices, the market will take care of this issue since the business and financial risks are too high. Therefore, regulation will drive this topic (as well as branding/reputation concerns of manufacturers)".

Some participants noted thought that "market literacy is an important factor: we don’t yet know enough about threats and vulnerabilities, and there must be corporate recognition and ownership of the problem. Things that may (but won’t necessarily) help here are legislation and standards". In any case, we must "avoid heavy-handed blanket regulations"

Collaboration between actors will be key to determine the way forward. "We need awareness raising and more collaboration among the stakeholders: security researchers, vendors, patients, policy makers, insurers, physicians, standards organisations, healthcare providers and government agencies". "Discussions with regulators and a multi-stakeholder approach should lead to social acceptance and adoption of the technology". "Manufacturing companies or products in these areas are going to have to partner far more closely with the security industry". "From standards development’s perspective, liaisons to cybersecurity expertise should be established to promote

collaboration and information exchange". "Communication with customers should be used to educate them about the safest use of the product".

Eventually, manufacturers should receive "an incentive to also consider the security aspects" and stakeholders are invited to "demonstrate transparently that and how cybersecurity is implemented".

In conclusion, a participant said: "if we see a disaster where human lives are lost due to cybersecurity issues, this may result in trust breakdown and innovation might be set back for a while. However, the society and market forces are driving towards everything being more and more connected, and we should instead of seeing cybersecurity as a costly 'add-on' adjust and adopt to this by considering it as a needed built-in feature that offers business opportunities. In this way cybersecurity will not hinder innovation, but instead foster it and create opportunities".

Acknowledgements

This workshop report was prepared by Marie-Valentine Florin, EPFL IRGC, with contributions from Maya Bundt, Chris James, Markus Riederer, Rudolf Waelti, and Patricia Williams. Editorial contributions from Anca Rusu and Marcel Bürkler. The views and recommendations in this paper, however, do not necessarily represent the views of workshop participants, individual members of the project writing team, other contributors, or their employers.

IRGC would like to thank all workshop participants for their time and expert contributions. A special thanks goes to Jim Larus and Maya Bundt for their help in preparing this workshop.

The following participants attended the expert workshop: Francis Blumberg (Swiss Re), Jeremy Bryans (Coventry University), Maya Bundt (Swiss Re), Alexis de Beauregard (AXA), Oliver Delvos (AIG), Bernd Fastenrath (Here), Linus Gasser (EPFL), Adrian Guan (ITS America), Sarbari Gupta (Electrosoft Services, Inc.), Marco Henrique (HDI Global SA), Claus Herbolzheimer (Oliver Wyman GmbH), Chris James (Paul Hastings), Russell Jones (Deloitte Advisory), Philipp Jovanovic (EPFL), Dorothea Köppe (Swiss Re), Jim Larus (EPFL), Eireann Leverett (Privacy International), Apostolos Malatras (ENISA), Nathalie Meyer (Chubb Insurance Ltd), Paul Miskovich (AXIS Insurance), Marie Moe (SINTEF), Gregory Neven (IBM Research), Chana O'Leary (OpenSky Corporation), Joerg Potzeba (AXA), Patrick Pype (NXP Semiconductors), Aanjhan Ranganathan (ETH Zurich), Markus Riederer (Swiss Federal Roads Office), Domenico Savarese (Swiss Re), Stephan Schreckenberg (Swiss Re), Eric Schuh (Swiss Re), Daniele Tonella (AXA Technology Services), James Tuplin (QBE), Rudolf Wälti (Swissmedic), Patricia Williams (Flinders University).

IRGC would also like to thank Swiss Re and AXA Technology Services, who provided support for this workshop and publication.

About IRGC

Since 2016, IRGC consists of two distinct and independent entities, which collaborate with and support each other:

- The EPFL International Risk Governance Center, a transdisciplinary centre at the École Polytechnique Fédérale de Lausanne, which organises IRGC activities, emphasising the role of risk governance for issues marked by complexity, uncertainty and ambiguity, and focusing on the creation of appropriate policy and regulatory environments for new technology where risk issues may be important. http://irgc.epfl.ch
- The International Risk Governance Council (IRGC), an independent non-profit foundation whose purpose it is to help improve the understanding and governance of systemic risks that have impacts on human health and safety, the environment, the economy and society at large. IRGC's mission includes developing risk governance concepts and providing risk governance policy advice to decision-makers in the private and public sectors on key emerging or neglected issues. IRGC was established in 2003 at the initiative of the Swiss government and works with partners in Asia, the US and Europe. www.irgc.org

EPFL International Risk Governance Center

c/o École Polytechnique Fédérale de Lausanne EPFL
CM 1 517, Station 10
1015 Lausanne
Switzerland

General enquiries: +41 21 693 82 90

irgc@epfl.ch
irgc.epfl.ch