# How Secure is Home: Assessing Human Susceptibility to IoT Threats

EMILY KATE PARSONS, EMMANOUIL PANAOUSIS, and GEORGE LOUKAS, University of Greenwich

The use of Internet of Things (IoT) devices within the home has become more popular in recent years and with the COVID-19 pandemic more employees are working from home. Risk management has become decentralised, which is problematic for organisations since potential risks towards the company can not be controlled in a standardised and formal way. On the other side, users are suffering from smart home attacks due to the nature of IoT such as its heterogeneity and non-standardised architecture. However, the behaviour and attitudes of the user can dictate the increase or decrease of risk and possible losses due to the end user's responsibility within the IoT life cycle. In this paper, we suggest that a user's behaviour and attitude towards IoT devices within the smart home is imperative when designing a risk model for the home. We then consider the human element in the risk assessment process in IoT. We present a Smart Home Behaviour and Attitude Risk Model (SH-BARM) to discuss the importance of human behaviour and attitudes within the home and propose a solution to that will aid smart home inhabitants and organisations.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**.

**ACM Reference Format:**
Emily Kate Parsons, Emmanouil Panaousis, and George Loukas. 2020. How Secure is Home: Assessing Human Susceptibility to IoT Threats. 1, 1 (November 2020), 12 pages.

## 1 INTRODUCTION

Within recent years, the progression towards working from home how has become more of a reality than ever before. Due to the COVID-19 pandemic, organisations forced into lockdown have started understanding the benefits of employees working from home, such as not being required to rent office buildings. As employees settle within their Work From Home-Remote Office (WFH-RO), managing risks caused by human behaviour has become part of the decentralisation of cyber risk management, where an employee's home can pose as a threat to an organisation since it is not a controlled environment. Alongside this, the use of the Internet of Things (IoT) within the home has increased, with many attacks targeting devices with different operations such as surveillance and automating daily tasks. The IoT security landscape has often been modelled with traditional static requirements which is a problematic feature within IoT's dynamic space, thus, the issue of scalability is prevalent with risk models being required to address many IoT nodes [1]. This makes focusing on the human factor integral as IoT risk models become more dynamic in nature. Bitsight [2] has shown that during the periods of March 2020, the IoT focused malware Mirai was observed to be least 20 times more frequent within WFH-RO networks than corporate networks. This sharp rise has the potential impact on not only on the home, but also an organisation due to employee access and knowledge of a remote system as well as the attitudes towards smart devices in the home. These attitudes manifest into the way a user utilises IoT technology, presenting a disconnect between positive feelings towards owning and operating devices, but uncaring and uninterested attitudes towards smart home security [3].

At the core, these attitudes can affect the security knowledge and understanding that users have, leading to a lack of basic safeguards. Research from Avast [4] found that over 40% of worldwide smart homes contain at

Authors' address: Emily Kate Parsons, emily.parsons@greenwich.ac.uk; Emmanouil Panaousis, e.panaousis@greenwich.ac.uk; George Loukas, g.loukas@greenwich.ac.uk, University of Greenwich.

least one vulnerable device, where under 70% of these having been vulnerable because of weak credentials and over 30% is due to software vulnerabilities. This shows that social and personal attitudes towards IoT have a great effect on risk [5], where humans are susceptible to fall for social engineering attacks and account hijacking based on smart home behaviour and attitudes. The problem within the smart home setting is that human related factors are the most significant causes of risk [6], with limited ways for smart home inhabitants to measure and understand the risk their behaviour and attitudes can cause. Smart vendors and government bodies do not have complete control over what users do within their home and whether good security practises are used. As this is the case, we suggest that the focus on the human role within the smart home are just as important as the roles smart vendors and government bodies play to ensure data and users are secure within the home.

In this paper, we present the Smart Home Behaviour and Attitude Risk Model (SH-BARM) which to the best of our knowledge is the first risk assessment model that focuses primarily on the user behaviour and attitudes within the home. Our novelty stems from the methodology we use to assess smart home risks, providing an interconnected approach that produces results that can be used to reduce and build awareness of smart home risks. We contribute not only our model but present a risk assessing approach which the model can be used within, as well as a small-scale case study discussing our findings. This model aims to identify the human elements that can increase and decrease the maximum expected loss when an attack occurs within the home to expose risky WFH-RO networks. This model can be used by an organisation with employees that work from home to discover the steps needed to decrease risk while in the decentralised state, with the possibility of being implemented into risk management plans. To the smart home user, this model can show the level of risk depending on their actions, allowing them to be self-defensive in a time where working from home has become normalised. The major gap we are aiming to close is the question of how to standardise accessing risk within the home while focusing on human factors that can affect this risk.

The rest of this paper is as follows. In Section 2, we present the related work expressing the current issues and methods to assess risk within IoT. In Section 3 we present our Smart Home Behaviour and Attitude Risk Model (SH-BARM) and discuss it's components, while in section 4 we discuss the risk assessment approach to implement SH-BARM. Next, in Section 5 we provide a case study which presents the use of our model within an attack scenario, comparing different risk level households. Finally, Section 6 concludes this paper.

## 2 RELATED WORK

The smart home landscape within research has portrayed the emerging technologies and creation of new automation methods, with innovative ideas that push the boundaries of IoT. Since these concepts are still growing, risk assessment approaches for generalised IoT applications are still in progress, with smart home risk assessments being very limited. The COVID-19 pandemic has created tension with the amplification of existing cyber risks including social engineering-focused attacks with Lallie et al. [7] finding that 86% of attacks assessed involved a form of phishing. This influx of attacks is now focusing on the pandemic to exploit people in need, using a sensitive subject to achieve an attack goal, where IoT devices can be used as a medium to transmit these attacks. The literature has shown the many attempts to assess risk within the IoT scope, with many frameworks being created for different IoT settings and different environments.

### 2.1 Risk Assessments for IoT

Mohsin et al. [8] proposed the IoTRiskAnalyzer, a framework which quantifies the likelihood of an attack against generic IoT system's configurations. The use case verified risk exposure, allowing for the manipulation of parameters such as vulnerable entry points and connectivity. While Shivraj et al. [9] proposed a model-driven risk assessment framework for IoT that is based on graph theory using similar risk components as Whitman [10] to create a framework that accommodates existing and new threat models for risk assessment. The missing

parameters for these frameworks that we suggest within this paper is the *user's ability to increase the likelihood and impact*, dependent on the behaviour and attitudes that are displayed. This suggests user accountability towards assessing risk, for example, how a user creates vulnerable entry points.

While the literature portrays assessing risk towards various IoT settings, others focus on identifying risks for individual devices or device functions. Huang et al. [11] proposed a risk assessment for embedded motion sensors to explore the risks of sensor use on IoT devices using Neural Networks, assessing the possible leakage of private information when a sensor is attacked. On the other hand, Tseng et al. [12] proposed a risk analysis process towards wearable IoT devices by presenting using a data flow diagram and an abuse model to identify possible attack paths towards the device.

Both works do not consider the human factor, and they do not focus on formulating situational risks dependant on an adversary's plan over a user's personal usage habits. Our work will address this missing factor, being a potential extension for analysing risk for a specific IoT device. Finally, we find that user accountability as a factor of risk has been considered before. Li et al. [13] proposed an information security risk assessment based on structured risk factors towards privacy, using the IoT assets, information flow and human factors. Here, the privacy cognition and lack of user awareness are considered within the human factors, suggesting the user accountability towards IoT privacy and the important role user's play within the IoT life cycle. The impact of privacy towards IoT users is an important aspect to address, however, we suggest that other types of impacts can be increased or decreased by the user attitude and behaviour, using this to establish a model which primarily focuses on the user accountability and self-defence.

Ali et al. [6] conducted a thorough security risk assessment using OCTAVE Allegro for a smart home setting, which identified critical cyber and physical assets. This work has presented the need to consider the human factor, with it being one of the critical cyber categories, clearly showing that humans are the greatest cause of risk. Our work takes this idea and focuses on human factors as the primary drive towards assessing and reducing risk within the smart home, to form a self-defensive stance against attacks.

## 2.2 User Behaviour and Attitudes within IoT

When it comes to number and types of IoT devices within the home, Psychoula et al. [14] reported that smart homes contain a large variety with the most common being wearables, thermostats, cameras, and personal assistants. The exponential growth and normalisation of IoT devices in many settings shows the value that society puts on these systems. The idea that IoT is an innovative and well-received technology can be discovered within Alraja et al. [15], where a positive correlation between user familiarity and use of new health care technologies was found, where high levels of certainty, reliability and guarantees increased the willingness for users to use smart healthcare devices. However, there is a disconnect between the attitudes to IoT as a innovate technology and IoT security where Oh et al. [3] shows that many users ignore IoT security because they undervalue their personal information.

To build a model based on the attitude and behaviour of users, we must understand what these mean within an IoT context. We define a user's attitude as the thoughts and feelings towards IoT and its security, correlating that these values present a smart home behaviour which can increase risk. These behaviours are the actions or lack of actions presented within the smart home, for example, knowing how to respond to a threat. Within the work of Asplund et al. [16] individuals with a technical background within critical infrastructure sectors were surveyed about the attitudes and perceptions they had for IoT. Interestingly, the results showed that many individuals have the opinion that there are no significant risks within IoT since, by design, risk should be accounted for. This shows the individuality based on the experience a user has with IoT, e.g. if an individual has friends with positive experience the awareness towards risk may be decreased.

## 3 RISK MODEL

We assume a household (we also refer to this as the Defender) that wishes to protect its infrastructure (cyber and physical) against cyber adversaries (abstracted by the entity that we refer to as Attacker). The latter aim to compromise one of the confidentiality, integrity, or availability of this infrastructure using different attack tactics to impact the members within the household. This model is independent of the risks outside of the home's control, focusing on a security level that dictates the maximum expected loss based on the users' *behaviour* and *attitudes* within the smart home.

Let assume a household with the a number of user groups where for each user group $i$ we define high-level major components [17], [9], [18]:

- Likelihood of occurrence $O_i$, which determines the degree, in the form of a probability, at which $i$ is targeted by the Attacker.
- Potential success rate $S_i$, which determines the probability of an attack that has occurred to be successful within $i$.
- Potential impact $M_i$, which determines the expected impact the exploitation of $i$ will have to the Defender.
- Efficacy of safeguards $E_i$, which determines the expected efficiency of an implemented safeguards to be effective against an attack on $i$.

Using these components, we define how to find the expected loss within a home. Let $R_i$ be the *expected loss* of the Defender from a user group $i$, given by

$$R_i = O_i \, S_i \, M_i \, (1 - E_i).$$

We make the assumption that the identification and valuation of assets precedes the risk model. During valuation, the cost of an asset is weighted against safeguards, defining the cost benefit, establishing if a safeguard is worth investing in. This valuation also affects how impact is assessed, with high cost, high risk assets producing a larger impact on the home. Next, we evaluate each component towards the smart home setting to address the attributes needed to successfully display the maximum expected loss.

### 3.1 Likelihood of Attack Occurrence

The National Institute of Standards and Technology (NIST) explains that the likelihood of occurrence is a risk component where a given threat is capable of exploiting a given vulnerability [18], [19] and is a highly suggested component to determine risk. Thus the goal is to consider smart home behaviours that can affect the likelihood of occurrence towards users within group $i$. We express by $AP_i$ the Risk Appetite of user group $i$, which refers to the risky behaviours [20] that a user may present, for example, downloading applications from unknown locations and ignoring best practises as advised by smart vendors. We express by $FA_i$ the Familiarity of user group $i$, in which rather than focusing on familiarity towards the operation of a device, it is aimed at key smart home security practises. This is key to SH-BARM since users are often familiar with technology and the operation of devices but not the security practises needed to protect the home [3]. For a user group $i$, we define the Likelihood of Occurrence as $O_i := AP_i \times FA_i \rightarrow [0, 1)$. In an optimal scenario, we would expect a user to be risk-averse and have a high familiarity with security practises.

### 3.2 Attack Success Rate

Users within group $i$ can affect the success of an attack by not displaying key behaviours that can prevent an attack from occurring or escalating. We suggest that for the rate of success to be reduced, a user must both perceive and prevent attacks. For an attack to be perceived, the user must have an awareness towards the potential attacks, thus knowing visual and auditory cues when an attack or threat is present. For an attack to be prevented, it must first be perceived [20] which refers to the ability to correctly identify distinguishable threats and attacks

before any prevention strategies can be implemented. When a threat or attack is not acknowledged or is ignored, the probability of minimising exploitation is lower, allowing for the adversary to remain hidden within the smart home network or application. We denote by $PE_i$ as the perception of user group $i$ and we denote by $PR_i$ as the prevention of user group $i$. In an optimal scenario, we would expect a user to have a high perception of threats and understand how to quickly and effectively prevent an attack from happening or escalating. While being able to perceive attacks is important, the act of prevention shows the ability to form a resolution, combating attacks. For a user group $i$, we define the Likelihood of Success as $S_i := PE_i \times PR_i \rightarrow [0, 1)$.

### 3.3 Potential Impact

The aftermath of an attack will affect each home differently depending on an adversary's end goal with the potential impact displaying the "magnitude of harm" [19] towards users in a group. These impacts can be targeted towards a human within the smart home or towards the smart home system and its assets [21], at different levels. The level of a potential impact measures the immensity of impact towards the smart home, with different impact types being measured by the probable chance of occurrence. For a user group $i$, the potential impact of an attack is the combination of cyber impact $CY_i$, and physical impact $PH_i$ towards the smart system's non-human assets, as well as the emotional impact $EM_i$ and direct impact $DR_i$ towards the domestic lives of the smart home inhabitants. The cyber impact refers to the consequences where an adversary compromises the confidentiality, integrity and availability of a smart asset, such as a device, application, or network communication components, with the added possibility of repudiation due to attacks that alter IoT data [21]. The physical impact makes reference to any physical damages of smart home assets, which includes the theft and tampering. This also includes the hijacking of device functionality, such as the incorrect, unauthorised, and delayed actuation of a device [21]. The emotional impact refers to the emotions, attitudes and behaviours exhibited by the user once an attack has occurred [21]. A victim's subjective feelings are "categorical, emotional, and embodied" [22] harnessing the idea that individuals will react in different manners, where the negative emotions exhibited are dependent on the seriousness of the attack and the experiences of the individual. The direct impact is the immediate results of smart home attack being successful, thus leading to financial, vocational, inconvenience, privacy, control, health and safety losses which affect the daily life of a victim, these consequences carry a direct impact on the user's life, affecting them for a period of time [21]. For a user group $i$, we define the potential impact level towards each impact type as the weighted sum of the individual impacts $M_i := w_1 CY_i + w_2 PH_i + w_3 EM_i + w_4 DR_i$.

### 3.4 Efficiency of Safeguards

For group $i$, the home may have implemented safeguards that minimise the impact of an attack protecting various smart home assets. We define the random variable $E_i$ as the efficiency of the safeguards implemented by user group $i$. These safeguards must be efficient and fit for purpose to successfully reduce risk. Using ENISA's guidance [23] we suggest there are two types of high-level safeguard categories for the home these being awareness-based and practical defences. The awareness regarding safeguards relate to the cognisance towards a smart home security culture and educating users, for example, training users to spot and prevent social engineering. The practical safeguards are the direct controls that protect smart assets, for example, the use of two-factor authentication to protect a user's account. Both examples are fit for protecting against social engineering and unauthorised account access respectfully, however, the efficiency relies on how well implemented these controls are, for example, a household with some understanding of social engineering may still fall victim to an attack.

## 4 SH-BARM ASSESSMENT APPROACH

To present our model's parameters function, we have adopted and adapted a risk assessment methodology based on the Health and Safety Guidance HSG48 [24], a study which examines the human factors of risk and how this

can affect the workplace. We adapt the 5-step guidance towards human factors within risk assessment onto the smart home setting.

### 4.1 Step 1: Look for hazardous behaviours and attitudes

The first step of HSG48 is to identify a range of hazards, with these being physical, chemical, biological and psychological. The focal point for our adaption is the idea human behaviours and attitudes will contribute to hazards, being a driving force that can cause an impact. Towards the smart home, hazardous behaviours and attitudes should be identified with the clear goal of recording risk increasing and decreasing practices. This encompasses the values presented by smart home behaviours and attitudes, addressing practices that influence the likelihood of an attack occurring and the probability of an adversary's success.

### 4.2 Step 2: Decide the assets that may be harmed and the impact towards this

The next step within HSG48 [24] is the consideration of those that are at risk and how these individuals may be harmed and establishing the groups that can be threatened and the impact of hazards. In the context of the smart home, this step identifies the smart home assets and users that are exposed to risk alongside the potential the impacts of attacks towards them. This portrays how risky behaviours and attitudes can not only affect other humans but also how it can affect a smart home's components such as a smartphone or a smart device's sensor.

### 4.3 Step 3: Decide whether existing precautions are adequate or if more should be done

The third step as suggested by HSG48 [24] is the understanding and assessment of implemented safeguards and whether these controls are best suited for a variety of attacks. For the smart home, this means addressing safeguards that are in place, and the efficiency towards stopping attacks thus determining if the set of safeguards are good enough or if they need to be improved. Using HSG48, insightful questions that can aid the implementation of safeguards for the home can be seen, proposing possible requirements:

- Do safeguards eliminate high-risk threats?
- Do users within the smart home understand how to use safeguards to their full potential?
- Do safeguards make risky situations more error-tolerant?
- Do safeguards influence human behaviours and attitudes?

### 4.4 Step 4: Record findings

HSG48 recommends that all significant findings from the risk assessment process must be recorded for ease of comparison. With the smart home setting, recording these findings will allow users to see the change of expected loss over time with changes to their behaviours and attitudes alongside implementing new controls and adapting to changes when new smart home assets are added.

### 4.5 Step 5: Review and revise the risk assessment

The final step of HSG48 explores is the need to review and revise the risk assessment process. Within the smart home, we can suggest that users can revisit and perform the risk assessment process when a change occurs, such as a new smart home user or device.

## 5 CASE STUDY

This section establishes a case study risk assessment using an realistic attack scenario based on a past hacking events in 2019. We compare the results of three households using the same scenario to portray different risk levels, these being low, moderate and high risk facing smart homes. We have adopted and modified the HSG48 [24] approach using steps one to three alongside SH-BARM to discuss and provide validation for the approach.

### 5.1 Establishing the Scenario

In December of 2019, news sources, reported on the cases of users whose Ring Home Security Cameras were compromised, with many cases of adults and children being harassed via the device's speakers, with some users were terrorised with death threats if they did not pay a ransom fee. Let us assume this same attack and examine the attack path process as shown in Figure 1.

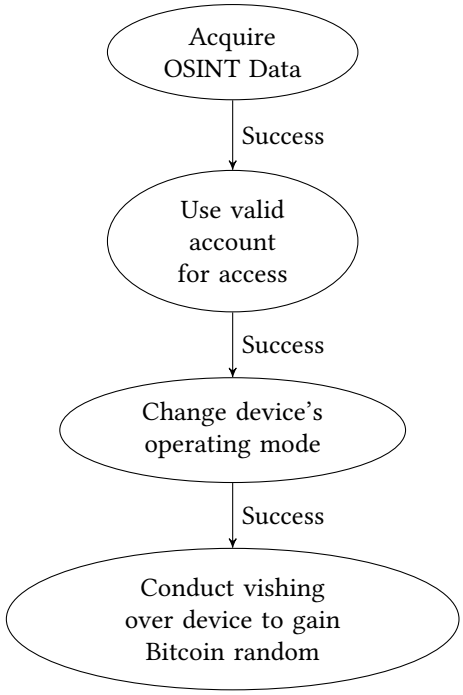


Fig. 1. A flow chart diagram depicting the adversary's attack path while using MITRE. Each oval represents an attack objective which is required to achieve the final goal.

To formulate this attack path, we use various MITRE techniques to describe the tactics of an adversary and what must be accomplished. Firstly, the adversary must acquire a target's account information, in this case, they wish to find available information using online Open-source intelligence (OSINT) from past data breaches [25]. This information is freely available and does not indicate to the target that they are of interest. If this is successful, the adversary uses the compromised credentials as a means to gain initial access to the Ring application, providing the ability to hijack control. If the adversary gains successful access to the device and its functions, the next step requires the change of operating mode, inhibiting the device's functionality and using it to perform the next step. The last step is to conduct the social engineering method of vishing via the smart camera to extort bitcoin from the victim. This technique aims at manipulating the victim, striking fear and provoking unusual behaviours that allow an adversary to gain the ransom money.

### 5.2 Step 1: Look for hazardous behaviours and attitudes

Let us assume 3 households, $S_1$, $S_2$ and $S_3$ which represent low, medium and high risk values respectfully. The first step is to identify the hazardous behaviours and attitudes that increase or decrease the likelihood of occurrence and the potential success rate, as seen in tables 1 and 2.

*5.2.1 Likelihood of occurrence.* Table 1 shows an example of risky behaviours which households exhibit with relevance to the attack scenario. These behaviours were collected from media articles documenting the Ring Home Security Camera attacks, where Ring suggested that affected users did not adhere to smart home security practices that have been provided. It was shown that many users would reuse passwords which could easily be found via the use of a credential stuffing attack, with data breach information being freely available online, as well as not implementing two-factor authentication. Another aspect of our attack scenario is the risky behaviour choice of not understanding social engineering attacks, whereby a household is not aware or has little knowledge.

Table 2 shows the security familiarity results of each household. Each household has a varying understanding of the good practices that take place within the smart home. The level of security familiarity carries two major factors, the awareness towards and knowledge of good security practices, where to carry a great security familiarity level, the household must achieve optimal comprehension. $S_1$ has a high awareness and comprehension toward smart home security practices, thus will contain great security familiarity. $S_2$ has some awareness and comprehension of the smart home security practices where some concepts may not be fully understood, thus there is room for improvement. Finally, $S_3$ has a security familiarity that is extremely limited with little to no concepts being understood alongside limited awareness.

| Risky Behaviours | Household Notation | | |
|---|---|---|---|
| | $S_1$ | $S_2$ | $S_3$ |
| Reusing passwords | - | ✓ | ✓ |
| No use of two-factor authentication | - | ✓ | ✓ |
| Limited knowledge of social engineering | - | - | ✓ |

Table 1. A representation of risky smart home behaviours toward each household.

| Security Familiarity | Household Notation | | |
|---|---|---|---|
| | $S_1$ | $S_2$ | $S_3$ |
| Limited Security familiarity | - | - | ✓ |
| Moderate Security familiarity | - | ✓ | - |
| Great Security familiarity | ✓ | - | - |

Table 2. A representation of the familiarity towards smart home security practices for each household.

*5.2.2 Attack Success Rate.* Table 3 shows the ability to both perceive and prevent each attack objective. Let us assume that all homes have been part of a data breach, OSINT can not be stopped or perceived by the homes as the activity is indistinguishable. The perception and prevention of the adversary's attack access to a valid account and the changing of operating mode can vary depending on the invisibility of the adversary accessing and using the device, we assume that the vendor application does not alert the user of a new login, making it a harder attack to perceive.

## 5.3 Step 2: Decide the assets that may be harmed and the impact towards this

The next step requires the collection of home assets and the types of impact each home could be faced with. For the sake of comparison, we assume that each household has the same number and types of assets that can be targeted. This contains the smart camera device alongside a smartphone which uses a smart application for control, as well as network components that allow devices to be connected. Finally, we consider that the smart home inhabitants are much like assets, as they can be targeted directly via the use of social engineering.

| Perceive and Prevention Ability | Household Notation | | |
|---|---|---|---|
| | S1 | S2 | S3 |
| Access to a valid account | High | Low | Low |
| Change operating mode | High | Low | Low |
| Vishing Attack | High | Moderate | Low |

Table 3. A representation of the perception and prevention ability towards smart home threats and attack for each household.

*5.3.1 Potential Impact.* Table 4 shows an example of impact types and the level at which they may affect each home. Negative emotional responses are subjective to the individual's thoughts and feelings once an attack event has occurred. The CIA compromise refers to the impact on the system, for example, the adversary accesses the account which lowers CIA. The privacy loss refers to the direct invasion of privacy when the adversary accesses and uses the device, which is further extended when considering the smart camera's function, allowing an adversary to spy inside the home. Finally, the financial loss considers the money extorted when the adversary performs the vishing attempt.

| Potential Impact | Household Notation and Impact Level | | |
|---|---|---|---|
| | $S_1$ | $S_2$ | $S_3$ |
| Negative emotional responses | Low | High | High |
| CIA compromise | Low | High | High |
| Privacy loss | Low | High | High |
| Financial loss | Low | Moderate | High |

Table 4. A representation of the potential impacts and level for each household considering the attack scenario.

## 5.4 Step 3: Decide whether existing precautions are adequate or if more should be done

The final step refers to the assessment of safeguards, addressing the efficiency to understand if the implemented safeguards are adequate for the home. Table 5 shows the possible safeguards within each home and the efficiency level towards each home. Formal training refers to training programmes that aim to increase understanding towards security thus aiming to provide insight into attack prevention, we assume that this training has been focused towards social engineering. The use of two-factor authentication is used to protect the smart camera's associated smartphone application account's access, providing an extra layer of protection and requiring information the adversary does not have.

| Safeguard Name | Household Notation and Impact Level | | |
|---|---|---|---|
| | S1 | S2 | S3 |
| Formal training (social engineering) | High | Moderate | Low |
| Use of two-factor authentication | High | Low | Low |

Table 5. A representation of the implemented and efficiency level of each for each household considering the attack scenario.

### 5.5 Case Study Results

SH-BARM suggests that the behaviours exhibited affected the expected loss, thus, when combining the model with the risk approach and an adversary attack path we can expose the problematic behaviours that make homes more susceptible. In the case study, we have shown an example of a low, moderate and high risk home using the Ring hacking events in 2019.

Within household $S_1$, the low-risk home, we show a best-case home with parameters that show a decreased risk towards the attack scenario. Since the household is aware and familiar with the threats toward the home, they do not exhibit risky behaviours that could increase the likelihood of the attack. This awareness also allows presents an increased perception and prevention ability, being able to identify and prevent an attack event with ease. On top of this, the susceptibility towards each attack event is low, since the safeguards have a high efficiency of preventing the attack. Finally, the potential impact towards the home is low, since the attack has a low chance of occurring and if it was to occur, the household would respond with high efficiency, minimising the impact.

Within household $S_2$, the moderate-risk home, we show a use case which decreases risk to an extent. This home portrays a home which, like real smart homes, combats attacks at various levels, with some attacks being at a higher risk than others. The home has a moderate security familiarity meaning that there is awareness and comprehension of smart home security practices, however, some concepts may not be fully understood, thus there is room for improvement. In turn, where this familiarity lacks, we find that risky behaviours are displayed showing the gap in awareness towards protecting the user account. Once again due to the awareness gaps, the rate of the attack being fully successfully is moderate, this is due to the perception and prevention of each attack event, with unauthorised access and use being low and vishing being moderate. The implemented safeguards have a low to moderate rate of efficiency, which is once again determined by the awareness to each attack, if a home is only partly aware of the threats, we can assume that the safeguards will reflect this. Finally, the impact shows that if the attack was to take place, the household can suffer many types of impacts, depending on the responses during the attack. If the home does not face a financial loss, they still risk losing privacy and having an impacted system where the adversary has control.

Within household $S_3$, the high-risk home, we find results that are the direct opposite of $S_1$, being riskier than $S_2$. We assume little to no familiarity which is reflected in by the risk behaviours that increase the likelihood of the attack happening. This lack of awareness shows poor perception and prevention ability when faced with an attack. If there is a lack of awareness toward an attack, the household may not implement any safeguards, thus making it harder to defend against the attack scenarios.

Our case study provides an example of how different behaviours can determine the outcome of an attack, with $S_1$ being of a low susceptibility and $S_3$ being high. An interesting finding from this study is that each home has a case base threshold if the attack happened. If the adversary targets $S_1$, it is highly likely they will fail to gain access due to out of date information or not enough information from $S_1$ not reusing passwords and use two-factor authentication. In the case of $S_2$, the adversary can gain asses and use the device, however, the chance of successfully achieving the end goal is moderate, since the household has some awareness to social engineering attacks.

Finally, if an adversary targets $S_3$ it is highly likely that the full attack goal will be achieved due to the lack of safeguards. $S_2$ and $S_3$ households lack of awareness for account hijacking reflects the two of the attack events that can be very hard to perceive. An adversary within $S_2$ and $S_3$ can also build the opportunity for a second attack if the households do not address the issues, thus the expected loss would grow. In doing this, not addressing the current risk allows the adversary to remain invisible whilst still using the comprised account.

### 5.6 Discussion and Challenges

Smart vendors such as Ring are starting to enforce mandatory security features that encourage good practice [26], however, access control and the safe operation of devices are inherently the responsibility of the smart home inhabitants. The overarching problem within the IoT scope is that devices have been created prioritising ease of use and automation, whereby users buy devices without considering the best security practises for their home. The encouragement to all users to change their IoT behaviour will be a strenuous job, matched by the rise of cyber-attacks and the likelihood of victim's fall for phishing attacks. However, smart home security has become more important than ever before, especially when devices with very high physical impact are being used within the home. For example, the proliferation of the Internet of Medical Things (IoMT) has brought a number of smart devices in the household, such as blood pressure monitors, portable EKG/ECG monitors, and glucose monitoring systems.

SH-BARM implies that users should be held accountable for smart home security where possible as their behaviours can affect risk, not just smart vendors and governments. This is a sentiment that IoT researchers should consider for their future works, targeting what smart home inhabitants should be doing to be defensive. The next challenge for our model is to identify a solution towards choosing the best safeguards for a home, which requires us to understand the types of safeguards within the human and practical categories. Another aspect is to test our model real setting, which was out of the scope for this work. Due to the lack of standardisation and homes containing fewer resources, safeguards are dependent on the needs of the smart home and the potential threats that could be faced. A core component to safeguards is to ensure that users have an updated awareness of risks so that the correct controls can be implemented at a high-efficiency level.

It would be interesting to propose a generalised, easy to implement risk management tool for the smart home to aid in the reducing of risks, selecting the most appropriate safeguards to not only protect the home inhabitants but organisations with employees working from home. This has the possibility of being extended towards any connected home network device, such as personal computers, displaying the differences in behaviour depending on the device. A tool such as this would benefit domestic users of various technologies to survive within the era of cybercrime to build a defensive and protected home that technology can thrive within.

## 6 CONCLUSIONS

In this paper, we have presented a smart home risk model which considers the human factor towards risk, alongside a realistic use case and risk assessing approach to help validate our solution. Our future work will be geared towards creating a smart home risk control model which aids in the decision making of countermeasures for the smart home and to examine our model in practice within a real-life setting.

The use of IoT within the home has been on the rise, with many more smart devices becoming normalised in day to day life. These devices are not always secure within the smart home, with many threats and attacks impacting households in various ways. If a home was to be attacked and the home is not prepared, the severity could be astronomical. This means that effective safeguard measures must be implemented to form a combative stance towards risk, creating a safer and more comfortable smart home experience for the end-user.

Risk assessments within the smart home setting are integral to aid the management of smart home attacks and threats, addressing factors that may increase the likelihood, success,and impact of an attack. As the number of potential risks grows, the more important user awareness towards smart home risk becomes, with smart home inhabitants sustaining their role within the IoT life cycle.

This paper proposed a Smart Home Behaviour and Attitude Risk Model which considers the human element of risk as a primary factor. We have presented a risk assessment approach for this model using HSG48 and provided a case study to further understand the importance of the human factor within risk assessments. The complexity

of smart services and devices was outside the scope of this work; thus, no smart home was created. Our future work will be to develop a solution towards aiding users to choose the best safeguards for their home.

## REFERENCES


[1] Orestis Mavropoulos, Haralambos Mouratidis, Andrew Fish, and Emmanouil Panaousis. Apparatus: A framework for security analysis in internet of things systems. *Ad Hoc Networks*, 92:101743, 2019.

[2] Dan Dahlberg. Identifying unique risks of work from home remote office networks. Online; accessed 19-09-2020.

[3] Junhyoung Oh, Ukjin Lee, and Kyungho Lee. Privacy fatigue in the internet of things (iot) environment. *IT CoNvergence PRActice (INPRA)*, 6(4):21–34, 2019.

[4] Avast. Avast smart home security report 2019, 2019. https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf. Online; accessed 19-09-2020.

[5] Jesus Pacheco and Salim Hariri. Iot security framework for smart cyber infrastructures. In *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W)*, pages 242–247. IEEE, 2016.

[6] Bako Ali and Ali Ismail Awad. Cyber and physical security vulnerability assessment for iot-based smart homes. *Sensors*, 18(3):817, 2018.

[7] Harjinder Singh Lallie, Lynsay A Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv preprint arXiv:2006.11929*, 2020.

[8] Mujahid Mohsin, Muhammad Usama Sardar, Osman Hasan, and Zahid Anwar. Iotriskanalyzer: A probabilistic model checking based framework for formal risk analytics of the internet of things. *IEEE Access*, 5:5494–5505, 2017.

[9] VL. Shivraj et al. A graph theory based generic risk assessment framework for internet of things (iot). In *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pages 1–6. IEEE, 2017.

[10] Michael E Whitman and Herbert J Mattord. *Principles of information security*. Cengage Learning, 2017.

[11] Yan Huang, Xin Guan, Hongyang Chen, Yi Liang, Shanshan Yuan, and Tomoaki Ohtsuki. Risk assessment of private information inference for motion sensor embedded iot devices. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2019.

[12] Tzu Wei Tseng, Chia Tung Wu, and Feipei Lai. Threat analysis for wearable health devices and environment monitoring internet of things integration system. *IEEE Access*, 7:144983–144994, 2019.

[13] Senyu Li, Fangming Bi, Wei Chen, Xuzhi Miao, Jin Liu, and Chaogang Tang. An improved information security risk assessments method for cyber-physical-social computing and networking. *IEEE Access*, 6:10311–10319, 2018.

[14] Ismini Psychoula, Deepika Singh, Liming Chen, Feng Chen, Andreas Holzinger, and Huansheng Ning. Users' privacy concerns in iot based applications. In *2018 IEEE SmartWorld*, pages 1887–1894. IEEE, 2018.

[15] Mansour Naser Alraja, Murtaza M Junaid Farooque, and Basel Khashab. The effect of security, privacy, familiarity and trust on users' attitudes towards the use of iot-based healthcare: The mediation role of risk perception. *IEEE Access*, 2019.

[16] Mikael Asplund and Simin Nadjm-Tehrani. Attitudes and perceptions of iot security in critical societal services. *IEEE Access*, 4:2130–2138, 2016.

[17] Sakshyam Panda, Emmanouil Panaousis, George Loukas, and Christos Laoudias. Optimizing investments in cyber hygiene for protecting healthcare users. *From Lambda Calculus to Cybersecurity Through Program Analysis*.

[18] RS Ross. Guide for conducting risk assessments nist special publication 800-30 revision 1. *US Dept. Commerce, NIST, Gaithersburg, MD, USA, Tech. Rep*, 2012.

[19] John Wunder, Adam Halbardier, and David Waltermire. *Specification for asset identification 1.1*. US Department of Commerce, National Institute of Standards and Technology, 2011.

[20] Alexander Kharlamov, Aakanksha Jaiswal, Glenn Parry, and Ganna Pogrebna. A cyber domain–specific risk attitudes scale to address security issues in the digital space, 2018.

[21] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny RJ Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, 78:398–428, 2018.

[22] Lauri Nummenmaa, Riitta Hari, Jari K Hietanen, and Enrico Glerean. Maps of subjective feelings. *Proceedings of the National Academy of Sciences*, 115(37):9198–9203, 2018.

[23] European Union Agency for Cybersecurity. Good practices for security of iot - secure software development lifecycle. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1, Dec 2019.

[24] HSE Books. Reducing error and influencing behaviour, 2009.

[25] Mitre. Pre-att&ck matrix. https://attack.mitre.org/matrices/pre/, 2019. Online; accessed 05-08-2020.

[26] Leila Rouhi. Extra layers of security and control. https://blog.ring.com/2020/02/18/extra-layers-of-security-and-control/, 2020. Online; accessed 05-08-2020.