Understanding the Knowledge Gap: How Security Awareness Influences the Adoption of Industrial IoT

Verena Schrama*, Carlo H. Gañán*, Doris Aschenbrenner*, Mark de Reuver*, Kevin Borgolte†, Tobias Fiebig*
*TU Delft
V.C.M.Schrama@student.tudelft.nl, {C.HernandezGanan,D.Aschenbrenner,G.A.deReuver,T.Fiebig}@tudelft.nl
†Princeton University
kevin@iseclab.org

***Abstract*—The Internet-of-Things is no longer confined to end-users and private homes. Industrial IoT (IIoT) is supposed to improve industrial processes and make them more efficient. However, IIoT technologies may also pose (significant) security threats. Therefore, it is important to understand the balance between security awareness and willingness to adopt IIoT among manufacturing companies.**

In this paper, we explore companies' willingness to adopt IIoT, their willingness to participate in trainings on IIoT, and contrast this to their current security awareness. We investigate classes of companies through latent class analysis based on a survey of over 130 industrial firms. We collected this sample from the Netherlands, as earlier research demonstrated that the Netherlands are generally comparable with other western countries in terms of technology adoption, while focusing on a single country reduces other potential noise effects.

We find that the class of companies most susceptible and willingness to participate in educational awareness programs is comprised of companies with a high intention to adopt IIoT technologies, but with lowest awareness of their security threats, that is, companies that may be impacted the most by insecure IIoT devices. In contrast, the companies of the other class are highly aware of risks associated with IIoT, but also averse to adopting IIoT for their production processes. Furthermore, we find that smaller companies are more likely to be risk-aware and IIoT averse, while larger companies embrace IIoT while being risk unaware. The classes that we identified are robust to company age, market segment, current information and communication technology usage, and degree of production focus. Our findings highlight the need for policy makers to target their security awareness programs on adopting IIoT technologies to "smarten up" industrial processes to specific company classes, which increases the educational efforts' efficacies. Otherwise, an apparent information imbalance skews the economic incentive model behind IIoT adoption, potentially leading to a future of dramatic IIoT security incidents.

I. Introduction

The industrial Internet of Things (IIoT) has revealed new ways of reducing costs while creating added value within industrial processes, by increasing connectivity and tracking activity across supply chains. Based on IoT technologies, the IIoT combines the benefits of machine learning, sensor data, and machine-to-machine (M2M) communications that have been present in industrial areas for years. However, while IIoT creates opportunities for the industry to transform into a smart industry, it also comes with risks. Conventionally, industrial companies are seen as conservative in adopting new technologies, and prior work identified risks and challenges that are further slowing down IIoT adoption [69, 71, 76, 83]. Security is always a major concern, and one of the largest perceived risks of IIoT are security errors caused by humans [29].

In this paper, we aim to gain a solid understanding of how companies cluster based on the IIoT risk awareness among *decision makers* in industrial companies, and how risk awareness relates to IIoT adoption willingness. We developed a questionnaire that 139 industrial companies across different sectors participated in. To reduce noise due to cultural differences [36], we sampled these companies from a single country, the Netherlands, which is a typical Type I culture in terms of social factors influencing technology adoption, comparable to the United States, Australia, or Germany [51].

Focusing on the industrial production process, we measure companies' willingness to adopt IIoT technologies based on their awareness and risk perception. We then extract response patterns to categorize industrial companies into groups using three indicators: *(i)* willingness to adopt IIoT, *(ii)* risk awareness, and *(iii)* willingness to participate in training. Leveraging Latent Class Analysis (LCA), we identify two homogeneous groups of companies.

Our groups differ significantly in willingness to adopt IIoT, risk awareness, and the willingness to participate in educational programs. The first group describes companies that are willing to adopt IIoT, willing to participate in training, but unaware of the security risks IIoT can pose. The second group is effectively the polar opposite: unwilling to adopt IIoT, and unwilling to participate in training, yet, aware of the security risks. The two homogeneous groups are robust to demographic properties of the companies, that is, company type and company age. We find that company size is a predictor for class membership, with smaller companies being more risk-aware and IIoT averse, while larger companies are less risk aware and more willing to adopt IIoT. This allows us to better tailor educational efforts to address this information imbalance, leading to a distortion of the underlying incentive model: Small and medium sized enterprises should receive more training on *mitigating* risks of IIoT, while larger companies should receive training on *identifying* risks of IIoT.

In this paper, we make the following contributions:

- We conduct the first survey on the interplay between IIoT risk awareness and willingness to adopt IIoT.

- We identify a divide between willingness to adopt and security awareness: Less security aware organizations are more willing to adopt IIoT technologies.
- We identify the most critical action-items with regard to IIoT security training for industrial companies.

Following, we first define IIoT and provide background information on the involved security challenges (Section II). Subsequently, we describe our methodology, including the survey design and validations (Section III). We then detail our questionnaire dissemination and report, and discuss the results of our analysis (Section IV). Finally, we compare to related work (Section V), report on the limitations of our study (Section VI), and conclude (Section VII).

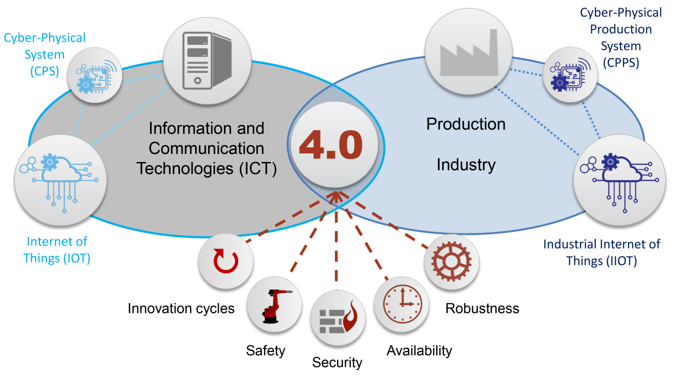

Cyber-Physical System (CPS)
Information and Communication Technologies (ICT)
4.0
Production Industry
Cyber-Physical Production System (CPPS)
Internet of Things (IOT)
Industrial Internet of Things (IIOT)
Innovation cycles
Safety
Security
Availability
Robustness

Figure 1: Terminology Overview within "Industry 4.0"

II. Industrial Internet of Things

The general security challenges that Internet-connected devices face are fairly well known, but over eighty percent (80%) of European companies still experienced one or more incidents in 2016 [62], possibly because approximately sixty-nine percent (69%) of European companies have no or only basic understanding of their security exposure [42]. Nonetheless, eighty-one percent (81%) of companies declare IoT to be critical to at least part of their businesses [63], with only thirty-nine percent (39%) being confident that they have "sufficient digital trust –security, privacy and data ethics– into their adoption of IoT."

While the topic of security itself, including IoT, is increasingly receiving the necessary political attention, the current transition of production industry toward "Industry 4.0" introduces a variety of factors that can lead to new vulnerabilities. Fortunately, at latest since the Stuxnet malware attacks [49], the possibility of Internet-based attacks on industrial infrastructure has also begun to attract the required attention.

Currently, the automation industry is changing, with the goal to transfer advancements from the information and communication technology to the production industry, to increase its efficiency. However, industrial plants and production machines are different from the ICT sector: they are high investment and typically follow slower innovation cycles, often decades, which stands in stark contrast to rapidly changing consumer goods, like smartphones. This means that the production ecosystem uses hardware and software for longer periods of time, which can lead to security issues if devices are being deprecated by manufactures and receive no more support. The security problem is further amplified because industrial machines are, by design, utilizing intellectual property, which can lead to product piracy, and also because of Internet-wide scanning and search engines, like Shodan [8], which can allow easy discovery of vulnerable industrial control systems.

The general goal of the "Industry 4.0" movement is more than the mere adoption of existing technology (Figure 1). In fact, this is driven by necessity because industrial companies are heavily regulated and have different and more stringent requirements: machines can injure human workers, so there are significant legal safety requirements. Industrial facilities also often run seven days a week, 24 hours a day, and failure-induced stops are generally very expensive. For example, a failure in the production process for an automotive company, like General Motors, that forces a one day stop would result in over 8,000 cars not being produced. Considering actual failure-inducing attacks, one can only imagine the potential impact on critical infrastructure, like water treatment plants. Already, forty percent (40%) of organizations using robotics or automation already fear a disruption of operations due to an attack [63]. Finally, industrial robustness requirements are very different than those for consumer goods due to heat, dirt, movement, etc., and one of the main promises of "Industry 4.0" and IIoT is "to bring the key characteristics of the web – modularity, abstraction, software above the level of a single device – to demanding physical settings [...]" [9].

III. Methodology

Following, we discuss the design of our questionnaire, its measurement goals, and its operationalization.

A. *Questionnaire*

We assess the willingness to adopt IIoT, the companies' IIoT risk awareness, and the willingness to participate in corresponding training through a questionnaire that we developed specifically for industrial companies across different sectors. For reference, the entire questionnaire is included as Appendix C.

1) *Target Group*

For our study, we focus on the C-level, i.e., the decision makers, in companies that engage in "commercial production," that is, companies whose main objective is continuity and profit from the production and sale of goods [35]. Specifically, we focus on industrial companies belonging to category C, i.e., manufacturing, of the Standard Industrial Classification (SIC) [84].

It is important that the respondents to our questionnaire are involved in decision-making processes in regard to IIoT. While engineers might have a different perspective than the C-level of a company, this will ultimately not reflect the *actual* decisions being taken, unless the management level shares this perspective. Identifying, whether there is a divide in technical understanding and adoption willingness between management and engineering is an alternative avenue of investigation, which we consider out-of-scope for the work at hand. Therefore, we disseminate questionnaire to individuals who are involved in the design and organization of the production process, both from a technical point of view and from the side of decision-making (for example, CEOs, other C-level executives, the executives' staff, technical managers, and technical directors).

The target group also had a high influence on our questionnaire design: To prevent survey fatigue, and ensure that the managerial target group—which might lack *in-depth* knowledge of security techniques—is able to provide meaningful responses, we opted for a comparatively simple design. While we acknowledge that the missing technical depth would be an issue for a survey of technical staff, in this paper, we aim to understand the *decision making processes around IIoT security*.

Furthermore, since the nationality of a company may be a confounding factor, we ask respondents about the location of their company's headquarter. The headquarter's location is important because it is often at the core of the decision-making process, including decisions on adopting IIoT technologies or participating in education-related activities.

2) Reliability and Validity

Following current best practices, to increase response rate and safeguard the reliability of our questionnaire, we conduct our survey anonymously, keep it brief, use closed questions and propositions, and define IIoT to provide a common foundation. To ensure that the participants actually have a sufficient and meaningful understanding of IIoT, we ask them to briefly define IIoT in a free-text-field, and matched their understanding to that presented in Section II. We only include respondents that provided a matching definition in our analysis.

Furthermore, we develop multiple questions to cover the complex concept in our study, like IIoT risk awareness and willingness to participate in training, which allows assessing validity and reliability. We can ask about a company's willingness to adopt IIoT and the company's properties, like type, size, and age, directly, which is why we measure each with one question.

In particular, we leverage a five-point Likert scale to provide a range in which a respondent can find an appropriate answer. We limit the influence of accidental circumstances, such as fatigue and accuracy, which may otherwise influence our results' reliability [65] through the following steps: We pay special attention to use concrete, specific, short, and simple questions and statements, so that respondents will interpret them consistently, and we provide explanations and examples for difficult, broad or new concepts, such as IIoT technology, education, and awareness activities.

Finally, we verify the reliability of our questionnaire through a Cronbach's alpha test (Section IV).

3) Pilot

To ensure the quality of our questionnaire, three experts in the field of IIoT technologies examined and analyzed the questionnaire. We approached the experts because IIoT is a relatively new and particularly technical concept given its industrial focus. The experts validated that all questions, examples, and explanations are technically correct and practically relevant, that is, relevant to industrial companies. Based on their findings, we adjusted the technical description and practical examples in the introduction of the questionnaire and Question 1.

We then asked three companies to complete the questionnaire and provide feedback, so that we can validate that the questionnaire is understandable, clear and relevant to the target group. Piloting the questionnaire with these companies also allowed us to verify that the questions leave no room for erroneous interpretations, and provide an estimated time of completion for the entire questionnaire, which helps to set respondents' expectations in terms of time commitment and it can counter fatigue. The pilot participants' feedback indicated that they understood the questions and propositions and answer them accordingly, and that they are relevant to their business.

B. Operationalization

We focus on three core concepts in our study: *(i)* the willingness to adopt IIoT, *(ii)* IIoT risk awareness, and *(iii)* the willingness to participate in IIoT-relevant training. Following, we describe how we translate these concepts into measurables that we can analyze. We provide an overview of the questionnaire's structure and its variables, and we describe the operationalization for the explanatory variables (covariates), the response variables, and the control variable. Response variables are the concepts that we wish to explain with our classes, that is, intention to adopt IIoT, IIoT risk awareness, and willingness to participate in IIoT-relevant training. Covariates are concepts that we expect to influence the membership of the classes, that is, company type, size and age. We use three explanatory variables, three response variables, and one control variable (Table I).

We use company type because prior studies show that IT maturity differs per industry sector [33]. For instance, companies in the IT sector have higher readiness and are more willing to adopt new technologies [59]. For IoT specifically, the level of adoption and maturity differs strongly per industry; for instance, it is higher in process industries [33], like agriculture [17]. The willingness to engage in training has also been found to strongly differ between industry sectors [32]. Company size is another variable of interest, although the direction of the relationship with innovation potential is not evident from existing literature. One stream of literature considers size positively related to innovation potential [16, 80] and adoption of IoT in particular [75]. The explanation is that small companies lack the resources needed to engage in innovation and adoption of technologies [34], and consequently invest less in IT innovations per employee [11]. Besides willingness to adopt, small companies more often lack the resources and expertise to secure information systems or to understand the importance of doing so [31]. While all this suggests a positive relation between size and adoption of IoT, other theorizations would suggest a negative relation.

Table I: Variables, Types, and Corresponding Questions

Variable	Type	Questions
Company Age	Explanatory	9
Company Size	Explanatory	10
Company Type	Explanatory	11, 12, 13
Willingness to Adopt IIoT Technology	Response	1, 2
IIoT Risk Awareness	Response	3
Willingness to Participate in Training	Response	4, 5, 6, 7
Headquarter Location	Control	8

Large firms are less flexible, and are therefore less willing to adopt new technologies quickly [37, 53]. Empirical studies support that large organizations are hindered by inertia and fragmented legacy systems, which complicates the adoption of new Internet-related technologies [88]. Company size is generally considered to be positively related to willingness to engage in training [43], although this effect becomes less strong after a certain threshold of number of employees [45]. Older companies have typically more resources, but are less flexible in adopting new routines. Company age is relevant since older companies have more time to build up resources, for instance for security and training [78]. On the other hand, existing resources, routines and systems may make older companies less likely to adopt new technologies [54].

1) Explanatory Variables

The explanatory variables in our analysis correspond to the variables that describe the classes: *(i)* company type, *(ii)* company size, and *(iii)* company age. The variables are also called covariates, and they are predictors of class membership, that is, their value indicates the class a company is statistically expected to be part of given its business properties [87].

Company Type

The type of company is defined by three terms: *(i)* the market in which it is active (Question 11; business to business, business to consumer, or both), *(ii)* whether the company belongs to the information and communications technology (ICT) sector (Question 12; yes or no), and *(iii)* the type of goods the company produces (Question 13; materials or end-user products). The questions are categorical, with Question 12 and 13 also being dichotomous.

Company Size

We measure a company's size in the number of employees. The corresponding question (Question 10) is ordinal because a large proportion of respondents may not know the exact number of employees. We follow Eurostat's definition [24, 26]: micro companies have fewer than 10 employees; small companies have more than 10, but less than 50 employees; medium-sized companies have more than 50, but less than 250 employees; and large companies have 250 or more employees.

Company Age

Similar to the company size, we do not expect that respondents know the exact age of their company. Therefore, we measure the company's age through an ordinal variable of different age groups (Question 9). We derive the corresponding age groups from prior research by the European Commission [25]: start-ups (younger than five years), companies (with an age between six and 11 years), and senior companies (older than 11 years).

2) Response Variables

The response variables in our study concern themselves with what we want to measure: *(i)* willingness to adopt IIoT, *(ii)* risk awareness, and *(iii)* willingness to participate in training.

Willingness to Adopt IIoT

The willingness to adopt IIoT is the intention of a company to incorporate (more) IIoT technologies in their production processes in the next year. We measure the willingness to adopt directly through a dichotomous question (yes or no, Question 2), similar to how Fosso Wamba et al. [30] measured the willingness of industrial companies to adopt radio-frequency identification (RFID) chips into their production processes. Additionally, we pose an open question to respondents about their current IIoT usage (Question 1), which increases reliability on Question 2 and it might address social desirability bias:[1] We can compare the answer to Question 1 to our definition of IIoT, and if they do not match sufficiently well, then we exclude the response to Question 2 from our analysis.

IIoT Risk Awareness

The concept of IIoT risk awareness is broad because awareness can relate to different aspects of adopting IIoT, which makes it challenging to measure it accurately in its entirety. Therefore, we limit the concept to the areas of security risk, similar to Drevin et al. [21]. We focus on the following areas that are particularly relevant to security risk awareness: knowledge of the existing production processes that rely on legacy computer systems, awareness of the risks arising from linking legacy computer systems to IoT technologies, and risks associated with (a lack of) systematic computer system updates. We measure these focus areas through nine statements (Question 3), which we formulated based on prior work [30], i.e., inspired by the general concepts of relative advantage, complexity, compatibility, and the competitive environment, interviewing employees of the Dutch Ministry of Economic Affairs and the Smart Industry program office, and interviewing IIoT experts (who later also verified the accuracy and representativeness of the statements). As a result, the statements are closely aligned to the errors most frequently encountered with IIoT technologies, and it ensures that they are relevant to measuring awareness as a predictor. Furthermore, we incorporate the notions of inattention, imprudence, and lack of knowledge to paint a complete picture.

It is important to note that the statements do not measure how secure a company's IIoT technology actually is, but that they concentrate on the stage that precedes

[1] A company might want to appear "hip" by claiming to have adopted IIoT in their production process already, while not having done so.

IIoT adoption. Specifically, we measure if a company is aware of the risks associated of managing and operating production processes linked with IIoT technology.

We assess each statement on a five-point Likert scale from 1. I strongly disagree, to 2. I disagree, to 3. I neither agree nor disagree, to 4. I agree, and to 5. I strongly agree. We use this common scale based on prior work that measured information security awareness at universities [48, 82].

Willingness to Participate in Training

We describe the willingness to participate in training terms of four factors, which we believe are exhaustive. We follow the idea from theory of planned behavior by Ajzen, that is, that the likelihood to engage in specific behavior depends on attitudes and perceived behavioral control [2]. Whereas attitudes are related to the desires and motivations of people, perceived behavioral control is related to the extent to which they feel capable of engaging in the desired behavior. For the desires to participate, we focus on motivations, which have more generally been shown to affect the success rates of educational activities [5]. For the capabilities to participate, we focus on availability of time [85], financial means [70], and ability to learn [20]. For each factor, we formulate a corresponding statement:

- time commitment (Question 4)
- financial investment (Question 5)
- motivation (Question 6)
- ability to learn (Question 7)

We measure each statement on a five-point Likert scale, based on prior research investigating the willingness of companies to participate in educational activities [3, 23, 56]. Each statement was phrased carefully, based on prior work by Redmiles et al. [65], to ensure that it accurately measures the corresponding factor.

In terms of time commitment, respondents indicated on a five-point Likert scale how many hours per week they want to commit to training (zero, one, two, three, or four hours). This scale prevents respondents from interpreting the time commitment differently, leading to a more accurate measurement. We limited the range for education activities to four hours per week because companies are unlikely to commit more than half a day per week for training activities per employee. Zero training hours indicate being unwilling to commit any time to educational activities. Accordingly, a low value on the Likert scale corresponds to a low willingness to engage in training activities, while a high value corresponds to high willingness.

We measure the remaining three factors on a Likert-scale from 1. I strongly disagree, to 2. I disagree, to 3. I neither agree nor disagree, to 4. I agree, to 5. I strongly agree. Therefore, a low value corresponds to a high willingness to participate in educational awareness programs, while a high value corresponds to a low willingness to engage.

3) *Control Variable and Knowledge Verification*

For our questionnaire, the control variable is the location of the companies' headquarters (Question 8). It allows us to test if companies located abroad differ significantly from companies based in the Netherlands. They may differ because company-wide decisions, like adopting IIoT or participating in training activities, are often made at the headquarter. However, if there is no significant difference in willingness to adopt IIoT, IIoT risk awareness, and willingness to participate in training, then we can include responses by foreign companies in our analysis.

Furthermore, we asked all participants to describe what they understand under the term "Industrial IoT." We used this question to: (i) verify whether the participants are knowledgeable on the topic of IIoT, (ii) ensure that participants definition of IIoT overlaps with ours, and (iii) identify invalid responses.

IV. Results

The goal of our research is to provide a foundation to better target educational awareness programs on IIoT for industrial companies. To understand how we can target them effectively, we disseminated our questionnaire (Section III) to industrial companies, collect data, and analyze it. For our analysis, we first we group companies through Principal Component Analysis (Appendix A1) with similar IIoT-related behavior (Section III-B2), and, we then analyze these groups via Latent Class Analysis (Appendix A2).

A. *Recruitment and Ethics*

We conducted our survey through SurveyMonkey [81]. We disseminated our questionnaire through the "Smart Industry" website [72], and their social media [74], including LinkedIn [73]. We also sent a reminder about our questionnaire through the "Smart Industry" email newsletter on June, 7 2018. Our dissemination efforts reached approximately 2,200 companies. As we aim to generalize to classes of companies, and not to the population of all smart industry companies, we chose to focus on one *representative* western country, the Netherlands [51]. Including multiple countries would introduce heterogeneity, for example, based on language differences or translations of the questionnaire [36], which, in turn, makes it *substantially* more difficult to interpret the classes found through LCA [22].

Concerning the ethical dimension of our work, prior to conducting the study, we completed a self-assessment form supplied by our local Human Research Ethics Council (IRB), which is used to assess the necessity of IRB approval prior a dedicated ethics review. IRB granted approval without a dedicated ethics review because we request explicit informed consent, do not collect Personally Identifiable Information (PII) of participants, and do not collect data that would make the employer of respondents identifiable. Our informed consent and privacy notice can be found in Appendix C.

B. *Survey Responses*

1) *Sample size*

We received 139 responses, resulting in a relatively low response rate (6.32%). However, this is sufficient for our

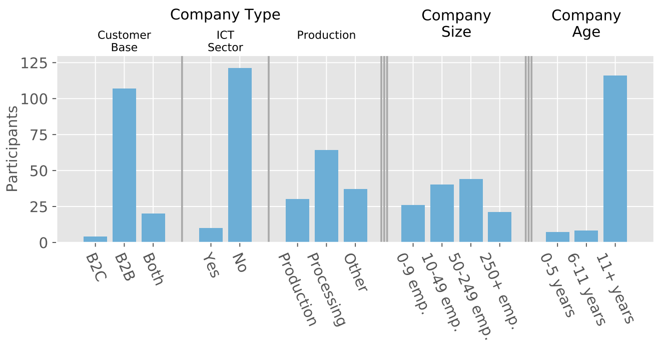


Figure 2: Overview of our Respondents' Demographics

purpose, as Dziak et al. recommend a sample size around $N = 120$ for medium effect sizes, and two class models, which is what we mainly use in our study [22]. In fact, combined with the qualitative answers, this already allows for observations on the state of IIoT technologies in industrial companies: IIoT appears to be a concept that is currently unfamiliar to Dutch industrial companies. Based on the answers respondents gave to the *invitation* to participate, it appears that IIoT is a deterrent. For example, one invitee responded with "I do not know what IIoT is." Frequently, companies responded that they are not yet using IIoT technologies (74.8%). However, current IIoT usage was not a requirement to participate (Section III-A1). Based on these responses, we believe that we are in the early stages of conducting research on the use of IIoT. Therefore, our research provides an initial evaluation on *where and how to focus* educational awareness initiatives.

2) *Validation*

Following data collection, we verified that all responses are correct and complete. Furthermore, we verified that the responses to our canary question on defining IIoT were correct (Section III). All respondents that indicated that they use IIoT technologies (25.2% of all respondents) correctly defined IIoT technologies. In one case, we had to correct a response from "Yes" to "No," as the participant described an application of IIoT that was not part of the production process (which we focus on), but it was used to improve the company's operational management. Concerning completeness, eight surveys were incomplete and we rejected them (listwise deletion), resulting in 131 responses that we can analyze.

Figure 2 shows an initial overview of our respondents' demographics, and we provide more detail when we discuss our results' generalization later (Section IV-B3).

3) *External Validity*

We utilize industrial companies in the Netherlands as so called "convenience sample" for our survey, due to the wide availability of open data to support our survey [13] and existing contacts to industry organizations useful for dissemination (Section IV). While this is common practice in behavioral sciences and awareness research, it also means that we have to validate whether our results generalize [77]. Therefore, we first validate whether our sample generalizes, that is, whether it has external validity [61] within its greater population (the Netherlands). Subsequently, we use our control variable (Section III-B3) to test whether there are significant differences between companies from the Netherlands and outside of it.

C. *Representativeness*

We validate our sample population of $N = 131$ against data published by the national statistics institute of the Netherlands for the second quarter of 2018 [13]. At this time, the Netherlands had a total of 63,425 industrial companies. For a tabular comparison between the general population and our sample, please see Appendix B.

Our sample differs from the population distribution in terms of company size and company age: the general population is dominated by small (0-9 employees) companies, while our sample shows a normal distribution. Concerning company age, our sample is dominated by older companies (11 years or older), while the population is normally distributed.

Unlike the general population, our sample is not dominated by the producing sector, and our sample diverges toward companies operating in the B2B sector. We can, however, attribute these divergences to our focus on *Industrial* IoT: Heavy industries and large-scale processing and production companies are generally more established B2B companies, that is, they are older and larger than disruptive B2C startups that are often seen in the IT sector. Indeed, end-users are simply far less likely to buy intermediate industrial products. Furthermore, companies may have not yet seriously considered IIoT, preventing them from participating in our study. Therefore, in some years time, a comparable future study may yield a more diverse sample and a higher response rate, simply because it is plausible that IIoT technologies play a more dominant role then.

We conclude that while our sample diverges in some key-aspects from the *general* population, these differences are based on a high portion of industrial companies in our sample. In fact, our analysis shows that more than a quarter (25.2%) of our participants currently already use *Industrial* IoT technologies in the production process. Furthermore, an additional 40.5% of companies in our sample plan to adopt *Industrial* IoT technologies included in the production process within the next year. Therefore, we conclude that our sample has sufficient external validity for our study.

D. *Principal Component Analysis*

We perform Principal Component Analysis (PCA) to check whether our scales measure the corresponding concept. The PCA's results give an indication of the validity of the measuring scale and show whether the items included cover the loading of the concept [6]. Specifically, we perform PCA to identify the items that load on the same component, which allows us to then create variables that better fit the data. The formation of the new variables takes into account that some items are more important and explain a larger part of the component than the other items. These items have a higher weight when calculating the factor score.

Before we perform PCA, we determine with the Kaiser-Meyer-Olkin (KMO) test [1, 40] if we can apply PCA to our sample, and given a KMO value of 0.734, we can use PCA to investigate the four variables we focus on. Furthermore, Barlett's test is significant, showing that there is a high correlation between the items, which is also necessary for PCA [28]. We then perform PCA twice: First, on the four questionnaire items that are related to willingness to receive training, based on our scale (Section III-B2). Second, for the part of the questionnaire that measures a company's level of IIoT risk awareness.

Consistent with our expectations, the analysis resulted in one component with an eigenvalue greater than one. This means, more generally, that the latent concept simplifies the structure of the original data, while an eigenvalue less than one would imply that the component explains less than the original items themselves. Therefore, only one component with an eigenvalue greater than one indicates that a one-factor solution adequately represents the four questionnaire items related to the willingness to participate in training. Importantly, all component loadings are greater than 0.5 and the communalities of the four items are greater than 0.25, indicating sufficient convergent validity. The items' loadings are sufficiently high on the component and the component explains a large part of the variance. This means that the we can combine the four items (Question 4 through 7) to one variable that covers the concept of willingness to receive training. To this end, a factor score is automatically calculated by SPSS based on the factor loadings [28].

We then performed a PCA on the nine items that are related to the level IIoT risk awareness of an industrial company (Section III-B2). Our sample is suitable for PCA regarding the nine propositions based on a KMO value of 0.671. The Barlett test is also significant, which indicates a sufficiently high correlation between the items to apply PCA. A first PCA resulted in three components with an eigenvalue greater than one. However, after using a Varimax rotation of the factor structure, only one item's (Table II, No. 6) loading is sufficiently high on the third component. As the item does not relate to the other eight items, we cannot use it to measure the same concept, which is why we remove it from the data set. The KMO value of the remaining variables increased to 0.673 as a result. Barlett's test remains significant. A Varimax rotation uncovers two interesting components with eigenvalues exceeding one, from which we can infer that awareness of risks is composed of two underlying dimensions. The component loadings and communalities suggest that the items that belong to the first dimension relate to the awareness of the current situation and of the required actions to prevent the occurrence of IIoT risks in the production process. We label this IIoT risk awareness as "awareness of managing the production process" (*awarenessPP*). The second dimension is composed of items that relate to statements about the risks related to combining legacy systems in the production process with IIoT technologies. We refer to this new dimension as "awareness of the vulnerability of connecting legacy systems to the Internet" (*awarenessLegInt*). SPSS automatically calculates the factor scores for both dimensions of risk awareness based on the PCA's components. Together, these two variables describe the IIoT risk awareness of industrial companies.

1) Reliability Scale Constructions

Because PCA provides insight into the extent to which the selected items are related to the latent concepts, the analysis says something about the validity of the measuring instrument. We perform a Cronbach alpha test for each variable found with PCA to measure the reliability of our scale constructions, that is, the inter-item reliability (i.e., whether you would get similar responses when slightly changing a questionnaire's item's wording). The items that, according to the PCA, conceptualize *awarenessPP* have $\alpha = 0.803$, the ones that describe *awarenessLegInt*, have $\alpha = 0.732$, and the items that form willingness to receive training have $\alpha = 0.785$. All α values are higher than 0.7, indicating adequate reliability. Therefore, based on the Cronbach's alpha test, there is sufficient coherence between the items for a reliable scale construction [7].

E. Latent Class Analysis

We perform Latent Class Analysis (LCA) to distinguish homogeneous groups of industrial companies. Next, we describe how we selected the latent classes, to what extent they can be generalized, and how we interpreted them.

We set up six class models in LatendGold 5.1 based on the three indicators (Section III-B2): willingness to adopt IIoT, risk awareness, and willingness to participate in training. We generate a series of class solutions, each one containing one class more than the previous solution. We compare the solutions on five criteria.

1) Criteria

a) Bayesian Information Criterion: First, we compare the models on their Bayesian Information Criterion (BIC) values, which is a criterion for model selection in which a balance is made between the model fit and its parsimony [27]. The model with the lowest value is the preferred model [57], and, more generally, a low value indicates that the model has more optimal balance between the model fit and parsimony.[2] The model with two classes has the lowest BIC value (Table III) and it is preferred over solutions with more classes, for which the BIC value increases, thus, indicating these models are worse solutions [15].

b) Akaike Information Criterion: Second, we investigate the models' Akaike Information Criterion (AIC). The AIC value determines how well a statistical model fits to the data, that is, it measures the amount of lost information (the risk of overfitting and underfitting). The lower a model's AIC value, the better it fits compared to the other models. In contrast to the BIC value, the AIC value decreases as we add more classes until sixth class, with which it increases (Table III). Therefore,

[2] Parsimony refers to choosing simple explanations of a phenomenon over complex explanations. In statistical analysis, this means that the model should be as simple as possible and that the explanatory variables should only be included if they contribute to the explanatory power of the model [15].

Table II: Responses to the likert scaled security awareness questions; strong disagreement (-2) to strong agreement (2).

No.	Statement	$+2$	$+1$	± 0	-1	-2	Plot (%)
1	I am aware for all systems in my production process whether they are connected to the internet or not.	3	5	23	56	44	
2	I am aware for all systems in my production process whether these are still supported by the supplier or by my own company (and therefore are or are not legacy systems).	1	13	38	51	28	
3	Legacy systems in a production process are not more vulnerable to malfunctions (for example, unintentional errors of own employees or external support staff) than other systems.	11	33	44	38	5	
4	Legacy systems in a production process are not more vulnerable to malicious activities (eg hacks by criminals) than other systems.	16	37	43	28	7	
5	I am aware for all systems and associated software in my company's production process whether they would be equipped for securely linking them to the internet.	2	30	35	52	12	
6	When I run a system update, I have no good idea how it affects my production process.	4	35	38	47	7	
7	I know which party is responsible for providing system updates for the systems of my production process (connected to the Internet).	0	9	26	73	23	
8	I know which party is responsible for performing system updates for the systems of my production process (connected to the Internet).	1	5	33	68	24	
9	I know what to do in case the supplier of systems of the production process is no longer able to deliver system updates.	4	30	47	43	7	

Table III: Overview of the Bayesian Information Criterion (BIC) values, Akaike Information Criterion (AIC) values, Proportion of Classification Errors (PCE), Bivariate Residuals (BVRs), which is significant for BVRs > 3.84, and the Likelihood Ratio Statistics (L2) to a one-class model for models up to six classes. Recommended solutions are bold.

No. Classes	BIC	AIC	PCE	BVRs (> 3.84)	BVRs (> 1)	L^2 reduction
1	1323.2047	1303.0784	0.0000	2	5	-
2	**1318.7212**	1275.5933	**0.1065**	**0**	1	**35%**
3	1329.6380	1263.5085	0.0358	**0**	4	16%
4	1349.3997	1260.2686	**0.0333**	**0**	3	20%
5	1367.0953	**1254.9626**	0.1371	**0**	**0**	25%
6	1392.4455	1257.3112	0.1740	**0**	**0**	28%

the model with five classes is the best fitting model according to AIC.

c) Proportion of Classification Errors: Third, we analyze the proportion of classification errors (PCE), which indicates the probability that, given a certain model, a respondent will be assigned to an incorrect class. Similar to AIC, the proportion of classification error also provides an indication of how well the model fits in comparison with the other models. Given the proportions (Table III), the four class model has the fewest wrong classifications.

d) Bivariate Residuals: Fourth, we examine the bivariate residuals (BVRs). The BVRs measure the proportion of the observed association between two variables that the model can reproduce [87]. Simply put, the relation between the indicator variables (e.g., the willingness to participate in training and IIoT adoption intention) should be explained by the latent class variables resulting from the model. The BVRs indicate the dependencies between the indicator variables that are not explained by the model, and, thus, their values should be small for a well-fitting model. In fact, they should be lower or equal to one [87], or the model should explain bivariate associations between indicators at least 85% of the time. A significant BVR value (> 3.84) refers to bivariate correlations between variables that the model can not adequately explain [87], and, hence, does not meet the local independence assumption. A model that has no significant BVR values fits the data well. In turn, the BVRs helps to identify bivariate relationships that cannot be explained by the model, and they can pinpoint the model that is the better solution. This means that, depending on the underlying latent class variable, there are no associations between the remaining indicators. Compared to the one-class solution, models with more classes have no significant BVR values (Table III), that is, each model with two or more classes meets the independence assumption. When one class is added to the two-class model, all BVR values become less than one, except one, which shows that the two-class model is a better model than the one-class model. Introducing additional classes, to three or four classes total, some BVR values are slightly higher than one, but they all remain significant. On the other hand, the BVRs of the five-class and six-class model are all lower than one, and, thus, they are the best models measured by their BVRs.

e) Likelihood Ratio Statistic: The final criterion that we use is the reduction in the likelihood ratio statistic (L2). L2 represents the proportion of the observed relationships between the indicators that the model cannot explain. The reduction in L2 represents the extent to which the original association between the indicators can be explained by adding a class. Therefore, the reduction in L2 is a model performance measure and it provides insight into what can be explained by adding a class. A high reduction value indicates that adding a class increases the explanation of the association between indicators. The reduction in L2 is expressed by two times the increase of the log-likelihood (LL) value associated with the model [87]. The L2 value of the two-class model has the largest decrease compared to the one-class model. Thirty-five percent (35%)

of the coherence that exists between indicators in the one-class model is created by adding an extra class (Table III). The models with multiple classes explain relatively less of the association between indicators. Overall, based on L2, the best model is the two-class model.

f) Criteria Summary: Overall, based on the BIC value and the decrease in L2, we can justify choosing the two-class model. All models meet the independence assumption according to the BVR values, thus, the criterion does not constitute an obstacle. However, the BVR values of the five-class and six-class models are below one, which indicates that a model with five or six classes reproduces a larger proportion of the observed association between two indicators than a model with two classes. Since the BIC values of these model solutions are considerably higher than those of the two-class model, the two-class model is preferable because it has a better balance between the model fit and parsimony. Generally, the BIC values tend toward the selection of simple models, while AIC values direct toward selecting complex models [28]. Therefore, we may limit ourselves to an overly simplistic interpretation and we might overlook relevant knowledge if we select the model with two classes based on the BIC value. Indeed, the AIC value provides a contradictory picture of the model that has the best fit compared to the BIC value: it recommends five classes instead of two. On the other hand, the proportion classification errors are minimal for a model with four classes. Fortunately, the four-class model is a compromise between the best models based on the BIC and the AIC values, and it satisfies independence. Therefore, in addition to an interpretation of the two-class model, we also examine whether a distribution of companies over four classes yields additional insight.

2) Significant Indicators

Before we investigate the individual classes, we check for significance of the underlying indicators. The Wald test shows if the indicators are statistically significant [87]. If the indicator's Wald value is not significant, then it does not cause a significant difference between the classes found. In this scenario, it is unlikely that there is a relationship between the latent class and the specific indicator in the population. The test's null hypothesis is that all parameters related to the indicator are equal to zero in the population. The alternative hypothesis states that at least one parameter is not equal to zero in the population. We accept the null hypothesis if $p > 0.05$. For a nominal variable, both the Wald test value and the corresponding p-value relate to all the categories of that variable [87]. The test results show that only *awarenessPP* ($p = 0.16$) is not a significant indicator for the two-class model. Based on these results, we infer that the class variables and *awarenessPP* are not related in the population, that is, the indicator variable *awarenessPP* does not causally explain the class variables, and, thus, it does not predict class membership. However, because *awarenessPP* may become significant when we add covariates to the model (e.g., because there may be interactions with a company's size), we cannot remove the variable from the model just yet. All indicators are significant when considering the four-class model. Therefore, the expectation is that there is a relationship between all the indicators and the class variables in the population.

3) Two-Class Model

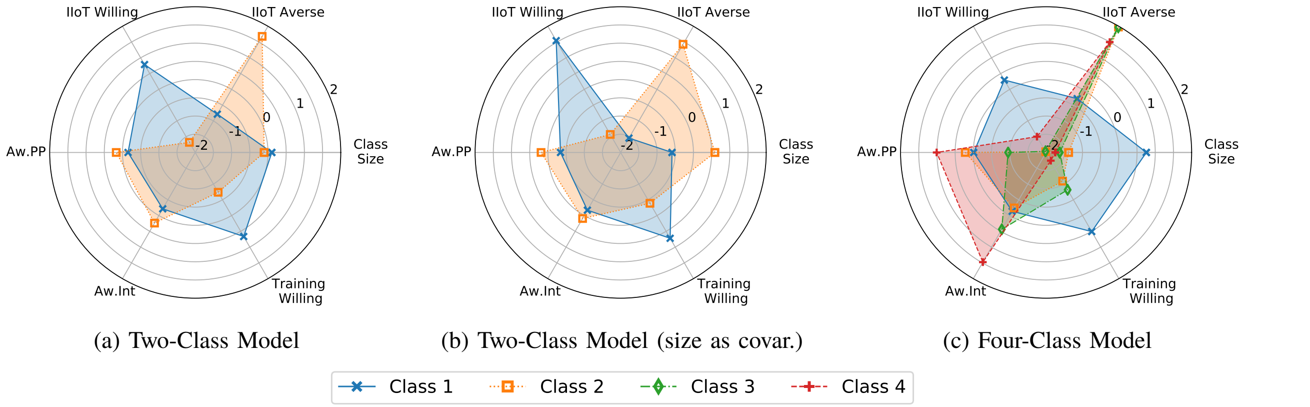
We examine the two-class model based on the BIC value for the various models, that is, we examine how the four indicator variables (as we split IIoT awareness into two dimensions (Section IV-D); i.e., intention to adopt IIoT, willingness to engage in education, risk awareness concerning legacy systems, and risk awareness concerning the production process) explain the latent class variables. Independent of the indicators, meaning the unconditional distribution, a slightly larger proportion belongs to the first class (52.6%), than to the second (47.4%).

Considering the conditional probability, we take the indicators into account. The percentage for willingness to adopt IIoT refer to conditional chances showing how the classes relate to the indicator variable. Naturally, the sum of both classes is 100%. Seventy percent (70%) of companies in the first class are willing to adopt IIoT technologies to improve the production process. For companies in the second class, the probability to be prepared to adopt IIoT technologies is eight percent (8%). As willingness to adopt has a significant Wald test value, the relationship between willingness to adopt and the class variables also holds for the population.

Indicators that are continuous, such as the willingness to participate training, *awarenessPP*, and *awarenessLegInt* show an average per class and do not represent probabilities. The willingness to participate in training is much higher in first class than it is in the second class (Figure 3a). The Wald test value is significant at $p = 1.1e^{-6}$. On average, companies that belong to the first class are more willing to participate in training. This aligns with their willingness to adopt IoT technologies to improve the production process. In fact, for both classes, the indicators of willingness to adopt and willingness to participate in training correlate strongly with each other (Figure 3a). Companies in the second class reject the idea of adopting IIoT technology, and, unsurprisingly, pursuing training on IIoT. They also score higher on the awareness components than the companies in the first class, that is, *awarenessPP* and *awarenessLegInt*.

The chances that companies in the first class are ill prepared to include IIoT in the production process is relatively high based on *awarenessPP* $= -0.1536$ and *awarenessLegInt* $= -0.2139$. Fortunately, they are also open to participate in the necessary training (0.6637) to support their willingness to adopt IIoT (69.7% plan to adopt IIoT). Companies in the second cluster hold an opposition position: While they are rather well equipped to deploy IIoT (*awarenessPP* $= 0.1708$ and *awarenessLegInt* $= 0.2378$), ninety-two percent (92.0%) reject the idea of adopting IIoT, associated with a rejection of participating in IIoT training (-0.7381). We conjecture that, companies in the second class are more aware of the risks of IIoT and, for that reason, are less willing to adopt IIoT in their production processes.

Therefore, we interpret the first class as a group of companies that is willing to use IIoT technologies in the production



(a) Two-Class Model

(b) Two-Class Model (size as covar.)

(c) Four-Class Model

Figure 3: Overview of the two and four class models. IIoT Willingness/aversity and class-size have been normalize to a $-2, 2$ scale to improve visualization.

process and that would like to know more about the associated risks in dealing with IIoT technologies, but they are currently relatively unaware of the risks involved. Therefore, we label members of the first class "risk-unaware IIoT-willing." Companies that are more aware of IIoT-related risks are in the second class, and they seem to have little desire to adopt IIoT technologies or to participate in training concerning IIoT. Correspondingly, we label members of the second class as "risk-aware IIoT-averse."

An important take-away for future security research from our observations is that the landscape for IIoT is split: On the one hand, companies see major practical challenges in adopting IIoT, and future research should attempt to investigate how these issues can be addressed. On the other hand, we must educate the companies that are willing to adopt IIoT, but that are currently unaware of security implications surrounding IIoT, so that they can assess their situation properly, for example, to prevent security incidents due to the unintended exposure of insecure IIoT equipment [19].

4) Four-Class Model

In addition to the two-class model, the model with four classes also fits the data reasonably well. The profiles of the four homogeneous groups of companies (Figure 3c) consist of one class similar to the first class from the two-model (68.9% of companies) and three classes that further break down the "risk-aware IIoT-averse" class (15.5%, 9.3%, and 6.3% of companies).

Companies in the first class are willing to adopt IIoT technologies in the production process within the next year, and, as for the two-class model, they are willing to participate in training, but they remain relatively oblivious about the security implications of IIoT (Figure 3c). The opposite is the case for the second, third, and fourth class. In fact, we observe a similar difference in the willingness to participate training, which reinforces our conclusion from the two-class model (Section IV-E3): Companies that are willing to participate in training and show willingness to adopt IIoT are not aware of the risks associated with it, while companies that are aware of the risks are opposed to adopting IIoT.

Based on the derived knowledge about the four classes (Figure 3c), we label the first class again as "risk-unaware IIoT-willing." In addition to this class, we now find two classes (Class 2 and 3 in Figure 3c) of companies that are similarly risk-unaware, but are also highly IIoT averse and largely reject the idea of participating in training concerning IIoT. Interestingly, contrary to the two-class model, we observe a difference in both awareness components for companies in the second and third class. Both classes score higher on one of the two awareness components and lower on the other component than the respondents in the first class: the second class scores higher on *awarenessPP* but lower on *awarenessLegInt*, and the third class scores lower on *awarenessPP* but higher on *awarenessLegInt*. This shows that it is important which component of awareness is measured when companies are compared to how aware of IIoT risks they are. Based on this difference, we label the second class as "risk-aware for managing the production process while legacy risk oblivious and IoT-averse," and the third class as "risk-aware for legacy systems while production process risk oblivious and IoT-averse." The fourth class is highly risk aware, both for the production process as well as for connecting legacy systems to the Internet, and we label it as "highly risk-aware and IIoT-averse."

The results of our four-class analysis indicates that we can further diversify the IIoT averse groups from two classes to four classes by differentiating those that lack a sufficient background on IIoT security, and probably IIoT in general, while also not planning to adopt IIoT. These groups that are not overly important for security researchers: While further awareness campaigns should cater toward them, they pose no imminent danger. In contrast, we find companies of the third class are dangerously unaware of the implications of connecting legacy systems to the Internet, which can cause immediate harm if they adopt IIoT, because they might accidentally expose IIoT devices when they deploy IIoT while only focusing on the potential risks for the production process.

Finally, the fourth class has outstanding awareness for issues around IIoT. Further studies should leverage members of this cluster to gain insight into the practical problems companies face when rolling out and adopting IIoT.

5) Covariates

Next, we examine if variables can explain class membership by looking at covariates, which are characteristics that are expected to influence class membership. Without investigating covariates, the division of class membership is constant. Specifically, we assume that a company's properties could predict class membership (Section III-B1), for example, that a large company might be more likely to be part of the first class. Effectively, we create a regression model that predicts class membership by adding covariates.

The only covariate with a significant impact on class membership in the two-class model is the company's size (Wald value of 0.0031). For example, we see a that there is only a 10.72% likelihood for a company from the first class to have less than 10 employees, while it is 29.67% for the second class. This is a reduction of 50.4% compared to the model without size as a covariate. This trend continues for companies with 10 to 49 employees (19.18% for the first class compared to 42.75% for the second class with a 39.9% decrease for the first class), and it turns for larger companies. For companies with 50 to 249 employees, the likelihood to be part of the first class increases by 48.2% (a likelihood of 47.94% of companies in the first class, and likelihood of 18.15% for companies in the second class), and it increases for companies with more than 250 employees by 42.1% to 22.16% for the first class and to 9.44% for the second class.

The variables company market, company sector, and company age (Section III-B1) do not predict class membership because their Wald test's p-value are not significant for $p = 0.05$. If we add the variable production to the two-class model with covariates, the company size is no longer significant with $p = 0.28$. This means that when examining the effect of the production type, company size has no unique effect on the class membership. Therefore, the distribution of this variable in the population will be the same for all classes. For the four-class model we do not find any covariates that significantly predict class membership in the population. Adding these covariates does not produce any difference in the distribution of companies over the classes.

F. Summary and Discussion

In our survey of 131 industrial companies, 25.2% of companies have adopted IIoT in the production process already, and nearly 40.5% of companies want to adopt IIoT technologies in the next year. Fortunately, our two-class and four-class results show that the companies that are willing to adopt IIoT are also more willing to participate in training. However, at the same time, these companies are less aware of the risks of linking IIoT with legacy systems and the importance of updating systems that are involved in the production process. This could lead to (catastrophic) security incidents, and, thus, requires educational efforts to mitigate them. We note that our covariate analysis revealed that smaller companies are significantly more likely to fall into the "risk-aware IIoT-averse" class, while bigger companies are more likely to be "risk-unaware IIoT-willing." This means that educational activities for small and medium companies should focus on teaching them how to effectively mitigate risks, while training programs for larger companies should focus on correctly assessing the potential risks of IIoT for the production process and from legacy devices.

However, our results also indicate that we should not develop educational activities on the management of IIoT in the production process in general. Instead, we should focus on addressing the risks associated with specific sub-topics because it increases the educational efforts efficacy. Luckily, because companies score differently on the awareness components (Section IV-E4 and Figure 3c), we can target educational and awareness activities related to IIoT. For example, in the four-class model, the third class is more aware of the risks associated with connecting legacy systems to the Internet but largely unaware of risks associated with the production process, while the second class exhibits the opposite level of awareness. Therefore, in terms of time, companies from the third class benefit more from education on risks associated with the production process, while companies from the second class benefit more from training on the risks of connecting legacy systems to the Internet. Overall, our results show *where and how to focus* educational activities related to IIoT risk awareness.

V. Related Work

In this section, we position our research and compare it to related work in the areas of Industrial IoT Adoption & Security, Practical Attacks on Industrial IoT, and research on Security Awareness.

A. Industrial IoT Adoption & Security

Sadeghi et al. found that security consideration represent the highest barrier when it comes to IIoT adoption [69]. Recent attacks leveraging IoT devices [67], numerous data breaches [41] and large-scale incidents involving consumers' devices [76] may have further contributed to the reluctance of adopting IIoT. Thiagarajan et al. further identified that stakeholders often struggle in deciding between real and perceived challenges. Stellios et al. investigate prominent attack paths for IIoT systems. They conclude that (Industrial) IoT devices introduce new threats when they are introduced, mostly due to their integration with other systems, misconfiguration opportunities [19], and poor security design choices [79].

Security considerations are not the only adoption barrier for IIoT. Other challenges concerning the integration of IIoT technologies include technical issues, such as connectivity, compatibility and longevity, or availability of standards [52], as well as human factors, like insufficient willingness of users to adapt to new technology [71]. Especially standardization is a major issue, as companies in different sector are regulated by different institutions that demand compliance with basic requirements, yet, manufacturers bring devices to the market that lack basic security requirements [52].

B. Practical Attacks on Industrial IoT

Quarta et al. conducted a security analysis of an industrial robot controller [64]. They found that the system suffers from serious security issues in its design in addition to opportunities for misconfigurations. They outline several stealthy attacks to alter the robot's operations in ways that impact production without being immediately noticeable. DeMarinis et al. published a technical report that discusses industrial robots exposed over the Internet [18]. They find several cases of industrial robots that could be controlled remotely via the Internet, requiring no additional authentication.

Earlier work largely focuses on automotive security, which is comparable to IIoT in so far as that computerization is introduced for (mostly) physical control in an equally sensitive area to industrial systems. Koscher et al. [44] and Checkoway et al. [14] conduct analyses of automotive security and they discover it to be in a similar dire state as IIoT security: poor design choices, insufficient isolation, and not incorporating the impact of networked devices lead to vulnerable systems. Their results are comparable to those of Quarta et al. nearly seven years later for an IIoT system [64].

The first major incident involving IIoT systems was the Stuxnet attack that targeted industrial control systems by Siemens that monitor and control industrial processes. The attack caused centrifuges that were used to enrich uranium in nuclear power plants in Iran to tear themselves apart, which highlights that IIoT invites new types of attacks, requires complete awareness of the environment, and introduces new threat models [10]. Indeed, Rochetto & Tippenhauer outline new threat models in the context of IIoT, based on the capabilities for users, cyber-criminals, hacktivists, insider attackers, nation-state attackers, and terrorists [66].

C. Security Awareness

Users' information security awareness is traditionally well connected with their willingness to follow security policies [12]. Still, high security awareness may in fact lead to an aversion of technologies, if the perceived risk is too high, or the benefit of using a technology is not clear enough [60]. In fact, too high of a perceived risk may even lead to straight out rejection of technology [38]. The canonical example our time are likely IT professionals avoiding to use services as end-users, like social media [46].

Asplund & Nadjm-Tehrani investigate perceived IoT security in critical infrastructures using a limited interview sample [4]. They find that risk perception is not consistent among stakeholders. However, as in their sample focuses on critical service availability (water, power, etc.) is the major asset, IT security risk awareness is not a major issue. As such, they remain observational in this matter, noting that–in general–risk awareness is medium to low. We extend on this work and provide insights into the connection between risk awareness and adoption willingness.

D. Summary

In this paper, we provide the first study comparing IIoT security risk awareness, willingness to adopt, and willingness to invest in additional training and support to improve IIoT security. Our findings extend prior work, and conform to expectations following earlier studies with end-users. Furthermore, we answer the question of how educational awareness activities should be focused to improve the security posture of industrial companies that want to adopt IIoT.

VI. Limitations

As common with empirical research, our study has some limitations, which we believe are important to share with the research community. While we are able to explain the differences in the distribution of companies' demographic factors between our selected population (Dutch companies) and our sample, future research should evaluate the accuracy of our explanation. The fluctuations we observe could also stem from our recruitment process: We specifically used contacts to a major industry organization, and larger and older companies are more likely to be affiliated to a trade association than startups. Similarly, our participants were self-selected, which yields a potential self-selection bias: respondents with higher interest in IoT may be more likely to participate in the study. Further, there is a potential self-reporting bias: especially respondents that have very low knowledge on IoT may in fact lack the ability to reflect on their level of awareness on IoT risks. Therefore, we suggest to investigate other methods to recruit participating companies, for example, collaborating with a national statistics bureau.

From a general standpoint, one might consider our sample size $N = 131$ a limitation. However, we did not survey individuals but companies, which generalize far better from comparatively small sample sizes due to their typically higher-quality answers than individuals [55], and our sample size is in the range recommended by Dziak et al. for studies like ours [22]. Furthermore, we found that only the variable *awarenessLegInt* (awareness of the potential vulnerabilities and risks when connecting legacy systems to the Internet) had a significant relationship with the two classes, and, because IIoT risk awareness is based on only two items, the component's measurement is limited.

Finally, the field of IoT and IIoT is in constant flux. Our dataset has been collected in 2018, nearly two years before the publication of this paper. The field may have developed from the snapshot we observed as the basis for our research. Hence, we recommend periodically revisiting our research questions, to get a continuous picture of these developments.

VII. Conclusion

While technological solutions for Internet-of-Things security are advancing rapidly, the human and operational component have received limited attention. In this paper, we examine the degree to which industrial companies are aware of Industrial IoT security risks, and how this interacts with their willingness to adopt IIoT technology and invest into training. Employing LCA over a sample of more than 130 Dutch industrial firms, we identify two classes of companies along these three dimensions.

We find that the degree of awareness differs among the companies in our sample, and that we can target educational awareness programs based on these observations. We argue that *risk identification* awareness programs are most likely to have a lasting impact on IIoT security when focused on firms that are: *(i)* interested to adopt IIoT, *(ii)* not yet aware of IIoT security threats, and *(iii)* willing to engage in awareness programs. In addition, *risk mitigation* awareness programs should focus on companies that are already aware of the threats and limitations of IIoT to enable them to adopt this technology. We note that the major obstacle here is that these companies do not have a high willingness to participate in such activities. However, our extended, four class model, also provides insights into a group of highly risk aware companies, which is a starting point for designing appropriate training material. Furthermore, we find that small companies are more likely to to be risk-aware organizations, while larger companies tend to be less risk-conscious. Hence, especially larger companies need to invest in trainings to identify risks of IIoT before deploying these technologies to prevent unforeseeable consequences.

A. *Future Research*

The Netherlands are a typical “Type I” culture (individualistic, weak uncertainty avoidance, and low long-term orientation) in terms of technology adoption, and they are comparable to other “Type I” countries like the U.S., Australia, Germany, or Canada [51]. Hence, we plan a follow-up study on a classical “Type II” culture (collectivistic, strong uncertainty avoidance, as well as high long-term orientation), for instance, Japan, Korea, or Taiwan would be required to investigate how cultural perspective may affect our model. We discovered the groups “risk-aware IIoT-averse” and “risk-unaware IIoT-willing” in the two-class model (Section IV-E3), and future work should investigate if this difference in IIoT risk awareness may be the underlying cause of the difference regarding the willingness to adopt IIoT in the production process, and the willingness to participate in training. Similarly, it is important to investigate whether companies have a high risk awareness because of prior IIoT security incidents, which could also lead to a higher adoption averseness.

References

[1] In: Barbara G. Tabachnick and Linda S. Fidell. *Using Multivariate Statistics*. 6th ed. Pearson, 2013. Chap. Principal Components and Factor Analysis, pp. 659–730. ISBN: 978-0-205-84957-4.

[2] Icek Ajzen. “The theory of planned behavior”. In: *Organizational Behavior and Human Decision Processes* 50 (2 Dec. 1991), pp. 179–211. ISSN: 0749-5978. DOI: 10.1016/0749-5978(91)90020-T.

[3] Hamiyet Ardiç. “Motivatie en participatie in training & ontwikkeling”. MA thesis. University of Utrecht, Aug. 2012. HDL: 1874/257663.

[4] Mikael Asplund and Simin Nadjm-Tehrani. “Attitudes and Perceptions of IoT Security in Critical Societal Services”. In: *IEEE Access* 4 (Apr. 29, 2016), pp. 2130–2138. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2016.2560919.

[5] Margaret E. Beier and Ruth Kanfer. “Motivation in Training and Development: A Phase Perspective”. In: *Learning, Training, and Development in Organizations*. Ed. by Steve W. J. Kozlowski and Eduardo Salas. 1st ed. Routledge, Aug. 6, 2009, pp. 65–97. ISBN: 978-0415649674.

[6] Gerda M van den Berg. *Princals voor beginners*. RUL, 1988.

[7] J. Martin Bland and Douglas G. Altman. “Statistics notes: Cronbach’s alpha”. In: *BMJ* 314.7080 (Feb. 22, 1997), p. 572. ISSN: 0959-8138. DOI: 10.1136/bmj.314.7080.572.

[8] Roland Bodenheim, Jonathan Butts, Stephen Dunlap, and Barry Mullins. “Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices”. In: *International Journal of Critical Infrastructure Protection* 7.2 (2014), pp. 114–123.

[9] Jon Bruner. *Industrial Internet*. ” O’Reilly Media, Inc.”, 2013.

[10] Martin Brunner, Hans Hofinger, Christoph Krauß, Christopher Roblee, Peter Schoo, and Sascha Todt. *Infiltrating Critical Infrastructures with Next-Generation Attacks*. Tech. rep. Fraunhofer Institute for Secure Information Technology (SIT), Dec. 17, 2010. URL: https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/studie_stuxnet.pdf (visited on 02/28/2019).

[11] Patricia Buckley and Sabrina Montes. *Main street in the digital age: how small and medium-sized businesses are using the tools of the new economy*. US Department of Commerce, Economics and Statistics Administration, 2002.

[12] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness”. In: *MIS Quarterly* 34 (3 Sept. 2010), pp. 523–548.

[13] Centraal Bureau voor de Statistiek. *StatLine: Bedrijven; bedrijfstak*. July 1, 2018. URL: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/81589ned/table?ts=1530723523193 (visited on 02/26/2019).

[14] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. “Comprehensive Experimental Analyses of Automotive Attack Surfaces”. In: *Proceedings of the 20th USENIX Security Symposium (USENIX Security)*. Ed. by David Wagner. San Francisco, CA, USA: USENIX Association, Aug. 2011, pp. 77–92. ISBN: 978-1-931971-87-4. URL: https://www.usenix.org/legacy/event/sec11/tech/full_papers/Checkoway.pdf.

[15] Jiahua Chen and Zehua Chen. “Extended Bayesian information criteria for model selection with large model spaces”. In: *Biometrika* 95 (3 Sept. 2008), pp. 759–771. ISSN: 1464-3510. DOI: 10.1093/biomet/asn034.

[16] Fariborz Damanpour. “Organizational size and innovation”. In: *Organization studies* 13.3 (1992), pp. 375–402.

[17] Fabian De Prieëlle, Mark De Reuver, and Jafar Rezaei. “The Role of Ecosystem Data Governance in Adoption of Data Platforms by Internet-of-Things Data Providers: Case of Dutch Horticulture Industry”. In: *IEEE Transactions on Engineering Management* (2020).

[18] Nicholas DeMarinis, Stefanie Tellex, Vasileios Kemerlis, George Konidaris, and Rodrigo Fonseca. *Scanning the Internet for ROS: A View of Security in Robotics Research*. arXiv: 1808.03322 [cs.CR].

[19] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. “Investigating System Operators’ Perspective on Security Misconfigurations”. In: *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. Ed. by Michael Backes and XiaoFeng Wang. Toronto, ON, Canada: ACM, Oct. 2018, pp. 1272–1289. ISBN: 978-1-4503-5693-0. DOI: 10.1145/3243734.3243794.

[20] C. Doets and J. Neuvel. *Monitoring BVE-net projecten*. CINOP, Den Bosch, 2000.

[21] Lynette Drevin, Hennie A. Kruger, and Tjaart Steyn. “Value-focused assessment of ICT security awareness in an academic environment”. In: *Computers & Security* 26 (1 Feb. 2007), pp. 36–43. ISSN: 0167-4048. DOI: 10.1016/j.cose.2006.10.006.

[22] John J Dziak, Stephanie T Lanza, and Xianming Tan. “Effect Size, Statistical Power, and Sample Size Requirements for the Bootstrap Likelihood Ratio Test in Latent Class Analysis”. In: *Structural Equation Modeling: A Multidisciplinary Journal* 21.4 (July 23, 2014), pp. 534–552. ISSN: 1070-5511. DOI: 10.1080/10705511.2014.919819.

[23] Nathalie van den Eshof. “De relatie tussen organisatie empowerment, leiderschap empowerment, en de veranderbereidheid van medewerkers. Met veerkracht als moderator”. MA thesis. University of Utrecht, Utretch, Netherlands, June 12, 2014. HDL: 1874/295050.

[24] European Commission. “Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises”. In: *Official Journal of the European Union* 46 (L124 May 20, 2003), pp. 36–41. ISSN: 1725-2555. URL: http://data.europa.eu/eli/reco/2003/361/oj (visited on 02/15/2019).

[25] European Commission. *State aid: Commission widens scope of the General Block Exemption Regulation – frequently asked questions*. May 17, 2017. URL: https://europa.eu/rapid/press-release_MEMO-17-1342_en.htm (visited on 02/28/2019).

[26] Eurostat. *Glossary: Enterprise size*. Oct. 31, 2016. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Enterprise_size (visited on 02/28/2019).

[27] Frank J. Fabozzi, Sergio M. Focardi, Svetlozar T. Rachev, and Bala G. Arshanapalli. *The Basics of Financial Econometrics: Tools, Concepts, and Asset Management Applications*. John Wiley & Sons, Mar. 7, 2014. DOI: 10.1002/9781118856406.

[28] Andy Field. *Discovering Statistics using IBM SPSS Statistics*. 4th ed. SAGE Publications, Mar. 31, 2013. ISBN: 978-9-351-50082-7.

[29] Barbara Filkins. *The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns*. Tech. rep. SANS Institute, July 18, 2018. URL: https://www.sans.org/reading-room/whitepapers/ICS/paper/38505 (visited on 02/28/2019).

[30] Samuel Fosso Wamba, Angappa Gunasekaran, Mithu Bhattacharya, and Rameshwar Dubey. “Determinants of RFID adoption intention by SMEs: an empirical investigation”. In: *Production Planning & Control* 27.12 (Apr. 7, 2016), pp. 979–990. ISSN: 1366-5871. DOI: 10.1080/09537287.2016.1167981.

[31] SM Furnell, M Gennatou, and PS Dowland. “A prototype tool for information security awareness and training”. In: *Logistics Information Management* (2002).

[32] Arie Gelderblom, Marion Collewet, and Jacob Koning. *Instrumentarium om deelname aan postinitiële scholing te vergroten*. SEOR, 2009.

[33] H. Gelevert, A. Smulders, and P. Van den Brink. *Digitaal Veilige Hard- en Software*. Tech. rep. TNO.

[34] Jonas Hansson and Bengt Klefsjö. “A core value model for implementing total quality management in small organisations”. In: *The TQM Magazine* (2003).

[35] Annelies Maria Hoevenaars. “Produktiestructuur en organisatievernieuwing: de mogelijkheid tot parallelliserennader onderzocht”. PhD thesis. Eindhoven University of Technology, Eindhoven, Netherlands, Nov. 29, 1991. DOI: 10.6100/IR360817.

[36] Geert Hofstede. “Dimensionalizing Cultures: The Hofstede Model in Context”. In: *Online Readings in Psychology and Culture* 2.1 (July 23, 2011). ISSN: 2307-0919.

[37] Justin JP Jansen, Michiel P Tempelaar, Frans AJ Van den Bosch, and Henk W Volberda. “Structural differentiation and ambidexterity: The mediating role of integration mechanisms”. In: *Organization science* 20.4 (2009), pp. 797–811.

[38] Allen C. Johnston and Merrill Warkentin. “Fear Appeals and Information Security Behaviors: An Empirical Study”. In: *MIS Quarterly* 34 (3 Sept. 2010), pp. 549–566.

[39] Ian T Jolliffe. “Principal Component Analysis: A Beginner’s Guide”. In: *Weather* 45 (10 Oct. 1990), pp. 375–382. ISSN: 1477-8696. DOI: 10.1002/j.1477-8696.1990.tb05558.x.

[40] Henry F. Kaiser. “An index of factorial simplicity”. In: *Psychometrika* 39 (1 Mar. 1974), pp. 31–36. ISSN: 1860-0980. DOI: 10.1007/BF02291575.

[41] Sowmya Karunakaran, Kurt Thomas, Elie Bursztein, and Oxana Comanescu. “Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data”. In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. Ed. by Sonia Chiasson and Rob Reeder. Baltimore, MD, USA: USENIX Association, June 2018. ISBN: 978-1-931971-45-4. URL: https://www.usenix.org/conference/soups2018/presentation/karunakaran (visited on 02/28/2019).

[42] Katarina Kertysova, Erik Frinking, Koen van den Dool, Aleksandar Maričić, and Kumar Bhattacharyya. *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks - Study*. Tech. rep. European Economic and Social Committee, 2018. URL: https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/cybersecurity-ensuring-awareness-and-resilience-private-sector-across-europe-face-mounting-cyber-risks-study.

[43] David Knoke and Arne L Kalleberg. “Job training in US organizations”. In: *American sociological review* (1994), pp. 537–546.

[44] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. “Experimental Security Analysis of a Modern Automobile”. In: *Proceedings of the 31th IEEE Symposium on Security & Privacy (S&P)*. Ed. by David Evans and Giovanni Vigna. Oakland, CA, USA: IEEE, May 2010, pp. 447–462. ISBN: 978-0-7695-4035-1. DOI: 10.1109/SP.2010.34.

[45] Bernice Kotey and Cathleen Folker. “Employee training in SMEs: Effect of size and firm typeFamily and nonfamily”. In: *Journal of Small Business Management* 45.2 (2007), pp. 214–238.

[46] Lydia Kraus, Tobias Fiebig, Viktor Miruchna, Sebastian Möller, and Asaf Shabtai. “Analyzing End-Users’ Knowledge and Feelings Surrounding Smartphone Security and Privacy”. In: *Proceedings of the 2015 Workshop on Mobile Operating System Security Techniques (MOST)*. Ed. by Jonathan Crussell. San Jose, CA, USA: IEEE, May 21, 2015. URL: http://www.ieee-security.org/TC/SPW2015/MoST/papers/s1p2.pdf (visited on 02/28/2019).

[47] Wim P. Krijnen. *The analysis of three-way arrays by constrained PARAFAC methods*. DSWO Press, Leiden University, 1993. ISBN: 978-9066950771.

[48] Hennie A Kruger and Wayne D Kearney. “A prototype for assessing information security awareness”. In: *Computers & Security* 25 (4 June 2006), pp. 289–296. ISSN: 0167-4048. DOI: 10.1016/j.cose.2006.02.008.

[49] Ralph Langner. “Stuxnet: Dissecting a cyberwarfare weapon”. In: *IEEE Security & Privacy* 9.3 (2011), pp. 49–51.

[50] Olav Laudy. “Bayesian Inequality Constrained Models for Categorical Data”. PhD thesis. Utrecht University, Utretcht, Netherlands, 2006. HDL: 1874/13477.

[51] Sang-Gun Lee, Silvana Trimi, and Changsoo Kim. “The Impact of Cultural Differences on Technology Adoption”. In: *Journal of World Business* 48.1 (2013), pp. 20–29. ISSN: 1090-9516. DOI: 10.1016/j.jwb.2012.06.003.

[52] Eireann Leverett, Richard Clayton, and Ross Anderson. “Standardisation and Certification of Safety, Security and Privacy in the ‘Internet of Things’”. In: *Proceedings of the 16th Workshop on the Economics of Information Security (WEIS)*. Ed. by Terrence August, Stefan Savage, and Goeffrey M. Voelker. San Diego, CA, USA, June 2017. URL: https://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf (visited on 02/28/2019).

[53] Michael H Lubatkin, Zeki Simsek, Yan Ling, and John F Veiga. “Ambidexterity and performance in small-to medium-sized firms: The pivotal role of top management team behavioral integration”. In: *Journal of management* 32.5 (2006), pp. 646–672.

[54] David Maslach. “Change and persistence with failed technological innovation”. In: *Strategic Management Journal* 37.4 (2016), pp. 714–723.

[55] Janice M. Morse. “Determining Sample Size”. In: *Qualitative Health Research* 10 (1 Jan. 2000), pp. 3–5. ISSN: 1552-7557. DOI: 10.1177/104973200129118183.

[56] D de Natris and W Brouwers. “De bereidheid van ziekenhuispersoneel tot deelname aan een communicatietraining”. In: *Tijdschrift voor Medisch Onderwijs* 27.3 (2008), pp. 120–128.

[57] Guy Notelaers, Hans De Witte, Jeroen K Vermunt, and Ståle Einarsen. “Pesten op het werk, gewikt en gewogen. Een latente-klassenbenadering op basis van de Negative Acts-vragenlijst (EN: How to measure bullying at work? A latent class analysis of the Negative Acts Questionnaire)”. In: *Gedrag en Organisatie* 19.2 (2006), pp. 140–160.

[58] Jum C Nunnally and Ira Bernstein. *Psychometric Theory*. 3rd ed. McGraw-Hill Higher Education, Nov. 1, 1993. ISBN: 978-0070478497.

[59] Tiago Oliveira and Maria Fraga Martins. “Firms patterns of e-business adoption: evidence for the European Union-27”. In: *Electronic Journal of Information Systems Evaluation* 13.1 (2010), p. 47.

[60] Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram. “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)”. In: *Computers & Security* 42 (May 2014), pp. 165–176. ISSN: 0167-4048. DOI: 10.1016/j.cose.2013.12.003.

[61] Geoff Payne and Malcolm Williams. “Generalization in Qualitative Research”. In: *Sociology* 39 (2 Feb. 2005), pp. 295–314. ISSN: 1469-8684. DOI: 10.1177/0038038505050540.

[62] CIO PwC and CSO. *The Global State of Information Security® Survey 2017*. Tech. rep. PwC, CIO and CSO, 2017.

[63] CIO PwC and CSO. *The Global State of Information Security® Survey 2018*. Tech. rep. PwC, CIO and CSO, 2018.

[64] Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, and Stefano Zanero. "An Experimental Security Analysis of an Industrial Robot Controller". In: *Proceedings of the 38th IEEE Symposium on Security & Privacy (S&P)*. Ed. by Úlfar Erlingsson and Bryan Parno. San Jose, CA, USA: IEEE, May 2017, pp. 268–286. isbn: 978-1-5090-5533-3. doi: 10.1109/SP.2017.20.

[65] Elissa M. Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L Mazurek. *A Summary of Survey Methodology Best Practices for Security and Privacy Researchers*. Tech. rep. University of Maryland, College Park, May 3, 2017. doi: 10.13016/M22K2W.

[66] Marco Rocchetto and Nils Ole Tippenhauer. "On Attacker Models and Profiles for Cyber-Physical Systems". In: *Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS)*. Ed. by Sokratis Katsikas and Catherine Meadows. Vol. 9879. Lecture Notes in Computer Science. Heraklion, Greece: Springer, Sept. 2016, pp. 427–449. isbn: 978-3-319-45741-3. doi: 10.1007/978-3-319-45741-3_22.

[67] Eyal Ronen and Adi Shamir. "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights". In: *Proceedings of the 1st IEEE European Symposium on Security & Privacy (EuroS&P)*. Ed. by Michael Backes. Saarbrücken, Germany: IEEE, Mar. 2016, pp. 3–12. isbn: 978-1-5090-1751-5. doi: 10.1109/EuroSP.2016.13.

[68] Ronan van Rossem. *Multivariate Analyse voor de Sociale Wetenschappen: Logistische Regressie*. Academia Press, Dec. 7, 2007. isbn: 978-9038211923.

[69] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. "Security and Privacy Challenges in Industrial Internet of Things". In: *Proceedings of the 52nd Design Automation Conference (DAC)*. Ed. by X. Sharon Hu and Robert Aitken. San Francisco, CA, USA: ACM/IEEE, June 2015. doi: 10.1145/2744769.2747942.

[70] P.F.M. Senden and J.S.M. Krumeich. "Follow the folder! Werving en promotie van de RealFit-cursus voor jongeren/adolescenten met (beginnend) overgewicht". In: *praktijk* 89.4 (2011), pp. 201–205.

[71] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. "Industrial internet of things: Challenges, opportunities, and directions". In: *IEEE Transaction on Industrial Informatics* 14 (11 Nov. 2018), pp. 4724–4734. issn: 1941-0050. doi: 10.1109/TII.2018.2852491.

[72] Smart Industry. *Doe mee: onderzoek naar adoptie Internet of Things in productieproces*. url: https://www.smartindustry.nl/doe-mee-onderzoek-naar-adoptie-internet-of-things-in-productieproces (visited on 02/27/2019).

[73] Smart Industry. *Smart Industry - Dutch Industry fit for the future*. url: https://www.linkedin.com/feed/update/urn:li:activity:6407216321179844608 (visited on 02/27/2019).

[74] Smart Industry. *Smart Industry Organization Tweet*. May 29, 2018. url: https://twitter.com/@in%5C-dus%5C-try%5C-smart (visited on 02/27/2019).

[75] W. Smit, S. Peters, K. David, R. Vos, and W. Sterk. *Industrial Internet of Things. Noodzaak voor industrie, kans voor IT-sector*. Tech. rep. ABN AMRO.

[76] Sean Smith. *The Internet of Risky Things: Trusting the Devices That Surround Us*. O'Reilly Media, Jan. 29, 2017. isbn: 978-1491963623.

[77] Valmi D. Sousa, Jaclene A. Zauszniewski, and Carol M. Musil. "How to determine whether a convenience sample represents the population". In: *Applied Nursing Research* 17 (2 May 2004), pp. 130–133. issn: 0897-1897. doi: 10.1016/j.apnr.2004.03.003.

[78] Wouter Stam and Tom Elfring. "Entrepreneurial orientation and new venture performance: The moderating role of intra-and extraindustry social capital". In: *Academy of management journal* 51.1 (2008), pp. 97–111.

[79] Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, and Javier Lopez. "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services". In: *IEEE Communications Surveys & Tutorials* 20 (4 Sept. 2018), pp. 3453–3495. issn: 1553-877X. doi: 10.1109/COMST.2018.2855563.

[80] Ashok Subramanian and Sree Nilakanta. "Organizational innovativeness: Exploring the relationship between organizational determinants of innovation, types of innovations, and measures of organizational performance". In: *Omega* 24.6 (1996), pp. 631–647.

[81] SurveyMonkey. *SurveyMonkey: The World's Most Popular Free Online Survey Tool*. url: https://www.surveymonkey.com/ (visited on 02/26/2019).

[82] Mehmet Tekerek and Adem Tekerek. "A research on students' information security awareness". In: *Turkish Journal of Education* 2.3 (2013).

[83] Darshini Thiagarajan. "Analysis of the Current State of Industrial Internet of Things (IIoT) adoption". MA thesis. Massachusetts Institute of Technology, Cambridge, MA, USA, Oct. 26, 2016. HDL: 1721.1/107361.

[84] United Nations, Department of Economic and Social Affairs, Statistical Division. *International Standard Industrial Classification of All Economic Activities (ISIC)*. 4. United Nations Publications, 2008. isbn: 978-9-211-61456-5. url: https://unstats.un.org/unsd/publication/seriesM/seriesm_4rev4e.pdf (visited on 02/28/2019).

[85] W Van der Valk. *Scholing in het MKB: waarom, hoe gevonden en bekostigd en wat knelt er*. Zoetermeer: eim, 2006.

[86] Ronan Van Rossem. *PC vs. PAF: een enigzins technische inleiding*. Tech. rep. 2. University of Gent, Center for Social Theory, Jan. 2011. HDL: 1854/LU-4256927.

[87] Jeroen K. Vermunt and Jay Magidson. "Latent Class Cluster Analysis". In: *Applied Latent Class Analysis*. Ed. by Jacques A. Hagenaars and Allan L. McCutcheon. Cambridge University Press, June 2002, pp. 89–106. isbn: 978-0521594516.

[88] Kevin Zhu, Shutao Dong, Sean Xin Xu, and Kenneth L Kraemer. "Innovation diffusion in global contexts: determinants of post-adoption digital transformation of European companies". In: *European journal of information systems* 15.6 (2006), pp. 601–616.

Appendix

A. Statistical Analysis Techniques

In this paper, we survey industrial companies through a questionnaire that we analyze through Principal Component Analysis (PCA) and Latent Class Analysis (LCA). Following, we provide a brief high-level overview about each technique.

1) Principal Component Analysis

We measure the concepts of our study through a number of questionnaire items (Section III). We validate that they measure the concept of our study through Principal Component Analysis (PCA). The idea behind PCA is to reduce the complexity of a model by discovering its principal components. To do so, PCA identifies the correlations between the measured items [86]. Based on the correlations, we can then reduce it to one or more variables that simplify the model [39]. Naturally, the chosen number of variables may not explain the original model entirely (only if some items in the original model were redundant, or if the number of principal components equals the number of items in the original model), but it explains a large proportion of the variance of the original items based on the principal components [47]. Therefore, by doing so, we can investigate whether a collection of items models the right concept [28].

This also means that PCA makes it possible to describe a set of items through fewer relevant components [47]. As the results provide insight into the extent to which the selected items cover the concept, the analysis gives an indication of convergent validity (i.e., whether a set of items measures the same concept) and discriminant validity (i.e., whether items distinguish different concepts). To test the reliability of our constructions, we also perform a Cronbach's alpha test to evaluate if the internal consistency is sufficient, with a threshold value of $\alpha = 0.7$ [7, 58]. After we establish validity

Table IV: Comparison of Company Demographics between the General Population and Our Sample.

Company Demographic			Population	Sample
Type	Customer Base	B2C	39.27%	3.05%
		B2B	48.19%	81.68%
		Both	12.53%	15.27%
	ICT Sector	Yes	1.36%	7.63%
		No	98.64%	92.37%
	Production Type	Production	65.56%	22.90%
		Processing	7.10%	48.86%
		Other	27.35%	28.24%
Size	0-9 Employees		86.68%	19.85%
	10-49 Employees		9.51%	30.53%
	50-249 Employees		3.17%	33.59%
	250+ Employees		0.65%	16.03%
Age	0-5 Years		35.37%	5.34%
	6-11 Years		26.71%	6.11%
	11+ Years		37.92%	88.55%

and reliability, we aggregate scores for each concept by taking the average of the corresponding indicators.

2) Latent Class Analysis

We perform Latent Class Analysis (LCA) on the computed aggregated scores for each concept. LCA is a statistical method that allows identifying unobserved classes of respondents in a dataset by analyzing the observed indicators. The classes indicate homogeneous groups of respondents. LCA thus offers the possibility to divide data into homogeneous subgroups [50].

One way to describe LCA is that it fits the number of classes to the data. Prior to analysis, it is unknown how many reasonable homogeneous groups the data has. We add classes to the model to the point where adding an additional class no longer contributes to a significantly better model fit, where a better model fit means that the homogeneity within the groups is higher, while it is smaller between groups. Ultimately, the goal is to find the model that maximizes the homogeneity within the groups and the heterogeneity between the groups.

In addition to LCA, we perform Wald's test to evaluate if the effect of individual variables is significant and, therefore, whether the variables add to the statistical model [68]. For our research, the Wald's test examines if a class has indeed a significant relationship with the indicators [87].

B. Data Representativeness

Please see Table IV for the tabular comparison of our sample and the general population in the Netherlands.

C. Questionnaire

Our questionnaire uses the following structure: Circles denote single selection answers. Tables with circles denote single response per row. Questions without selections allow free text answers.

Please note: The survey was conducted in a foreign language. The questionnaire was translated by the authors.

Research Goal

The Internet of Things (IoT) connects devices and machines to the Internet, so that sensor data can be collected and exchanged with other devices. IoT provides advantages, such as increased efficiency and productivity of the production process. At the same time, Industrial IoT introduces new risks associated with connecting existing production processes to the Internet. *[Sentence removed for anonymity.]* Therefore, better understanding the level of awareness of industrial companies concerning the adoption of Internet of Things (IoT) applications to augment and improve their primary production processes is crucial. In general, Industrial IoT encompasses machines' Internet-connected that produce useful data and communicate to other machines or external parties, such as the machine supplier. For example, an air conditioning system in an office may be connected to the Internet via IoT applications.

In order to enable industrial companies to successfully deploy and use IoT, we aim to provide the federal government with insight into how to develop and implement the most effective education and awareness activities. These activities aim to increase risk awareness when connecting existing production systems to the Internet via new Internet-connected technologies. With your participation in this survey, you contribute to more effective policy making for supporting industrial companies in the adoption of IoT in their production processes.

Instructions and Privacy Notice

- Please select exactly one answer per question or statement.
- Please answer all questions (1 through 13).
- The expected time commitment is 4 minutes.
- All answers will be stored and processed anonymously. Analyses and reporting occurs at the aggregated level only, individual participants cannot be inferred.
- Upon completion of the survey, you can opt-in to receive our complete research report upon publication.

I agree to the following by clicking "Continue:" I declare that I have been informed in a clear manner about the nature, method, purpose, and burden of the research I am participating in. I know that the data and results of the research will be disclosed to third parties in anonymized form. I voluntarily agree to participate in this study. I understand that I retain the right to withdraw my participation in this research at any time and without cause.

Survey

1) An IoT technology is a hardware or software component within the production process that is connected to the internet and collects and exchanges data with other devices, allowing intelligent actions to be carried out. This with the aim of optimizing the production process and increasing its productivity. Consider, for example, vibration sensors in a machine of the production process of a candy manufacturer, which measure when a piece of metal from a machine is about to fall into the candy. With a changing vibration frequency, the data can be sent to the central data center such that employees are alerted. Does your company already use IoT technologies within the production process? Write down yes or no below. If yes, briefly describe what it is.

Table V: To what extent would you agree with the following statements?

	I strongly disagree.	I disagree.	I neither agree nor disagree.	I agree.	I strongly agree.
I am aware for all systems in my production process whether they are connected to the internet or not.	○	○	○	○	○
I am aware for all systems in my production process whether these are still supported by the supplier or by my own company (and therefore are or are not legacy systems).	○	○	○	○	○
Legacy systems in a production process are *not* more vulnerable to malfunctions (for example, unintentional errors of own employees or external support staff) than other systems.	○	○	○	○	○
Legacy systems in a production process are *not* more vulnerable to malicious activities (eg hacks by criminals) than other systems.	○	○	○	○	○
I am aware for all systems and associated software in my company's production process whether they would be equipped for securely linking them to the internet.	○	○	○	○	○
When I run a system update, I have *no* good idea how it affects my production process.	○	○	○	○	○
I know which party is responsible for providing system updates for the systems of my production process (connected to the Internet).	○	○	○	○	○
I know which party is responsible for performing system updates for the systems of my production process (connected to the Internet).	○	○	○	○	○
I know what to do in case the supplier of systems of the production process is no longer able to deliver system updates.	○	○	○	○	○

2) Is your company planning to purchase IoT technology for the production process in the coming year (in addition to any IoT technologies already used in the production process)?
   - ○ Yes.
   - ○ No.
3) Please respond to following statements about dealing with systems in the production process. See Table V.
4) I want to free and commit ___ hours per week for education and awareness programs for IoT technologies.
   ○ 0. ○ 1. ○ 2. ○ 3. ○ 4.
5) I prefer *not* to spend any money on education and awareness programs for IoT technologies.
   - ○ I strongly disagree.
   - ○ I disagree.
   - ○ I neither agree nor disagree.
   - ○ I agree.
   - ○ I strongly agree.
6) It is *not* useful for my company to use education and awareness programs for IoT technologies.
   - ○ I strongly disagree.
   - ○ I disagree.
   - ○ I neither agree nor disagree.
   - ○ I agree.
   - ○ I strongly agree.
7) Education and awareness programs for IoT technologies are too complex for my company to participate.
   - ○ I strongly disagree.
   - ○ I disagree.
   - ○ I neither agree nor disagree.
   - ○ I agree.
   - ○ I strongly agree.
8) Where is the head office of your company located?
   - ○ Netherlands.
   - ○ Europe.
   - ○ Rest of the world.
9) How many employees does your company have?
   - ○ Less than 10 employees.
   - ○ Between 10 and 49 employees.
   - ○ Between 50 and 249 employees.
   - ○ More than 250 employees.
10) How old is your company?
    - ○ Less than 5 years.
    - ○ Between 5 and 11 years.
    - ○ More than 11 years.
11) To whom do you supply products or materials?
    - ○ Consumer market
    - ○ Business market
    - ○ Both
12) Does your company mainly operate in the Information and Communication Technology (ICT) sector?
    - ○ Yes.
    - ○ No.
13) What does your company primarily produce?
    - ○ Materials, such as industries that rely primarily on chemical, biochemical, mechanical, or physical processes.
    - ○ Discrete products, such as manufacturing industry of objects and other packaged products.
    - ○ Other.
14) **(Optional)** Your participation is truly appreciated. To thank you, I would like to offer you an IoT-related pleasantry. I am also prepared to give you access to the report with research results, based on a large number of comparable companies. If you are interested in this please leave me an email address where I can send it to: