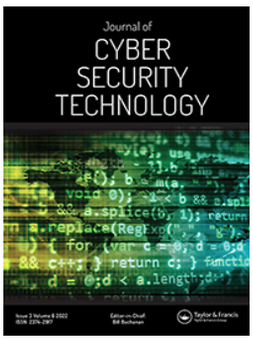

Journal of Cyber Security Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tsec20

The baseline of global consumer cyber security standards for IoT: quality evaluation

Kes Olga Greuter & Dipti Kapoor Sarmah

To cite this article: Kes Olga Greuter & Dipti Kapoor Sarmah (2022): The baseline of global consumer cyber security standards for IoT: quality evaluation, Journal of Cyber Security Technology, DOI: 10.1080/23742917.2022.2105192

To link to this article: https://doi.org/10.1080/23742917.2022.2105192

Published online: 27 Jul 2022.

JOURNAL OF CYBER SECURITY TECHNOLOGY
https://doi.org/10.1080/23742917.2022.2105192

The baseline of global consumer cyber security standards for IoT: quality evaluation

Kes Olga Greuter[a,b] and Dipti Kapoor Sarmah[a,c]

[a]EEMCS, Universiteit Twente, Drienerlolaan 5, 7522 NB Enschede,Netherlands; [b]BMS/EEMCS, Universiteit Twente, Drienerlolaan 5, 7522 NB Enschede, The Netherlands; [c]SCS/EEMCS, University of Twente, Drienerlolaan 5, 7522 NB Enschede, The Netherlands

ABSTRACT

The popularity of the Internet of Things (IoT) devices has been gaining interest amongst consumers. The rise of consumers benefiting from IoT devices has increased the threat of cyber-attacks. The safety, security, and privacy of consumers can be negatively affected if vulnerabilities of IoT devices are exploited. Therefore, there is a need of understanding what within IoT devices is necessary to secure. Further, the implementation of necessary and important requirements is needed to ensure protection against cyber-attacks on IoT devices. The recently published Cyber Security for Consumer Internet of Things (CSCIoT) standard, called ETSI EN 303 645, is a global standard that describes requirements on implementing a minimum level of security for IoT devices. This paper evaluates the sufficiency of cyber security of the consumer IoT standards' requirements and gradation. The evaluation is done by comparing CSCIoT to the international professional IoT standard, called IEC 62443, and with the other related work, such as the Secure by Design report of the UK Department for Digital, Culture Media & Sport. Also, this paper discusses implications regarding consumer responsibility on security. This paper aims to stimulate more precision and extension of requirements for consumer IoT devices to lower the risk of cyber-attacks.

ARTICLE HISTORY
Received 31 January 2022
Revised 17 June 2022
Accepted 20 July 2022

KEYWORDS
Internet of things; cyber-security and privacy; international consumer IoT standards; international professional IoT standards; consumer responsibility

1. Introduction

There is a growing trend of the use of Internet-connected [1] devices in homes, such as smart refrigerators, Bluetooth-connected toothbrushes, or mobile phones. IoT devices can be equipped with sensors [2] as cameras and microphones and actuators as lights and speakers. Through these devices, consumers are enabled to remotely monitor and manage their IoT devices in their homes [2]. The abuse of such sensors and actuators can have a great impact on the safety, security, and privacy of the consumer. Cyber-attacks such as Distributed Denial of Service (DDoS) [3] and computer viruses [4] could be executed

CONTACT Dipti Kapoor Sarmah d.k.sarmah@utwente.nl Services and Cyber security/EEMCS, Universiteit Twente Netherlands

through IoT systems. The need for a threshold [5] of cyber security that can mitigate cyber threats of these IoT devices is growing. The individuals benefiting from IoT devices need to be provided safety by mapping the necessary security and privacy requirements [6]. IoT devices lacking sufficient cyber security bring two risks [6]. First of all, by making use of the vulnerabilities of individual devices the consumers' security, privacy and safety are undermined. Secondly, a vast number of economical instances face large-scale cyber-attack threats. These attacks are executed from large volumes of insufficiently secured IoT devices.

Recent cyber-attacks such as the Mirai botnet [7] and Reaper botnet [8] took advantage of poor configuration and open design of IoT devices. This caused disruptions in many services of news and media websites by executing DDoS attacks [3]. During the attack, Mirai botnets managed to control almost half a million IoT devices. Reaper botnets had executed DDoS attacks on routers as well as internet-connected cameras. Cyber-attacks with a great impact on society such as Mirai and Reaper have led to more awareness towards the legislation of cyber security implementation on IoT devices for consumer purposes [6]. The Minister for Digital and Creative industries of the UK responded to the need for better protection of citizens and the wider economy [6]. As a result, requirements for cyber security implementation for IoT devices for consumer use were published [6]. The report intended to stimulate further discussion with the industry, academic institutions, and civil society. A landscape report [9] responded to the lack of a universal standard as well. This report examined a cross-section of fifteen existing regulations, in five jurisdictions (as of September 2018) and how these are applied to IoT products [9]. This report [9] maps out the similarities and differences in regulation on consumer IoT cyber security. The intention here is to help manufacturers and regulators understand these similarities and differences.

The final draft of the international Cyber Security for Consumer Internet of Things (CSCIoT) [5] standard has been published in April 2020, named ETSI EN 303 645. This standard tackles requirements for developing IoT devices securely and according to the data protection rights. The importance of good quality of the CSCIoT [5] is great to ensure protection against cyber threats. It has not been researched whether this standard is sufficient to offer the best security possible compared to other requirements from related work. Related work here includes the professional IoT devices cyber security standard and requirements published nationally. There are significantly fewer requirements available for the security of consumer IoT devices than the security of professional IoT devices [10–13]. Furthermore, the CSCIoT [5] standard assumes that all consumer IoT devices require the same security level. The purpose of this paper is to evaluate the sufficiency of cyber security of the consumer IoT standards' requirements and gradation. This is done by comparing the international consumer IoT [5] standard to the international professional IoT standard, called IEC 62443: Cyber Security for Industrial Automation and Control Systems (CSIACS) [10–13], and

related work. The international professional standard is chosen for comparison as there are significant differences between the standards on security demanded from IoT devices for consumers and on security demanded from IoT devices for businesses. Examples of such differences are the lack of gradation of the CSCIoT and the number of requirements of the CSCIoT. These differences will be further explained later in this section. CSCIoT [5] and CSIACS [10–13] are used for similar IoT devices yet for different markets. For instance, smart building lighting can be used both in consumer and professional environments, yet according to the standard they would have completely different product security requirements. The intention being the comparison is to align so that security of consumer products is more in line with professional products. Besides, the environment of an IoT device in a professional environment is mostly much more secured than in a home environment. For example, professional environment has more network security e.g. firewalls and network separation. While in a home environment, it is usually limited to a router. Looking at this, a similar IoT device in a home environment is less protected by the environment and more at risk, while also having less protection from the CSCIoT standard for the product itself. In general, there are more consumer IoT devices thus making it a larger attack surface and more attractive for hackers The related work that will be compared consists of documents that state requirements for consumer IoT devices. This includes the Secure by design report as mentioned in [6], Good practices for security of IoT by the European Union Agency for Cyber Security [14], and a paper on the top 20 design principles for IoT security, as mentioned in [15]. The importance of this research is the stimulation of the development of more elaborate requirements in the cyber security legislation for IoT devices used by consumers. This is necessary to provide better security and/or security guidance to manufacturers and end-users.

In 2013, the system security requirements and security levels of the CSIACS [10–13] standard were published. This standard offers a flexible framework addressing current and future security vulnerabilities in professional systems by categorizing thirteen modules into General, Policies & Procedures, System, and Component [16]. The modules, 62,243-X within the CSIACS are depicted in Figure 1. IEC 62443 requirements intend to manufacture, install and operate the IoT device securely. For the EN 303 645, the requirements are also intended to secure the consumer IoT device throughout its lifecycle. The General category includes the modules 62,243–1. The foundations of information are described in these modules, including models, concepts, and terminologies. Within the Policies & Procedures, the modules 62,443–2 describe the creation and maintenance of an effective Cyber Security Management System. The modules of 62,443–3 are in the System category. Here the technical requirements of system design and guiding principles for secure development and integration of the system are described. Finally, the Component includes the 62,443–4 modules

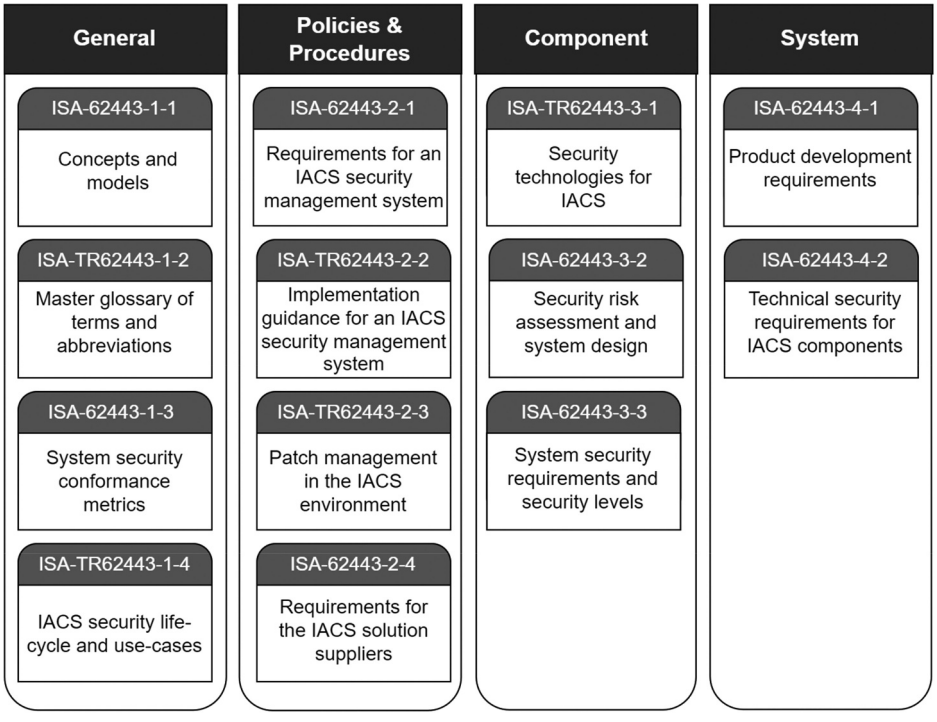

Figure 1. The modules within the CSIACS [10–13].

and focuses on the technical guidelines that must be implemented during development. It is important to note that only modules 2–4, 3–3, 4–2, and 4–1 [10–13] are relevant to this paper as they are on requirements for the Industrial Automation Control System solution suppliers (2–4), system security requirements and security levels (3–3), secure product development lifecycle requirements (4–1) and technical security requirements for Industrial Automation Control System components (4–2). While only IEC 62443–4 is aimed at IoT device manufacturers, IEC 62443 modules 2–4 and 4–1 are included in the comparison as they include security requirements for processes of product requirements. Therefore, they will assist to evaluate the availability and quality of process requirements within the CSCIoT. Other modules are not relevant for this paper as they do not mention any requirements, as can be seen in Figure 1. An exception to this is module 2–1. This module focusses on professional system security management systems aimed at the asset owner, as shown in Figure 1. Module 2–1 has not been considered for two reasons. First, most requirements of 2–1 overlap with 4–1 and 4–2. Second, 2–1 are requirements for the asset owner which is less relevant for consumer IoT devices. Therefore, with agreement of IoT security expert Ir. Barbara Oosterveld CISSP CISM CSSLP [17] module 2–1 was considered not relevant for this paper.

Table 1. Security levels used in the CSIACS [10,13].

Layer	Description
SL1	Protection against casual or coincidental violation.
SL2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation.
SL3	Protection against intentional violation using sophisticated means with moderate resources, system-specific skills, and moderate motivation.
SL4	Protection against intentional violation using sophisticated means with extended resources, system-specific skills, and high motivation.

In modules 3–3 and 4–2, the security levels SL1, SL2, SL3, and SL4, as shown in Table 1 below, are described. These security levels [10,13] are based on an assessment of potential consequences and the assumed nature of the attack. For example, a connected system holding confidential information of a government instance will be assigned SL4 and will thus have stricter security requirements. A connected toothbrush, on the other hand, will generally not be able to do much damage and therefore be assigned to SL1.

Reading the standard for consumers, the CSCIoT [5], shows that there is a significant difference between the standards on security demanded from IoT devices for consumers and on security demanded from IoT devices for businesses. This difference is mainly within the lack of gradation and the number of requirements of the CSCIoT. As mentioned earlier, the CSIACS [10–13] offers a framework and four security assurance levels (refer to Table 1). For each product requirement listed in the CSIACS, one of the security assurance levels is assigned in a framework. The CSCIoT [5] limits to thirteen main guidelines, under which provisions are categorized, on migrating cyber threats, listed in Table 3 in the methodology section, and includes no gradation. IoT devices could range from products that can only have little impact on the safety, security, and privacy of the consumer (such as a Bluetooth-connected toothbrush [18]), to items that can have an enormous impact (such as self-driving vehicles [19]). While some consumer IoT devices may need very basic security as they do not endanger any lives, others may need more security as they could harm the user or leak sensitive data. Also, here it is important to note that the environment of the consumer is already less secure. For example, if an IoT device regulating temperature in the house is connected to an insecure router, while being minimally secure according to the CSCIoT, an attacker could more easily exploit this and cause financial harm or, if the temperature really rises, physical harm. Looking at the wide range of different devices available, it is questionable that it is adequate to assume equal security measures, thus no gradation, on all IoT consumer devices. This while the recent best practice of IoTSF [20] on IoT consumer security does use gradation on devices. Considering the difference between the approach to protecting IoT consumer devices and IoT devices for professional use, the trade-off has to be made on whether the CSCIoT, also named ETSI EN303645[5], is sufficient in quality.

This paper evaluates the CSCIoT [5] standard in two ways. First, by mapping out the differences in requirements and gradation with the professional CSIACS [10–13] standard. Second, by assessing the adequacy of the requirements for consumers, supported by requirements on IoT consumer cyber security specified in related work, consisting of [6,14,15]. This is done by answering three associated research questions, regarding 1) quality of requirements; 2) sufficiency of requirements and 3) need of gradation. These research questions are described more elaborately in the methodology of Section 3.

The structure of this paper is as follows. Section 2 discusses related work, in which related literature and how this paper adds on to that is discussed. The subsequent sections go into more detail on the research performed in this paper. Section 3 covers methodology, in which the research questions, the data collection, the use of frameworks, and the setup of a survey are elaborated on. The methodology also covers a discussion on consumer responsibility regarding IoT device security. The survey in the methodology serves as a part of the justification of the results. Section 4 discusses the obtained results from the execution of the steps mentioned in the methodology. This also includes a discussion on consumer responsibility. Finally, conclusions and future work are discussed in section 5.

2. Related work

In this section, related literature is discussed. First, literature that focuses on mitigation strategies against cyber-attacks is analysed, and following that, literature that specifies requirements for IoT security is discussed.

There has been a lot of research done on specifying mitigation strategies against cyber threats for consumer IoT cyber security. For instance, a case study on vulnerabilities for IoT consumers [21] suggests potential mitigation strategies by analysing common attacks executed on consumer IoT devices and what vulnerabilities they exploit. Examples of such common attacks are malicious code injection, unauthorized access, social engineering attack and eavesdropping attack [21]. Seven IoT devices, including a video doorbell, a smart home cam and a connected water boiler, were tested on vulnerabilities [1]. Out of these seven IoT devices, five were found insufficiently secured [1]. An example of an attack that the research [1] was able to do is using forged commands to keep the water boiler heating up, even if the water boils dry. This can potentially cause fire. Therefore, a mitigation framework is developed in which these vulnerabilities are mapped to their solutions. Finally, security threats within each architectural layer, being the perception layer, transportation layer, and application layer, of IoT architectures can be discussed, as done in [22,23]. Based on these results, mitigation strategies are also analysed. Above research has shown different approaches to developing mitigation strategies. None of the research above, however, specify requirements that could be implemented in

legislation on consumer IoT cyber security. This is an interesting and challenging open area for researchers. Multiple research has been done on specifying requirements for IoT cyber security. For instance, one research [24] analyses integration and security issues in IoT and offers possible solutions. Several requirements to provide security on data storage, cloud, big data, and Radio Frequency Identification for IoT devices are specified. Goals for achieving trust management in IoT are listed as well. Another approach is to specify requirements based on security concerns, detailed asset taxonomies, threat taxonomies, and good practices to enhance the cyber security of the IoT Software Development Life Cycle [14]. These requirements are categorized in People, Processes, and Technologies, and mapped to related existing standards, guidelines, and schemes [14]. The IoT Security Assurance Framework by IoTSF [20] is a best practice published in November 2021 and mentions around 270 requirements while categorizing products into Assurance classes based on their level of risk. Their requirements are categorized based on three aspects. First, whether they are mandatory or not. Second, if they are related to the system or to the business practices of the organization. Third, what concept they cover. The concepts are categorized in Responsibility, Policy, Process, Hardware, Physical, or Software [20]. This best practice document covers important requirements for consumer IoT security yet is not a standard and therefore organizations do not have to comply with these requirements. A publication by NIST [25] describes baseline requirements for consumer software cybersecurity labeling. Finally, UL cybersecurity describes their top 20 IoT design principles [15] based on their experience in the IoT security industry.

The research above was written with the same purpose as the CSCIoT standard, to specify requirements needed for the cyber security of consumer IoT devices. However, the work does not cover analysing the current standard by comparison with the professional standard, CSIACS [10–13]. Comparison with the professional standard is an open door for researchers to fulfill the need for improvement of the CSCIoT [5] standard, and therefore is selected for the research and discussed in this paper.

The next section is on the methodology used in this paper. In this section, the research questions, the data collection, the use of frameworks, the survey set up, and the further look on consumer responsibility are described.

3. Methodology

This section regards the methodology used in this paper to evaluate the quality of the CSCIoT [5]. Research questions are specified and following this, the use of sources and frameworks to answer the research questions are explained. The main question of this research is as follows: '*To which extent is the CSCIoT* [5] *sufficient and adequate for consumer protection of IoT devices?*'. To answer the main question, three sub research questions (RESQ1, RESQ2 and RESQ3) are

Table 2. The research questions, the corresponding data sources, and the purposes.

Reference	Research Question	Data Sources	Purpose
RESQ1	How do the requirements of the Cyber Security for Consumer IoT standard differ from the requirements of the Cyber Security for Industrial Automation and Control Systems standard? (Comparison of requirements between standards)	CSCIoT [5] CSIACS [10–13]	Determine how the requirements for consumers differ from the requirements for professional systems. This is needed to determine how IoT products for consumers are protected by use of the CSCIoT compared to how IoT products are protected by the CSIACS.
RESQ2	How do the requirements of the Cyber Security for Consumer IoT standard differ from the requirements of a set of related work, consisting of [6,14,15] specifying requirements on consumer IoT cyber security? (Comparison of requirements between CSCIoT standard and related work)	CSCIoT [5] Secure by Design: Improving the Cyber Security of Consumer Internet of Things report [6] Good Practices for Security of IoT [14] IoT Security Top 20 Design Principles [15]	Determine whether the requirements in CSCIoT are somewhat overlapping with the requirements mentioned in related work [6,14,15] that also states requirements for consumer IoT security.
RESQ3	To what extent is the lack of gradation in the Cyber Security for Consumer IoT standard adequate? (Evaluation of gradation)	CSCIoT [5] Framework on similar requirements between CSCIoT and CSIACS created in RESQ1	Determine whether the consumer standard adequately makes no use of gradation by comparing the similar requirements of the CSIACS and research if security levels differ for these requirements. This is needed to determine if the CSCIoT should have had security levels for requirements that were classified in security levels in the CSIACS standard.

Table 3. Main thirteen guidelines of CSCIoT [5].

Requirement	Guideline	Requirement	Guideline
R1	No universal default passwords.	R8	Ensure that personal data is secure.
R2	Implement a means to manage reports of vulnerabilities.	R9	Make systems resilient to outrages.
R3	Keep software updated.	R10	Examine system telemetry data.
R4	Securely store sensitive security parameters.	R11	Make it easy for users to delete user data.
R5	Communicate securely.	R12	Make installation and maintenance of devices easy.
R6	Minimize exposed attack surfaces.	R13	Validate input data.
R7	Ensure software integrity.		

specified and showcased in Table 2, with the information of data sources and their purpose respectively. Furthermore, the setup of a survey on important findings from research question 1 (RESQ1) and research question 2 (RESQ2) is discussed. Finally, the adequacy of assuming consumer responsibility for the security of IoT products is discussed.

Data sources as mentioned in Table 2 refer to the documents from which information is used to answer the research questions. A flowchart of the proposed methodology and the expected results are showcased in Figure 2.

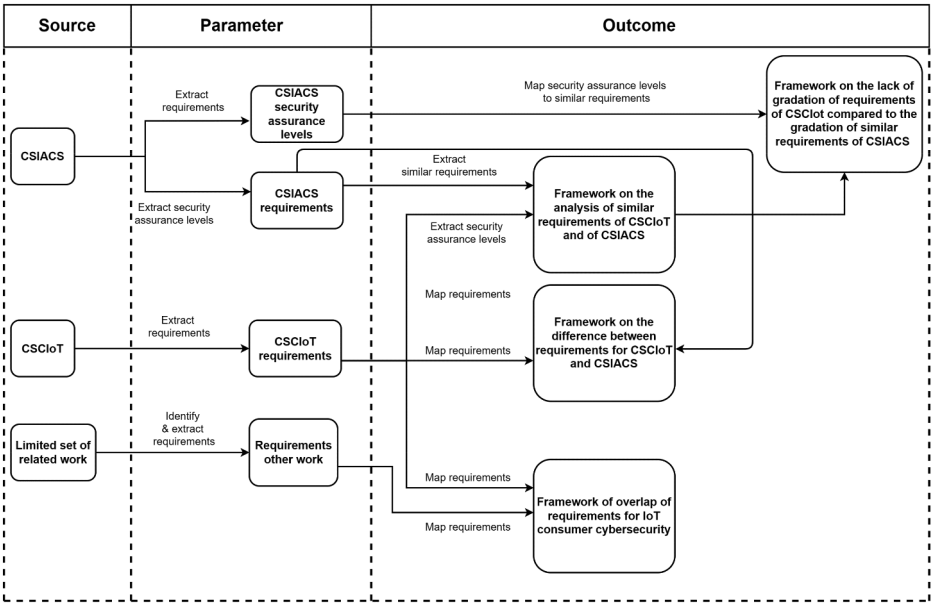

Figure 2. Flowchart of methodologies.

This flowchart depicts the data sources, parameters, and outcomes. The parameters are the specific components of the data sources used for the frameworks, for example, the parameter security assurance levels from the data source CSIACS. Also, the flowchart gives an overview of what parameters each framework consists of. Note that in the flowchart, the line that goes from the parameter 'CSIACS requirements' to the outcome 'framework on the difference between requirements for CSCIoT and CSIACS' has rounded corners. This design choice has been made to distinguish this line more easily from any overlapping lines.

The research questions are answered by following specific steps as listed below.

(i) RESQ1 steps:

1. Extract requirements from CSCIoT [5] and CSIACS [10–13].
2. Map differences in requirements in a framework.
3. Map similar requirements in a framework, comparing the depth and execution of the requirements.

(ii) RESQ2 steps:

1. Extract requirements from a set of related work, consisting of [6,14,15].
2. Map requirements in a framework, comparing whether they are similar or not.

(iii) RESQ3 steps:

1. Map security assurance levels, as in Table 1, linked to CSIACS requirements to the similar requirements of CSCIoT. This is done using the similar requirements between CSIACS and CSCIoT which is the result of RESQ1.

2. Identify requirements with lacking gradation and list these.

During the research period, a survey [26] on the need for a more elaborate cyber security consumer IoT legislation was distributed amongst 16 people. These people have a profession related to the cyber security of IoT consumer devices. This survey is intended to support the goal of this research, which is the improvement of cybersecurity legislation on consumer IoT devices. The survey contains 18 requirements, as listed in Table 9. These requirements are related to lacking aspects of the CSCIoT [5] standard, and they are recognized while executing the steps to answer RESQ1 and RESQ3. More information on the survey is available in section 3.3.

3.1 Data collection

To answer the research questions RESQ1, RESQ2, and RESQ3, the data sources, and parameters have been chosen carefully by evaluating whether their content is appropriate for comparison with CSCIoT [5]. All research questions include the CSCIoT [5] of which the main thirteen guidelines, under which the requirements are placed, are listed in Table 3. These thirteen main guidelines can be found in chapter 5 of CSCIoT [5].

The sources used for comparison in this paper can be found in Table 4. This table also provides the number of requirements per source and the purpose of the source. This information helps the reader to understand the nature and size of the sources. To answer RESQ1, a comparison of the CSCIoT [5] with the CSCIACS [10–13] was made. The CSCIACS consists of thirteen modules, shown in Figure 1, of which four state security requirements, modules 2–4 [10], 3–3 [11], 4–1 [12] and 4–2 [13]. For the comparison, each of these four requirements has been evaluated and 2–4, 3–3, and 4–1 have been selected for the comparison. Most requirements of 4–2 were identical to requirements of 3–3 and were therefore not considered. Only a small selection of requirements of 4–2, which consisted of component-specific requirements needed for the mapping of similar requirements between the CSCIoT and the CSCIACS, were used. This was only necessary for provisions 5.3–1, 5.3–10, and 5.4–2 of the CSCIoT. The decision to leave out the repeated requirements of 4–2 has been discussed with and agreed on by IoT security expert Ir. Barbara Oosterveld CISSP CISM CSSLP [17].

3.2 Frameworks

To evaluate the depth and quality of the requirements of the CSCIoT, for each requirement, a similar requirement of the CSIACS was mapped [27] using Microsoft Excel spreadsheets Further, we identified the coverage difference of the requirements between CSCIoT and CSIACS with the following mapping:

Table 4. Requirements per identified data source.

Source	Number of requirements	Purpose	Publication year
CSCIoT [5]	68	The document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure and their interactions with associated services [5].	2020
CSCIACS 2–4 [10]	123	The document specifies requirements for the Industrial Automation Control System solution suppliers.	2015
CSCIACS 3–3 [11]	100	The document specifies requirements for Industrial Automation Control System Security.	2013
CSCIACS 4–1 [12]	47	The document specifies requirements for secure product development lifecycle requirements for Industrial Automation Control Systems	2018
Secure by design [6]	13	A Code of Practice aimed at manufacturers of consumer IoT products and associated services. The document sets out thirteen practical steps to improve the cyber security of consumer IoT. [6]	2017
Good practices [14]	81	The document introduces good practices for IoT security with a focus on software development guidelines for secure IoT products and services throughout their lifetime. [14]	2019
Top 20 requirements [15]	20	The document provides simple steps that can be taken to increase the security of connected systems. [15]	2019

a) the CSCIoT requirement covers the CSIACS requirement.

b) the CSCIoT requirement covers less than the CSIACS requirement; or

c) the CSCIoT requirement covers more than the CSIACS requirement.

As shown in Table 5, the difference between the requirements from the CSCIoT and the CSIACS was observed to identify which requirement has more or less coverage. One can access the full framework available on the Github repository [27] regarding this research. Further analysis of the framework is discussed in section 4.

The framework as shown in Table 6 was used to determine the requirements that were available in the CSIACS but not in the CSCIoT, while they should have been available in CSCIoT. For each requirement of the CSIACS 2–4, 3–3, and 4–1, it was determined whether the requirement would be necessary for the legislation of cybersecurity of consumer IoT devices. This was done with justification from IoT security expert Barbara Oosterveld [17]. Then, for all requirements that were necessary for the consumer legislation, it was determined whether a similar requirement like this was available in the CSCIoT. When a similar requirement was available, it is stated what provision is similar. In case the requirement was necessary, while not being in the CSCIoT, the input for mapping was 'Not available'. In case the requirement was not necessary and also not available, the input for the mapping was 'N.A'., for non-applicable. There were no cases in which a requirement was labeled not necessary yet was available in the CSCIoT.

Table 5. Framework: comparison of similar requirements between CSCIoT [5] and CSIACS [10–12].

CSCIoT requirement	CSIACS mapping to provision	Coverage	Difference
Provision 5.1–1	IEC 62443-2-4 SP-09.02–2	3.2 a	No difference
Provision 5.3–15	IEC 62443-3-3 SR 5.2 RE 2	3.2 c	The CIACS states that products should be isolated (island mode) but does not state that hardware should be replaceable, which CSCIoT does.
Provision 5.3–11	IEC 62443-4-1 SUM-2	3.2 b	The CSCIoT only states that the risks mitigated by the update should be documented. The CSIACS, besides the risks of not applying, also requires the product version numbers to which the patch applies. It further requires instructions on how to apply patches manually and automatically, a description of the impacts that applying the patch to the product can have.

Table 6. Framework: comparison of different requirements between CSCIoT [5] and CSIACS [10–12].

CSIACS requirement	Need in consumer legislation	Availability in CSCIoT	Mapping to CSCIoT requirement
IEC 62443-3-3 SR 1.1	Necessary	Available	Provision 5.1–3, Provision 5.5–4
IEC 62443-3-3 SR 1.1 RE 1	Necessary	Not available	Not available
IEC 62443-3-3 SR 1.1 RE 2	Not necessary	Not available	Non applicable (N.A.)

RESQ2 included the use of other related work [6,14,15] to compare requirements of the CSCIoT [5] to IoT security requirements determined by papers or reports [6,14,15]. The requirements of the related work were compared to the CSCIoT to see whether they were similar or not. The requirements of Good Practices for IoT security [14] and Top 20 Design Principles for IoT security [15] were also compared to each other to see their similarity. The Secure by Design report was not included in the comparison between related work, as the related requirements of this paper were identical to the requirements of the CSCIoT. This is most likely because the CSCIoT used the Secure by Design paper as a source. This is further discussed in the results in section 4.

For RESQ3, the framework that was the result of the comparison of similar requirements of the CSCIoT and the CSIACS was used. In this comparison, requirements of the CSCIoT were mapped to a requirement of module 3–3 or 4–2 of the CSIACS. These were then analysed on their accuracy of lacking in gradation. This was done by checking the security level of that similar requirement in the CSIACS. In case the security level of a similar requirement was higher than 1, the requirement was listed as having an inadequate lack of gradation [27]. Once the data was collected, the setup of a survey was done to get the opinions of 16 security experts, which is described in the next section 3.3.

3.3 Survey set up

As described in Section 3, a survey was set up as a means of justification for some of the requirements or subjects that have been labelled necessary but not available in RESQ1. Furthermore, the survey investigated the experts' opinions on whether gradation within consumer legislation is necessary, which is researched in RESQ3.

The survey was published on LinkedIn [26] and filled in by 16 participants. The participants were asked to only participate if they have a basic knowledge or understanding of consumer IoT security, either obtained from working experience or study. The participants did not need to be aware of the CSCIoT standard to fill in the survey. For thirteen days, these IoT security experts had the opportunity to submit their judgment on the statements provided in the survey. The survey consisted of nine sections representing the topic the statements belonged to. The represented topics and the number of related statements can be found in Table 7.

The statements from the survey originated from a selection process starting with 138 statements [27]. 137 of these statements were formulations of requirements that were labeled necessary but unavailable in CSCIoT [5]. The other statement was a formulation of RESQ3 and was added to investigate the expert's opinions on the lack of gradation for the requirements of the CSCIoT [5]. This statement, which can be found in RQ1 in Table 9, is as follows: *'A Bluetooth-connected toothbrush, connected smoke detectors, door locks, window sensors, and self-driving vehicles should all be categorized into the same security level'*. Out of the 138 statements, the statements that were related to the most incomplete or missing topics were selected. The selected statements therefore can indicate an overall opinion on whether that topic should be (better) represented. The analysis of the survey can be found in the results, section 4.4.

3.4 Consumer responsibility

Another important aspect that is discussed in this research is the assumption of consumer responsibility regarding IoT security. While setting security requirements for consumer products it is important to consider the adequacy of assuming consumer responsibility. Requirements on passwords settings [5] e.g. specify that the devices cannot be provided with default login data as username: 'admin' and password: 'admin'. There are, however, no requirements on limiting user input

Table 7. Topics included in the survey [26].

Topic	Number of statements	Topic	Number of statements
Gradation	1	Remote Access	3
Authentication	3	Backup	3
Wireless Connections	3	Documentation	7
Sessions	4	Processes	5

from changing passwords to simple, or possibly even default passwords. A lack of requirements on consumer behaviour could result in unwanted configurations set by the consumer that impact the security of the IoT device and consumer. It is questionable whether it is appropriate to assume the consumer is responsible for malicious exploitation of inadequate settings set by the consumer if the product allows for these settings to be altered in the first place. Requirements on user data such as passwords [5] require the user to read the manual of the device. It is, however, questionable whether consumers read the manuals [28]. Research [28] found that users avoid using both paper and online help systems. The users report that they would rather solve problems by discussion with others or experimenting on their own. The research found that more than half of the participants abandoned a task rather than that they used printed documentation [28]. The research mentions the most likely reasons for not using printed manuals are their perceived unavailability, bulkiness, difficulty of navigation, inappropriate level of detail or expertise relative to the used and being out of date [28]. Another option is to adapt the IoT device itself. One way to do this is to ensure security requirements that involve consumer responsibility are implemented in such a way that the IoT device limits any potential alteration or input that a consumer can make that impacts the security. It might, however, be infeasible to limit every potential insecure input and alteration within a product. Therefore, another option is for the field of Security and the field of User Experience to collaborate and make secure use of features of the IoT products self-explanatory [29]. This paper investigates above mentioned discussions by use of identified papers [29,30] and presents suggestions in the results, section 4.5. The first identified paper [30] is on the improvement of the presentation of security related information in manuals. The second identified paper [29] is on the collaboration of security and User Experience.

The following section discusses the results obtained from the previously discussed frameworks, a survey, and suggestions regarding consumer responsibility.

4. Results and discussion

This section discusses the results that were obtained from the methods used in this paper to evaluate the quality of the CSCIoT [5]. First, results from the comparison of similar requirements of CSCIoT and CSIACS [10–13] are discussed. The first subsection also discusses the results from the comparison of different requirements between CSCIoT and CSIACS. These results represent the answer to RESQ1. The following subsection, aiming to answer RESQ2, analyses the results from the comparison of requirements available in the CSCIoT and related work [6,14,15]. Next, the results of the survey are discussed. Finally, suggestions from identified literature [29,30] regarding consumer responsibility are stated and discussed.

4.1 Comparison of requirements between standards

Figure 3 shows the results of the comparison of similar requirements of CSCIoT and CSIACS. This was concluded from the result of the framework as presented in Table 5. The full framework can be found on the Github [27]. From these results, it can be concluded that 32% of the requirements in the CSCIoT could improve in depth and scope. For every CSCIoT requirement that covers more or less than the CSIACS, the difference between these requirements was analyzed. Out of these differences, there were some frequently occurring differences between requirements from the CSCIoT and the CSIACS, as listed below.

- The CSIACS includes the role responsible for every requirement, while only a few requirements of CSCIoT specify the task owner.
- The CSIACS covers processes that are necessary to execute to create or maintain a sufficient level of security, while CSCIoT does not have any requirements on processes.
- The CSIACS has separate requirements for the necessary documentation, while CSCIoT rarely speaks of documentation.

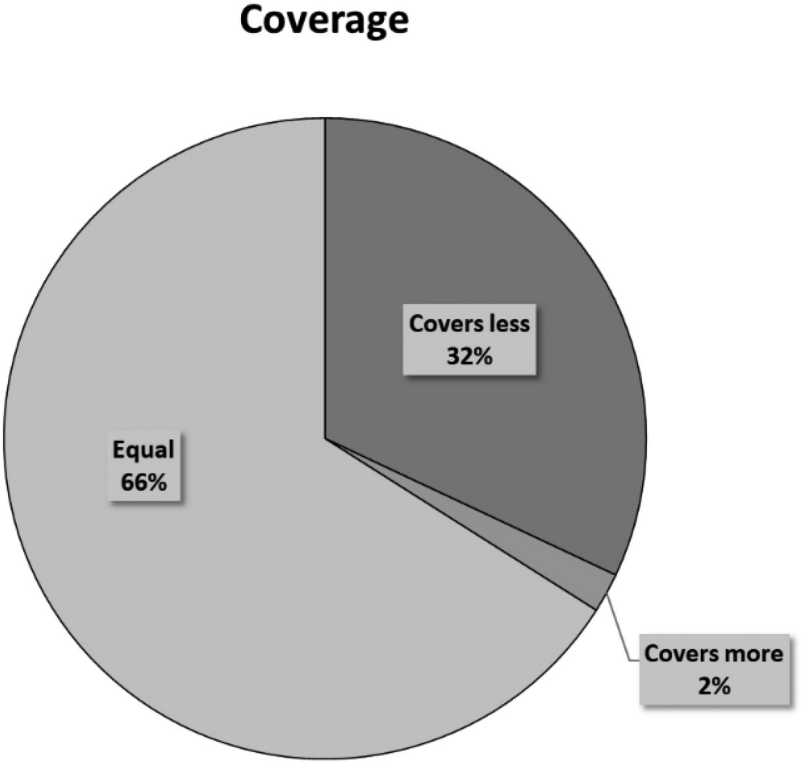

Figure 3. Coverage of CSCIoT [5] requirements against similar requirements of CSIACS [10–13].

- The CSCIoT specifies the need of each requirement by recommended and mandatory, while all requirements are mandatory in CSIACS
- The CSCIoT sometimes specifies advice or justification of the provision in the text between provisions, while the CSIACS does not provide advice but rather states the necessities in the requirements.

While these remarks are mostly regarding the scope of the requirements in CSCIoT, they are each important to consider as they clarify requirements and stimulate better cyber security management. The noted differences per provision are available in the 'RQ1 – similar requirements' framework of the Github repository [27].

Figure 4 shows the results of the comparison of different requirements between CSCIoT and CSIACS. The requirements identified in CSIACS that should be in CSCIoT but are not, are called missing requirements. As depicted in the figure, there is a total of 84 requirements for module 2–4 of CSIACS. The missing requirements for module 2–1 are observed 76.2% for CSCIoT. For module 3–3, this is 44 missing requirements out of 68 requirements, which is 64.7%. Finally, for module 4–1 this is 29 missing requirements out of 47 total requirements, which is 61.7%. These results show that a significant amount of the requirements that should have been available in the CSCIoT but were not. Looking at modules 2–4, 3–3 and 4–1 together, it is found that 137 out of 199 total requirements (68,9%) are missing.

From figures 3 and 4 it is concluded that first, there is a (68,9%) lack of requirements of the CSCIoT when comparing requirements of CSIACS that were deemed necessary for consumers by IoT expert Barbara Oosterveld. Second, out of the requirements that were available, 32% were lacking depth. For example, some requirements were less detailed or did not demand documentation while the similar CSCIACS requirement does. These numbers indicate that for requirements deemed necessary for consumer, the CSCIoT sets a much lower baseline

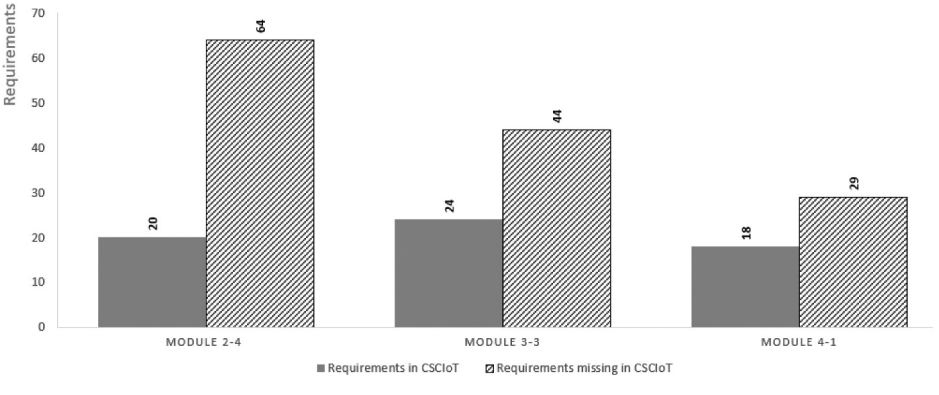

Figure 4. Comparison of different requirements between CSCIoT [5] and CSIACS [10–13].

to protect the IoT product than the CSCIACS does. This supports the argument that the consumers of IoT devices are not sufficiently protected by legislation when looking at what the protection the professional standard offers.

4.2 Comparison of requirements between standard and related work

In this section, the results of the comparison of requirements between the CSCIoT and related work [14,15] are represented in the Venn diagram in Figure 5. From the diagram, it can be concluded that the requirements of the CSCIoT cover (8 out of 20) 40% of related work Top 20 Design Principles for IoT security [15] and (21 out of 77) 27% of Good Practices for IoT security [14].

The different sources that were used contain different numbers of requirements, as shown in Table 4. Therefore, the amount per source should be taken into consideration while researching how well the CSCIoT covered other related work, compared to how well the reports and papers of the related work covered each other, and the CSCIoT. This coverage of a source considering their number of requirements is calculated as follows

$$Coverage_x = \frac{MR_1}{R_x} + \frac{MR_2}{R_x} \tag{1}$$

Where $Coverage_x$ represents the percentage of the source x's coverage of the requirements of all other sources selected for this comparison, MR_n corresponds to the amount of matched requirements from source n and R_x is the total amount of requirements from source x.

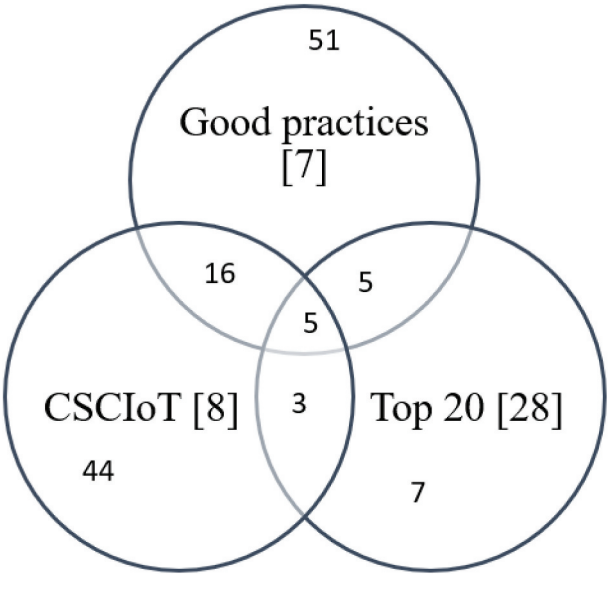

Figure 5. Venn diagram of similar requirements of related work [14,15] and CSCIoT [5].

Table 8. Weighted coverage of CSCIoT [5] and related work [14,15].

Source	Top 20	Good practices	CSCIoT	Total
Top 20	N.A.	50,0%	40,0%	65,0%
Good Practices	13,0%	N.A.	27,0%	33,8%
CSCIoT	11.8%	30,8%	N.A.	35,3%

The results of these calculations can be found in Table 8. From this table we can conclude that the Top 20 Design Principles on IoT security covers the other sources best, having coverage of 65% total. The CSCIoT follows with 35,3% and Good Practices for IoT security covers other sources the least, with 33,8%. This result can be explained, as Good Practices for IoT security contains three categories; processes, people, and product, of which requirements on processes and people are not available, or only a limited number of requirements is available in the CSCIoT and Top 20 Design Principles on IoT security. The CSCIoT has no similar requirements with the requirements from the people category of Good Practices for IoT Security, and only 8 similar process requirements out of the 33 process requirements available in Good Practices for IoT security.

4.3 Evaluation of gradation

Figure 6 shows the comparison between the similar requirements as well as the survey requirements for security levels 1, 2, or higher. The left side of Figure 6 shows the results of the research on whether the CSCIoT lacks gradation adequately. Here, for the requirements of CSCIoT that were similar to the requirements of CSIACS, a total of 32 similar requirements, a further look was taken at the assigned security levels of those requirements. The similar requirements analysis is discussed in section 4.1. Out of the 32 similar requirements, 9 requirements of CSCIACS have a security level higher than 1. CSCIoT contains similar requirements to these yet does not specify any security level. This shows that over a set of similar requirements, the CSIACS does distinguish security levels while the CSCIoT does not. From these results, it can be concluded that 9 out of 68 (13,2%), of the total amount of requirements of the CSCIoT should have been categorized into a higher security level.

Figure 6 (right) shows the division in security levels from the requirements that originated from modules 3–3 [11] of which more than 70% of the IoT security experts agreed on the requirement being necessary for the legislation of consumer IoT devices. From these requirements, 5 out of 6 (83%) should be categorized into a security level of 2 or higher. Furthermore, from RQ1, Table 10, where 100% of the IoT cyber security experts disagreed that various IoT devices should all require the same requirements for cyber security, it can be concluded that the survey group thinks gradation of security levels is necessary.

Table 9. Requirements.

Reference	Requirement
RQ1	A Bluetooth-connected toothbrush, connected smoke detectors, door locks, window sensors, and self-driving vehicles should all be categorized into the same security level.
RQ2	For devices that use public key authentication, the device shall provide the capability to validate certificates by using techniques such as; 1. checking the signature of a given certificate; 2. constructing a certification path to an accepted CA or deploying leaf certificates to all hosts communicating to the owner to whom the certificate is issued; 3. checking the certificate's revocation status; 4. establishing the user control of the corresponding private key; and 5. mapping the authenticated identity to a user
RQ3	For accounts having an administrative role, there shall be multi-factor authentication available. This includes accounts that are used for administration and maintenance by the manufacturer.
RQ4	The device shall be able to authorize, monitor, and enforce usage restrictions for wireless connectivity.
RQ5	Access to wireless devices should be protected by authentication and access control mechanisms.
RQ6	After a configurable time period of inactivity or by manual initiation, further access to the device should be prevented by initiating a session lock. This session lock shall remain in effect until the human user who owns the session or another authorized human accesses via appropriate identification and authentication procedures.
RQ7	The integrity of sessions shall be protected. Any usage of invalid session IDs shall be rejected.
RQ8	The number of concurrent sessions per interface by any given user shall be limited to a configurable number of sessions.
RQ9	Approval of the user shall be obtained every time before using remote access connections.
RQ10	All remote access connections conducted over the Internet or other publically accessible media shall be authenticated and encrypted.
RQ11	The reliability of a backup mechanism shall be verified.
RQ12	It shall be possible to perform a complete backup of the device and it shall be possible to restore a fully functioning device from this backup.
RQ13	The device shall be able to enable and disable the security configuration mode. While disabled, the interface shall prohibit security configurations.
RQ14	Communication loads shall be managed, e.g. by use of rate-limiting, to mitigate the effects of DoS events.
RQ15	There shall be documentation available for the user on the secure behavior of the consumer.
RQ16	There shall be documentation available for the user on the retention capabilities of the device for storing sensitive data.
RQ17	There shall be documentation available for the user on data exchange between other devices, such as wireless and remote devices.
RQ18	There shall be documentation available for the user on instructions for configuration, operation, and termination of remote access applications.
RQ19	There shall be documentation available for the user on instructions for proper installation, configuration, and update of malware protections mechanisms.
RQ20	There shall be documentation available for the user on how security patches for the software of the device are evaluated and approved.
RQ21	There shall be documentation available on recommended backup procedures.
RQ22	The manufacturing company shall have processes on identifying the personnel responsible for security processes required by the standard.
RQ23	The manufacturing company shall have processes on providing an integrity verification mechanism for all scripts, executables, and other important files in the device.
RQ24	The manufacturing company shall have processes for identifying and managing security risks within the devices.
RQ25	The manufacturing company shall have processes for verifying that the security functions meet the security requirements.
RQ26	The manufacturing company shall have processes for testing the effectiveness of the mitigation of threats as identified and validated in the threat model.

4.4 Survey justification

The results of the survey can be found in Table 10. RQ2 until RQ26 tested the necessity of adoption into the consumer legislation. The results show that at least 50% of the IoT security experts agreed that the requirement is necessary. Figure 7

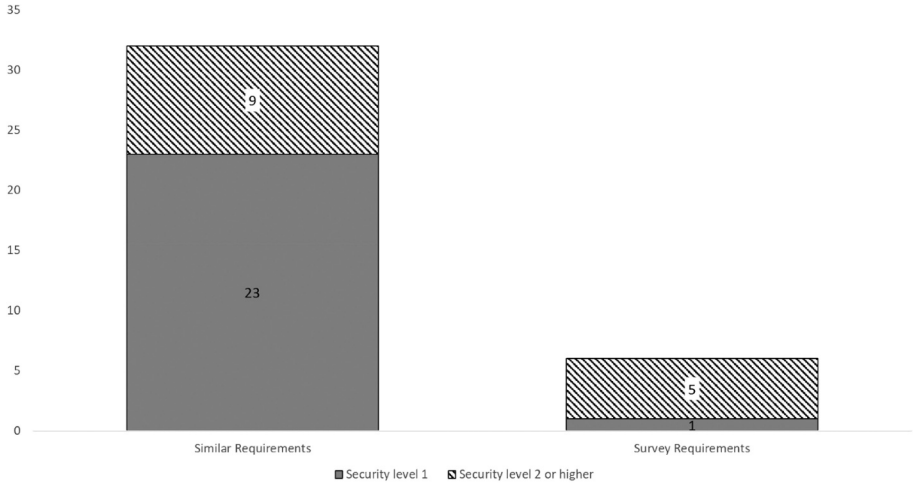

Figure 6. Gradation of similar requirements (left) and gradation of survey requirements (right).

Table 10. Survey results.

No.	Agree	Neither agree nor disagree	Disagree	Other	No.	Agree	Neither agree nor disagree	Disagree	Other
RQ1	0,00%	0,00%	100,00%	0,00%	RQ14	81,25%	12,50%	0,00%	6,25%
RQ2	81,25%	12,50%	6,25%	0,00%	RQ15	68,75%	18,75%	12,50%	0,00%
RQ3	93,75%	0,00%	0,00%	6,25%	RQ16	81,25%	12,50%	6,25%	0,00%
RQ4	81,25%	0,00%	18,75%	0,00%	RQ17	75.00%	18,75%	6,25%	0,00%
RQ5	93,75%	0,00%	0,00%	6,25%	RQ18	75.00%	25,00%	0,00%	0,00%
RQ6	68,75%	18,75%	6,25%	6,25%	RQ19	75.00%	18,75%	6,25%	0,00%
RQ7	100,00%	0,00%	0,00%	0,00%	RQ20	50,00%	31,25%	18,75%	0,00%
RQ8	75.00%	12,50%	12,50%	0,00%	RQ21	68,75%	31,25%	0,00%	0,00%
RQ9	81,25%	12,50%	6,25%	0,00%	RQ22	62,50%	25,00%	12,5%	0,00%
RQ10	93,75%	6,25%	0,00%	0,00%	RQ23	81,25%	12,5%	6,25%	0,00%
RQ11	93,75%	6,25%	0,00%	0,00%	RQ24	93,75%	0,00%	6,25%	0,00%
RQ12	62,50%	31,25%	0,00%	6,25%	RQ25	93,75%	0,00%	6,25%	0,00%
RQ13	75,00%	12,50%	12,50%	0,00%	RQ26	81,25%	12,50%	6,25%	0,00%

below shows the agreement on the requirements of the IoT security experts. In this figure, it is shown that for only one requirement, 50% of the experts agreed. This requirement was RQ20, as can be seen in Table 10: *'There shall be documentation available for the user on how security patches for software of the device are evaluated and approved'*. Other requirements were agreed on by at least 60% of the experts, of which 13 requirements were agreed on by 80% to 100% of the experts. The conclusion that can be drawn from this figure is that all requirements, except RQ20, were found necessary by the majority of the experts. Also, as mentioned in the previous subsection, the results of RQ1 show that the experts disagree with the lack of gradation. Concluding from the results obtained from the survey, the topics on which these requirements (RQ2 to RQ26) were based on as listed in Table 7 should be (better) represented in the CSCIoT.

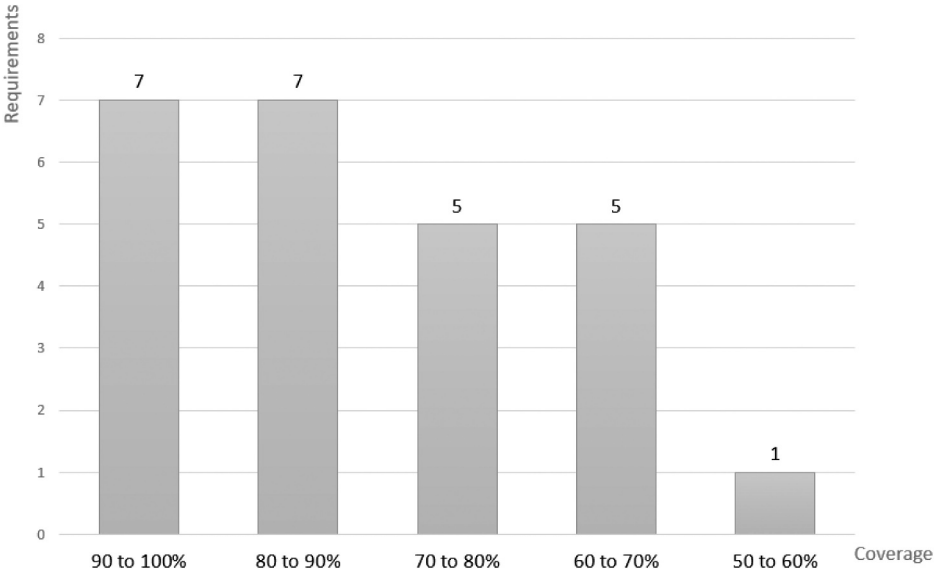

Figure 7. Number of requirements per agreement coverage of experts.

4.5 Discussion on consumer responsibility

To improve the collaboration with the consumer on complying with security requirements manufacturers can consider altering the security information provided to the consumer in the manual [30]. The manual can state the most important information at the start of the section. Detailed security information can be located somewhere after the section containing the most important information to not overwhelm consumers with too much information. This ensures the user is aware of the most important security-related statements and can deepen in security risks and control of the product. Emami-Naeini et. al. [30] researched the impact of security and privacy on the consumer's perception and willingness to purchase IoT devices. They propose changes to be made to the manual to better convey risk to consumers. The changes listed below could be made to inform the consumers of the security risks and measures of an IoT product.

- Justification as to why the manufacturer has a specific privacy and security practice in place.

- In what way a specific privacy and security practice could protect or harm consumers

- What controls consumers have related to each privacy and security attribute.

- If an option is being offered to control a specific privacy and security practice, what steps do users need to take to enable that option.

The research [30] found that several participants believed that the need for updates and patches implied poor security. Such misconceptions on security could be reduced by explaining the reasoning behind measures in place and security patches [30]. It is also important to include the consumer responsibilities regarding security [30]. It should be prevented that misuse of a feature of the product can cause implications for the security of the product. However, when a consumer is expected to use a feature only according to the intended use, this should be clearly stated. Also, if altering any configurations for the IoT product would impact the security this has to be stated.

An additional method to improve consumer interaction with consumer responsibility is to further include security in the User Experience (UX) design cycle and consider UX within the design of security requirements [29]. UX can be used to simplify and streamline features related to security within products and make user actions that are necessary to comply with security requirements self-evident. Chalhoub et. al. [29] researched the rule of UX in the Security and Privacy Design of an IoT product and found that *'UX was not factored into the design of security solutions due to lack of expertise and the misconception of security being a low-priority technical-only problem'*. Better collaboration between the UX and Security fields can improve user-dependent security. The first step towards this could be to include Security Experts in the UX team. This research also found that regulation triggered security design considerations. For example, a security audit on weak passwords prompted an evaluation of password strength and the creation of UX-aware password requirements [29].

The following section states the conclusions that can be made from this paper and discusses the future work that could be done regarding this paper and topic.

5. Conclusion and future work

To protect the safety, security, and privacy of the consumer there has to be a sufficient threshold on the legislation on the cybersecurity of consumer IoT devices. Sufficient and adequate legislation also protects the other stakeholders as manufacturers and distributors against cyber-attacks. This paper has evaluated the sufficiency of the CSCIoT standard based on its requirements and lack of gradation. As opposed to related work, this research has attempted to stimulate improvement of consumer IoT cyber security by comparing the CSCIoT standard to a more elaborate professional standard (CSIACS) and other related work stating IoT security requirements. This has resulted in four frameworks. Analysis of the first two frameworks has shown that almost one-third of the requirements of the CSCIoT are less elaborate than similar requirements available for professional IoT systems. The CSCIoT generally lacks documentation, task division, and processes specified in the available requirements. Furthermore, more than half of the requirements found necessary for consumer

legislation are not available in the CSCIoT. Analysis of the third framework shows that the CSCIoT also has a low coverage (35,8%) of other reports or papers stating IoT security requirements. The results of the fourth framework show that the lack of gradation in the CSCIoT is inadequate as 13,2% of the requirements in the standard should have had a security level higher than 1. Further, from the requirements that should have been available in the CSCIoT 83% should be categorized into a security level higher than 1. This resulted from the survey for IoT security experts. The survey included statements that represented topics that were not or insufficiently specified by requirements. The results of that survey show that the 16 IoT security experts that participated agreed that the topics authentication, wireless connections, sessions, remote access, backup, documentation, and processes should be available or better represented in the legislation on cybersecurity for IoT consumer devices. This work has also looked at the consumer role in following security requirements listed in the manual of an IoT product. The most important findings discussed, first of all, the altering of information on security in the manual to make the consumer more aware of any risks related to the product. Second, the collaboration between User Experience and Security could improve to e.g. streamline security features within the product. The evaluation done by this research gives readers an understanding of the sufficiency of implementing only the requirements given in the CSCIoT standard. For regulators, this research could serve as a stimulation for the development of more elaborate and adequate consumer IoT legislation.

The ultimate goal is for all international standards and legislations to be aligned so global IoT manufacturers can have one set of requirements and with one labelling scheme. This paper aims to contribute to this goal by setting the first step of indicating the problem of insufficient consumer of IoT devices protection by legislation. The evaluation of the requirements and lack of gradation give a proper image of the sufficiency of the CSCIoT. There are, however, more factors to sufficient cyber security legislation for consumer IoT devices. These factors are dependent on stakeholder behavior throughout the lifecycle of the IoT device. As discussed in related work, the recent best practice of IoTSF [20] is an important publication to consider and could support legislators in finding the balance between the necessary requirements for consumers and professional standards. Further research could focus on the content of the IoTSF best practice [20] and suggest which requirements of this best practice could be included in the consumer standard. The willingness and capabilities of manufacturers play a role in the risk of cyber-attacks. In fact, according to the Department for Digital, Culture, Media, and Sport (UK) [6], *'The main disincentives center around cost and the challenge of justifying time and money when a business's focus is to get their product off the market as soon as possible'*. Therefore, there is a need for research to be done on finding the balance between quick and cheap product development and a sufficient baseline of cyber security. Next, research should be done on possible implications that

implementing such requirements might bring. The National Institute of Standards and Technology has performed such research, as mentioned in [31], for several requirements from which some requirements are mentioned in the CSCIoT [5]. Finally, to improve upon this research, the executed survey could be extended with more requirements from CSCIACS that were not but should have been available in CSCIoT. With the inclusion of more requirements, as well as an increase in participants, the survey could bring an adequate opinion on what requirements should be available in a consumer standard.

Acknowledgments

I would like to thank Barbara Oosterveld CISSP CISM CSSLP [24] for providing justification for the analysed requirements and supporting me with cyber-security concepts.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Kes Greuter holds a bachelor's degree in business and IT. Currently, she is pursuing her Master's degree in Computer Science with a specialization in Cyber Security.

Dr. Dipti K. Sarmah works as a Lecturer in Semantics and Cyber Security (SCS) research group in the EEMCS Department at the University of Twente, Netherlands. She has around 15 years of teaching and research experience with strong publications in Steganography, and Cryptography. She has been serving as a reviewer for many reputed journals.

ORCID

Dipti Kapoor Sarmah http://orcid.org/0000-0002-0802-4280

References

[1] Ye C, Indra PP, Aspinall D (2019): "*Retrofitting security and privacy measures to smart home devices*", Sixth International Conference on Internet of Things: Systems, Management and Security *(IOTSMS*), Granada, Spain, pp 283–290.

[2] Notra S, Siddiqi M, Gharakheili HH, et al. (2014): *"An experimental study of security and privacy risks with emerging household appliances*", IEEE Conference on Communications and Network Security, San Francisco, CA, USA, pp. 79–84.

[3] Perakovic D, Perisa, M., Cvitic, I.(2015): "*Analysis of the IoT impact on volume of DDoS attacks*", 33rd Symposium on New Technologies in Postal and Telecommunication Traffic, Beograd, pp 295–304.

[4] Milosevic J, Sklavos N, Koutsikou K (2016): "*Malware in IoT Software and Hardware*", Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, pp 8–11, Barcelona, Spain.
[5] European Telecommunications Standards Institute (2020): "*Final draft ETSI Cyber Security for Consumer Internet of Things: Requirements Baseline*". [Cited 2022 Jun 6]. Available at: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf
[6] Department for Digital, Culture Media & Sport, Great Brittan (2017): "*Secure by design: improving the cyber security of consumer internet of things report*". Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf Accessed 2022 Jun 6.
[7] Kambourakis G, Kolias C, Stavrou A (2017): "*The mirai botnet and the IoT zombie armies*.", IEEE Military communications conference, pp 267–272, USA.
[8] Greenberg A (2017): Wired. "*The Reaper Botnet Has Already Infected a Million Networks*". [Cited 2022 Jun 6]. https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/
[9] IOT Security Foundation (2018): "*IoT cybersecurity: regulation ready a landscape report*". Available at: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Cybersecurity-Regulation-Ready-White-Paper-Concise-Version.pdf Accessed 2022 Jun 6
[10] IEC 62443-2-4: "*Security for industrial automation and control systems-part 2-4: security program requirements for IACS providers"* (IEC 62443-2-4:2015). Last accessed on 2022, July 25. Available at: https://webstore.iec.ch/publication/22810
[11] IEC 62443-3-3: "*Industrial communication networks- network and system security- part 3-3: system security requirements and security levels"* (IEC 62443-3-3: 2013). Last accessed on 2022, July 25. Available at: https://webstore.iec.ch/publication/7033
[12] ISA-62443-4-1 *"Security for industrial automation and control systems part 4-1: secure product development life- cycle requirements"* (IEC 62443-4-1: 2018). Last accessed on 2022, July 25. Available at: https://webstore.iec.ch/publication/33615
[13] ISA –62443-4-2 "*Security for industrial automation and control systems technical security requirements for IACS components"* (IEC 62443-4-2: 2019). Last accessed on 2022, July 25. Available at: https://webstore.iec.ch/publication/34421
[14] European Union Agency for Cybersecurity. (2019): "*Good Practices for Security of IoT*". [Cited 2022 Jun 6]. Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
[15] UL cybersecurity (2019): *"IoT Security Top 20 Design Principles*". Last accessed on 2022, July 25Available at: https://www.ul.com/resources/iot-security-top-20-design-principles
[16] Arampatzis A (2020): *"What Is The ISA/IEC 62443 Framework?*" The State of Security. [Cited 2022 Jun 7]. https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/
[17] Oosterveld B (2020): LinkedIn profile. Last accessed on 2022, July 25. Available at: https://www.linkedin.com/in/barbaraoosterveld/
[18] Vesanen J (2019): "*" I know when you brush your teeth" - Cyber security on personal medical devices*", Thesis from Metropolia University of Applied Sciences. Last accessed on 2022, July 25. Available at: http://urn.fi/URN:NBN:fi:amk-201901301748
[19] Prevost S, Kettani H (2019): "*On data privacy in modern personal vehicles*", The 4th International Conference On Big Data and Internet of Things, Rabat Morocco, pp 1–4.
[20] IoT Security Foundation. (2021): *"IoT Security Assurance Framework Release 3.0*"
[21] Alladi T, Choo KR. Consumer IoT: security vulnerability case studies and solutions. IEEE Consum Electron Mag. 2020;9(2):17–25

[22] Ande R, Adebisi B, Hammoudeh M, et al. Internet of Things: evolution and Technologies from a Security Perspective. Sustainable Cities Soc. 2020;54:101728.
[23] Tewari A, Gupta BB. Security, privacy and trust of different layers in internet-of-Things (IoTs) framework. Future Gener Comput Syst. 2020;108:909–920.
[24] Zekeriya M, Das R. "Cyber-security on smart grid: threats and potential solutions". Comput Netw. 2020;169:1–8.
[25] DRAFT baseline criteria for consumer software cybersecurity labeling. National Institute of Standards and Technology (NIST), 2021.
[26] Greuter K (2020): Survey post, linkedin. Last accessed on 2022, July 25. Available at: https://www.linkedin.com/feed/update/urn:li:activity:6673556891160969216/
[27] Greuter K (2020): "Evaluation-paper", Github repository. Last accessed on 2022, July 25. Available at: https://github.com/Kes-G/Evaluation-paper
[28] Novick D, Ward K (2006): "*Why don't people read the manual?*" . The 24th ACM international conference on Design of communication, Myrtle Beach SC USA, pp 11–18.
[29] Chalhoub G, Flechais I, Nthala N, et al. (2020): *"Innovation inaction or in action? The role of user experience in the security and privacy design of smart home cameras*", Sixteenth Symposium on Usable Privacy and Security, Boston, USA, pp 185–204.
[30] Emami-Naeini P, Dheenaadhayalan J, Agarwal Y, et al. (2021): *" Which privacy and security attributes most impact consumers' Risk Perception and Willingness to Purchase IoT devices?"*, IEEE Symposium on Security and Privacy, San Francisco, CA, USA, pp 519–536.
[31] National Institute of Standards and Technology (2019): *"Considerations for Managing Internet of Things Cybersecurity and Privacy Risks"*. Last accessed on 2022, July 25. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf