



Review

On the Identification, Evaluation and Treatment of Risks in Smart Homes: A Systematic Literature Review

Raphael Iten ^{1,2,†} , Joël Wagner ^{2,3,*,†}  and Angela Zeier Röschmann ^{1,†}

- ¹ Institute for Risk & Insurance, ZHAW School of Management and Law, Technoparkstrasse 2, 8400 Winterthur, Switzerland; raphael.iten@zhaw.ch (R.I.); angela.zeierroeschmann@zhaw.ch (A.Z.R.)
² Department of Actuarial Science, Faculty of Business and Economics (HEC), University of Lausanne, Extranef, 1015 Lausanne, Switzerland
³ Swiss Finance Institute, University of Lausanne, 1015 Lausanne, Switzerland
* Correspondence: joel.wagner@unil.ch
† These authors contributed equally to this work.

Abstract: The emergence of smart technologies in homes comes with various services and functions for everyday life. While a smart home (SH) is associated with great potential in terms of comfort and risk treatment, it also introduces new and alters existing risks. Despite a growing number of academic studies on SH risks, research is fragmented with regard to its focus on certain disciplines and is still rather technology-focused. In this paper, we fill this gap by providing a comprehensive understanding of relevant risks through a systematic literature review. Following the guidelines of the PRISMA reporting protocol, we search 1196 academic and practitioners' publications related to household risks or risk perceptions of SH users. A final set of 59 records results in three main themes. They include (1) a synthesis of pre-existing and emerging risks sketching the new risk landscape of SH households, (2) a discussion of the prevailing risk evaluation methods, and (3) a presentation of SH-related risk treatment options with a particular emphasis on insurance. We specify the influence of SH on risks and risk perception, and highlight the relevance of analyzing the interconnection of risks in complex systems, such as SH. Our review lays the basis for assessing SH risks and for enabling more comprehensive and effective risk management optimization.

Keywords: smart home; risk identification; risk evaluation; risk treatment; insurance



Citation: Iten, R., Wagner, J., and Röschmann, A.Z.. 2021. On the Identification, Evaluation and Treatment of Risks in Smart Homes: A Systematic Literature Review. *Risks* 9: 113. <https://doi.org/10.3390/risks9060113>

Academic Editor: Mogens Steffensen

Received: 7 May 2021

Accepted: 28 May 2021

Published: 8 June 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Increasing households' inclusiveness, safety, resilience, and sustainability is a global trend supported by the emergence of new technologies (Salhi et al. 2019). Smart technologies and services also facilitate the integration of work life into the private home, a trend that has been amplified by the surge in momentum brought by the COVID-19 pandemic (Von Gaudecker et al. 2020). A smart home (SH) can address needs as energy management (Reinisch et al. 2011; Scott 2007), health (Alam et al. 2012; Ehrenhard et al. 2014), security (Blythe and Johnson 2019; Schiefer 2015), lifestyle, and convenience (Chan et al. 2012) through the use of connected and embedded devices. Early definitions by Lutolf (1992), and later Aldrich (2006), discuss the essence of SH in a capacious manner. They capture the technical dimension, the services and functions that SHs provide, and the types of user needs that the technologies are designed to meet. Today, two types of SH definitions are used: one that refers to the technological attributes and another that characterizes the service perspective (Sovacool and Furszyfer Del Rio 2020). However, Marikyan et al. (2019) show that both types of definitions address three typical attributes of SH, namely the technological aspects regarding hardware and software, the services enabled by SH, and, thus, the ability to satisfy certain household needs. In this research, we consider SH as a home equipped with a set of smart technologies that offer remote, digitalized, and automated services to a resident improving its quality of home life.

As homes become “smarter”, our way of living changes accordingly (Keller et al. 2018). As such, the risks associated with a household change fundamentally. SH is associated with great potential in terms of risk treatment, but, at the same time, causes new risks (Denning et al. 2013). In fact, new risks, especially in the area of cyber security and privacy, emerge and have been discussed in recent literature (Loi et al. 2017). Thereby, human-related or software-related risk sources, e.g., inadequate access control, are identified as crucial (Jacobsson et al. 2016). While much attention is given to privacy and cyber security risks, other household risks, such as water, fire, or theft, have attracted little academic attention in SH settings so far. Practitioners’ studies, however, promote SH as an important risk mitigation measure. For example, a study by Davis (2020b) show that the risk of water damage could be significantly reduced with the implementation of SH. To date, there are no systematic reviews of the literature on risks in SH. Various reviews following more narrow approaches exist. For example, Amiribesheli et al. (2015) summarize the state of affairs from a health perspective, Hosseini et al. (2017) take the viewpoint of energy management services and Marikyan et al. (2019) conduct a use-case overarching user-centered analysis. In addition to some purely technical analyses of cyber risks (Ali et al. 2019; Nawir et al. 2016), the study by Blythe and Johnson (2019) synthesizes the literature on crimes facilitated by Internet of Things (IoT) environments, with a particular emphasis on the home environment.

Hence, despite a growing number of academic studies on SH and the associated risks, research is fragmented in that it focuses on selected risks or risk perception in the context of SH acceptance. As such risks are mainly analyzed from information security or technology acceptance disciplines, separately and predominantly field-specific but have not yet been systematically synthesized. As a consequence, the literature on risks in SH lacks a comprehensive picture about which risks emerge or change with SH dynamics.

In this systematic literature review, we identify and analyze the risks that are associated with SH households. By adopting an interdisciplinary approach, we aim to improve the understanding of the (changing) risk exposure of SHs. A more comprehensive understanding of risks and their drivers lays the basis for the optimization of risk management. This also enables future research to propose measures that effectively address risks in their entirety and thereby generate value out of SH from a risk management perspective.

From an initial collection of 1196 academic and practitioners’ publications, we retain 59 references that we include in our systematic literature review. The study of the final corpus resulted in three main themes of SH risk research. First, we identify pre-existing and emerging risks in SH on the basis of an inductive categorization. Emerging risks related to cyber and dependency are the most prominent in the literature. In the case of pre-existing risks, the extant literature mainly focuses on financial aspects or household risks known from the insurance business. Second, we present applied risk evaluation methods, most of which are methods from the information security discipline or from acceptance research. In addition, risks are evaluated using well-known frameworks (e.g., ISO 31000). Third, we structure risk treatment options in two groups. Those that are recommendations for SH technology and service providers and those representing options for end-users. Implications for the insurance industry are studied hereunder.

The paper is organized as follows. In Section 2, we present the methodology used to review the literature and to derive the corpus of records that we analyze. We present our findings on the risk identification in SHs and our synthesis on pre-existing and emerging risks in Section 3. In Section 4, we discuss the prevailing risk evaluation methods. Finally, we present the identified risk treatment options in Section 5. Thereby, we put special emphasis on the risk transfer to insurance in the SH context. We conclude in Section 6. In the Appendix, we provide a comprehensive synopsis of the reviewed papers (Tables A1 and A2), as well as a detailed overview of the identified risks (Table A3).

2. Methodology

In this section, we present the review strategy and descriptive statistics on the retained body of literature. Finally, we synthesize the final corpus by presenting the main themes and by introducing the underlying theoretical concepts and terminology.

2.1. Review Strategy and Data Collection

Our review identifies and summarizes risks in SHs, using a systematic methodological approach. To ensure a high degree of reliability, we follow [Tranfield et al. \(2003\)](#) and use the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol ([Page et al. 2020](#)) as a reporting guide.

Before starting the systematic review and to obtain an initial understanding of the topic, we conducted a preparatory literature review which included the identification of gaps in research, study objectives and development of a review protocol. This preparatory review has revealed several gaps that pointed to the need for a systematic investigation of risks in the context of SHs. It has also shown that beyond academic research, an increasing number of practitioners' studies point to relevant aspects regarding risks in SHs. For this reason, we organize our research in two streams (see [Figure 1](#)). In the first search stream, we focus on academic research articles. In the second search, we pinpoint relevant industry expertise, such as reports from risk management experts, government departments, or insurance companies. We view them as a relevant expert group, especially, since insurance companies, for example, have the most comprehensive data on household risks and possess distinct risk analysis skills.

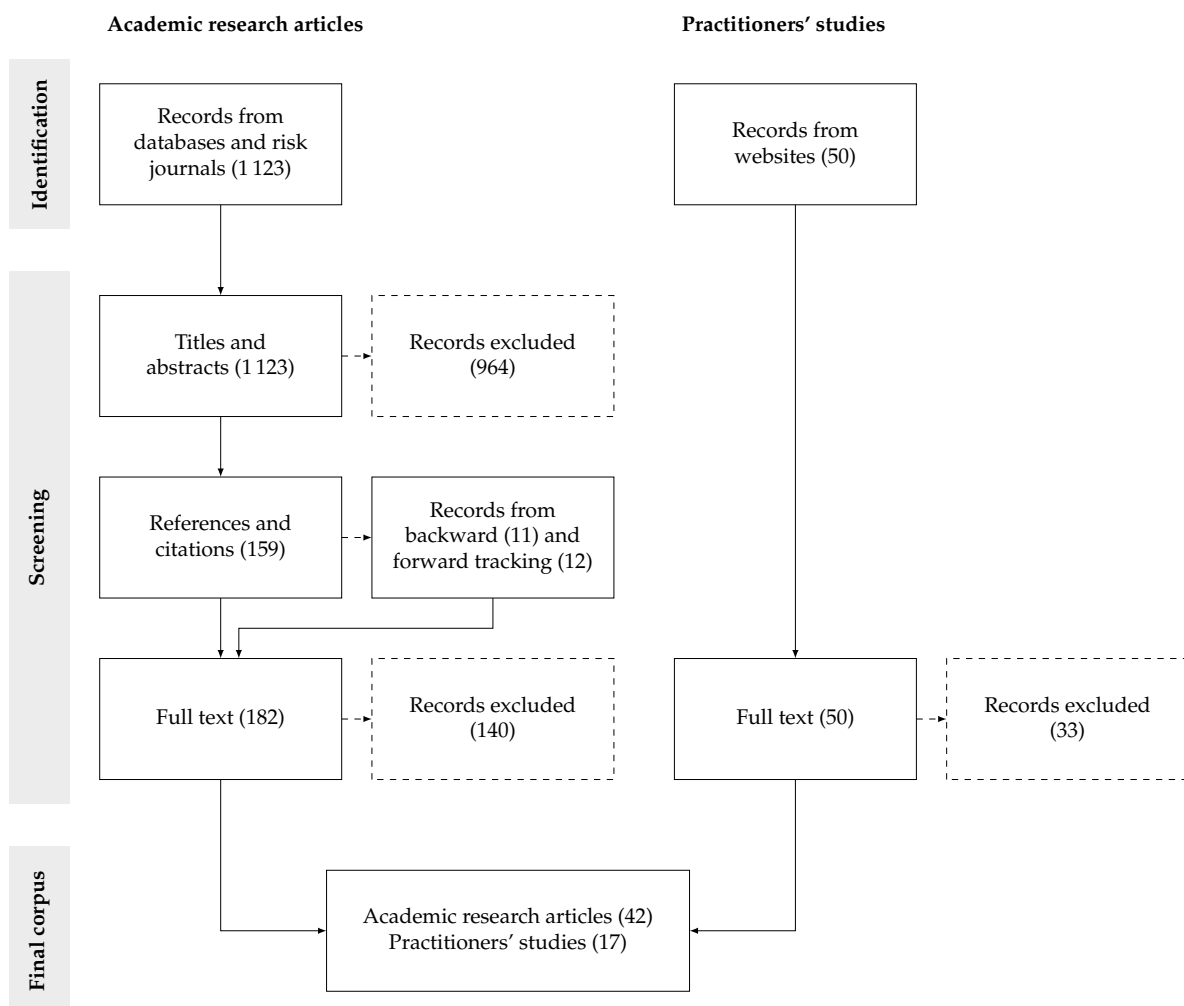


Figure 1. Flow diagram for the identification and screening of records along PRISMA guidelines.

For the academic search stream, we selected Web of Science, EbscoHost, and ProQuest as information sources, considering all citation indexes of the Web of Science Core Collection, only Business Source Premier in EbscoHost, and ABI/INFORM Global, as well as ABI/INFORM Trade and Industry, in ProQuest. To guarantee a holistic view of all risks that appear in SHs, we further identified 16 risk journals (e.g., Risk Management and Insurance Review or Asia-Pacific Journal of Risk and Insurance), which were not covered by the selected databases. We screened these journals using the same selection criteria. The choice of keywords focused on the terms “smart home” and “risk”. (The full search streams used are as follows: *AB("smart home*" OR "connected home*" OR "smart living" OR "smart building*" OR "smart technology") AND AB("risk*" OR "threat*" OR "barrier*" OR "limit*")*, as well as *AB("iot" OR "internet of things" OR "big data") AND AB("risk*" OR "threat*" OR "limit*") AND AB("home*" OR "household*" OR "house*")*.) We defined eligibility criteria in terms of time span (years from 2002 to 2020), language (English, German, French, and Italian), and included all types of sources since no prior work systematically covered risks in SHs. The data collection process was facilitated by the use of a reference manager software (Mendeley) and clear decision rules on the origin of the data. If two sources pointed to the same results, the primary dataset was collected. The final query in the databases and the risk journals was performed in July 2020 and resulted in 1123 records.

Following the identification of the academic research articles, a screening process was conducted (see Figure 1). We used inclusion criteria coded on a scale ranging from 0 to 3 as follows: Level 3 is used when risks are analyzed in a systematic and holistic way in the source, level 2 indicates that risks are discussed but the focus is on a single risk (e.g., technological risk), level 1 denotes work wherein some aspects of risk management are mentioned, or where the context suggests that risks may be discussed, and level 0 indicates that no relevant aspects on risks are discussed. Further, we excluded studies focusing on medical aspects concerning certain disease risks (e.g., risk of a stroke in a home-care setting) or technical studies (e.g., household energy management) that do not discuss risks. While one of the authors handled the selection and scoping of the articles, the other authors acted as reviewers and conducted the proof-reading to validate the collection. Independence was guaranteed since no knowledge on the other reviewer’s scoring was shared. Disagreements were resolved afterwards by a look-up of the detailed results and, if necessary, by a discussion whether the study should be ranked up or down. (To limit any inappropriate use of the methodology and to counteract the risk of bias, the recommendations of Thomé et al. (2016) were followed. The review protocol and the inclusion criteria were jointly developed by the team of authors. We consequently sought to work with more than one independent reviewer and compared individual selections only after scoring was completed. Finally, for certainty assessment of the literature, we included several factors. One indicator was the degree to which additional search streams led to known results identified in a prior search stream. Dedicated search processes were done for grey literature to validate the existing knowledge and reveal new content. Moreover, we performed text mining on the final corpus of records to validate whether any relevant themes were not covered by the full-text articles.) In the first step of screening, reviewers scored the studies based on the titles and the abstract, resulting in 159 references scored 1 or higher that were retained.

Based on these 159 records, a backward and forward citation search was performed. This led to 11 and 12 documents being added, respectively, from backward and forward tracking. A set of 182 records was considered for full-text assessment. After excluding 140 records that did not meet the SH inclusion criteria, 42 academic research articles ranked as relevant.

In the second search stream, we identified practitioner’s studies in the grey literature. A dedicated web search pursued a specific search strategy focusing exclusively on organizations engaged in household risks or SH technology. A total of 24 insurance companies and 63 other organizations were included in the search. (An example query for web search is as follows: *"smart home" AND "risk" site:lexisnexis.com.*) We extracted the results of the top-ranked results for each organization and retained 50 references scoring 1 or higher.

Full-text screening on these records resulted in the exclusion of 33 records and, finally, 17 practitioners' studies are retained.

The final corpus of literature that we use in the sequel includes 59 records: 42 academic research articles and 17 practitioners' studies. A synopsis of the records is provided in Tables A1 and A2 in Appendix A. For each record, we provide the geographical scope (column "region"), type of publication (column "type"), and the research method used (column "method"), as well as information on key contents and main results. Further, we identify the records related to risk identification (RI), risk evaluation (RE), and risk treatment methods (RT), including insurance.

2.2. Descriptive Statistics

In the following, we provide descriptive statistics on the screened records and the final corpus of literature. We perform a frequency analysis on the records sought for full-text screening (182 research articles and 50 practitioners' studies; see Figure 1) and text mining on the final body of records (42 articles and 17 studies). These analyses visualize key metrics of the literature and the results help to provide an initial mapping of the main concepts.

Frequency analysis of the screened records

Using the 182 academic research articles and the 50 practitioners' studies retained for full-text screening, we perform a frequency analysis on the publication year of the records and on the geographical region under investigation. The graph in Figure 2a shows the development of the number of records between 2011 and 2020. It becomes evident that the relevant research field steadily grows. The number of publications in our database increased from 2 records in 2012 to 56 records in 2019. In the earlier 2000s, there are only sporadic occurrences with one or two records per year. We do not discuss the figure for 2020, as it is incomplete since the search covered publications until July 2020. We illustrate the geographical distribution of records in Figure 2b. The anglo-saxon region dominates the research activities, with the U.S. and UK contributing most, respectively, with 52 and 34 records. South Korea (KR, 19) and China (CN, 12) follow next. Overall, more publications originate from Europe (57) than Asia (47).

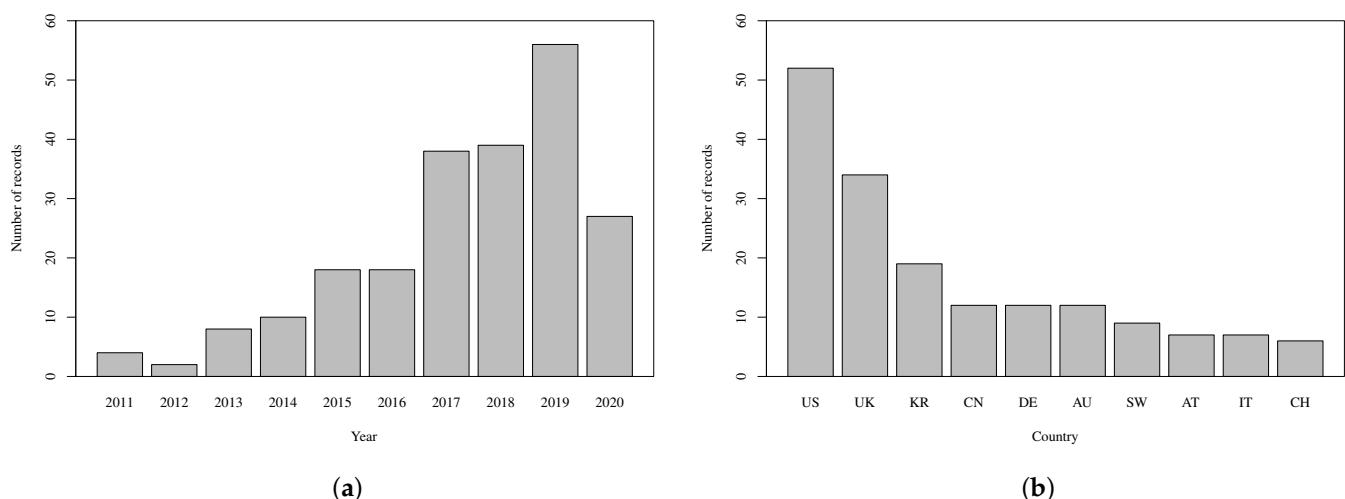


Figure 2. Frequency analysis of the screened records from 2011 to 2020 and per country. (a) Development over time. (b) Distribution by country. Note: For 2020, records include publications until July.

Text mining on the final body of records

Text mining on the main corpus of 42 research articles and 17 practitioners' studies was used to quantitatively assess the concepts included in the body of literature. A visualization of the results is given in Figure 3. (The criteria for the scoring were English language, at least

3 letters and on the basis of a word stem (e.g., the key term “secur” includes among others the words “security” and “secure”).) Expectedly, the key terms “smart”, “home”, and “risk” are the most frequent since they were searched for to initially determine the records. An interesting finding is that “secur” appears far more often than “privac”. This reflects the relevance of security, which is of particular concern for the SH risk literature in terms of cyber security and physical security (see Section 3.1). The relatively high frequency of terms with “use”, especially compared to “technology”, is likewise of interest. It indicates that usage drives risks, yet research remains primarily technology-focused. Insurance-related research (“insur”) counts a relatively high number of hits when compared to the keys “servic”, “user”, or “perceiv”. This is mainly due to the range of insurance-related practitioners’ studies that resulted from the web search.

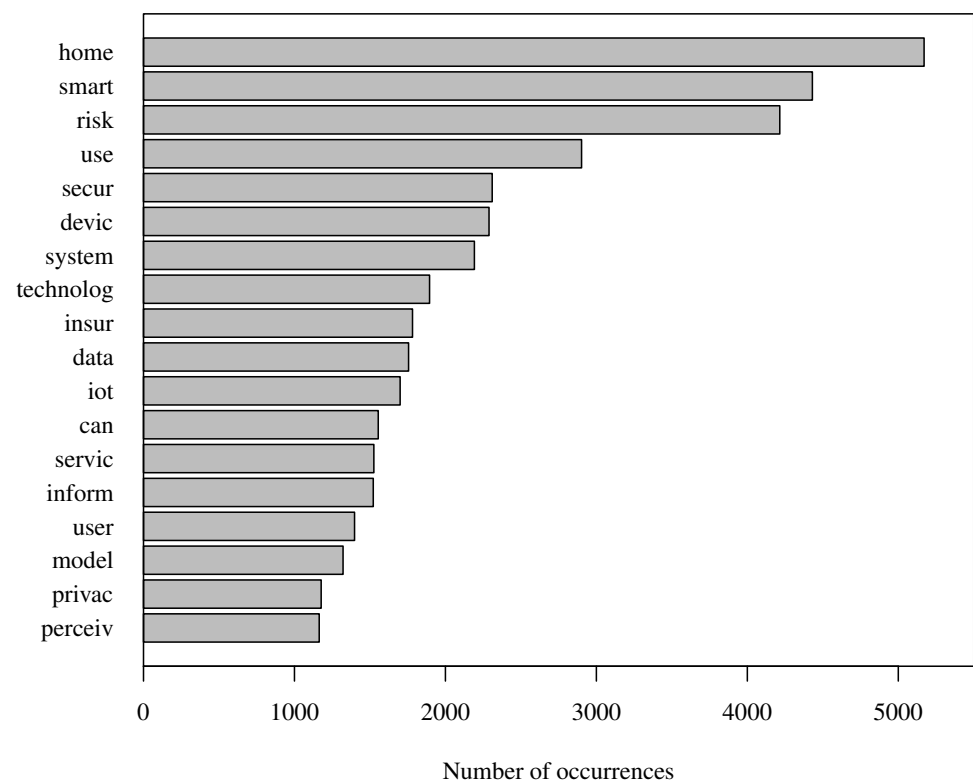


Figure 3. Text mining of key terms in the final corpus of records.

2.3. Data Synthesis

To synthesize the data, we adopted an inductive thematic analysis method as defined by Braun and Clarke (2006). To minimize the risk of bias, we pursued a six-phase process where topics are coded with no pre-existing categorization within the research field (see, e.g., the orientation by Mikkonen and Kääriäinen (2020)). The value of an inductive thematic analysis for our research question relates to the capacity to analyze latent themes. Since there is no prior work reviewing risks in SH and we combine different disciplines analyzing risks separately, the chosen bottom-up approach leads to the best possible completeness. Our analysis results in three main themes, to which all risk relevant statements can be assigned. The relevant themes are the following:

- *Risk identification.* The difficulty of identifying risks for SHs resides in having different terminologies due to the diversity of disciplinary origins. We present our findings on risk in SHs in Section 3 and attempt to keep a simple structure. For this reason, we adopt the risk management framework ISO 31000 (ISO, International Organization for Standardization 2018). That framework is generally applicable, simple to use and proven in the corporate context. We summarize the identified risks along their

influence on impact and acceptance (see Table 1 in Section 3 and Table A3 in Appendix A).

- *Risk evaluation.* Methods to assess risks can be found in different research areas. In Section 4, we present the risk evaluation methods available from the literature and attribute them to the respective disciplines. Findings from academic literature are synthesized together with the methods found in practitioners' studies (see Table 2 in Section 4).
- *Risk treatment and insurance.* Finally, selecting and implementing appropriate measures to address risks of SHs represents a nascent topic of SH risk research. However, the focus here is still entirely on cyber risks. Since we cannot fall back on any established concepts for structuring, the measures are divided into two categories. The first presents options that act as recommendations for SH providers. The second presents options for the users. The effect of SH on insurance, which represent a treatment option in their own right, is further discussed in depth.

While other topics, such as technology characteristics, benefits, adoption, sustainability, society, commercial, and legal, emerged, they are interesting for SH overall, but, since they are not relevant for our risk focus, we do not discuss them further. Both Tables A1 and A2 in Appendix A provide a synopsis of the final corpus of records and the association of the literature to the three main themes.

3. Risk Identification

In general terms, a risk is a deviation from a desired condition (ISO, [International Organization for Standardization 2018](#)). With the broad variety of technology available for home, likewise, various targets and various possible deviations arise ([Nurse et al. 2016](#)). This section presents the risks identified from the final corpus of 59 records. We summarize the risks along their influence on impact and acceptance. Furthermore, we structure our synthesis in emerging and pre-existing risks. On the one hand, pre-existing risks are considered as those already being discussed for households without SH devices or services. Often, they include risks from insurance-related studies. Emerging risks, on the other hand, refer to risks emerging with the integration of SH applications in a household. They are typically developing or changing risks that are more difficult to quantify ([Mazri 2017](#)). Emerging risks to privacy and cyber security have been signaled early on by [Radomirovic \(2010\)](#). (We observe that risk analyses from the information security literature often take a distinct approach in describing risks by identifying the asset, vulnerability and threat of a risk ([Jacobsson et al. 2016](#)). For such risks, we follow this structure. Similarly, risk analyses from the technology acceptance literature use a specific vocabulary. Given their user-centric orientation, the risks identified from this literature are described as perceived risks by lay users. As an example, perceived privacy risks relate to consumers' concern of having personal data misused or disclosed to third parties without their agreement ([Kang and Kim 2009](#)). Thus, the focus is fully on the user's perception.) At the end of the section, we provide an overview of the risks that we discuss (see Table 1).

3.1. Emerging Risks

The implementation and use of smart technologies in homes gives rise to emerging risks ([Denning et al. 2013](#)). In the literature, these emerging risks are studied in particular from the viewpoints of information security and technology acceptance. In the former, cyber risks and their technological treatment are examined, whereas in the latter, the focus is on societal risks that affect users to varying degrees.

- *Privacy.* We find emerging cyber risks related to privacy and cyber security among the most relevant risks for SH ([Loi et al. 2017](#)). Privacy risks refer to the inappropriate handling of personal user data collected from SH ([Gerber et al. 2019](#)). As devices, like surveillance cameras or personal wearables, become part of the SH ecosystem, [Jacobsson et al. \(2016\)](#), among others, names privacy risks as the most undesirable consequence. [Sovacool and Furszyfer Del Rio \(2020\)](#), for example, attributes the

highest probability of occurrence to privacy risks, while [Park et al. \(2019\)](#) attribute the highest severity to it. In addition, [Tanczer et al. \(2018\)](#) sees the status of privacy as the most fundamental risk under the dynamics of SH. The authors further warn that privacy risks are most likely to be accepted on an individual level, thus creating long-term risks for society as a whole.

In research on the acceptance of SH technology and services, perceived privacy risks are extensively analyzed. Several studies state that privacy risks contribute the strongest to the users' overall risk perception ([Marikyan et al. 2019](#)). Interestingly, all studies agree that while privacy risks have a strong influence on risk perception, overall risk perception does not influence acceptance ([Kim et al. 2017](#); [Klobas et al. 2019](#); [Wang et al. 2020](#)). [Hubert et al. \(2019\)](#) shares the opinion but argue that perceived privacy risks remain significant in the context of adoption, as they have an indirect influence on other acceptance variables. Studies from [Alaiad and Zhou \(2017\)](#) and [Wilson et al. \(2017\)](#) also conclude that perceived privacy risks are not the most relevant factor for the overall risk perception. [Park et al. \(2018\)](#) categorizes the surveyed sample into three groups: low, moderate and high overall risk perceivers. For the low risk perceivers, privacy risks do not influence the overall risk perception, whereas for the modest and high risk perceivers, they have the largest influence. Lastly, the work of [Hong et al. \(2020\)](#) show no direct influence of perceived privacy risks, and thereby does not investigate the overall risk perception.

In our literature study, we found two unique approaches to perceived privacy risks. On the one hand, [Lee \(2020\)](#) analyzes how users perceive certain vulnerabilities. Vulnerabilities relating to user behavior are perceived as the most significant, technology vulnerabilities also result to be important, legal vulnerabilities are considered vaguely significant and provider vulnerabilities are not significant. On the other hand, [Gerber et al. \(2019\)](#) compares the significance of perceived privacy risk in the overall risk perception in SHs to the significance in social media and in smart health. Especially abstract risk scenarios, where consequences of privacy are rather vaguely defined without suggesting how users might be damaged (e.g., collection of usage patterns) are perceived the most likely, yet, in terms of severity, rated similarly significant throughout all domains.

Overall, we conclude that privacy risks are well-researched. Within the field of information security, experts' analyses of cyber risks consistently emphasize the importance of privacy risks. The literature points also to a large body of studies in the context of technology acceptance, although there is not yet conclusive agreement on the influence of privacy risks on acceptance.

- *Cyber security.* In contrast to the misuse of personal data associated with privacy risks, cyber security risks refer to vulnerabilities and threats in hardware, software, and data of SH devices and services ([Klobas et al. 2019](#)). Technical studies providing risk analysis in this context are numerous. Across all studies, statements can be assigned to one of the following three themes, namely asset, vulnerability, or threat. The interplay of these three aspects leads to the definition of a given cyber risk. For example, [Ali et al. \(2019\)](#) defines a cyber risk as the potential loss caused to the SH ecosystem by a threat exploiting certain vulnerabilities. Assets are typically defined at the beginning of the risk analysis, based on a given SH architecture ([Alexandrov et al. 2019](#); [Ali et al. 2019](#); [Jacobsson et al. 2016](#)). Such assets include sensors, gateways, servers, application programming interfaces, mobile devices, and the mobile device apps. Within these components of the SH architecture, certain categories, such as software, hardware, information, communication protocols, and human factors, are ubiquitous. Overall, the assets that are qualified as risky are mostly those that are used and whose properties are configured by the end user. Thus, cyber risks primarily arise from software and mobile devices and the related applications and services. Most reviewed studies proceed by identifying vulnerabilities of SHs based on the assets. In particular, the work by [Jacobsson et al. \(2016\)](#) is most comprehensive. In

their study, 4 of 32 vulnerabilities result in high risks, 19 are classified as medium risks, 9 are low risks. The most relevant vulnerabilities are poor password selection, sloppy end user, gullible users and software security in applications. They all belong to the asset categories of human factors and software. Various studies emphasize the importance of human factors (e.g., [Ali and Awad 2018](#); [Li et al. 2018](#); [Van Hoorde et al. 2018](#)) and stress the relevance of software vulnerabilities (e.g., [Ali et al. 2019](#)).

A threat can be defined as a potential action that results in a loss ([Ali et al. 2019](#)). New capabilities of smart homes enable new types of attacks while permitting traditional attacks with novel consequences ([Denning et al. 2013](#)). The literature emphasizes this trend and discusses threats in greater detail compared to assets or vulnerabilities. Most studies derive threats on the basis of previously identified vulnerabilities and the assets thereof. [Jacobsson et al. \(2016\)](#) identifies, in order of rank, circumvention of authentication mechanism, social engineering and unauthorized modification to a system as the top three threats to SHs. All are mainly caused by human-software combinations. The authors also note privacy and manipulation threats to hardware and communication protocols. [Van Hoorde et al. \(2018\)](#) emphasizes the fact that hardware-related manipulation should not be neglected, yet prioritize threats linked to privacy disclosure, inadequate access control and malware mitigation. Threats targeted toward smartphones, due to high risk exposure, are considered by [Brauchli and Li \(2015\)](#) the most relevant. Another prominent approach evaluates specific forms of attacks. Thereby, possible attacks from areas, such as information security, are summarized and then evaluated by assessing the vulnerabilities and assets (see [Blythe and Johnson 2019](#) for an overview). There is a consensus that attacks with denial of service and eavesdropping are main threats ([Ali et al. 2019](#); [Nurse et al. 2016](#)). Finally, some concepts take an in-depth look at the threats for a specific SH technology (e.g., RFID, Zigbee and Wi-Fi technologies in [Krishnan et al. 2017](#); Zigbee technology in [Wongvises et al. 2017](#)).

In risk analyses from technology acceptance research, the perceived importance of cyber security risks is minimal. [Park et al. \(2018\)](#) attributes minimal influence of cyber security to the overall risk perception, while [Wang et al. \(2020\)](#) attributes none at all. A possible reason for this could be the lack of understanding and the complexity of the topic, which prevents perception at all ([Mani and Chouk 2017](#)). Therefore, [Klobas et al. \(2019\)](#) analyzes cyber security risks separately from other risks.

We conclude that cyber security is a major research subject in information security risk analyses. Human factors and software components are presented as critical sources of risks. Comparing these results to the technology acceptance literature illustrates how risk assessment depends on the perspective. Users rate the significance of cyber security risks as less important than information security experts.

- *Performance.* The loss in performance of a SH product or service is linked to an emerging performance risk ([Hong et al. 2020](#)). Typically, performance risks stem from considerations about topics of broader technological interest and, thus, have almost general applicability to all technologies ([Sovacool and Furszyfer Del Rio 2020](#)). Risks, such as technical reliability, warranties, or obsolescence, should be noted here. In studies from acceptance research, perceived performance risks are largely considered irrelevant ([Hubert et al. 2019](#); [Wang et al. 2020](#)). Yet, the work of [Park et al. \(2018\)](#) highlights the perceived performance risks. They categorize the surveyed sample (1008 respondents) into three groups, depending on the resulting level of total risk perception. For the middle group, perceived performance risks resulted as the most significant. [Hong et al. \(2020\)](#) follows a similar approach, dividing the surveyed sample (553 respondents) into SH technology rejecters and postponers. For both, performance risk is perceived as relevant, even if only mediocre.
- *Dependence.* According to [Sovacool and Furszyfer Del Rio \(2020\)](#), there is a risk that SH technologies become a black box for average households, leading to isolation, vulnerability to fraud or lock-in effects. In the study by [Wilson et al. \(2017\)](#), other

aspects, like mental aspects of a resulting dependence, are identified (e.g., SH as non-essential luxuries or driver of laziness). In acceptance research, the increase in dependence is studied as the effect of SHs on users' control perception (Sovacool and Furszyfer Del Rio 2020). Initially, SHs were supposed to increase control. However, usage may also result in a loss of control (Wilson et al. 2017). Such risks potentially have negative effects on the users' peace of mind. Hong et al. (2020) considers that dependence risks become increasingly important and have, for example, stronger influence on the overall risk perception than performance risks.

- *Access to technology.* On a societal level, new risks related to the access to SH technology emerge. From a risk perspective, this is a distinct but cross-cutting risk. The exposure to today's pre-existing risks, such as water or fire, which we will address below, can largely be attributed to socio-economic factors (Banks and Bowman 2018). Today, it is still unclear whether SHs reinforces the significance of these factors or balance them out socially (Nilson and Bonander 2020).
- *Social isolation.* Marikyan et al. (2019) and Sovacool and Furszyfer Del Rio (2020) identify two types of social isolation. Besides the social divide in terms of technology access that may emerge, SH technology and services can lead to increasing technology-human interactions, and thereby displace human-human interactions. These considerations are closely related to human detachment concerns, which are a prominent topic in SH acceptance research. Users of SHs may feel disconnected from interpersonal contact and especially in SH studies with elderly users or with a clear health focus, such concerns are dominant (Alaiad and Zhou 2017).
- *Legal.* A study from the acceptance research area mentions that users perceive a certain risk associated with the lack of corporate accountability of SH vendors (Sovacool and Furszyfer Del Rio 2020). These considerations embody the user perspective and originate from unclear regulatory conditions or potentially limited longevity of vendors, as the latter are often start-ups.
- *Time.* Perceived time risk refers to the time wasted when using SH technologies (Wang et al. 2020). However, this risk has been found to be insignificant in other studies (Klobas et al. 2019; Wang et al. 2020).

3.2. Pre-Existing Risks

The literature suggests that SHs have an influence on pre-existing risks, such as fire, water, or burglary. As an example, Blythe and Johnson (2019) state the case where thousands of cameras were exploited by attackers in 2016 and emphasize that the potential for crime can take increases with the use of interconnected devices. Tanczer et al. (2018), studying risk patterns for IoT risk scenarios, rate the SH ecosystem as the most significant affected by this tendency. They conclude that crime exploits an increasing number of cyber-physical dependencies. Thus, it is likely that SHs may lead to an increase in illegal activities for economic, personal or political gain.

- *Theft.* Blythe and Johnson (2019) map specific attacks related to cyber security to pre-existing risks. On the one hand, they emphasize that exploiting insecure SH devices by eavesdropping offers criminals a wider variety of options to perform crimes, such as stalking or burglary. On the other hand, insurance experts (AXA 2019; Octotelematics 2019) see significant advantages of SH technologies concerning theft. They refer for example to a study of the Federal Bureau of Investigation (2016), where the probability of a burglary rose by 300% if no preventive measures were in place. Light and camera systems play a crucial role here. One may conclude that crime risk, mainly associated to burglary and theft, is changing, but a consensus is not yet found in the literature. In addition, studies on theft provide some initial indications of connections between SH risks.
- *Waste of resources.* SH is promoted as an important lever for new climate targets. Using the example of intelligent ventilation systems, Psomas et al. (2017) show how SHs can foster a more careful and targeted use of resources. However, other studies show how the increasing data consumption resulting from SH technologies greatly increases global

electricity usage (Vidal 2017) or even daily household labor (Strengers and Nicholls 2017) and, thus, reinforce unsustainable energy consumption (Tirado Herrero et al. 2018).

- Financial.* Unexpected additional expenses or loss of income are often the results of household damages (i.e., fire, water, burglary) (Tanczer et al. 2018). The SH context broadens the potential sources of financial consequences. According to a study by Hartford Steam Boiler (HSB) insurance company (Milewski 2017), 87% of the victims of cyber attacks in the U.S. suffered financial losses. Likewise, derived as a consequence of potentially increased dependence, there is a real risk that SH technologies leads to greater financial dependence (Sovacool and Furszyfer Del Rio 2020). Thus, emerging risks come with relevant new financial risks and many pre-existing risks ultimately have a financial impact on the household's individual.

In technology acceptance studies, perceived financial risks denote the possibility by which the product or service may not be worth its price (Hong et al. 2020). However, numerous studies find that the influence of perceived financial risks on overall risk perception is not significant (Alaiad and Zhou 2017; Hong et al. 2020; Kim et al. 2017; Sovacool and Furszyfer Del Rio 2020; Wang et al. 2020). The work of Park et al. (2018) is an exception as they point out that, in those that perceive financial risks as low, they have by far the greatest influence on the overall risk perception.
- Fire.* Average fire-related insurance claims are the most expensive losses for non-SH households (Insurance Information Institute 2020). Several studies point to SHs' potential in reducing the probability, as well as the severity of a fire incident (Feuerstein and Karmann 2017). Roost (Goldberg et al. 2019), an insurtech whose business model is built on the use of SH, reports a 15% reduction in claims frequency. BI Intelligence (Meola 2016) sees even greater potential in reducing the severity of the risk. Banks and Bowman (2018) confirm the potential mitigation of fire risk by SHs. Likewise, in comparison to commercial buildings, the potential of SH technologies for private households becomes especially obvious (Salhi et al. 2019). While the use of SH to prevent and treat fire risk is widely discussed, we found no indication of a change of the underlying risk.
- Water.* The risk of water damage is assessed in insurance practitioners' studies. Contrarywise to fire losses, the probability of water damage is high and the severity low (Insurance Information Institute 2020). ACE Group (2011) points out that 93% of all insurance costs from water damage could be prevented by SH technology. More recently, an empirical study from LexisNexis (Davis 2020b) confirm the finding by comparing households equipped with and without water sensors. One year after the installation of sensors, SHs saw a 96% decrease in paid water leakage claims and a 72% decrease in claims severity, while the control group recorded a 10% increase in frequency with unchanged severity levels. The risk of flooding has its own major field of research intensively discussing risk treatment measures. SH technology is listed by Azam et al. (2017) for reducing the severity of potential losses.
- Health.* Many SH use cases seek to promote health and well-being (Alam et al. 2012; Ehrenhard et al. 2014). In contradiction to these benefits, it is unclear whether new health risks arise from SH use (Sovacool and Furszyfer Del Rio 2020; Tanczer et al. 2018). The literature related to technology acceptance is scarce (Sovacool and Furszyfer Del Rio 2020). We only found Park et al. (2018) discussing the polarizing issue of electromagnetic radiation. For high risk perceivers, such radiation becomes overwhelmingly salient, while, for moderate and low risk perceivers, radiation leaves a low impact, respectively, negatively affecting the overall risk perception.
- Other property damage.* Finally, the reviewed literature mentions other pre-existing risks of non-SH households. The risks of property damage, excluding fire and water, that are discussed are for example wind and hail (Feuerstein and Karmann 2017). Early warning systems based on SH technology demonstrate their positive effect on pre-existing risks. In sum, while SH provides early warning or new risk treatment options, there is no indication of a change in the underlying risk.

In Table 1, we provide a summary of the risks identified in the literature. We also indicate the impact of SH on the risks (higher risk “H”, lower risk “L”, unclear effect “–”). Thereby, three risks result with SH as higher, eight as lower and for four the effect is unclear. Likewise, we indicate how strongly the various risks affect the acceptance of SH by lay users (high influence on acceptance “H”, low influence on acceptance “L”, unclear effect “–”). Five risks have a relevant influence on SH acceptance, five have no influence, and, in five others, the effect is unclear. More details on the identified risks are available in Table A3 in Appendix A.

Finally, there are interesting attempts to compare the risks of different use cases for a certain technology ecosystem to each other. König et al. (2017) discuss use case risks of ambient assisted living associated with inexperienced users and rank privacy the highest, followed by physical safety, social impact, and poorly secured devices. In contrast, for convenience use cases, i.e., disconnected from health considerations, physical safety is the most relevant, and privacy is ranked explicitly the lowest risk.

We observe that SH technology and related services change the risks landscape associated to a household. Especially, new risks related to technology usage emerge while treatment options for pre-existing risks improve. For the most part, extant research considers risks separately from each other. In particular, emerging cyber risks are well-researched in technical analyses. Further, results from the technology acceptance literature provide new perspectives and lead to the identification of additional risks. We also note that financial aspects are often overlooked. The security and comfort of SHs yields high maintenance and repair costs putting additional financial burden on the owners which may result in the risk of losing financial liquidity. In addition, although SH technology provides additional security, property damage from theft, fire, and water may incur higher costs for repair in SHs compared to other houses. Finally, a comparison of the results indicates that the assessment of risks differs by technical experts and users. Overall, we note that risks are not yet analyzed holistically nor evaluated with consistent metrics. A closer look at the methods and disciplines of risk research in the SH context in the next section confirms this shortcoming.

Table 1. Overview of the pre-existing and emerging risks identified in the review.

Risk	Description	Impact	Acceptance
<i>Emerging risks</i>			
Privacy	Inappropriate handling, disclosure, or use of data collected by SH system leading to interference to the right to keep personal matters private	H	H
Cyber security	Inadequate use of hardware or software by user, attacker or others, leading to damages, such as denial of service or mal-performance	H	L
Performance	Undesired performance variations resulting from usage of a young technology	–	H
Dependence	Degree of dependence that leads to undesired outcomes, such as loss of choice, lock-in, or anxiety	H	H
Access to technology	Disparities in access to technology due to, e.g., socio-economic factors, unwillingness to share data	–	L
Social isolation	Feeling of loneliness resulting from lacking technology access or increasing substitution of human-human interaction	L	H
Legal	Unclear regulatory conditions or supplier longevity leading to uncertainty regarding accountability	L	L

Table 1. Cont.

Risk	Description	Impact	Acceptance
Time	Disappointing benefits or opportunity costs in relation to time invested	L	L
<i>Pre-existing risks</i>			
Theft	Loss of physical or digital property and non-financial losses as a consequence of unauthorized access, use, and misappropriation	–	–
Waste of resources	Unnecessary or wrong use of money, substances, time, energy, or abilities resulting in waste of resources	L	–
Financial	Unexpected deterioration of the value of SH system or extra expenses or loss of income leading to financial loss	–	L
Fire	Bodily injury, death, property damages, and loss of income resulting from fire in and around the house	L	–
Water	Property damages resulting from water leakage in and around the house	L	–
Health	Impairments of physical and psychological health resulting from use of SH technology	L	H
Other property damage	Non-water or fire related property damage in and around the house	L	–

Note: “Impact” describes the influence of SH on a risk, where “H” stands for higher risk, “L” for lower risk, and “–” for an unclear effect. “Acceptance” describes the risks’ influence on the acceptance of SH, where “H” stands for high influence on acceptance, “L” for low influence on acceptance, and “–” for an unclear effect.

4. Risk Evaluation

The results on the risks identified in the previous section illustrate that they are researched from different areas. Accordingly, the choice of methods for their evaluation is broad. The most prominent field of study for risks in SHs is the information security discipline. Three main approaches can be found here: a risk-based, a security-based, and a privacy-based approach. The latter two typically emphasize a technological innovation for risk identification and mitigation (Ali and Awad 2018; Park et al. 2019; Schiefer 2015). Conversely, risk-based approaches attempt to address cyber risks comprehensively and focus on risk identification and assessment. Often used methods are, for example, information security risk analysis (Jacobsson et al. 2016), fuzzy set theory (Li et al. 2018), and fault tree analysis (Wongvises et al. 2017). All approaches share the common feature that they assess the risk based on a system’s ability to meet three basic goals of system security, namely confidentiality, integrity, and availability (Jacobsson et al. 2014). Cyber risks result from a combination of assets, vulnerabilities and threats and are assessed by means of the probability and severity of the risk. More sophisticated models have evolved from this basis. Jacobsson et al. (2016) use a matrix-like risk map dividing the analysis into architecture components and subcategories derived from information systems. Li et al. (2018) complement the analysis with concepts from grey system theory to cover the relationship between the probability, severity and detection of a system failure. All risk-based methods share a semi-qualitative character. They combine qualitative interview techniques with quantitative assessment methods and validation metrics to varying extents of sophistication. Jacobsson et al. (2016) summarize that mixed methods can accommodate the heterogeneous structure and complex relationships between connected devices and people.

Despite technological maturity, SH technology and service adoption and diffusion rates remain low (Marikyan et al. 2019). Hence, there is a relevant body of literature studying risks in SHs from the perspective of technology acceptance. Since these studies are user-oriented, they describe perceived risks by users as potential downsides to acceptance (Sovacool and Furszyfer Del Rio 2020). Perceived risks by lay users differ from the objective assessment of an expert. However, while perception is a key driver of risk behavior, it does not change the underlying risk. Various papers examine the influence of perceived risks on technology acceptance using structural equation models (Alaiad and Zhou 2017; Klobas et al. 2019; Wang et al. 2020). Thereby, the overall risk perception is considered to be composed by individual risks. Some models are derived from resistance theory (Hong et al. 2020; Lee 2020), while Park et al. (2018) exclusively focus on risk perception without considering the acceptance context. Finally, further studies (Gerber et al. 2019) build on the comparison of risks in SHs with those from other online services and draw conclusions on the relative users' perception of privacy and cyber security risks.

Other risk evaluation methods are based on the international standards for risk management (ISO, International Organization for Standardization 2018). Analyses building on this framework commonly follow its explicit generic approach. The advantage in that approach is that the standard is ubiquitously applicable to every kind of system, regardless of its type, perspective or size (ISO, International Organization for Standardization 2018). Thus, frameworks specifically adapted to SH also build on the three phases of risk identification, risk assessment, and risk treatment. When comparing the methodology to other approaches, we observe an emphasis on the risk identification. The advanced SH risk management framework from Nurse et al. (2016) divide the ISO 31000 standard into five phases, with risk identification making up three of the five phases. One of the most recent publications based on ISO 31000 combines elements from the above mentioned information security risk analysis and risk management (James 2019). In addition to probability and impact of a risk, they introduce an additional factor described as the attractiveness of the targeted system as a compromised system.

Similar to the ISO 31000 framework, several other industry standards are used for risk analysis in SHs. König et al. (2017) provides an overview of relevant industry standards for IoT systems. These approaches pursue risk, cyber-security, or privacy goals. The ISO 27000 standard summarizes best practices on information security, the ISA/IEC 62443 design cyber-security robustness and different publications under NIST SP800 give guidance on cyber vulnerabilities (NIST SP800-53), systems security engineering (800-160), or networks of things (NIST SP800-183). Several security-based or privacy-based frameworks (Nurse et al. 2016; Park et al. 2019; Varghese and Hayajneh 2018) of the information security discipline refer to these models indicating the incorporation its principles.

Finally, analyses from the insurance discipline also contribute to the methodological portfolio. Understanding and analyzing risks is a key pillar of the insurance business (Sheng et al. 2017). The focus today is on applying actuarial rate making to pre-existing household risks, such as fire, water, and theft. The shift to more sophisticated approaches to analyze behavior-related risks is gaining momentum (Banks and Bowman 2018). There is agreement on the importance of behavioral data for rate making of household risks. However, no specific methodologies for SHs can be found in the academic literature. For SHs, there are practitioners studies similar to the ones in the area of telematics that refer to models without going into greater depth (Matera and Salvador 2018). In addition, claims data analyses can be found that compare loss data from households with and without specific SH products (Davis 2020b).

In summary, the risk evaluation methods we found can be assigned to five areas: information security, acceptance, risk management frameworks, industry standards and insurance practice (see Table 2). For all but two studies (Li et al. 2018; Nurse et al. 2016), the reviewed works focus on applying risk analysis models to the field of SHs. The two exceptions are conceptual contributions that suggest changes to existing models or combine models to better address specific questions. All disciplines bring their own perspective and,

thus, come with certain advantages. As such, the focus on information security has led to various risk evaluation methodologies for cyber security and privacy. Yet, as with the risks themselves, there are still no attempts to evaluate risks on the basis of an integrated risk metric. Such an approach would allow to assess and prioritize risks in SHs relative to each other, to assess risk scenarios with interrelations among several risks, to quantify the impact of SH, or to evaluate investments into risk treatment options.

Table 2. Overview of the risk evaluation methods identified in the review.

Method	Description	References
<i>Information security</i>		
Information security risk analysis	Review of a system's risk exposure based on its ability to fulfill the three basic goals of system security, i.e., confidentiality, integrity, and availability	Alexandrov et al. (2019) ; Ali and Awad (2018) ; Ali et al. (2019) ; Bondarev and Prokhorov (2017) ; Jacobson et al. (2016) ; Tanczer et al. (2018)
Failure mode and effects analysis	Identification of potential failure modes (causes, effects, and areas) affecting a system's safety, reliability, and maintainability; integration of the fuzzy set theory to evaluate failure modes and of the grey relational theory to calculate the degree of relation among failure modes	Li et al. (2018)
Fault tree analysis	Boolean logic expressed as tree or diagram, where the top event is the failure of a system, and the other events are components' failures	Wongvises et al. (2017)
Factor analysis of information risk	Risk measurement based on likelihood and probability, consisting of loss event frequency and magnitude factors that represent threats and damage to assets	Park et al. (2019)
<i>Acceptance</i>		
Technology acceptance models	Structural equation models where predetermined hypotheses of the risks' influence on acceptance are assessed through, e.g., perceived risk or resistance theories	Hubert et al. (2019) ; Kim et al. (2017) ; Lee (2020) ; Park et al. (2018)
Scenario-based perception differences	Definition of different risk scenarios based on detail level of a resulting consequence (abstract vs. specific) or on the SH use case (health vs. comfort)	Gerber et al. (2019) ; Hong et al. (2020)
<i>Risk management</i>		
ISO 31000	International risk management standard aiming to develop a common understanding on risk management concepts	James (2019)
Individual enhancements	Frameworks based on ISO 31000 specifically adapted to SH settings	Nurse et al. (2016)
<i>Industry standards</i>		
ISO 27000	Best practice in information security management aiming to manage information risks by information security means	König et al. (2017)
NIST SP800	Frameworks developed to address the security and privacy needs, e.g., systems security engineering (NIST SP800-160) and networks of things (NIST SP800-183)	König et al. (2017)
ISA/IEC-62443	Design framework to improve cyber security robustness and resilience in industrial automation control systems	König et al. (2017)
<i>Insurance</i>		
Actuarial rate making	Determination of the price charged by insurance companies for pre-existing household risks	Matera and Salvador (2018) ; Sheng et al. (2017)
Claims data analysis	Comparison of insurance claims data from households with and without specific SH products, e.g., water leakage or fire sensors	Davis (2020b)

5. Risk Treatment

The reviewed literature also provides evidence on how to deal with the identified risks in SHs. This risk treatment is about the selection and implementation of suitable measures to address risks (ISO, [International Organization for Standardization 2018](#)). However, systematic studies are limited to the treatment of cyber risks and are technical. Thereby, we find recommendations that are addressed to SH technology and service providers and those directed to the users.

Among the former are the studies of [Klobas et al. \(2019\)](#) and [Sovacool and Furszyfer Del Rio \(2020\)](#). The focus therein is on initiatives that raise awareness, disseminate knowledge and empower users. The primary goal is to align the perceived level of risk to the objective level. In addition, it is important to consider the user interface of SH systems, devices and services and to enable users to simply participate in the protection of their systems. This is also the direction taken by [Jacobsson et al. \(2016\)](#), referring to the need for a model of security and privacy in the design phase of SHs. Accordingly, SH systems should be designed to provide users with methods to evaluate their own risk exposure, to provide them with security principles, and to point out privacy-sensitive information. The study is the only one that defines highly specific treatment measures for cyber risks aimed at the end-user. Based on the risks presented in Section 3, we draw on measures related to human factors and software as they represent a major source of cyber risks. The enforcement of password policies and verification tools represents an effective option for weak passwords, whereas policies and legal contracts are tools to address gullible end-users. Software-related vulnerabilities regarding the authentication mechanism can be mitigated through methods of public key infrastructure-based or multi-factor authentication and the continuous installation of updated software packages when available. However, keeping systems dynamic remains important. Even with security and privacy settings, users should configure their own settings instead of static patterns.

Our final corpus of academic research articles does not expand on treatments beyond cyber risks. However, practitioners' studies explore other risks. Thereby, SH is presented as an actual treatment option to address pre-existing risks in non-SH settings. The statement on SH by [Sevillano 2018](#) in the Swiss Re study is exemplary: for water, fire, and theft, the study predicts a 50% reduction of total insurance claims resulting from the use of connected devices (see Section 3).

Buying insurance is one option to mutualize risks (ISO, [International Organization for Standardization 2018](#)). We identify literature contributions that discuss new forms of insurance enabled by SHs. The assertion that the individualization of actuarial rate making creates opportunities with respect to insurance access is of particular interest for SH ([Banks and Bowman 2018](#)). Traditionally-rated high-risk households may be more attractive risks for insurance companies thanks to additional shared behavioral data stemming from SHs. The confirmation by practitioners' studies gives further weight to these considerations ([Feuerstein and Karmann 2017](#)). In addition, insurance is a technique to finance risks and serves for compensation of losses from specific risks. For example, emerging cyber security threats often result in a financial loss, and, where available, insurance can be an option that is rapidly implemented. Finally, insurers also act as experts and represent a source of knowledge for risk mitigation.

6. Conclusions

With the growing presence of technology and an increasing connectivity in many homes, SH technology and services pose substantial opportunities, but also introduce new risks and change the pre-existing landscape. The dynamics of SHs are fundamentally changing home life and, thus, the risks associated with it. Today, research on SH risks is primarily conducted in the disciplines of information security and technology acceptance. As such, in this literature review we present a comprehensive analysis of the extant research on the identification, evaluation and treatment of SH risks. Our results show that research continues to be technology-focused. With SH, a technology itself, this is obvious. From

a risk perspective, however, such a specific focus results in risks being overlooked and hence not being managed holistically. Looking into the findings of SH acceptance studies shows that lay users perceive certain risks differently than experts. Thus, interdisciplinary analysis of the qualified literature is important. Beyond the synopsis on emerging and pre-existing risks, we also summarize the learnings on risk evaluation and risk treatment methods. Thereby, our study contributes to aggregating the findings from research “silos” and provides a more comprehensive risk understanding. Overall, we identify various emerging risks, such as cyber security, privacy, and dependency risks, which households using SH are exposed to. Likewise, we identify existing risks, such as theft, fire, and water, which were already present in non-SH settings.

In complex systems, such as SHs, relationships and dependencies among risks emerge and are greatly relevant. Their occurrence depends on the usage context and the behavior of the user. At present, though, research ignores these relationships. Our review offers a starting point for future research in this field that should take both context and use of SHs into account, as well as distinguish different risk scenarios. In addition, findings from various methods should be aggregated. The current risk assessment research is undertaken with a narrow focus on selected risks, foremost isolated on cyber risks or relating to technology acceptance. Thus, the results form a relative prioritization of the risks under study and their drivers rather than a quantitative assessment of the probability and severity. In our review, we outline the influence that SH technology and services have on risks. However, a systematic assessment of all risks using the same metric is missing. This should also be considered in further research. After all, an assessment is a prerequisite, for SH providers and end-users, to make an informed choice of alternatives or on potential risk treatment measures. Finally, risk exposure considerably depends on the users’ behavior. However, risk behavior has yet to become a focal point for SH risk research. Therefore, future research should take behavioral components into account, not only concerning acceptance, but also with regard to SH usage.

The limitations of this review stem largely from the objective of the research. The intended identification of risks in SH led to a large number of papers that provide partial assessment of the risks identified. Our study takes these risks up where available but is not conclusive. The same applies when taking a risk management perspective. As a literature review, this paper does not ensure a comprehensive systematic identification of risks. Moreover, there are inherent limitations in academic studies on technologies due to the lower speed of research getting published. Our review presents a current picture of the state of research that needs to be updated vis-à-vis the fast-evolving technology concept of SH.

Author Contributions: Conceptualization, J.W. and A.Z.R.; methodology, R.I.; investigation, R.I.; formal analysis, R.I., J.W., and A.Z.R.; data curation, R.I.; writing—original draft preparation, R.I.; writing—review and editing, R.I., J.W., and A.Z.R.; supervision, J.W. and A.Z.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

The following tables provide additional information.

Table A1. Synopsis of academic research articles identified.

Reference	Region	Type	Method	Key Contents and Main Results	RI	RE	RT
Alaiad and Zhou (2017)	U.S.	A	Interviews ($N = 15$); survey ($N = 140$)	<ul style="list-style-type: none"> – Human detachment concerns as emerging risks for SH healthcare systems adoption – Other perceived features are privacy concerns, life-quality expectancy, and cost 	✓		
Alexandrov et al. (2019)	RU	A	Discussion (information security risk analysis)	<ul style="list-style-type: none"> – Different types of vulnerabilities lead to similar threats – Lack of backups and unprotected communication change integrity of information – Based on some protective measures identified, some risks are permissible 	✓	✓	
Ali and Awad (2018)	SE	A	Discussion (information security risk analysis)	<ul style="list-style-type: none"> – Human factors as largest risk source because of different know-how of SH users – Risks related to cyber or information assets score high, e.g., user credentials and mobile personal data user applications stemming from inadequate authentication 	✓	✓	✓
Ali et al. (2019)	SA	A	Discussion (systematic literature review)	<ul style="list-style-type: none"> – Risk defined as damage impacting system by a threat advanced from vulnerabilities – Various vulnerabilities identified and described, e.g., heterogeneous architecture – Various threats identified and described, e.g., DoS or eavesdropping 	✓	✓	
Azam et al. (2017)	KR	A	Case study (floods in Mushim stream region)	<ul style="list-style-type: none"> – Frequency and impact of natural disasters native to hydrological events increase – In South Korea, floods cause the greatest damage among all natural disasters – SH as a potential risk treatment option 	✓		
Balakrishnan et al. (2018)	MY	P	Discussion (systematic literature review)	<ul style="list-style-type: none"> – Some factors prevent mass commercialization of SH systems, e.g., interoperability, relevance of extracted data, security and privacy, cost, or societal changes – Expectations, user involvement, and capability of the systems act as constraints 	✓		
Blythe and Johnson (2019)	UK	A	Discussion (systematic literature review)	<ul style="list-style-type: none"> – At least half of all crime now committed online, IoT represents substantial part – Different IoT ecosystems suffer from this trend; home is heavily exposed to it – New types of crimes include burglary, stalking, sex crimes, and political subjugation 	✓		
Bondarev and Prokhorov (2017)	RU	P	Discussion (information security risk analysis)	<ul style="list-style-type: none"> – Filtering of outward parameters proposed to treat internal SH threats – Internal threats are threats to sensor, servers and other hardware components – Sensor failures categorized in equipment, software, network, or human factor 		✓	✓
Brauchli and Li (2015)	U.S.	P	Case study (SH digitalSTROM environment)	<ul style="list-style-type: none"> – Attack vectors can be grouped into vulnerability categories – Categories are server, communication bus, control-device, and third party services – Control-device refers to the greatest risk 	✓		
Bugeja et al. (2017)	SE	P	Discussion (information security risk analysis)	<ul style="list-style-type: none"> – Threat agents are nations, terrorists, organized crime, hacktivists, thieves, hackers – Threat motivations are curiosity, personal gain, terrorism, and national interests – Combination of intruders, motivations, and capabilities lead to a new threat model 	✓		

Table A1. Cont.

Reference	Region	Type	Method	Key Contents and Main Results	RI	RE	RT
Clark et al. (2015)	UK	A	Discussion (UK fire incidents statistics)	<ul style="list-style-type: none"> – Percentage of dwelling fires relatively to all fires tends to increase in the past decade – Fires are not equally distributed across socio-demographic or geographical domains – Social science should be included in fire risk analysis 	✓		✓
Dahmen et al. (2017)	U.S.	A	Case study (CASAS SH framework)	<ul style="list-style-type: none"> – Improving home security is a practical use case for SH – Monitoring activity-based anomalies supports detection and treatment of threats – Anomalies naturally exist; thus, not all represent security threats 	✓		
Gerber et al. (2019)	DE	A	Survey ($N = 942$, technology acceptance)	<ul style="list-style-type: none"> – Abstract risk scenarios are perceived as likely, but only moderately severe – Specific risk scenarios are perceived as moderately likely, but rather severe – Specific risk scenarios has great influence on users' risk perception 	✓		
Hong et al. (2017)	KR	P	Survey ($N = 533$, technology acceptance)	<ul style="list-style-type: none"> – Perceived risks divided into performance, financial, privacy, and psychological risk – Only minor differences when surveyed sample divided into postponers and rejecters – Exception forms perceived privacy risks and perceived financial risks 	✓		
Hong et al. (2020)	KR	A	Survey ($N = 533$, technology acceptance)	<ul style="list-style-type: none"> – Perceived risks divided into performance, financial, privacy, and psychological risk – Only minor differences when surveyed sample divided into postponers and rejecters – Exception from perceived privacy and financial risks 	✓		
Hubert et al. (2019)	DE	A	Survey ($N = 409$, technology acceptance)	<ul style="list-style-type: none"> – Overall risk perception (ORP) is a valid inhibitor of use intention and acceptance – Perceived usefulness predictors are more significant to acceptance than ORP – Perceived security risk contributes strongest to ORP, followed by performance risk 	✓		
Jacobsson et al. (2014)	SE	P	Interviews ($N = 9$)	<ul style="list-style-type: none"> – Most significant risks result from combination of software and human end-user – Security and privacy mechanisms to be included in design phase of SH – Enforcing privacy in IoT environments is main barrier to realize the vision SH 	✓	✓	
Jacobsson and Davidsson (2015)	SE	P	Interviews ($N = 9$)	<ul style="list-style-type: none"> – Most significant risks result from combination of software and human end-user – Security and privacy mechanisms to be included in design phase of SH – Enforcing privacy in IoT environments is main barrier to realize the vision SH 	✓	✓	
Jacobsson et al. (2016)	SE	A	Interviews ($N = 9$)	<ul style="list-style-type: none"> – Most significant risks result from combination of software and human end-user – Implementation of standard security features significantly reduces software risks – Human factors need careful consideration as they are inherently complex to handle 	✓	✓	✓
James (2019)	U.S.	P	Discussion (authors' expertise)	<ul style="list-style-type: none"> – Recently, there has been a great deal of SH device development – Risk model based on probability, impact, attractiveness as compromised platform – Human factors and security goals considered as main features to determine impact 	✓	✓	

Table A1. Cont.

Reference	Region	Type	Method	Key Contents and Main Results	RI	RE	RT
Kim et al. (2017)	KR	A	Survey ($N = 269$, value-based adoption model)	<ul style="list-style-type: none"> – Privacy risk and innovation resistance were found to limit perceived value – Yet, perceived benefits have a stronger influence on perceived value – SH acceptance affected more by positive factors than risks 	✓		
Kirkham et al. (2014)	UK	A	Case study (connected washing machine)	<ul style="list-style-type: none"> – Risk-based integrated management of devices improves utilization of home resources – Risk calculated as sum of legal risk, appliance failure risk, and resource security risk – Holistic view on risk includes trust, risk, eco-efficiency, cost, and their relationship 	✓	✓	
Klobas et al. (2019)	AU	A	Survey ($N = 415$, technology acceptance)	<ul style="list-style-type: none"> – Perceived security risks have a significant indirect effect on SH adoption decisions – Indirect influence is equally important for acceptance – Guiding users to develop knowledge and skills needed for secure use is key 	✓		
Krishnan et al. (2017)	IN	P	Scenario-based analysis (authors' expertise)	<ul style="list-style-type: none"> – RFID security threats are eavesdropping, physical attacks, DoS, and spoofing – For Zigbee, they are replay attack, eavesdropping, data manipulation – For WiFi, they are MITM attacks, eavesdropping, DoS, and packet re-routing 	✓		
Lee (2020)	KR	A	Survey ($N = 265$, resistance theory)	<ul style="list-style-type: none"> – Influence of users' privacy concerns on resistance statistically confirmed for SH – Privacy vulnerabilities are categorized into technology, law, provider, and user – User vulnerabilities have the strongest impact on SH users privacy concerns 	✓		
Li et al. (2018)	CN	A	Discussion (information security risk analysis)	<ul style="list-style-type: none"> – Effective risk management for smart cities combines different evaluation techniques – Threats in natural, contrived, and physical aspects are most relevant for cyber risks – Policy measures should educate, improve public safety, and provide guidance 			✓
Marikyan et al. (2019)	UK	A	Discussion (systematic literature review)	<ul style="list-style-type: none"> – SHs share three aspects: technology, services, and ability to satisfy users' needs – Perceived risks act as significant barriers to adoption – Technological barriers are the most important factors to be addressed 	✓		
Nawir et al. (2016)	MY	P	Discussion (authors' expertise)	<ul style="list-style-type: none"> – Clear outline of various attack types supports development of apt security measures – Resulting taxonomy divides attack types into device property, location, strategy, access level, protocol, information damage, host, and communication stack protocol 	✓		
Nilson and Bonander (2020)	SE	A	Survey ($N = 7507$, household panel)	<ul style="list-style-type: none"> – Large risk reductions in fire-related deaths observed in most high-income countries – Reductions are disproportionate for different socio-demographic groups – Household fires remain a considerable societal problem 	✓		
Nurse et al. (2016)	UK	P	Discussion (authors' expertise)	<ul style="list-style-type: none"> – Accessibility of security and risk management process promotes risk understanding – Risk frameworks include use case definition, assets & network analysis, threat & attack analysis, risk definition & prioritization, and control definition & alignment 		✓	✓

Table A1. Cont.

Reference	Region	Type	Method	Key Contents and Main Results	RI	RE	RT
Park et al. (2018)	KR	A	Survey ($N = 1008$, technology acceptance)	<ul style="list-style-type: none"> – Perceived risks include financial, performance, security, privacy, and health risk – Electromagnetic radiation (EMR) as one health risk with great influence on ORP – Experts emphasize cyber security risks, but users are more likely to perceive EMR 	✓		
Park et al. (2019)	KR	A	Scenario-based analysis (FAIR risk analysis)	<ul style="list-style-type: none"> – Risk = Threat \times Vulnerability \times Impact, where Threat \times Vulnerability = Likelihood – Existing qualitative risk assessments update on risk indicators once determined – Risk distribution can change with each scenario, country, and time 	✓	✓	
Pechon et al. (2021)	BE	A	Actuarial rate making (policies $N = 842, 896$)	<ul style="list-style-type: none"> – Dependence between home and motor insurance claims frequency – Multivariate credibility models allow to better identify the riskiest households 	✓		✓
Psomas et al. (2017)	DK	A	Case study (summer window ventilation)	<ul style="list-style-type: none"> – Trends towards nearly-zero energy houses increases overheating occurrences indoors – Use of automated roof window control system truly decreases overheating risk – Comes without any significant compromise of the indoor air quality 	✓		
Salhi et al. (2019)	JP	P	Case study (fire and gas leakage)	<ul style="list-style-type: none"> – Smoke and fire detection devices considered as first line of defense to leakage risk – Compared to industrial domains, detection systems in residential houses are basic – Detection systems work separately and are not embedded in home ecosystem 	✓		
Schiefer (2015)	DE	P	Discussion (authors' expertise)	<ul style="list-style-type: none"> – Higher market penetration makes SH devices more attractive for offenders – Raw sensors are limited on memory and computing power – Lower risk to be target of an attack 	✓		
Sovacool and Furszyfer Del Rio (2020)	UK	A	Interviews ($N = 31$); retail visits	<ul style="list-style-type: none"> – Privacy and security risks rank highest, health risk lowest – Several other technical issues are seen as barriers to adoption, e.g., reliability – Ability to better manage energy services is the most prominent benefit 	✓		
Tanczer et al. (2018)	UK	P	Interviews ($N = 19$, IoT experts)	<ul style="list-style-type: none"> – Four emerging risk patterns are extracted for all IoT risk scenarios (incl. home) – Physical safety, crime and exploitation, loss of control, and social norms and structures are named 	✓	✓	
Varghese and Hayajneh (2018)	U.S.	P	Case study ($N = 7$ popular SH devices)	<ul style="list-style-type: none"> – Frameworks for SH product purchase decision are available – Almost all products fail to effectively promote security awareness – Security awareness is particularly missed on product packaging or product website 	✓	✓	
Wang et al. (2020)	AU	A	Survey ($N = 351$, technology acceptance)	<ul style="list-style-type: none"> – Individuals ignore potential risks and focus on potential benefits from SH usage – Perceived privacy, performance, and time risk significantly influence ORP – Perceived security and financial risk have no influence on ORP 	✓		

Table A1. Cont.

Reference	Region	Type	Method	Key Contents and Main Results	RI	RE	RT
Wilson et al. (2017)	UK	A	Interviews ($N = 42$); survey ($N = 1025$)	<ul style="list-style-type: none"> – Ceding autonomy and independence are the main perceived risks – Policy-makers can play an important role in mitigating perceived risks – They support design and operating standards, guidelines on data privacy, and more 	✓		
Wongvises et al. (2017)	TH	P	Case study (Zigbee lighting system)	<ul style="list-style-type: none"> – In Fault Trees, top event is systems' failure and basic events components' failures – Events leading to failure are compromising sensors, vulnerable controlling device, infection attack, and DoS attack 	✓	✓	

Table A2. Synopsis of practitioners' studies identified.

Reference	Region	Type	Method	Key Contents and Main Results	RI	RE	RT
ACE Group (2011)	U.S.	R	Discussion (insurance claims, 2007–09)	<ul style="list-style-type: none"> – Water caused annually USD 9.1 billion property losses from 2007 to 2009 – Losses from water claims reflect 23% of all property losses – 93% could be minimized with automatic water leak detection and shut-off system 	✓		✓
Banks and Bowman (2018)	AU	R	Interviews ($N = 75$)	<ul style="list-style-type: none"> – Low-income households live in areas rated high risk with the highest premiums – Improvements in detecting or preventing risks have impact on risk assessment – With access to SH, low-income households may benefit particularly 	✓		✓
Davis (2020a)	U.S.	R	Survey ($N = 2500$, technology acceptance)	<ul style="list-style-type: none"> – SH devices meet needs, such as convenience, energy savings, or desire being modish – Adoption rates of specific devices indicate perception of certain needs – For example, 75% own a smoke detector, 2/3 a thermostat or security installation 	✓		
Davis (2020b)	U.S.	R	Experiment (water sensor claims)	<ul style="list-style-type: none"> – One year with sensor, SH homes saw a 96% decrease in paid water leak claims – Within the same period, control group's claims (without sensor) increased by 10% – Severity decreased by 72% after one year (remained stable in the control group) 	✓		✓
Donlon (2015)	U.S.	I	Case study (wine storage)	<ul style="list-style-type: none"> – Top five claims for wine received by AIG from 2004 to 2014 are water damage (26%), power outage (25%), theft (21%), natural catastrophe (18%), breakage (10%) – SH may reduce severity of loss, especially for power failure or temperature drops 	✓		✓
Fasano et al. (2017)	CH	R	Discussion (authors' expertise)	<ul style="list-style-type: none"> – Time is a key factor when dealing with domestic damages – Cost of damage increases at rate of USD 3000 per fire per minute of response time – Predictive modeling around behavior within the home will become a key domain 	✓		✓

Table A2. Cont.

Reference	Region	Type	Method	Key Contents and Main Results	RI	RE	RT
Feuerstein and Karmann (2017)	CH	R	Discussion (authors' expertise)	<ul style="list-style-type: none"> – At present, behavior is not taken into account beyond claims data – Studies suggest behavioral changes can significantly reduce risk exposure – Claims data for all insurance-related risks are assessed 	✓		✓
Fitzpatrick (2019)	U.S.	I	Discussion (author's expertise)	<ul style="list-style-type: none"> – Worthwhile SH devices have low acquisition cost compared to premium counterparts – Fire alarms have the most attractive ratio 	✓		
Insurance Information Institute (2020)	U.S.	R	Discussion (insurance claims, 2014–18)	<ul style="list-style-type: none"> – Homeowner losses are ranked by claims severity and frequency – Fire losses are highest in severity, and wind & hail are highest in probability 	✓		
König et al. (2017)	AT	R	Survey ($N = 109$, IoT experts)	<ul style="list-style-type: none"> – Main risk in healthcare settings is that devices are used by inexperienced people – Another risk is that devices may compromise privacy – Devices may also introduce safety hazards 	✓	✓	
Marsh Private Client Services (2020)	U.S.	R	Discussion (insurance claims, 2016)	<ul style="list-style-type: none"> – Cooking equipment is leading cause of home fires, igniting 46% of all home fires – In order of priority, candles, electrical causes, heating, and smoking follow 	✓		
Matera and Salvador (2018)	IT	R	Discussion (authors' expertise)	<ul style="list-style-type: none"> – Proposed risk evaluation method builds on objective and quantitative analyses – Measures include maximum possible loss and normal loss expectancy – Novel approaches emphasize importance of risk prevention 		✓	✓
Milewski (2017)	U.S.	R	Survey	<ul style="list-style-type: none"> – 87% of cyber attack victims suffer from financial losses by paying money to attacker – Problem will likely worsen as the number of connected home devices increases – New cyber insurance coverage is one alternative of risk treatment 	✓		✓
Octotelematics (2019)	IT	R	Discussion (authors' expertise)	<ul style="list-style-type: none"> – Traditionally, insurers use proxy data to identify the risk of loss for an asset – IoT gives access to real-time, individual, and observable data on risks – Data is directly actionable for risk pricing and treatment 	✓	✓	✓
Sevillano (2018)	CH	R	Survey	<ul style="list-style-type: none"> – Water, theft, and fire are source of around 50% of insurance claims (2013) – Technology will play a vital role in reducing these risks 	✓		✓
Sheng et al. (2017)	CN	R	Discussion (authors' expertise)	<ul style="list-style-type: none"> – Individual coverage concepts are complex and time consuming – Technology makes these concepts possible within retail and commercial space – Coverage to adapt automatically and real-time to changing life and risk situations 			✓

Table A2. Cont.

Reference	Region	Type	Method	Key Contents and Main Results	RI	RE	RT
Van Hoorde et al. (2018)	BE	B	Discussion (authors' expertise)	<ul style="list-style-type: none"> – Threats mainly relate to privacy, inadequate access control and malware mitigation – Additional risks to hardware are theft, manipulation and sabotage – Overall, the end-user still represents one of the weakest links 	✓		

Note: The types of references are coded as follows. "A" = article, "B" = book, "I" = insurance magazine, "P" = proceeding paper, "R" = report. The columns "RI", "RE", and "RT" stand for = risk identification, risk evaluation, and risk treatment and insurance, respectively.

Table A3. Pre-existing and emerging risks identified in the review.

Risk	Source	Events	Consequences	Likelihood	References
<i>Emerging risks</i> Privacy	Bundle of highly sensitive information resulting from SH behavior (e.g., unaware usage or threats linked to privacy disclosure)	Specific cyber attacks directed towards data leakage or unauthorized retention of personal data	Inappropriate handling of personal user data collected from SH	High probability, as privacy experiences fundamental change within SH settings and risk often accepted by users	Gerber et al. (2019) ; Jacobsson et al. (2016) ; Klobas et al. (2019) ; Loi et al. (2017) ; Park et al. (2019) ; Sovacool and Furszyfer Del Rio (2020) ; Tanczer et al. (2018)
Cyber security	Inadequate access control and malware mitigation directed to SHs' user behavior or software (e.g., poor user credentials, identity credential theft, unauthorized modification to systems)	Specific attacks directed at the software-human interface (e.g., eavesdropping, DoS, DDoS)	Damage experienced personally as a user or societal damage building on hijacked personal SH system	High probability, as household-related crime shifts increasingly into the cyber space	Alexandrov et al. (2019) ; Ali and Awad (2018) ; Ali et al. (2019) ; Blythe and Johnson (2019) ; Brauchli and Li (2015) ; Denning et al. (2013) ; Jacobsson et al. (2016) ; Krishnan et al. (2017) ; Li et al. (2018) ; Nurse et al. (2016) ; Van Hoorde et al. (2018) ; Wongvises et al. (2017)
Performance	Loss in performance of a SH product or service derived from topics of broader technological interest (e.g., reliability, obsolescence)	n.a.	Uncertainty or experienced loss in performance	n.a.	Hong et al. (2020) ; Hubert et al. (2019) ; Park et al. (2018) ; Wang et al. (2020)

Table A3. *Cont.*

Risk	Source	Events	Consequences	Likelihood	References
Dependence	Lack of technical understanding, users' laziness or lack of alternatives to SH	n.a.	Technology dependency or greater laziness with greater levels of usage	n.a.	Alaiad and Zhou (2017) ; Hong et al. (2020) ; Sovacool and Furszyfer Del Rio (2020) ; Wilson et al. (2017)
Access to technology	Technology access disparities related to socio-economic factors or willful non-access	n.a.	Individual isolation from certain SH benefits	n.a.	Nilson and Bonander (2020) ; Park et al. (2019) ; Sovacool and Furszyfer Del Rio (2020)
Social isolation	High levels of dependency or non-access to technology	n.a.	Non-access to SH, technology-human interactions displacing human-human interaction or human detachment	n.a.	Alaiad and Zhou (2017) ; Hong et al. (2020) ; Park et al. (2019) ; Sovacool and Furszyfer Del Rio (2020) ; Wilson et al. (2017)
Legal	Limited longevity of supplier (start-ups) or unclear regulatory conditions	n.a.	Lack of corporate accountability or legal clarity on safeguards in the event of a dispute	n.a.	Sovacool and Furszyfer Del Rio (2020)
Time	n.a.	n.a.	Time wasted when using SH technologies	n.a.	Klobas et al. (2019) ; Wang et al. (2020)
<i>Pre-existing risks</i>					
Theft	Regional aspects, period, infrastructure, behavior or insecure SH systems	Break-in	Physical or psychological consequences	Low probability, compared to other pre-existing risks, such as water	AXA (2019) ; Blythe and Johnson (2019) ; Nurse et al. (2016) ; Octotelematics (2019) ; Tanczer et al. (2018) ; Van Hoorde et al. (2018)
Waste of resources	Unenlightened use of technology and additional devices that are powered and connected to the internet	n.a.	Increase in global electricity usage or increase in daily household labor	n.a.	Hong et al. (2020) ; Jacobsson et al. (2016) ; Psomas et al. (2017) ; Strengers and Nicholls (2017) ; Tirado Herrero et al. (2018) ; Vidal (2017)

Table A3. Cont.

Risk	Source	Events	Consequences	Likelihood	References
Financial	Insecure SH systems or extend by which SHs may not be worth the financial price	n.a.	Financial losses (aggregated from all risks)	High probability, as emerging cyber risks entail new financial consequences and also pre-existing risks often result in financial loss	Alaiad and Zhou (2017) ; Hong et al. (2020) ; Kim et al. (2017) ; Milewski (2017) ; Park et al. (2019) ; Sovacool and Furszyfer Del Rio (2020) ; Wang et al. (2020)
Fire	n.a.	n.a.	Health and financial consequences	Low probability, compared to other pre-existing risks, such as water or theft	Feuerstein and Karmann (2017) ; Goldberg et al. (2019) ; Meola (2016) ; Octotelematics (2019) ; Salhi et al. (2019)
Water	n.a.	Pipes bursting, water overflow, roof leakage, or frost damage	Water waster (leaks waste more than one trillion gallons of water annually in the U.S.)	High probability, compared to other pre-existing risks, such as fire or theft	ACE Group (2011) ; Azam et al. (2017) ; Davis (2020b)
Health	Health-related hazards arising from incorrect use of SH or potentially unknown effects of electromagnetic radiation	n.a.	n.a.	n.a.	Park et al. (2018) ; Sovacool and Furszyfer Del Rio (2020) ; Tanczer et al. (2018)
Other property damage	Non-awareness of fragility at certain state	Power outages or long periods of inactivity	Breakage of the item	n.a.	Feuerstein and Karmann (2017)

Note: The dimensions in this table stem from the ISO 31000 standard on risk management (ISO, [International Organization for Standardization 2018](#)). “Source” refers to the element which alone or in combination has the potential to give rise to the risk. “Events” denotes the occurrence or change of a particular set of circumstances. “Consequences” are outcomes of an event affecting the objectives. “Likelihood” is the chance of something happening. “n.a.” stands for not available and refers to the fact that no information relating to the dimension can be found in the body of literature.

References

- ACE Group. 2011. *Device Could Reduce 93 Percent of Homeowner Water Damage Claims*. San Diego: Wells Media Group.
- Alaiad, Ahmad, and Lina Zhou. 2017. Patients' Adoption of WSN-Based Smart Home Healthcare Systems: An Integrated Model of Facilitators and Barriers. *IEEE Transactions on Professional Communication* 60: 4–23. [\[CrossRef\]](#)
- Alam, Muhammad Raisul, Mamun Bin Ibne Reaz, and Mohd Alauddin Mohd Ali. 2012. A Review of Smart Homes—Past, Present, and Future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 42: 1190–203. [\[CrossRef\]](#)
- Aldrich, Frances K. 2006. Smart Homes: Past, Present and Future. In *Inside the Smart Home*. London: Springer, Chp. 2, pp. 17–39. [\[CrossRef\]](#)
- Alexandrov, Vladislav Andreevich, Vasily A. Desnitsky, and Dmitrii Yur'evich Chaly. 2019. Design and Security Analysis of a Fragment of Internet of Things Telecommunication System. *Automatic Control and Computer Sciences* 53: 851–56. [\[CrossRef\]](#)
- Ali, Bako, and Ali Awad. 2018. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* 18: 817. [\[CrossRef\]](#) [\[PubMed\]](#)
- Ali, Waleed, Sharaf Malebary, Adel A. Ahmed Abdullah, Talal A. A. Abdullah, and Adel Ali Ahmed. 2019. A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home. *International Journal of Computer Science and Network Security* 2019: 139–146. Seoul: IJCSNS.
- Amiribesheli, Mohsen, Asma Benmansour, and Abdelhamid Bouchachia. 2015. A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing* 6: 495–517. [\[CrossRef\]](#)
- AXA. 2019. *Burglary: In Which Canton the Danger is Particularly High*. Winterthur: AXA Insurance.
- Azam, Muhammad, Hyung San Kim, and Seung Jin Maeng. 2017. Development of flood alert application in Mushim stream watershed Korea. *International Journal of Disaster Risk Reduction* 21: 11–26. [\[CrossRef\]](#)
- Balakrishnan, Sumathi, Hemalata Vasudavan, and Raja Kumar Murugesan. 2018. Smart Home Technologies. Paper presented at 6th International Conference on Information Technology: IoT and Smart City—ICIT 2018, Hong Kong, China, December 29–31; pp. 120–27. [\[CrossRef\]](#)
- Banks, Marcus, and Dina Bowman. 2018. *Juggling Risks Insurance in Households Struggling with Financial Insecurity*. Technical Report. Fitzroy: The Brotherhood of St Laurence. [\[CrossRef\]](#)
- Blythe, John M., and Shane D. Johnson. 2019. A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal* 2019: 1–29. [\[CrossRef\]](#)
- Bondarev, Sergey E., and Andrey S. Prokhorov. 2017. Analysis of internal threats of the system “smart home” and assessment of ways to prevent them. Paper presented at 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, February 1–3; pp. 788–90. [\[CrossRef\]](#)
- Brauchli, Andreas, and Depeng Li. 2015. A solution based analysis of attack vectors on smart home systems. Paper presented at 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, August 5–7; pp. 1–6. [\[CrossRef\]](#)
- Braun, Virginia, and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3: 77–101. [\[CrossRef\]](#)
- Bugeja, Joseph, Andreas Jacobsson, and Paul Davidsson. 2017. An analysis of malicious threat agents for the smart connected home. Paper presented at 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, March 13–17; pp. 557–62. [\[CrossRef\]](#)
- Chan, Marie, Daniel Estève, Jean-Yves Fourniols, Christophe Escriba, and Eric Campo. 2012. Smart wearable systems: Current status and future challenges. *Artificial Intelligence in Medicine* 56: 137–56. [\[CrossRef\]](#)
- Clark, Andrew, Jessica Smith, and Carole Conroy. 2015. Domestic fire risk: A narrative review of social science literature and implications for further research. *Journal of Risk Research* 18: 1113–29. [\[CrossRef\]](#)
- Dahmen, Jessamyn, Brian Thomas, Diane Cook, and Xiaobo Wang. 2017. Activity Learning as a Foundation for Security Monitoring in Smart Homes. *Sensors* 17: 737. [\[CrossRef\]](#) [\[PubMed\]](#)
- Davis, Dan. 2020a. *Insights and Strategies for Smart Home Insurance Programs*. Technical Report. Alpharetta: LexisNexis Risk Solutions.
- Davis, Dan. 2020b. *Preventing Water Claims: Understanding the Value of Smart Home Technology*. Technical Report. Alpharetta: LexisNexis Risk Solutions.
- Denning, Tamara, Tadayoshi Kohno, and Henry M. Levy. 2013. Computer security and the modern home. *Communications of the ACM* 56: 94–103. [\[CrossRef\]](#)
- Donlon, Rosalie. 2015. *Do You Collect Wine? Here Are Some Tips for Keeping Your Bottles Safe*. New York: ALM Media.
- Ehrenhard, Michel, Bjorn Kijl, and Lambert Nieuwenhuis. 2014. Market adoption barriers of multi-stakeholder technology: Smart homes for the aging population. *Technological Forecasting and Social Change* 89: 306–15. [\[CrossRef\]](#)
- Fasano, Pierluigi, Cecilia Sevillano, James Stansberry, Leigh Carlton, Arthur Houannic, and Domenico Saravese. 2017. *Risk Talk on Smart Homes*. Technical Report. Ruschlikon: Swiss Re Centre for Global Dialogue.
- Federal Bureau of Investigation. 2016. *Uniform Crime Report Crime in the Property Crime*. Technical Report. Washington, DC: Federal Bureau of Investigation.

- Feuerstein, Daniel, and Maximilian Karmann. 2017. *The Insurer's Playbook on Smart Home Point of View*. Technical Report. Zurich: Deloitte.
- Fitzpatrick, Marc. 2019. *Are Smart Device Home Insurance Discounts Worth It?* Charlotte: ValuePenguin.
- Gerber, Nina, Benjamin Reinheimer, and Melanie Volkamer. 2019. Investigating People's Privacy Risk Perception. *Proceedings on Privacy Enhancing Technologies* 2019: 267–88. [\[CrossRef\]](#)
- Goldberg, Jeff, Roel Peeters, and Assaf Wand. 2019. *The Present And Future Of Home Telematics*. New York: SourceMedia.
- Hong, Areum, Changi Nam, and Seongcheol Kim. 2017. Analysis of the barriers that consumers encounter when smart home service is introduced in South Korea. In *Mapping ICT into Transformation for the Next Information Society*. Kyoto and Calgary: International Telecommunications Society (ITS).
- Hong, Areum, Changi Nam, and Seongcheol Kim. 2020. What will be the possible barriers to consumers' adoption of smart home services? *Telecommunications Policy* 44: 101867. [\[CrossRef\]](#)
- Hosseini, Sayed Saeed, Kodjo Agbossou, Souso Kelouwani, and Alben Cardenas. 2017. Non-intrusive load monitoring through home energy management systems: A comprehensive review. *Renewable and Sustainable Energy Reviews* 79: 1266–74. [\[CrossRef\]](#)
- Hubert, Marco, Markus Blut, Christian Brock, Ruby Wenjiao Zhang, Vincent Koch, and René Riedl. 2019. The influence of acceptance and adoption drivers on smart home usage. *European Journal of Marketing* 53: 1073–98. [\[CrossRef\]](#)
- Insurance Information Institute. 2020. *Facts + Statistics: Homeowners and Renters Insurance*. New York: Insurance Information Institute.
- International Organization for Standardization. 2018. *Risk Management: ISO 31000*. Geneva: International Organization for Standardization
- Jacobsson, Andreas, Martin Boldt, and Bengt Carlsson. 2014. On the Risk Exposure of Smart Home Automation Systems. Paper presented at 2014 International Conference on Future Internet of Things and Cloud, Barcelona, Spain, August 27–29; pp. 183–90. [\[CrossRef\]](#)
- Jacobsson, Andreas, Martin Boldt, and Bengt Carlsson. 2016. A risk analysis of a smart home automation system. *Future Generation Computer Systems* 56: 719–33. [\[CrossRef\]](#)
- Jacobsson, Andreas, and Paul Davidsson. 2015. Towards a model of privacy and security for smart homes. Paper presented at 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, December 14–16. pp. 727–32. [\[CrossRef\]](#)
- James, Fathima. 2019. A Risk Management Framework and A Generalized Attack Automata for IoT based Smart Home Environment. Paper presented at 2019 3rd Cyber Security in Networking Conference (CSNet), Quito, Ecuador, October 23–25; pp. 86–90. [\[CrossRef\]](#)
- Kang, Yoolee, and Seongcheol Kim. 2009. Understanding User Resistance to Participation in Multihop Communications. *Journal of Computer-Mediated Communication* 14: 328–51. [\[CrossRef\]](#)
- Keller, Benno, Martin Eling, Hato Schmeiser, Markus Christen, and Michele Loi. 2018. *Big Data and Insurance: Implications for Innovation, Competition and Privacy*. Zurich: The Geneva Association.
- Kim, Yonghee, Youngju Park, and Jeongil Choi. 2017. A study on the adoption of IoT smart home service: Using Value-based Adoption Model. *Total Quality Management & Business Excellence* 28: 1149–65. [\[CrossRef\]](#)
- Kirkham, Tom, Django Armstrong, Karim Djemame, and Ming Jiang. 2014. Risk driven Smart Home resource management using cloud services. *Future Generation Computer Systems* 38: 13–22. [\[CrossRef\]](#)
- Klobas, Jane E., Tanya McGill, and Xuequn Wang. 2019. How perceived security risk affects intention to use smart home devices: A reasoned action explanation. *Computers & Security* 87: 101571. [\[CrossRef\]](#)
- König, Sandra, Stefan Schiebeck, Stefan Schauer, Martin Latzenhofer, Peter Mayer, Geraldine Fitzpatrick, and Iot Risks. 2017. *Deliverable 3: Internet of Things Risk Analysis and Assessment*. Technical Report. Vienna: The Austrian Research Promotion Agency.
- Krishnan, Silpa, MS Anjana, and Sethuraman N. Rao. 2017. Security Considerations for IoT in Smart Buildings. Paper presented at 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICIC), Tamil Nadu, India, December 14–16. pp. 1–4. [\[CrossRef\]](#)
- Lee, Hwansoo. 2020. Home IoT resistance: Extended privacy and vulnerability perspective. *Telematics and Informatics* 49: 101377. [\[CrossRef\]](#)
- Li, Xiaotong, Hua Li, Bingzhen Sun, and Fang Wang. 2018. Assessing information security risk for an evolving smart city based on fuzzy and grey FMEA. *Journal of Intelligent & Fuzzy Systems* 34: 2491–501. [\[CrossRef\]](#)
- Loi, Franco, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford, and Vijay Sivaraman. 2017. Systematically Evaluating Security and Privacy for Consumer IoT Devices. Paper presented at 2017 Workshop on Internet of Things Security and Privacy, Dallas, TX, USA, November 3; pp. 1–6. [\[CrossRef\]](#)
- Lutolf, Remo. 1992. Smart Home concept and the integration of energy meters into a home based system. Paper presented at Seventh International Conference on Metering Apparatus and Tariffs for Electricity Supply 1992, Glasgow, UK, November 17–19; pp. 77–78.
- Mani, Zied, and Inès Chouk. 2017. Drivers of consumers' resistance to smart products. *Journal of Marketing Management* 33: 76–97. [\[CrossRef\]](#)
- Marikyan, Davit, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change* 138: 139–54. [\[CrossRef\]](#)
- Marsh Private Client Services. 2020. *Fire Safety at Home: Prevention and Precautions*. Edmonton: Marsh Private Client Services.

- Matera, Fabio, and Emanuele Salvador. 2018. *An Innovative Approach to Measuring and Controlling Risk*. Technical Report. Boston: Arthur D. Little.
- Mazri, Chabane. 2017. (Re) Defining Emerging Risks. *Risk Analysis* 37: 2053–65. [\[CrossRef\]](#)
- Meola, Andrew. 2016. *IoT Insurance: Trends in Home, Life & Auto Insurance Industries*. New York: Insider Inc.
- Mikkonen, Kristina, and Maria Kääriäinen. 2020. Content Analysis in Systematic Reviews. In *The Application of Content Analysis in Nursing Science Research*. Cham: Springer International Publishing, pp. 105–15. [\[CrossRef\]](#)
- Milewski, Dennis. 2017. *HSB Cyber Survey Shows Increase in Smart Home Devices Adds New Hacking Risks*. Hartford: The Hartford Steam Boiler Inspection and Insurance Company.
- Nawir, Mukrimah, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. Paper presented at 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, August 11–12; pp. 321–26. [\[CrossRef\]](#)
- Nilson, Finn, and Carl Bonander. 2020. Household Fire Protection Practices in Relation to Socio-demographic Characteristics: Evidence from a Swedish National Survey. *Fire Technology* 56: 1077–98. [\[CrossRef\]](#)
- Nurse, Jason R. C., Ahmad Atamli, and Andrew Martin. 2016. Towards a Usable Framework for Modelling Security and Privacy Risks in the Smart Home. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Berlin: Springer, vol. 9750, pp. 255–67. [\[CrossRef\]](#)
- Octotelematics. 2019. *The Power of Insurance IoT for Risk Management*. Rome: Octotelematics.
- Page, Matthew James, David Moher, Patrick Bossuyt, Isabelle Boutron, Tammy Hoffmann, Cynthia Mulrow, Larissa Shamseer, Jennifer Tetzlaff, Elie Akl, Sue E. Brennan, and et al. 2020. *PRISMA 2020 Explanation and Elaboration: Updated Guidance and Exemplars for Reporting Systematic Reviews*. MetaArXiv Preprint. Charlottesville: Center for Open Science. [\[CrossRef\]](#)
- Park, Chankook, Yangsoo Kim, and Min Jeong. 2018. Influencing factors on risk perception of IoT-based home energy management services. *Telematics and Informatics* 35: 2355–65. [\[CrossRef\]](#)
- Park, Mookyu, Haengrok Oh, and Kyungho Lee. 2019. Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. *Sensors* 19: 2148. [\[CrossRef\]](#) [\[PubMed\]](#)
- Pechon, Florian, Michel Denuit, and Julien Trufin. 2021. Home and Motor insurance joined at a household level using multivariate credibility. *Annals of Actuarial Science* 15: 82–114. [\[CrossRef\]](#)
- Psomas, Theofanis, Per Heiselberg, Thøger Lyme, and Karsten Duer. 2017. Automated roof window control system to address overheating on renovated houses: Summertime assessment and intercomparison. *Energy and Buildings* 138: 35–46. [\[CrossRef\]](#)
- Radomirovic, Saša. 2010. Towards a Model for Security and Privacy in the Internet of Things. In *Proceedings of the First International Conference on Security of Internet of Things*. New York: Association for Computing Machinery.
- Reinisch, Christian, Mario J. Kofler, Félix Iglesias, and Wolfgang Kastner. 2011. ThinkHome Energy Efficiency in Future Smart Homes. *EURASIP Journal on Embedded Systems* 2011: 1–18. [\[CrossRef\]](#)
- Salhi, Lamine, Thomas Silverston, Taku Yamazaki, and Takumi Miyoshi. 2019. Early Detection System for Gas Leakage and Fire in Smart Home Using Machine Learning. Paper presented at 2019 IEEE International Conference on Consumer Electronics (ICCE), Berlin, Germany, September 8–11; pp. 1–6. [\[CrossRef\]](#)
- Schiefer, Michael. 2015. Smart Home Definition and Security Threats. Paper presented at 2015 Ninth International Conference on IT Security Incident Management & IT Forensics, Magdeburg, Germany, May 18–20; pp. 114–118. [\[CrossRef\]](#)
- Scott, Faye. 2007. *Teaching Homes to be Green: Smart Homes and the Environment*. London: Green Alliance.
- Sevillano, Cecilia. 2018. Smart Homes. Paper presented at EMEA Claims Conference, Rüşchlikon, Switzerland, March 6–7.
- Sheng, Cliff, Dietmar Kottmann, Kang Liu, Kai Prestinari, Xing Jiang, Wei Chen, and Xuefeng Li. 2017. *Technology-Driven Value Generation in Insurance*. Technical Report. Hong Kong, China: Oliver Wyman.
- Sovacool, Benjamin K., and Dylan D. Furszyfer Del Rio. 2020. Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and Sustainable Energy Reviews* 120: 109663. [\[CrossRef\]](#)
- Strengers, Yolande, and Larissa Nicholls. 2017. Convenience and energy consumption in the smart home of the future: Industry visions from Australia and beyond. *Energy Research & Social Science* 32: 86–93. [\[CrossRef\]](#)
- Tanczer, Leonie Maria, Ine Steenmans, Miles Elsdon, Jason Blackstock, and Madeline Carr. 2018. Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? Paper presented at Living in the Internet of Things: Cybersecurity of the IoT— 2018, London, UK, March 28–29. vol. 2018 doi:10.1049/cp.2018.0033.
- Thomé, Antônio Márcio Tavares, Luiz Felipe Scavarda, and Annibal José Scavarda. 2016. Conducting systematic literature review in operations management. *Production Planning & Control* 27: 408–20. [\[CrossRef\]](#)
- Tirado Herrero, Sergio, Larissa Nicholls, and Yolande Strengers. 2018. Smart home technologies in everyday life: Do they address key energy challenges in households? *Current Opinion in Environmental Sustainability* 31: 65–70. [\[CrossRef\]](#)
- Tranfield, David, David Denyer, and Palminder Smart. 2003. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management* 14: 207–22. [\[CrossRef\]](#)
- Van Hoorde, Kim, Evelien De Pauw, Hans Vermeersch, and Wim Hardyns. 2018. The influence of technological innovations on theft prevention. In *Socially Responsible Innovation in Security: Critical Reflections*. Edited by J. Peter Burgess, Genserik Reniers, Koen Ponnet, Wim Hardyns and Wim Smit. London: Routledge, Chp. 3.

- Varghese, Joel, and Thayer Hayajneh. 2018. A Framework to Identify Security and Privacy Issues of Smart Home Devices. Paper presented at 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, November 8–10; pp. 135–43. [[CrossRef](#)]
- Vidal, John. 2017. 'Tsunami of data' could consume one fifth of global electricity by 2025. Broadstairs: Climate Home News.
- Von Gaudecker, Hans-Martin, Radost Holler, Lena Janys, Bettina Siflinger, and Christian Zimpelmann. 2020. *Labour Supply in the Early Stages of the COVID-19 Pandemic: Empirical Evidence on Hours, Home Office, and Expectations*. Technical Report. Bonn: Institute of Labor Economics (IZA)
- Wang, Xuequn, Tanya Jane McGill, and Jane E. Klobas. 2020. I Want It Anyway: Consumer Perceptions of Smart Home Devices. *Journal of Computer Information Systems* 60: 437–47. [[CrossRef](#)]
- Wilson, Charlie, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2017. Benefits and risks of smart home technologies. *Energy Policy* 103: 72–83. [[CrossRef](#)]
- Wongvises, Chanoksuda, Assadarat Khurat, Doudou Fall, and Shigeru Kashihara. 2017. Fault tree analysis-based risk quantification of smart homes. Paper presented at 2017 2nd International Conference on Information Technology (INCIT), Salaya, Thailand, November 2–3; pp. 1–6. [[CrossRef](#)]