The Internet of Things is already here, but who bears the risks?

A model to explain coverage disputes

in a world of interconnected, autonomous devices.

(**working paper, Jul 2015**)

Andreas Haas*

Chair for Insurance Economics and Social System, Hohenheim

Markus Haas**

Munich Risk and Insurance Center, Munich

Markus Weinert¥

Chair for Insurance Economics and Social System, Hohenheim

Paper for Presentation at the

World Risk and Insurance Economics Congress (WRIEC)

Munich

August 2015

---

* **Andreas Haas**, Chair for Insurance Economics and Social Security, University of Hohenheim, Fruwirthstr. 48, 70599 Stuttgart, Germany; +49 (711) 459 22118; Email: a.haas@uni-hohenheim.de

** **Markus Haas,** Munich RIsk and Insurance Center, Ludwigs-Maximilians-University, Schackstr. 4 / III, 80539 Munich, Germany; +49 (89) 2180 3693; Email: markus.haas@bwl.lmu.de

¥**Markus Weinert**, Chair for Insurance Economics and Social Security, University of Hohenheim, Fruwirthstr. 48, 70599 Stuttgart, Germany; +49 (711) 459 23422; Email: m.weinert@uni-hohenheim.de

The Internet of Things is already here, but who bears the risks?

A model to explain coverage disputes in a world of interconnected, autonomous devices.

Andreas Haas, Markus Haas, Markus Weinert

July 2015

ABSTRACT

We analyze the question of risk bearing in the emerging market of the Internet of Things. While this field is currently part of the ongoing research in respect to technical aspects as well as cyber insurance coverage on the firm level, the actual risk attribution for the implementation of intelligent objects on the household level is a neglected topic so far. Given the fact, that a majority of innovations in this field is driven by startup companies with limited financial capacities, we emphasize their behaviour in terms of risk taking in this novel field of business. We expect that startups currently do not internalize their exposure to third party losses associated with the development and provision of interconnected applications and devices. Due to their limited equity base, they leave the loss exposure to the end consumer. To illustrate this behavior, we adjust a model introduced by Olovsson (1992) to consider various levels of risk bearing under consideration of the development stage of the company. We show that especially young startups have no incentive to cover risks associated with the offered solutions. They externalize these risks. With increasing market value and maturity of the form however, these companies are opposed to a growing incentive to internalize loss coverage resulting from their products, because of reputational risks associated with negative company news. This behaviour however challenges the insurance industry with an exposure to cumulative losses if consumers make use of Internet of Things solutions from startups. Hence we conclude that regulatory requirements will need to be adjusted in order to protect consumers and finally the insurance industry from free riding incentives, startups currently can participate in.

Keywords

Internet of Things, cyber insurance, insurance, risk bearing, startups

1. Introduction

The Internet of Things (IoT) is a generic term for everyday products, such as washing machines, bulbs, wireless switches, heating systems, door locks, cars, but also medical, industrial and agricultural devices, that become **accessible and controllable** via computers, smartphones and tablets. In addition to conventional interactions, i.e. user-to-machine control commands, the IoT is enabling smart items to **interact autonomously** and **independently** with other smart devices. Possibly this aspect can be considered as the most meaningful novelty on the markets, bearing challenges for the risk and liability management of companies and hence for the insurance industry.

As every element of the Internet of Things features various digital sensors, an enormous amount of data is generated. Such information is valuable e.g. for retailers, financial intermediaries and insurance companies as well as for the power industry. Moreover, it enables **data-based** and **contextual triggers** to automate executions with the aim of improving our lives and optimizing industrial processes. This great leap in technological development is supported and reinforced by cross-industry collaborations, ranging from small startups to long-standing enterprises. On the one hand global players in technology are developing necessary interfaces (e.g. HomeKit - a framework in iOS offered by Apple) or add data hubs to their product range (e.g. Nest - an intelligent heating management system, recently acquired by Google) to aggregate and exchange data created by each product within the Internet of Things. On the other hand more and more startups are focusing on products, solutions and services, which are related to the Internet of Things.

Although intended to make our daily lives more convenient and production processes more efficient, this development is challenging users, manufacturer and other market participants with **new questions about liabilities and responsibilities** in case of malfunctions and cyber threats. A new and important question in the context of cyber risks hereby is, how to handle **physical damages and related financial losses** resulting from cyber-attacks in the IoT. By interconnecting household appliances for instance, previously isolated devices are suddenly exposed to cyber risks facing the threat of physical damages. Thus, recently end-consumers are also exposed to the damage potential of cyber risks. This new risk situation consists of a wide array of exposures, mainly driven by the increased connectivity, (autonomous) interconnectivity options and data sharing approaches. The **World Economic Forum** estimates the potential **economic risk exposure related to the IoT** up to **$3 trillion by 2020**, mainly resulting from cyber security issues (WEF, 2015).

As mentioned before, the relevant and so far unanswered question is: **Who is in charge of bearing the resulting novel risk?** Cyber risks per se are a pretty new field, at least on the individual

level. Legal frameworks are currently not designed to take those aspects into account, though legislative initiatives are recently addressing these questions. Hence liabilities of manufacturers are limited and challenges to proof failures are to a large extent left to the owner of a device.

The insurance industry is exposed to these potential enormous losses mainly in terms of homeowners insurance (and where applicable fire insurance, in case a malfunction or attack causes a fire). Accumulation risks, resulting from the interconnectedness of devices is also an issue as well as the lack of historical data for the premium calculation, insurance provision is dependent on. In terms of an insurance perspective, such emerging risks cannot be validated by historical data. Even transferring the knowledge from any comparable risk situation is not necessarily possible due to lack of comparability. In contrast to most traditional insurance products, the understanding of the emerging risk situation of an Internet of Things is not assured yet.

The aim of this paper is the **risk assessment** for the **Internet of Things**. Therefore, we first identify and analyze the new risk situation caused by the Internet of Things, which companies as well as consumers are exposed to by adapting **smart interconnected devices**. After that, we show, that this new risk situation mainly results from a high incentive of risk externalization by startup companies. As these companies are currently the main innovators in this area, we suggest insurance solutions or stronger regulatory requirements as possible way to prevent risk externalization of these companies.

2. Internet of Things

Eric Schmidt, executive chairman of Google Inc., caught attention this year by proclaiming that the future will lead to the disappearance of the internet in our active perception. To explain this statement further, he stated at the end of a panel at the World Economic Forum in Davos, Switzerland: "There will be so many IP addresses, [...] so many devices, sensors, things that you are wearing, things that you are interacting with, that you won't even sense it. [...] It will be part of your presence all the time. Imagine you walk into a room and the room is dynamic [and] you are interacting with the things going on in the room" (Forbes, 2015). Schmidt describes hereby the Internet of Things as numerous interconnected devices, that will be an integrative and ubiquitous part of our daily lives.

2.1 What is the Internet of Things about?

The Internet of Things (IoT) is characterised by three main components: (1) Digital objects, things or assets with sensors; (2) Hubs or computing systems that collect generated data and make use of it; (3) A communication network to connect the digital objects and data storage solutions, to

enable interaction among all involved items. This structural predisposition leads to the specific IoT features interconnectivity, heterogeneity, dynamic changes, things related services and enormous scalability. The inherent **interconnectivity** describes devices to be part of networks and able to interact within the global communication infrastructure. **Heterogeneity** is a result of the open character of the IoT: Any interconnectable device can be part of the IoT. Hence different hardware and software platforms, as well as networks involved lead to high heterogeneity in terms of participating systems. The option for any device to connect with other devices and services through different networks enable **dynamic changes** of the same. Modes of devices can switch e.g. from sleeping to awake, connected or disconnected. Moreover, the number of devices can change dynamically. As most of the services in the IoT are things-related, resulting constraints are determined by the implemented and based things. For instance these limitations apply to privacy protection and semantic consistency between physical things and their associated virtual reproduction. In order to provide thing-related services within the constraints of things, both the technologies in the physical world and information world will change. The IoT is also opposed to enormous scales, simply because the number of devices that need to be managed and communicate with each others is at least an order of magnitude larger than those currently connected to the internet. Also the ratio of communications triggered by devices compared to communication triggered by humans will noticeably shift towards device-triggered communication. A relevant aspect with even more critical implementations is the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling requirements. Summarizing, the **Internet of Things** can be defined in short as the interconnection of smart, generic objects through the internet (Atzori et al., 2010) to communicate and interact with each others and with people, to alleviate and optimized our daily lives (Miorandi et al.,2012). Framing this different, the **Internet of Things** is enabling objects to interact in a social way (Atzori et al., 2012).

2.2 How does it work and who is affected?

The Internet of Things consists of devices (things) with sensors, which are able to communicate with digital hubs, smartphones or other connected devices through the Internet. Every device in this network generates data, by e.g. taking pictures, metering environmental factors or just logging its current digital activity status.

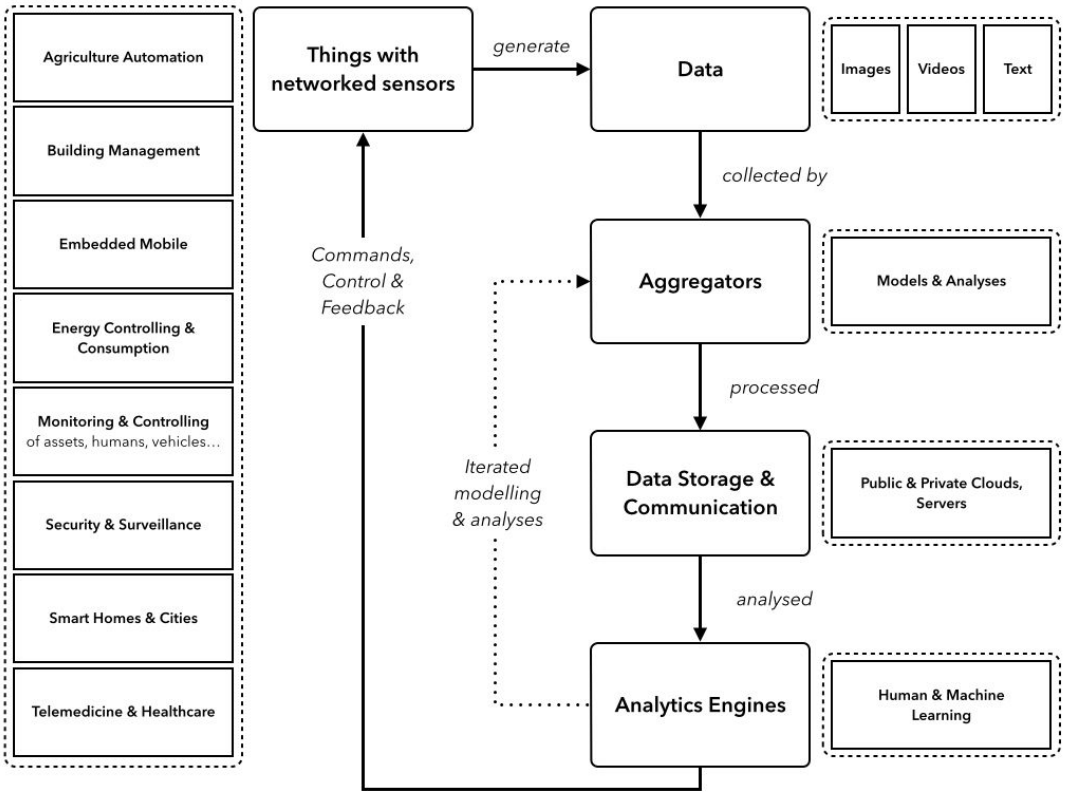

Fig. 1. Data processing in the Internet of Things.

This data is collected by data aggregators, which are either also interconnected things operating as data hubs or software solutions on smartphones. To store the aggregated data and to start an analyzing process if required, most Internet of Things services are using public or private clouds. Cloud Computing is therefore an important part of using the data for more processes and further interaction. Finally the processed data is used to interact with the thing, which originally generated the data.

On the one hand, this technological evolution takes place both in private households and public life. Things like home appliances, house heating and cooling systems, lights or even cars are going to become connected and accessible through the internet. On the other hand, connected devices will also sustainably change industrial capabilities. Sensors in machines are used to create new data, which can be used to optimize the production process and its coordination in order to increase efficiency. Even farmers are using the data of connected sensors to automatically send out their tractors for seeding or harvesting (Jahangir, 2014). These examples highlight a development, which opens up various opportunities and leads to changes for industries and consumers.

To sum up, the Internet of Things is not only about managing “things” in any place and any time. The newly created interconnectivity also generates a huge amount of data, which provides an added value compared to today's possibilities of technology usage and production processes. The IoT is currently probably the largest driver of technological innovations. The estimations about market development of connected objects in the next decade range from 11 trillion US$ (TECH TIMES, 2015) to 19 trillion US$ (Washington Post, 2014). Although the wide range of estimations indicate a certain degree of uncertainty, the figures per se show the enormous potential and importance market participants attribute to the IoT.

2.3 Why does it matter and is there a new risk?

As more and more devices become interconnected within the next years, these risk networks are likely to become an interesting target for hackers as well as a relevant field for malfunctions. The main difference between today's understanding of cyber risks and the likely reality of Internet of Things in the near future, is the exceeding potential for physical damage resulting from of these new products and services. In the current understanding of cyber risks, a hacker does e.g. attack a database, disclose credit card information or cause a business interruption. Whereas a financial damage results of the attack, the scenario is completely digital. In the Internet of Things, the risk situation changes: when a cyber attack results in the access to home automation systems, a manipulation of the management of diverse products in the house can **lead to physical damages**. The modification of the temperature of a washing machine or a fridge, results in a property damage. Further think of a cyber attack that grants access to an interconnected building management system, even alarm systems or cooling systems for server rooms could be shut down. Physical manifestations and property damages are a new and emerging risk in the Internet of Things. This new risk situation manifests in the following three important areas.

2.3.1 Risk potentials in consumer devices

By making daily life devices accessible via the internet in various ways, all of these objects are opposed at the same time to the risk of malicious attacks or malfunctions caused by this channel in the device itself or by proprietary interconnected access points. An anecdotal evidence for the risk exposure resulting from the introduced technological progress, offers the case of August smart lock. The startup developed a door lock, whereby the key is replaced by a smartphone application. The smartness of this approach is, beside the general option to lock and unlock a door just by using a smartphone, the introduced option to grant access right on demand without physical presence. For instance, the user can enable a friend to enter the house in case he arrives late by granting a temporary permission to this person via the app. The technological

approach however is based on bluetooth communication between the mobile device and the door lock. Unfortunately the sold locks initially opposed the user to two security issues: First, the locks could be located easily by simply using the bluetooth module of a mobile phone. With its bluetooth connection detection option, the names of the promoted devices are visible and also characteristically for the lock only. Second, a security issue allowed intruders to unlock doors unauthorized by just sending a command to the server (CBC News, 2015). This exposure is furthermore critical, because August. Inc. does not offer any wireless option to update the firmware of the installed lock. A required patch demands the owner of the lock to connect it to a computer or to install the update in any other feasible way. This could leave the vast majority of owners opposed to the detected vulnerability, at least for some periods. Though it can be argued, that this is a specific case, it illustrates well the potential risks associated with such products and services in the Internet of Things.

2.3.2 Risk potentials in industry-specific devices

The Internet of Things however is not restricted to items for the private, individual sphere but most likely will impact industry specific solutions to a comparable depth. For instance manufacturing systems, navigation systems as well as supply chain management systems appear to offer attractive productivity gains by linking them to the internet for controlling purpose and even more relevant for using and coordinating resulting data and information. Professional applications are e.g. navigation systems, used in various types of transportation systems like trucks, planes and ships. These systems are of enormous relevance as any hack can affect not only physical damage but also endanger human lives. Similar threats may result from intrusions in cargo and postal systems. Any IT linked solution accessible through an interface linking it to the internet offers a potential access point for an attack. Non proprietary structures endanger system security per se further.

2.3.3 Risk potentials in infrastructure-specific devices

A third, and so far rather unconnected area, is the field of infrastructure related items. Infrastructural access points are available in electrical systems, building management and fire detection systems. The latter are of special relevance within the implementation of renewable energies. Solar power generation and wind farms are not a steady source of power provision but to a large extent weather dependent. Resulting peaks already challenges existing power grids up to their limits. More detailed information about the consumption of individual users as well as options to manage the grid on a microlevel is in the focus of the ongoing development within this field. This is especially facilitating the options to steer the power provision intelligent, with a strong focus hence on the options offered by the Internet of Things. One could imagine the

potential risks and losses, a lasting failure of power provision can enfold on the local or even global economy, including medical support and civil order as well as security. Though these areas address stakeholders on the individual as well as institutional level, the challenges and general threads are relatively similar. Hence in the next chapter we introduce a simplified risk assessment process to identify general risk exposures and access points for (cyber) risks. **Hereby, we focus on the household level - the so far mostly neglected area within recent research, but with a high growth potential.** This approach however may be analogously applied to other areas of interconnected, self-automated intelligent devices.

2.4 Literature Review and research issue

The insurance and risk management related literature addressing the Internet of Things is currently in an emerging state. Nevertheless there is already relevant research in related fields such as technical aspects as well as legal topics. Additionally challenges of interconnected risks are investigated in selected scholarly work.

Research focusing on technical aspects is for instance the work of **Weber** (2010), who investigates legal and privacy aspects associated with the Internet of Things, based on the special case of product codes submitted through RFID chips. The aspects he addresses however are applicable to various areas, whenever objects communicate with each others, as they do in the Internet of Things. In detail he identifies challenges for data security and privacy aspects, which potentially may not be solvable just on national levels only, but require global regulations, due to the ubiquitary characteristics of the used applications. **Atzori et al.** (2010) provide basic research on summarizing existing IoT approaches from available literature. They conclude, that networking, security and privacy issues are the most relevant topics for future research. **Miorandi et al.** (2012) review ongoing research attempts and address challenges for researchers associated within the evolving field of the IoT from a technical perspective. Beside a broad overview on potential applications to be targeted within the IoT, they investigate in detail (technical) security challenges associated with the implementation of smart and connected devices. **Atzori et al.** (2012) propose the integration of social networks within the IoT. They provide an overview on technical challenges and investigate the distribution of mobile items within this ongoing development. Therefore they use a Small World In Motion simulation technique due to a lack of empirical data. They show, that the "resulting network structure offers the desired features in terms of navigability and scalability".

A relevant field of research is considering interconnected risks. **Van Eeten and Bauer** (2009) target interconnected risks by investigating Distributed Denial of Service (DDoS) attacks executed by botnets. As in this case individual systems interact globally, they discuss critically how

to address resulting issues by not overstating the risks as well as not undermining the innovative power the internet and its solutions offer. **Hofmann and Ramaj** (2011) also focus on interdependent risk structures. They identify a need for governments to implement sound legal frameworks to improve the protection against cyber attacks. **Allianz** reviews in a 2014 paper generally the rise of interconnected risks, not solely but also including the field of cyber attacks. They currently identify the most relevant topics in this field to result from natural catastrophes and resulting business interruptions. Few papers deal with insurance industry related aspects related to questions within our work: **Biener et al.** (2015) investigate in their most recent paper the insurability of cyber risks empirically. They investigate 994 cases of cyber losses on the enterprise level. By doing so, they identify critical and less critical limitations for the insurability of cyber risks, based on the criterias of Berliner (1982). However, they conclude, that a growing market will overcome current obstacles to market growth. **Schwarz and Sastry** (2014) investigate cyber insurance as a tool to improve network security in large scale networks, due to its ability to enforce security standards.

Most related to our work in terms of model theoretical considerations is the work of **Dynes et al.** (2008), who investigate incentives for cybersecurity investments. Their research on for-profit public infrastructure entities indicates that incentives to invest in cyber security may result from the interaction with other companies to assure their reliability and resilience. Our contribution to the existing literature is as follows: The mentioned research papers target data security and privacy issues to a large extent resulting from the internet of things, also interconnected risks play a relevant role as well as cyber insurance on the firm level. However, addressing the costs of related breaches on the individual level in the context of the IoT stay untargeted to our knowledge. We provide within this paper a fruitful contribution to the existing literature by adding an early stage risk assessment with a special focus on the special problems associated with startup companies in the context of the IoT, as these companies represent the driver of this innovative market field.

3. Internet of Things - a risk assessment approach

The identification of risk exposures in the context of the Internet of Things requires a solid risk assessment. We introduce a framework for this target based on a generic risk model.

3.1 A Generic Risk Model with Key Risk Factors

The risks we address in this paper are occurring from the introduced ongoing technological development in the field of the Internet of Things. Especially the novelty of this field opposes users

from a multiplicity of undetermined legal and liability aspects. The starting point to provide a framework to tackle these aspects, is the identification of potentially risky areas. To address these aspects in a methodically structured way, we stick to the risk management process developed by the **National Institute of Standards and Technology (2012) and Gordon et. al. (2003)**. Gordon et. al. (2003) recommend assessing threats and vulnerabilities. We extend these two steps according to the National Institute of Standards and Technology (2012) by distinguishing between threat sources and threat events. The steps within our risk assessment are specified in the following figure:

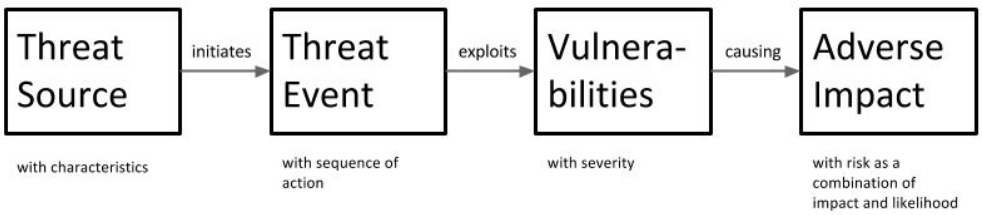

Fig. 2. Risk Model (National Institute of Standards and Technology, 2012)

3.2 The Threat Sources

The identification of potential threat sources within the IoT requires a more precise determination of the interaction process. Threat sources are dependent on the items implemented within the various occurrences of the Internet of Things. The understanding of the IoT prerequisites to analyze any risk sources, as their interaction possibilities and the access points for malicious attacks or technical errors determine the exposure situation in the IoT. A novelty and challenge at the same time, is the interaction of interconnected tools, apps and (cloud) servers. This structure creates digital risk chains, where weak coding or technical issues in each access point can imply insecurity of the whole system.

The simplest example for the Internet of Things is the opportunity to manage devices through a mobile application. If the application and the device can communicate directly to each other (bluetooth or near field communication), the connection is a **1:1** relationship. However 1:1 connections are rarely used within the Internet of Things, as the automatisation process and other advantages of a decentralized controlling cannot be achieved. Hence the prevailing majority of Internet of Things include any type of cloud computing to store, exchange and process data. Gubbia et al. (2013) also assume, that cloud computing is a constituting characteristic of the Internet of Things. Examples for 1:1 devices, even with in-between cloud solutions, are **accessible domestic appliances** like door locks, washing machines and light bulbs. The option to interconnect existing internet ready items also paves the way for the development and integration of so called

hubs. Hubs manage and coordinate more than one device. In particular hubs are required to enable the communication of internet connected things among themselves - another key feature of the Internet of Things (e.g. Sundmaeker et al., 2010; Miorandi et al., 2012).

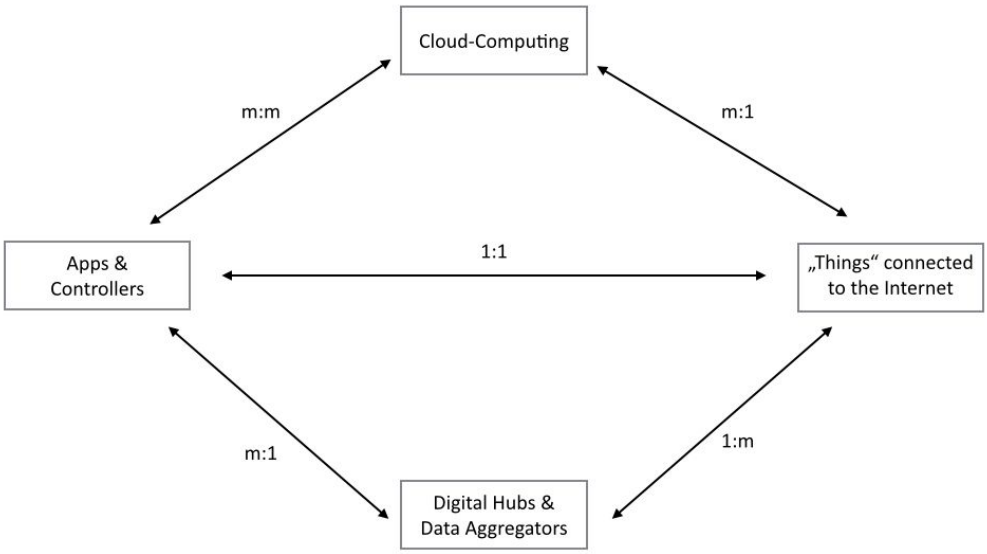

Fig. 3. Connection and interconnection in the Internet of Things.

An example for an currently emerging hub is the digital and interconnected thermostat “NEST”. Intended to originally steer existing heating system more efficiently by considering demand driven aspects, the appliance once installed can support the user also by additionally coordinate related items. Already now NEST offers the opportunity to interact with hue light bulbs, august door locks, Whirlpool washing machines, Kevo Smart Locks, LIFX light bulbs, Ooma Telo call forwarding service, rachio garden sprinklers, Mercedes Benz for determining your arrival, Big Ass fans and an NEST car adapter to determine your arrival (NEST, 2015). Hubs hence represent a solution of **1:n** connections, making them especially critical as they are mostly attractive for malicious attacks due to their spreading capabilities. In terms of an risk assessment perspective, hubs possess cumulative characteristics due to their multiplicative character. Concluding, the Internet of Things also offers **n:1** connections. A multitude of software companies grant access to their solutions through an application programming interface (API). This is attractive for various reasons. For instance it enables users to additionally use new software solutions through existing applications. This is facilitation the market penetration. By granting

access though through APIs for internet linked items, there is an exposure resulting by non-proprietary software and related risks. Quality assurance of third party app is difficult or event not assessable. Malicious attacks can be executed through more sources, even malicious applications could be created and uploaded for distribution to app stores. Additionally the data handling within third party application is opaque. Login credentials may just as well be abstracted as information gained from the application, e.g. the absence from a home.

The introduced technical view on the interconnectedness of objects in the IoT represents the foundation to address hereafter the potential threat sources. According to the National Institute of Standards and Technology (2012) these sources might be of different types. In the generic model we distinguish between **adversarial, accidental, structural and environmental threat sources**. With adversarial threat sources we address risks, which are based the assumption that individuals or groups might seek to exploit the interconnectedness of the Internet of Things in order to enrich themselves or to cause harm to the individual of whom the cyber-physicals are attacked. Accidental threat sources are based on the assumption that erroneous actions might be taken by users or administrators. Structural threat sources result from failures of hard- or software due to structural weaknesses that have not been fixed yet. Environmental threat sources have to be considered due to exogenous events that causes failures of malfunction to a specific part of the interconnected and communicating things.

With a certain likelihood of occurrence these threat sources might initiate corresponding threat events. Threat sources and threat events are in a n to n relationship, i.e. one single threat sources might initiate various threat events or several threat sources might together initiate one single threat event. Threat events are described by their sequence of possible actions, activities or scenarios and furthermore we have to assign a likelihood of a successfully exploitation of a vulnerability in the interconnected system.

The next step after assessing threat sources and events is according to **Gordon et. al. (2003)** assessing the vulnerabilities. The generic case describes a vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Most of these weaknesses arise with security controls that either not have been applied or have been applied but retain some weakness. Furthermore we need to take into account the possibility of emergent vulnerabilities that can arise naturally over time as organizational missions/business functions evolve, environments of operation change, new technologies proliferate, and new threats emerge.

The National Institute of Standards and Technology (2012) describes Vulnerabilities also in a broader sense. Referring to this, vulnerabilities can also be found in external relationships (e.g.

dependencies on particular energy sources) mission/business processes (e.g. poorly defined processes by a server provider that communicates with the interconnected devices) and information security architectures.

A threat event that has successfully exploited a vulnerability might cause an adverse impact. The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of such a successful exploitation. Such harm can be experienced by a variety of stakeholders including the users of the Internet of Things as well as the providers.

The combination of potential adverse impact and the likelihood that a threat event will occur and successfully exploit a vulnerability results in an organizational risk, which has to be managed.

3.3 Threat Event

Threat events can be differentiated on a meta level into intended events or random ones. Intended events may be triggered by internal or external attacks, whereas the latter are the more relevant aspects within this context.[1] Intended threat events might be initiated by Hackers, Cyber-Criminals, organizational Crime, Cyber-Terrorists, spies, etc. in various ways. These ways may differ in the methodology which is used to exploit a vulnerability like Malware, Trojan Horses, Viruses, DDoS-Attacks on Servers etc. and the attacked targets within the interconnected infrastructure, for example servers, hubs or end user devices. Attackers might be motivated by different aspects. Within these aspects, attackers might seek to cause harm either to providers of IoT or to an individual person or household. As a consequence attackers are likely to focus on servers/providers instead of individual persons, since a successful overtaking of a server might imply to get access to lots of end user devices and furthermore to potential sensitive data, which is also a possible desire of the attackers.

Within random threat events we distinguish between human failures and technical failures. Human failures can be erroneous actions taken by users or by the provider, i.e. administrators, service-employees or other persons employed by the provider. Erroneous actions taken by users are more likely than that ones taken by the provider, since the user in general do not have the experience of a professional training for using their devices. However, theses human failures in general only have impact on their own household and should not affect servers or other households in a serious manner. On the other side, erroneous actions taken by the providers are less likely, since especially administrators who have access to sensitive nodes of the infrastructure

[1] Internal attacks would require an internal access point. Internet of Things solutions can hardly be accessed internally. A most probably source for internal attacks represents however the cloud component as the concretizing element of an internet-linked thing environment.

are trained and experienced in administrative actions on the servers. Nevertheless, these human failures may have impact on servers and consequently on many households.

Technical failures may occur at different nodes of the interconnected infrastructure and therefore may have different impacts, e.g. hardware at end-user level or server level and the corresponding services that are provided by the servers. These technical failures can either be a result of weaknesses in hardware or weaknesses in software and are very difficult to handle because of the strong heterogeneity within software, especially operating systems and firmware, and hardware. Typical examples for technical failures are malfunction devices or apps, which are used to control the devices, unavailability of apps and servers or the unavailability of hubs, which acts as an interface between devices and servers.

The described threat events will lead per definition to a successful exploitation if digital protection goals are violated. Referring to Bedner and Ackermann (2010) we distinguish between the following digital protection goals:

- **Access control**, i.e. there is an adversarial access on information resources by an instance which is not authorized.
- **Authenticity**, i.e. the identity of involved communication parties is maliciously manipulated, in order to fake an authorized instance.
- **Communication security**, i.e. the secure communication between authorized instances is influenced.
- **Integrity**, i.e. the substantial Correctness of data is influenced.
- **Availability**, i.e. there is a temporary or permanent malfunction regarding the availability of data, services, servers or devices.
- **Confidentiality**, i.e. the necessary level of confidentially regarding the information resources is not guaranteed.
- **Privacy**, i.e. there is a violation against national or international privacy regulations.

3.4 Vulnerabilities

The vulnerabilities determine the impact of a threat event on a threat source. Pronounced vulnerabilities cause severe (financial) losses in case an event takes place, while low vulnerabilities in turn lead to limited losses.

Vulnerabilities may be influenced by a variety of aspects. For instance the technical vulnerability of a mobile application is determined by the efforts spent on coding accuracy and security expenditures. The setting of an optimal level of vulnerability however is based on a variety of variable. Hereafter we introduce a short model to target this aspect.

We categorize the vulnerabilities on a scale of severity that depends on the likelihood that a successful threat event took place and the magnitude of impact on the threat source.
According to the **National Institute of Standards and Technology (2002)** we distinguish between three likelihood levels: A high likelihood level implies that the threat source is highly capable to exploit the corresponding vulnerabilities and controls to prevent the vulnerabilities from being exploited are ineffective. A medium likelihood level implies that the threat source is capable to exploit a vulnerability, but efficient controls are protecting the vulnerabilities. A low likelihood level implies that the threat source is not sufficiently capable and efficient controls are in place, to protect the vulnerabilities. Furthermore we distinguish, again according to the **National Institute of Standards and Technology (2002)** between three magnitude of impact levels. A high magnitude of impact implies that the successful exploitation of a vulnerability may lead to high loss of monetary or nonmonetary resources, or may significantly cause harm to provider or household and the involved persons. This also includes serious injury to these involved persons. A medium magnitude of impact implies that the successful exploitation of a vulnerability may lead to monetary or nonmonetary losses and injury to involved persons. A low magnitude of impact implies that there only may be small losses and no injury to involved persons. **Fig. 4 summarizes these two aspects and assigns overall severity levels to the vulnerabilities.**

Likelihood	**Impact**		
	Low	**Medium**	**High**
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

Fig. 4. Impact and likelihood as measures for vulnerability. (Source: National Institute of Standards and Technology, 2002)

According to the **National Institute of Standards and Technology (2002)** a high severity level corresponds to a strong need for corrective measures. Such measures will lower the severity level but inherent costs, such that there is a tradeoff between these costs and the severity level. The given infrastructure and operating systems in place may continue to operate, but a corrective action plan must be realized as soon as possible. A medium severity level implies that corrective measures are needed but there is no need of ad hoc corrective actions. If there is a low severity

level, correction measures do not have to be implemented anyhow. There is also the possibility of accepting this level and consequently accept the corresponding risk.

4. Adverse Impact

The previous mentioned examples of damages illustrate, that risks associated with the Internet of Things can not be completely prevented. And, more important, the remaining risks can cause a high loss potential with a considerable economic relevance for the companies affected. The preliminary risk assessment highlights the risks associated with the Internet of Things and the importance of creating a risk awareness in this context.

Currently, the new digital economy is promoting new products and services, shaping today's digital world of an Internet of Things. This innovation is still at a relatively early stage of development and although global internet players like Google or Apple are already creating digital hubs (in the form of software or products) for data aggregation, the development of interconnected products and services in the sense of an Internet of Things is mainly lead by startups and young companies (Basiliere, 2014). The aforementioned cyber risks may limit and influence the sales of a product, negatively affect the reputation of brands, business models or competitive positions (Haas and Hofmann, 2014). However these risks are still not at the top of the agendas throughout the industry (Koussa, 2013; Wortham and Perlroth, 2014). **But, if the main market innovators don't address the risks of an Internet of Things, who bears the risks?**

We discuss this question by analyzing the risk situation from three main point of views: (1) The innovators, creating products or services for the Internet of Things; (2) The consequences for consumers, using and adapting the Internet of Things; (3) The legal framework, defining liability and obligations.

4.1 IoT Innovator's product liability and responsibility

Any (physical) damage to interconnected devices or services in the Internet of Things as a result of a malicious cyber-attack, leads to the question about the innovator's product and service liability. We give a short overview about the legal framework in Germany, as no regulation or law directly addresses the requirements of IT security.

First, the supplier might be able to limit or exclude any liability based on individual contractual agreements, at least towards consumers. Such conditions and limitations are basically possible due to the principle of the freedom of contract. However, there are limits in the design of

contracts between consumers and companies, if these limitations implies disadvantages to the consumers. Therefore a general limitation of liability in case of a damage is not very likely. On the opposite site, the supplier could also explicitly cover potential risks of malicious cyber attacks. But as this currently hardly happens anywhere in the context of cyber risks, it is also unlikely for the Internet of Things.

Second, according to the current interpretation of german (and to some extend also international) law, a company must meet standards for the IT security of its products and services. A legal relevant standard are the so-called Common Criteria-Standards, which define the minimum security measures for IT-services and products. This includes criterias for testing and assessing the security of products and services offered (Spindler, 2007). However, the definition of the legal situation in the context of cyber risks is not trivial. Spindler (2007) describes in his paper comprehensively the liability situation in terms of cyber risks, which is quite complex and legal judgements still must be made from case to case.

Nevertheless, we conduct that the level of cyber security is to some extend predefined by law and regulation. The aforementioned security standards are necessary to avoid any considerable negative consequences derived from tort law. Companies offering services and products for the Internet of Things must be aware of product liabilities and the limits to exclude liability with respect to these risks contractually. In consequence, legal requirements concerning the cyber security imply a technological standard, which must be achieved by companies offering products and services for the Internet of Things. With the implementation of generally accepted state-of-the-art security standards and prevention measures, companies are able to reduce their liability in case of an cyber attack on their services and products. For the following analysis, we assume that every company offering interconnected services and products to the customer, is able to fulfill these technological security standards.

4.2 IoT Innovator's limited risk bearing capacity

Startups companies often mainly depend from the success of one product or service. As observable in practice, young companies - especially in IT-related sectors - will accept high risks to gain market share as fast as possible. We see here a discrepancy between potential business risks compared to the risk bearing capacities of these companies. In practice, there are several examples of startups entered markets without an adequate risk bearing capacity. As business risks have been realized, some of the companies were not able to handle these risks financially and consequently quitted the market and closed down the company. This kind of startup failure is especially observable within crowdfunding products and services in the last years. Established

companies on the other hand are looking for a long term business perspective. Consequently these companies are taking care of business risks and provide sufficient risk bearing capacity.

4.3 An analysis of the IoT innovator's incentives to improve its cyber security level

In order to develop a model to analyse innovator's incentive to improve its cyber security level and consequently to describe the risk situation of the Internet of Things, we make the following set of assumptions:

- We differ newcomers (STARTUP) and established, mature companies (MAT), both offering interconnected products and services for the Internet of Things.
- Startup companies
  - have only one product or service;
  - rely financially on its one-product business model;
  - are not able to diversify business risks;
  - have a limited risk budget **($RB_{STARTUP}$)**, and therefore a limited risk bearing capacity;
  - will exit the market, if any sustainable reputational or financial damage occurs.
- Established companies
  - have a portfolio of products and services;
  - are able to diversify business risks;
  - have a sufficient risk budget **(RB_{MAT})**, and therefore a high risk bearing capacity;
  - will avoid any sustainable reputational or financial damage, due to sustainable risk management.
- The risk budget corresponds to the risk bearing capacity of each company.
- All companies are profit-maximizing / cost minimizing.
- All companies are facing cyber-risks, affecting their products and services and generate first and third party risks.
- All companies fulfil an appropriate technological security standard by offering products or services for the Internet of Things, which is defined by legal requirements: $\mathbf{CSL_{LEG} \leq CSL}$
- Creating cyber security in products and services of the Internet of Things is costly. Exceeding security standards is the best way to further improve cyber security, but will lead to an exponentially rise of security costs.

Furthermore we use the following expressions in our model:

- **cyber attack costs;** costs resulting from first and/or third party costs in case of a cyber attack; will decrease with an increasing security level.

- **costs of cyber security level**; costs resulting from investments in cyber security of products and services in the Internet of Things.
- **total cost of cyber security**; combined costs of cyber attacks and cyber security investment costs; to companies both are expenses in terms of cyber security.
- **cyber security level;** security level which can be achieved by the company; varies from low **CSL_{LOW}** to high **CSL_{HIGH} .**

4.3.1 Innovator's general risk incentive and cyber prevention level

As the IoT's market is still immature, threats and damages affecting products and services of the Internet of Things are not realized on a grand scale yet. Whereas the general knowledge about cyber-risks is increasing, the damage potential of digital attacks resulting in physical damages is still unknown. Therefore it is difficult to specify an adequate security level, based on historical damage data. The level of vulnerability results from the probability and extent of loss, a company faces by joining the market of highly interconnected devices. Even though, while cyber risks cannot be completely prevented due to their technological nature, a risk reduction can be achieved by implementing security solutions like encryption, secure connections, antivirus software and firewalls into services and physical devices. Complementary to this technological approach, higher expenses for qualified security designer and knowledge creation might be necessary to secure the interconnected products and services. Both measures will increase the cyber security level (CSL) of the innovator's product or service.

The main problem of creating cyber security are costs. Even if investments in cyber security are necessary, budget restrains raise the question about its economic viability and the obtained prevention effect. The costs of creating cyber security by design follow an exponential function, especially if a security level above standards (CSL_{LEG}) is aimed at.

In our model, we assume a minimum cyber security level of CSL_{LEG} that is fulfilled by all innovators entering the market. Otherwise they wouldn't be in line with the legal requirements concerning product liability or contractual law and will not enter the market. A cyber security level above CSL_{LEG} is mainly an economical decision. A higher cyber security level requires higher cyber prevention measures, reducing the costs of first and third party damages in case of a cyber attack. But cyber investments also count as security costs, so the totals costs of cyber security will only decrease until an optimal investment level (CSL_{OPT}) is reached. At CSL_{OPT} any higher investments will decrease the cyber attack costs, but the total costs of cyber security will further increase. That is, because costs for security prevention measures are getting very high at a certain point. A **security level greater than CSL_{OPT}** will be realized, if the product's pricing and the company's profit can compensate the higher costs, e.g. because security is an elementary part of the product

design. In any other case, the company's investment decision for cyber security can be described as $\mathbf{CSL_{LEG} \leq CSL \leq CSL_{OPT}}$. **Fig. 5** illustrates this situation.

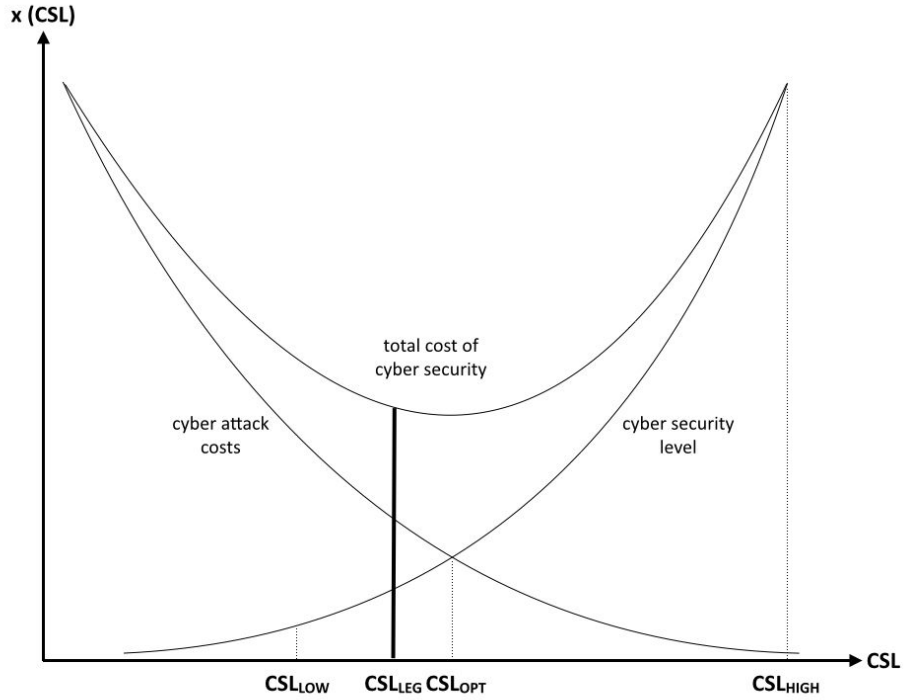

Fig. 5: The innovator's general choices of cyber security level (modelled after Olovsson, 1992).

4.3.2 The influence of risk budget on cyber security level

We see a potential limitation of the general security investment decision by the risk budget (RB) of companies. In contrast to legal requirements concerning product liability and cyber security standards, there is no regulation for the risk bearing capacity (RBC) of companies offering services for the Internet of Things. As we will show in the following models, the risk budget will influence the choice of cyber security level. To illustrate our assumptions, we differentiate between innovators as newcomer companies ($RB_{STARTUP}$) and mature companies (RB_{MAT}). The risk budget and therefore the risk bearing capacity of a mature company differs vastly from that of startups, due to their different funding and growth model. Both kind of companies have finite financial capacities to cover business risks. Beyond this threshold, the financial loss leads to insolvency. Startup companies might tend to take more risk than mature companies, even if their RB doesn't cover these risks. They operate at and above the limits of their RB to fastly establish their products and services in the market, by accepting the risk of insolvency at the same time. As opposed to

this, mature companies operate more conservatively, usually having more RB than necessary for their operations.

4.3.3 The influence of risk budget on cyber security level: established companies

So, the aforementioned decision problem about security investments depends mainly on the company's risk budget. First, for established companies, we assume a risk budget which allows the realization of nearly any cyber security level of its products and services above the legal requirements **($CSL_{MAT} \geq CSL_{LEG}$)**. Second, it will additionally fully **reflect the costs of a cyber attack** in its investment decision, as it's able to cover respectively bear the risk as it has no intention to externalize the risks (Bauer 2009). It tries to avoid any reputational losses and internalize the costs of cyber attacks. Therefore, the company must consider both, the costs of cyber attack and the investment costs of cyber security. If the company's risk budget (and thereby its risk bearing capacity) covers the total cost of cyber security **(TSC)**, thus **$RB_{MAT} \geq c$ (TSC)**, it will choose the security level **CSL_{OPT}** corresponding to the total cost optimum **TSC_{OPT}**. As we assume a profit-maximizing company, **CSL_{OPT}** is achieved, because it implies the lowest total cost of cyber security. As mentioned before a higher security level **($CSL_{MAT} > CSL_{OPT}$)** will only be realized if security is a specific component of its business model.

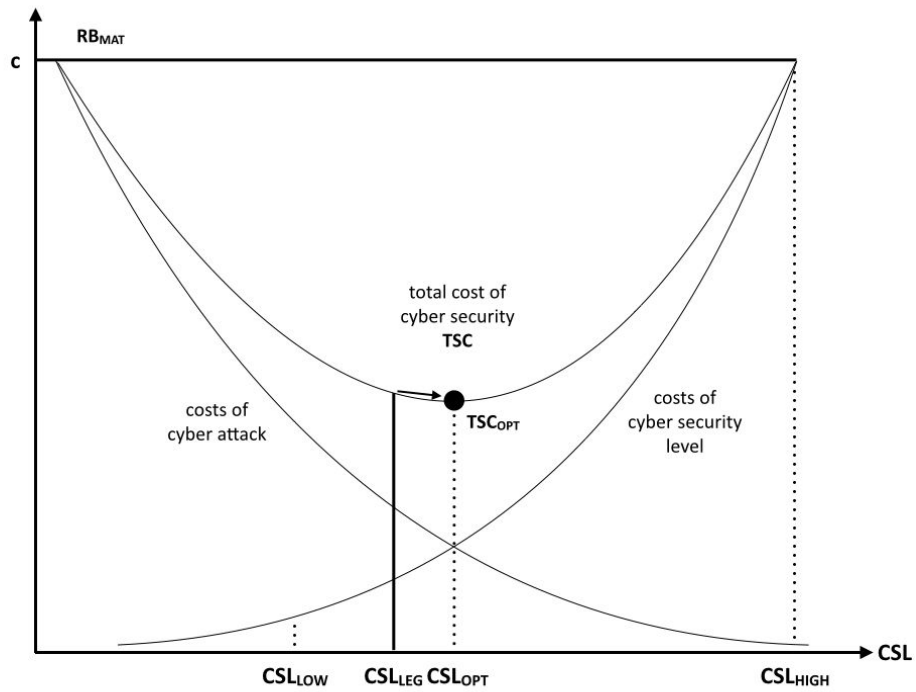

Fig. 6. The choice of CSL by mature companies for the Internet of Things.

This assumption can be confirmed from reality: Sony experienced a huge data breach and services interruption in 2011. The financial consequences were not covered by the insurance policy, so Sony covered the damage costs within its own risk bearing capacity to avoid further reputational losses.

4.3.4 The influence of risk budget on cyber security level: startups companies

The CSL investment decision of startup companies is different to the one described above. The risk bearing capacity of these companies is generally low, while their risk appetite and risk tolerance is often higher compared to matured companies. This interplay of factors builds an important part of the business when entering new markets and establishing new products and services as a newcomer. The ability of startups - as the main innovators of the Internet of Things - to invest into cyber security is restricted by their risk budget.

We differentiate two different financial states of a startup entering the market of the Internet of Things:

(1) $RB_{STARTUP} < c\,(CLS_{LEG})$

In state (1) the startup is not able to fulfill legal requirements concerning cyber security standards due to budget limits. The company's risk budget is too low to meet the requirements defined by law, legal requirements or product liability. This might happen, if the startup has low capital resources or limited access to credits. We assume in state (1) the company will not enter the market of Internet of Things.

(2) $c\,(CLS_{LEG}) < RB_{STARTUP} < c\,(TSC_{LEG})$

In state (2) the startup company is able to fulfill a security level defined by legal regulatory requirements. It will take the chance to enter the market as $\mathbf{CSL_{LEG}}$ can be met. But as it risk budget is limited, the related risk bearing capacity plays an important role in the decision of the cost optimal $\mathbf{CSL_{OPT.}}$ In this situation, the company is not able to cover the costs of cyber attack, is the risk bearing capacity is low. Covering all costs will lead to the insolvency of the company. As a consequence it will externalize any cyber attack cost and take these expenses not into consideration when choosing the cyber security level. As a result, the company has no incentives to improve its cyber security level. Instead it will choose its cost optimal security level and remain at the legally minimum security standard $\mathbf{CSL_{LEG}}$. Optimizing its security investment strategy, the company has incentives to fulfil only the legal minimum security standard. When the company is not able to cover any third party cyber risk costs above its $\mathbf{RB_{STARTUP}}$, the investment decision is

restricted to the area between $\mathbf{CSL_{LEG}}$ and $\mathbf{CSL_{HIGH}}$. As there are no incentives to improve the cyber security level above accepted standards, $\mathbf{CSL_{LEG}}$ will be achieved as security level.

This means in state (2), if the risk budget and the risk bearing capacity is too low, any negative (financial) effect on the consumer will not affect the company's security investment decision (Brown, 1973). Especially for startups supplying the Internet of Things, this argumentation is valid as the seed capital and consequently the financial risk-bearing capacity of these companies is often limited. Moreover, their reputational or company value is no incentive to bear these expenses, as both are low in the beginning. Finally, new companies prefer a legal form with limited liabilities and a lower required founding capital when establishing, like LLCs in the US or private company limited by shares in the UK. This legal limitation of financial liability implies an economic incentive for externalizing risk-costs and lowering the level of technological prevention, especially if financial damages to third parties exceed the company’s risk-bearing capacity (Posey, 1993).

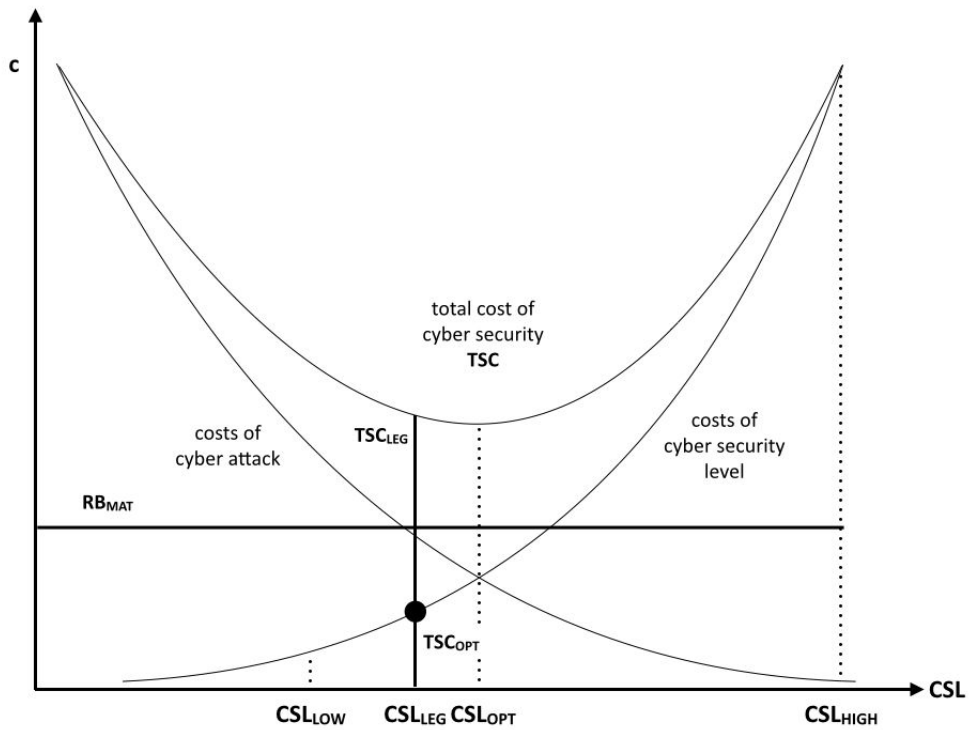

Fig. 6. The negative influence of a lower RBC on the CSL.

4.4 Risk externalization as a result of low risk bearing capacities

Companies may face damage costs resulting from realized cyber risks within the Internet of Things. While product liability and legal conditions support the implementation of security standards into products and services of the Internet of Things, these measures do not avoid the realization of cyber risks. Due to low risk bearing capacities of new companies, they have a high economic incentive to (legally) externalize the upcoming risks as long as the minimum security standards are met by the company. Cyber risk costs above the own risk bearing capacity will not be considered into the cyber security investment decision.

This described situation is valid for startup and newcomer companies, the main innovators of the Internet of Things. The extent of risk externalization is certainly limited by legal regulations, as criminal responsibility of the providers will be legally prosecuted. Nethertheless current laws allow companies to restrict their product liability in terms of cyber attacks as long as security standards, consumers protection and customer due diligence measures are compiled.

In our model, we assume that companies are in line with legal regulations, if they meet approved security standards. In that case, they are able to restrict their product liability and to establish contractual agreements, that considerably limit their liability in terms of cyber attacks.

4.5 Influence of cyber insurance to risk externalization and risk bearing capacities

Cyber insurance can increase the risk bearing capacities of an exposed company and therefore reduce the incentives to externalize the cyber attack risks. With cyber insurance coverage the company will reduce the its cyber attack damage costs, while the cost of cyber security level will increase for the amount of insurance premium. Externalized risks will get internalized, if the costs of insurance premium and risk internalization remains below RB. In that case, the company does not face insolvency in case of an cyber attack on its devices anymore, so its able to handle the risk in terms of financial and reputational damage. Insurance could be one solution to increase the risk bearing capacity of affected companies and therefore change their incentives to risk externalization. This situation is shown in Fig. 7.

4.6 Influence of regulatory measures to risk externalization

Last, a regulatory institution should define a global framework for cyber security in the Internet of Things and force the implementation of security standards including manufacturers' liability to ensure, that above mentioned measures will be adopted by the industry and increase the risk perception on both sides of the market. A possible way is to create certification for interconnected devices, comparable to the CE mark used to mark conformity of electronic devices with the legal requirements in the European Union. However the conclusion of this example out of many is not to criticize the related technological progress, but to point out where and how this

type of progress requires regulatory adjustments to fit in existing insurance concepts and to guarantee the future progress for this desirable development.

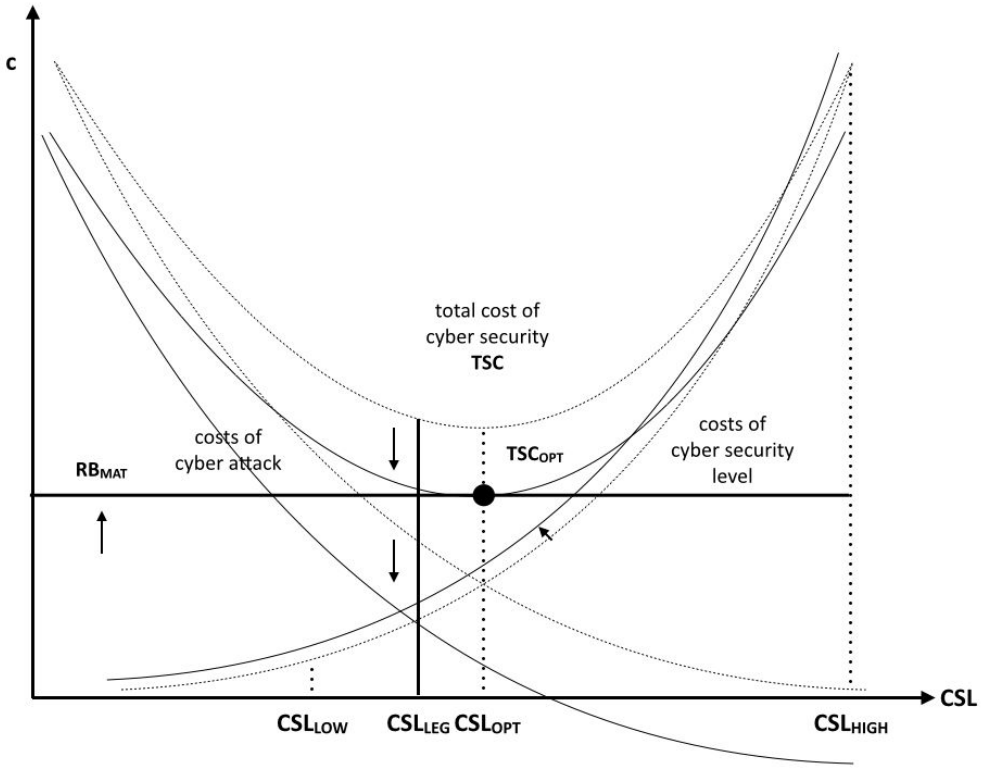

Fig. 7. Influence of cyber insurance on the risk bearing capacity and incentive for cyber security.

5. Conclusion and outcomes from an insurance industry perspective

The before introduced model identified an freeriding tendency for startup companies. This incentive to externalize prevailing risk exposures however primarily leaves the individual user exposed to resulting damages and linked losses. In case the damage is concretizing within the household, the coverage potentially may be provided by household contents insurance, but at the moment household content insurance is not including cyber related damages.

However, it still remains doubtful whether insurance companies within the early stage of the market adoption of internet connected items are able to attribute a claim to the actual source cyber. Hence companies can successfully externalize product related loss potential to the end customer. The insurance industry will be opposed to additional costs and demand regulatory improvements.

As mentioned before, the allocation of a loss cause is of essential importance within this context. This also includes the implementation of transparent forensic technical solutions to identify the actual loss source. This will be of high relevance to reattribute actual responsibilities, not only for the individual user but also for the insurance industry. Furthermore, consumer protection demands urgently limitations within the field of risk externalization. Regulatory impacts for sensitive startup companies however will not only be able to extend the intended confrontation with reasonable risk consideration and carrying, but implicitly by doing so will lead to higher capital requirements. Similar to regulated branches like banks and insurance companies, potentially also certain types of startups will require such supervision, too, with all resulting limitations to the segment growth. However the changes caused by the IoT not only leave the insurance industry opposed to new challenges but also offer massive amount of data. The IoT is hence offering opportunities already now targeted within the field of Big Data. The client becomes transparent in terms risk characteristics and behavior to an hereto unarchived level, improving premium calculation and the balance within the portfolio.

The relevant question for users of the Internet of Things is twofold. First of all, who is in charge of covering damages and resulting financial losses from any interconnected device. Second, is such a loss included in any of the existing or, more interestingly, purchasable insurance policies? These two questions however are additionally challenged by a proof of liability problem, resulting from external threats. We are going to address this aspect at the end of this chapter.

6. References

Allianz (2014): The rise of interconnected risks. Allianz Risk Barometer on Business Risks 2014. 1-9

Anderson, J. M., N. Kalra, K. D. Stanley, P. Sorensen, C. Samaras and O. A. Oluwatola (2014): Autonomous Vehicle Technology. A Guide for Policymakers. RAND Corporation.

Basiliere, P. (2014): Big Business Fail: Makers and Startups are The Ones Shaping the Internet of Things. [24.04.2015] http://blogs.gartner.com/pete-basiliere/2014/11/20/big-business-fail-makers-and-startups-are-the-ones-shaping-the-internet-of-things/

Bedner, M. and T. Ackermann (2010): Schutzziele der IT-Sicherheit. Datenschutz und Datensicherheit. 34(5): 323– 328

Biener, C., M. Eling and J. H. Wirfs (2015): Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers. 40: 131–158

Brown, J. P. (1973). Toward an economic theory of liability. The Journal of Legal Studies. 2(2): 323–349

CBC News (2015): Smart locks could make your home less secure. Access date 28.06.2015 under http://www.cbc.ca/news/technology/smart-locks-could-make-your-home-less-secure-1.3057872

Dynes, S., E. Goetz and M. Freeman (2008): Cyber Security: are Economic Incentives Adequate? In: Critical Infrastructure Protection, Springer, editors Eric Goetz and Sujeet Shenoi, 2008

Eeten, M. van and J.M. Bauer (2009): Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. Journal of Contingencies and Crisis Management. 17(4):221-232

Gubbia, J., R. Buyyab, S. Marusic and M. Palaniswami (2013): Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 29:1645–1660

Gordon, L.A., Loeb, M.P., Sohail, P. (2003): A framework for using insurance for cyber-risk management – Seeking to protect on organization against a new form of business losses. Communication of the ACM 46, 81–85

Hofmann, A. and H. Ramaj (2011): Interdependent risk networks: the threat of cyber attack. Int. J. Management and Decision Making. 11 (5/6): 312-323

Koussa, S. (2013): Should Startups care about application security? Technology Innovation Management Review, Access date 22.01.2015 under http://timreview.ca/article/706.

Miorandi, D., S. Sicari, F. De Pellegrini and Imrich Chlamtac (2012): Internet of Things: Vision, applications and research challenges. Ad Hoc Networks. 10:1497–1516

Nest (2015): https://nest.com/works-with-nest/ [11th July 2015]

National Institute of Standards and Technology (2002): Risk Management Guide for Information Technology Systems, Gaithersburg.

National Institute of Standards and Technology (2012): Guide for Conducting Risk Assessments, Gaithersburg.

Patel, S., J. Zaveri, and J. Z. S. Patel (2010): A Risk-Assessment Model for Cyber Attacks on Information Systems. Journal of Computers. 5(3):352-359

Posey, L. L. (1993). Limited liability and incentives when firms can inflict damages greater than net worth. International Review of Law & Economics. 13(3):325–330

Schwartz, G. A. and S. S. Sastry (2014): Cyber-Insurance Framework for Large Scale Interdependent Networks. Proceedings of the 3rd international conference on high confidence networked systems. 145-154.

Sundmaeker, H., P. Guillemin, P. Friess and S. Woelfflé (2010): Vision and challenges for realising the Internet of Things. Cluster of European Research Projects on the Internet of Things—CERP IoT, 2010.

Spindler, G. (2007): Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären. Bundesamt für Sicherhheit in der Informationstechnik. Access date 20.12.2014 under www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30962/Gutachten_pdf.pdf

Wef (2015): Industrial Internet of Things, Unleashing the Potential of Connected Products and Services. Access date 03.03.2015 under http://www3.weforum.org/docs/WEFUSA_ IndustrialInternet_Report2015.pdf

Wortham, J. and Perlroth, n. (2014): When Statups don't lock the door. Access date 25.01.2015 under http://www.nytimes.com/2014/03/03/technology/ when-start-ups-dont-lock-the-doors.html.