Evaluating the Quality of the International Consumer IoT Cyber Security Standard

Kes Greuter
University of Twente
PO Box 217, 7500 AE Enschede
the Netherlands
k.o.greuter@student.utwente.nl

ABSTRACT

The popularity of the Internet of Things (IoT) devices is increasing amongst consumers. Now that more consumers benefit from the IoT devices, the threat of cyber-attacks increases as well. The safety, security and privacy of consumers can be negatively affected if vulnerabilities of the IoT devices are exploited. Therefore the understanding of what is necessary to secure and the implementation of requirements are needed to ensure protection against cyber-attacks on the 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 the IoT devices. This paper evaluates the sufficiency of cyber security of the consumer IoT standards' requirements and gradation by comparing it to the international professional IoT standard, called IEC 62443, and other related work, such as the Secure by Design report of the UK Department for Digital, Culture Media & Sport, to stimulate more precision and extension of requirements in the legislation of cyber security for consumer IoT devices to lower the risk of cyber-attacks.

Keywords

Internet of Things, Cyber-security, Privacy, Consumer IoT Standards

1. INTRODUCTION

There is a growing trend of the use of Internet-connected [26] devices in homes, such as smart refrigerators, Bluetooth-connected toothbrushes, mobile phones, or cars. IoT devices can be equipped with sensors [18] 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 [18]. 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) [21] and computer viruses [16] could be executed through IoT systems.

The need for a threshold [6] 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 [4].

33th Twente Student Conference on IT, Jul. 3rd, 2020, Enschede, The Netherlands.

IoT devices lacking sufficient cyber security brings two risks [4]. First of all, by making use of the vulnerabilities of individual devices the consumers' security, privacy and safety are undermined. Secondly, a vast amount of economical instances face large scale cyber-attack threats executed from large volumes of insufficiently secured IoT devices.

Recent cyber-attacks such as Mirai [15] and Reaper [7] took advantage of poor configuration and open design of IoT devices and caused disruptions in many services of news and media websites by executing DDoS attacks [21]. 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 [4].

As a response to the need for better protection of citizens and the wider economy, the Minister for Digital and Creative industries of the UK published requirements for cyber security implementation for IoT devices for consumer use [4]. The report intended to stimulate further discussion with the industry, academic institutions and civil society. Responding to the lack of a universal standard as well, a cross-section of fifteen existing regulations, in five jurisdictions (as of September 2018) and how these are applied to IoT products was examined in a landscape report [14]. This report maps out the similarities and differences in regulation on consumer IoT cyber security and is intended to help manufacturers and regulators understand these.

The final draft of the international Cyber Security for Consumer Internet of Things (CSCIoT) [6] 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. Whereas the importance of good quality of the CSCIoT [6] 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 as the professional IoT devices cyber security standard and requirements published nationally. There are significantly few requirements available for the security of consumer IoT devices than the security of professional IoT devices [10,11,12,13] and the CSCIoT [6] standard is based on the assumption 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 by comparing the international consumer IoT [6] standard to the international professional IoT standard, called IEC 62443: Cyber Security for Industrial Automation and Control Systems (CSIACS) [10,11,12,13], and other related work, being the Secure by design report as mentioned in [4], Good practices for security of IoT by the

European Union Agency for Cyber Security [5], and a paper on the top 20 design principles for IoT security, as mentioned in [24]. The importance of this paper is the stimulation of development of more elaborate requirements in the cyber security for IoT devices used by consumers, so that product manufacturers and end-users are provided better security and/or security guidance.

In 2013, the system security requirements and security levels of the CSIACS [10,11,12,13] 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 [3].

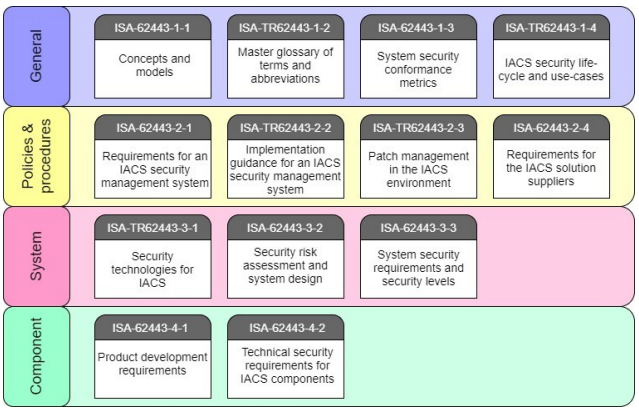

Figure 1: The modules within the CSIACS [10,11,12,13]

In modules 3-3 and 4-2, the security levels, 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.

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.

Reading the standard for consumers, the CSCIoT [6], 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. As mentioned earlier, the CSIACS [10,11,12,13] offers a framework and four security assurance levels (Table 1). For each product requirement listed in the CSIACS, one of the security assurance levels is assigned in a framework. The CSCIoT [6] limits to thirteen main guidelines, under which provisions are categorized, on migrating cyber threats, listed in Table 2 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 [25]), to items that can have an enormous impact (such as self-driving vehicles [22]). 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. 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 EN 303 645 [6], is sufficient in quality.

This paper evaluates the CSCIoT [6] standard, by mapping out the differences in requirements and gradation with the professional CSIACS [10,11,12,13] standard, and assess the adequacy of the requirements for consumers, supported by requirements on IoT consumer cyber security specified in related work, consisting of [4,5,24]. 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 be described more elaborately in the methodology section.

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 set up of a survey, that serves as a part of the justification of the results, is elaborated on. Section 4 discusses the obtained results from the execution of the steps mentioned in the methodology. Finally, conclusions are discussed in section 5, and future work in section 6.

2. RELATED WORK

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

2.1 Mitigation strategies

There has been a lot of research done on specifying mitigation strategies against cyber threats for consumer IoT cyber security. For instance, Alladi et. al [1] suggest potential mitigation strategies by analysing common attacks executed on consumer IoT devices and what vulnerabilities they exploit. Seven IoT devices were tested on vulnerabilities and five out of seven devices found insufficiently secured [26]. Therefore a mitigation framework is developed in which these vulnerabilities are mapped to their solutions. Finally, IoT architectures can be compared and security threats within each architectural layer can be discussed, as done in [2,23]. Based on these results, mitigation strategies can also be analysed and discussed. These researches have shown different approaches to developing mitigation strategies, however none specify requirements that could be implemented in legislation on consumer IoT cyber security.

2.2 Specifying requirements

In the following years, multiple research has been done on specifying requirements for IoT cyber security. For instance, Zekeriya et. al [27] analyse integration and security issues in IoT and offer 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, as done in [5]. These requirements are categorized in People, Processes and Technologies, and mapped to related existing standards, guidelines and schemes. Finally, UL cybersecurity describes their top 20 IoT design principles [24] based on their experience in the IoT security industry.

The researches above were 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 [10,11,12,13]. Comparison with the professional standard is an open door for researchers to fulfill the need for improvement of the CSCIoT [6] standard, and therefore is researched 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, and the survey set up are described.

3. METHODOLOGY

This section regards the methodology used in this paper to evaluate the quality of the CSCIoT [6]. First, the research questions are specified. After, the identified data is specified. Then, the use of frameworks to answer the research questions are explained and finally, the set up of a survey, that serves as a part of the justification of the found results, is discussed.

Below are the research questions necessary to answer to get an adequate view of the sufficiency of CSCIoT [6].

RQ1: 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)

RQ2: How do the requirements of the Cyber Security for Consumer IoT standard differ from the requirements of a set of related work, consisting of [4,5,24] specifying requirements on consumer IoT cyber security? (Comparison of requirements between CSCIoT standard and related work)

RQ3: To what extent is the lack of gradation in the Cyber Security for Consumer IoT standard adequate? (Evaluation of gradation)

Literature research is executed to answer the above-mentioned questions. Below steps considered for answering the research questions are specified. A flowchart of the proposed methodology and the expected results can be found in Figure 2. The flowchart depicts the data sources, parameters and outcomes. It gives an overview of what parameters each framework consists of and from what data source those parameters origin.

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

RQ1 steps:

1. Extract requirements from both standards.
2. Map differences in requirements in a framework.
3. Map similar requirements in a framework, comparing the depth and execution of the requirements.

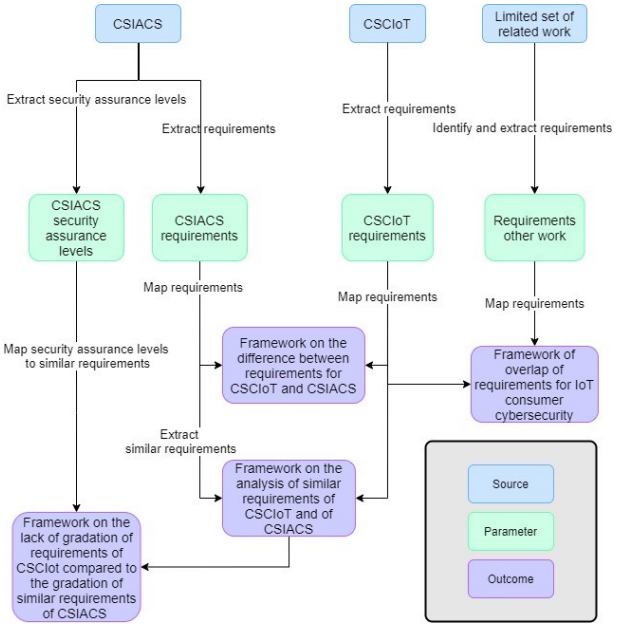

Figure 2: Flowchart of methodologies in this thesis

RQ2 steps:

1. Extract requirements from a set of related work, consisting of [4,5,24].
2. Map requirements in a framework, comparing whether they are similar or not.

RQ3 steps:

1. Map security assurance levels to the similar requirements of CSCIoT to CSIACS (the result of RQ1).
2. Identify requirements with lacking gradation and list these.

During the research period, a survey on the need for a more elaborate cyber security consumer IoT legislation was distributed amongst 16 people with a profession related to the cyber security of IoT consumer devices. This survey is intended to support the goal, the improvement of cybersecurity legislation on consumer IoT devices, of this research. The survey contains questions, as listed in Table 7, related to lacking aspects of the CSCIoT [6] standard, found while executing the steps to answer RQ1 and RQ3.

3.1 Data collection

To answer the research questions, the data sources and parameters needed to be chosen carefully by evaluating whether their content is appropriate for comparison with CSCIoT [6]. All research questions include the CSCIoT [6] of which the main thirteen guidelines, under which the requirements are placed, are listed in Table 2. The number of requirements per source can be found in Table 3.

To answer RQ1, a comparison of the CSCIoT [6] with the CSCIACS [10,11,12,13] 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 has been evaluated and 2-4, 3-3, and 4-1 have been selected for the comparison.

Table 2: Main thirteen guidelines of CSCIoT [6]

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

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 [20].

Table 3: Requirements per identified data source.

Source	Amount of requirements
CSCIoT [6]	68
CSCIACS 2-4 [10]	123
CSCIACS 3-3 [11]	100
CSCIACS 4-1 [12]	47
Secure by design [4]	13
Good practices [5]	81
Top 20 requirements [24]	20

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 using Excel spreadsheets.

Then, for each mapping it is specified whether:

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.

For each requirement that has more or less coverage, the difference between the requirements from the CSCIoT and the CSIACS was noted. Table 4 shows a selection of this framework. The full framework is available on the Github repository [8] regarding this paper. To determine the requirements that were available in the CSIACS but not in the CSCIoT while they should have been available, the framework as shown in Table 5 was used.

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 [20]. Then, for all requirements that were necessary for the consumer legislation, it was determined whether this requirement was available in the CSCIoT, and as what provision. 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 but was available in the CSCIoT.

RQ2 included the use of other related work [4,5,24] to compare requirements of the CSCIoT [6] to IoT security requirements determined by papers or reports. To do this, the framework consisted of several parts, representing one of the works each. In each part, 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 [5] and Top 20 Design Principles for IoT security [24] 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.

For RQ3, the framework that was the result of the comparison of similar requirements of the CSCIoT and the CSIACS was used. All requirements of the CSCIoT that were mapped to a requirement of module 3-3 or 4-2 of the CSIACS were analysed on their accuracy of lacking in gradation 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.

Table 4: Framework *comparison of similar requirements*.

CSCIoT requirement	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 isolatable (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, instructions on how to apply patches manually and automatically, a description of impacts that applying the patch to the product can have.

Table 5: Framework: *Comparison of different requirements.*

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	N.A.

3.3 Survey Set Up

The survey was set up as a means of justification for some of the requirements or subjects that have been labeled necessary but not available in RQ1 and for support on research on whether gradation is necessary, as done in RQ3.

The survey was published on LinkedIn [9] and shared amongst several IoT security experts. For thirteen days, IoT security experts had the opportunity to submit their judgement on the statements provided in the survey.

The survey consisted of nine sections representing the topic the statements belonged to. The following topics were represented:

- Gradation (1 statement)
- Authentication (3 statements)
- Wireless connections (3 statements)
- Sessions (4 statements)
- Remote access (3 statements)
- Backup (3 statements)
- Documentation (7 statements)
- Processes (5 statements)

The statements from the survey originated from a selection process starting with 138 statements. 137 of these statements were formulations of requirements that were labeled necessary but unavailable in CSCIoT [6]. The other statement was a formulation of RQ3. Out of these 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.

The following section discusses the results obtained from the previously discussed frameworks and a survey.

4. RESULTS

This section discusses the results that were obtained from the methods used in this paper to evaluate the quality of the CSCIoT [6]. First, results from the comparison of similar requirements of CSCIoT and CSIACS [10,11,12,13] 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 RQ1. The following subsection, aiming to answer RQ2, analyses the results from the comparison of requirements available in the CSCIoT and related work [4,5,24]. Finally, the results of the survey are shown.

4.1 Comparison of requirements between standards

Figure 3 shows the results of the comparison of similar requirements of CSCIoT and CSIACS. 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.
- 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 framework of the Github repository [8].

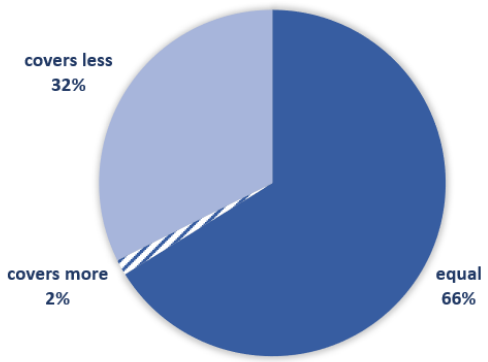

Figure 3: Coverage of CSCIoT [6] requirements against CSIACS [10,11,12,13].

Figure 4 shows the results of the comparison of different requirements between CSCIoT and CSIACS. From these results, it is found that 51% of the total amount of requirements that are necessary for the consumer standard, 199 requirements, are not available in the consumer standard.

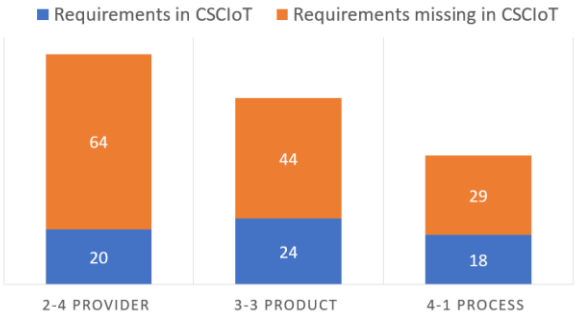

Figure 4: Comparison of different requirements between CSCIoT [6] and CSIACS [10,11,12,13].

4.2 Comparison of requirements between standard and related work

The results of the comparison of requirements between the CSCIoT and related work [5,24] are represented in the Venn diagram in Figure 5. From the diagram, it can be concluded that the requirements of the CSCIoT cover 40% of related work Top 20 Design Principles for IoT security [24] and 27% of Good Practices for IoT security [5].

Because the different sources that were used contain different amounts of requirements, 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 amount of requirements is calculated as follows

$$Coverage_x = \frac{MR_1}{R_x} + \frac{MR_2}{R_x} \quad (1)$$

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.

Table 6: Weighted coverage of CSCIoT [6] and related work [5,24].

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

The results of these calculations can be found in Table 6. From this table we can conclude that 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.

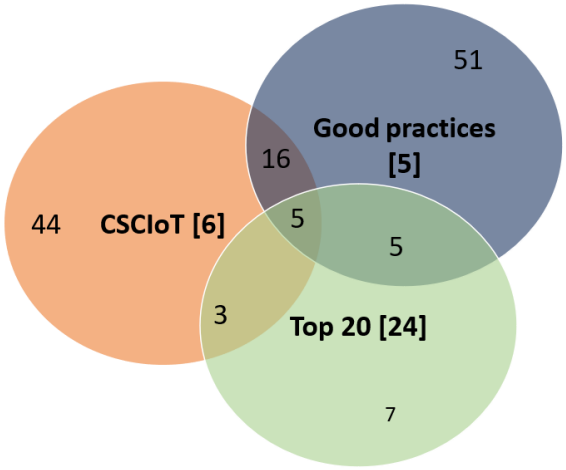

Figure 5: Venn diagram of similar requirements of related work [5,24] and CSCIoT [6]

4.3 Evaluation of gradation

The results of the research on whether the CSCIoT lacks gradation adequately are shown in Figure 6 (left). From these results, it can be concluded that 13,2 % of the total amount of requirements of the CSCIoT should have been categorized into a higher security level than the other requirements available in the CSCIoT, and thus, that there should be gradation implemented in the CSCIoT.

From statement 1, Table 7, 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.

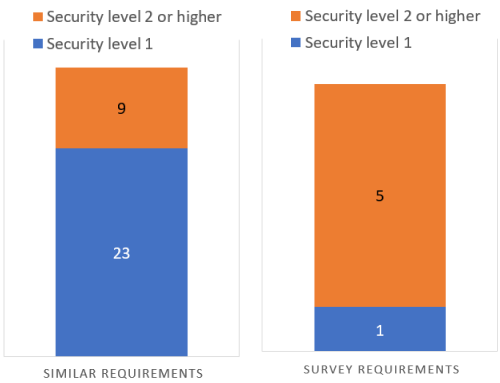

Figure 6: Gradation of similar requirements (left) and gradation of survey requirements (right)

Figure 6 (right) shows the division in security levels from the requirements that originated from module 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, 83% should be categorized into a security level of 2 or higher.

4.4 Survey justification

The results of the survey can be found in Table 7. For each statement of which the necessity of adoption into the consumer legislation was tested, statements 2 until 26, at least 50 percent of the IoT security experts agreed that the requirement is necessary. Figure 7 below shows the agreement on the statements of the IoT security experts. In this figure it is shown that for only one statement, 50% of the experts agreed. This statement was statement 20: *"There shall be documentation available for the user on how security patches for software of the device are evaluated and approved."*. Other statements were agreed on by at least 60% of the experts, of which 13 statements were agreed on by 80% to 100% of the experts. The conclusion that can be drawn from this figure is that all statements, with an exception of statement 20, were found necessary by the majority of the experts. Also, as mentioned in the previous subsection, the results of statement 1 show that the experts disagree with the lack of gradation.

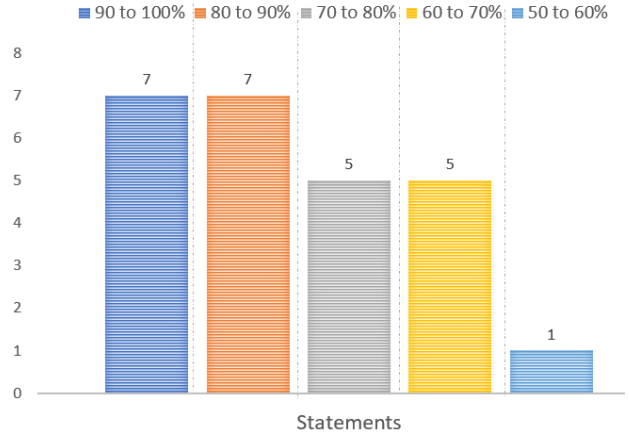

Figure 7: Amount of statements per agreement coverage of experts.

Concluding from the results obtained from the survey, the topics as listed in section 3.3 should be (better) represented in the CSCIoT.

5. CONCLUSION

To protect the safety, security and privacy of the consumer but also other stakeholders as manufacturers and distributors against cyber-attacks, there has to be a sufficient threshold on the legislation on the cybersecurity of consumer IoT devices. 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, according to a survey for IoT security experts, 83% should be categorized into a security level higher than 1. The survey included statements that represented topics that were not or insufficiently specified by requirements. The results of that survey show that the 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. Adopting the evaluation done by this research gives manufacturers 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.

6. FUTURE WORK

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. Future work could research on the adequacy of assuming consumer responsibility. Requirements on passwords settings [6] e.g. specify that the devices cannot be provided with default login data as 'admin' 'admin'. There are, however, no requirements on limiting user input from changing passwords to simple, or possibly even default, passwords. A lack of requirements on consumer behavior as in the example above makes it questionable whether the assumption of consumer responsibility is appropriate. Requirements on user data [6] require the user to read the manual of the device. It is questionable whether consumers read the manuals [19].

Not only the behavior of the consumer could inflict a higher risk on cyber-attacks, but also the willingness and capabilities of manufacturers play a role in this. In fact, according to the Department for Digital, Culture Media and Sport (UK) [4], *"The main disincentives centre around cost and the challenge of justifying time and money when a business's focus is to get their product of 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.

Finally, 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 [17], for several requirements from which some requirements are mentioned in the CSCIoT [6].

7. ACKNOWLEDGEMENTS

I would first like to thank my thesis supervisor Dr. Dipti K. Sarmah MSC for her valuable feedback and supporting my choices while steering me into the right direction. I would also like to thank Barbara Oosterveld for providing justification for the analysed requirements and supporting me with cyber-security concepts.

Table 7: Survey results

No.	Statement	Agree	Neither agree nor disagree	Disagree	Other
1	A Bluetooth-connected toothbrush, connected smoke detectors, door locks and window sensors, and self-driving vehicles should all be categorized into the same security level.	0,00%	0,00%	100,00%	0,00%
2	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	81,25%	12,50 %	6,25%	0,00%
3	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.	93,75%	0,00%	0,00%	6,25%
4	The device shall be able to authorize, monitor and enforce usage restrictions for wireless connectivity.	81,25%	0,00%	18,75%	0,00%
5	Access to wireless devices should be protected by authentication and access control mechanisms.	93,75%	0,00%	0,00%	6,25%
6	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.	68,75%	18,75%	6,25%	6,25%
7	The integrity of sessions shall be protected. Any usage of invalid session IDs shall be rejected.	100,00%	0,00%	0,00%	0,00%
8	The number of concurrent sessions per interface by any given user shall be limited to a configurable number of sessions.	75.00%	12,50 %	12,50 %	0,00%
9	Approval of the user shall be obtained every time before using remote access connections.	81,25%	12,50 %	6,25%	0,00%
10	All remote access connections conducted over the Internet or other publically accessible media shall be authenticated and encrypted.	93,75%	6,25%	0,00%	0,00%
11	The reliability of a backup mechanism shall be verified.	93,75%	6,25%	0,00%	0,00%
12	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.	62,50%	31,25%	0,00%	6,25%
13	The device shall be able to enable and disable the security configuration mode. While disabled, the interface shall prohibit security configurations.	75,00%	12,50 %	12,50 %	0,00%
14	Communication loads shall be managed, e.g. by use of rate limiting, to mitigate the effects of DoS events.	81,25%	12,50 %	0,00%	6,25%
15	There shall be documentation available for the user on secure behaviour of the consumer.	68,75%	18,75%	12,50 %	0,00%
16	There shall be documentation available for the user on retention capabilities of the device for storing sensitive data.	81,25%	12,50 %	6,25%	0,00%
17	There shall be documentation available for the user on data exchange between other devices, such as wireless and remote devices.	75.00%	18,75%	6,25%	0,00%
18	There shall be documentation available for the user on instructions for configuration, operation and termination of remote access applications.	75.00%	25,00%	0,00%	0,00%
19	There shall be documentation available for the user on instructions for proper installation, configuration and update of malware protections mechanisms.	75.00%	18,75%	6,25%	0,00%
20	There shall be documentation available for the user on how security patches for software of the device are evaluated and approved.	50,00%	31,25%	18,75%	0,00%
21	There shall be documentation available on recommended backup procedures.	68,75%	31,25%	0,00%	0,00%
22	The manufacturing company shall have processes on identifying the personnel responsible for security processes required by the standard.	62,50%	25,00%	12,5 %	0,00%
23	The manufacturing company shall have processes on providing an integrity verification mechanism for all scripts, executables and other important files in the device.	81,25%	12,5 %	6,25%	0,00%
24	The manufacturing company shall have processes on identifying and managing security risks within the devices.	93,75%	0,00%	6,25%	0,00%
25	The manufacturing company shall have processes on verifying that the security functions meet the security requirements.	93,75%	0,00%	6,25%	0,00%
26	The manufacturing company shall have processes on testing the effectiveness of the mitigation of threats as identified and validated in the threat model.	81,25%	12,50 %	6,25%	0,00%

8. REFERENCES

[1] Alladi, T., & Choo, K. R. (2020): "*Consumer IoT : Security Vulnerability Case Studies and Solutions*." IEEE Consumer Electronics Magazine, 9 (2), pp 17-25.

[2] Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020): "*Internet of Things : Evolution and Technologies from a Security Perspective*". Sustainable Cities and Society, 54.

[3] Arampatzis A. (2020): *"What Is The ISA/IEC 62443 Framework?*" The State of Security. https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/ Accessed May 3 May, 2020.

[4] 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 20 April, 2020.

[5] European Union Agency for Cybersecurity. (2019): "*Good Practices for Security of IoT"*. Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1 Accessed 20 April, 2020.

[6] European Telecommunications Standards Institute (2020): "*Final draft ETSI Cyber Security for Consumer Internet of Things: Requirements Baseline".* Available at: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf Accessed 10 April 2020.

[7] Greenberg A. (2017): Wired. "*The Reaper Botnet Has Already Infected a Million Networks."* https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/. Accessed May 3, 2020.

[8] Greuter K. (2020): "*Bachelor-Thesis*", Github repository. Available at: https://github.com/Kes-G/Bachelor-thesis

[9] Greuter K. (2020): Survey post, LinkedIn. Available at: https://www.linkedin.com/feed/update/urn:li:activity:6673556891160969216/

[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). 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). 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). 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). Available at: https://webstore.iec.ch/publication/34421

[14] 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 20 april, 2020

[15] Kambourakis, G., Kolias, C., & Stavrou, A. (2017): "*The Mirai Botnet and the IoT Zombie Armies*.", IEEE Military communications conference, pp 267-272.

[16] 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.

[17] National Institute of Standards and Technology (2019): *"Considerations for Managing Internet of Things Cybersecurity and Privacy Risks".* Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

[18] Notra, S., Siddiqi, M., Gharakheili, H. H., Sivaraman, V., & Boreli, R. (2014): *"An Experimental Study of Security and Privacy Risks with Emerging Household Appliances*", IEEE Conference on Communications and Network Security, pp. 79-84.

[19] Novick, D, Ward, K. (2006): "*Why Don't People Read the Manual?"* . The 24th ACM international conference on Design of communication, pp 11-18.

[20] Oosterveld, B. (2020): LinkedIn profile. Available at: https://www.linkedin.com/in/barbaraoosterveld/

[21] Perakovic, D. (2015): "*Analysis of the IoT Impact on Volume of DDoS Attacks"*, 33rd Symposium on New Technologies in Postal and Telecommunication Traffic, pp 295-304.

[22] Prevost, S., Kettani, H. (2019): "*On Data Privacy in Modern Personal Vehicles"*, The 4th International Conference On Big Data and Internet of Things, pp 1-4.

[23] Tewari, A., Gupta, B. B. (2020*): "Security , Privacy and Trust of Different Layers in Internet-of-Things (IoTs) Framework*", Future Generation Computer Systems, 108, pp 909–920.

[24] UL cybersecurity (2019): *"IoT Security Top 20 Design Principles*" Available at: https://ctech.ul.com/wp-content/uploads/2015/01/UL-IoT-Security-Top-20-Design-Principles-whitepaper1.pdf

[25] Vesanen, J. (2019): "*" I Know When You Brush Your Teeth " - Cyber Security on Personal Medical Devices",* Thesis from Metropolia University of Applied Sciences. Available at: http://urn.fi/URN:NBN:fi:amk-201901301748

[26] Ye, C., Indra, P. P., Aspinall, D. (2019): "*Retrofitting Security and Privacy Measures to Smart Home Devices"*, Sixth International Conference on Internet of Things: Systems, Management and Security *(IOTSMS)*, pp 283-290.

[27] Zekeriya, M., Das, R. (2020): *"Cyber-security on Smart Grid : Threats and Potential Solutions",* Computer Networks, 169, pp 1-8.