The invisible cyber intruder

An experimental study into the effects of type of smart home device, type of security attack on crisis responsibility, trust towards the organisation, trust towards the device, perceived threat, and intention to use.

Carlijn van den Heuvel
S1740849
c.m.vandenheuvel@student.utwente.nl

Submitted in partial fulfilment of the requirements for a degree of Master of Science, program Communication Science, Faculty of Behavioural, Management and Social Sciences, University of Twente

20-07-2023

First supervisor
Drs. M.H. Tempelman

Second supervisor
Dr. A. van der Zeeuw

Abstract

Aim. The popularity of smart home devices has increased, though these internet-connected devices are a vulnerable target for security attacks. However, security attacks are a rather new phenomenon and have therefore not been taken into account in crisis communication research before. This study aims to explore the impact of cyberattacks on consumers' attitudes towards smart home devices and develop crisis communication strategies specifically tailored to this new and vulnerable phenomenon. By incorporating Coombs' Situational Crisis Communication Theory (SCCT), the research seeks to provide valuable insights for effective post-crisis communication in the context of smart home devices.

Method. An online experiment, using a scenario based 2 (type of smart home device: high intrusiveness vs. low intrusiveness) x 2 (type of security attack: passive vs. active) between-subjects experimental design was executed among 215 participants.

Findings. The results of this study revealed that passive security attacks had a greater influence on trust towards the organisation and the device compared to active attacks. However, the type of security attack did not significantly affect perceived threat or crisis responsibility, except for masquerade attacks, which resulted in higher crisis responsibility attributed to the smart home device manufacturer. Additionally, the level of intrusiveness of smart home devices did not significantly affect trust, perceived threat, or crisis responsibility. Interestingly, the study revealed that trust towards the device found to be the only significant predictors of intention to use smart home devices. In contrast, trust towards the organisation, crisis responsibility and perceived threat, did not significantly affect the intention to use smart home devices.

Conclusion. This study highlights the crucial role of trust in the context of smart home technologies. Trust in the device was found to be the only significant predictor, which underscores the importance of building and maintaining trust in the smart home devices themselves, with reliable performance and robust security measures being prioritised by manufacturers. The study also revealed different effects of different types of security attacks on consumer perceptions, highlighting the need for effective crisis communication strategies. The study provides valuable insights for effective post-crisis communication and contributes to understanding and strengthening consumer trust in the rapidly evolving digital landscape.

Keywords: Crisis communication, smart home environments, smart home devices, home automation, security attacks

Index

1. Introduction

A key element of the future Internet is the domain of smart home environments. Houses are becoming "smarter" by using the Internet of Things (IoT) technology (Jacobsson & Davidsson, 2015). The term IoT was introduced in 1999 and described as “objects that are able to communicate via the Internet” (Uckelmann, Harrison & Michahelles, as cited in Lee, 2018, p. 536). The popularity of smart home devices has been on a rise, encompassing a wide range of products such as smart plugs, thermostats, cameras, voice-activated devices, and TVs. According to recent research, the number of IoT-connected devices had already reached approximately eleven billion by 2020, and by 2025, that number is anticipated to reach thirty billion (Zlatolas, Fehrer & Hölbl, 2022).

However, the rapid growth in the use of these devices has also led to a growing concern: the risk of cyber-attacks. As smart devices are connected to the internet and communicate with each other, they become vulnerable to cybersecurity threats. For example, in 2019, a family in the United States reported that their smart home system had been hacked, which allowed an intruder to gain access to their indoor security cameras and thermostats. Using the system, the hacker spoke to the family through the cameras and adjusted the thermostat to uncomfortable levels (Sears, 2019).

Cybersecurity attacks on smart home devices can be divided into active and passive Active attacks are attempts by an attacker to alter or disrupt the normal operation of a system or network, either by gaining unauthorized access, altering data, or introducing malware. In an active attack, the attacker seeks to actively manipulate or damage the target system or network. Passive attacks are attempts by an attacker to intercept or monitor communications without changing the content of the message, to gather information that can be used for malicious purposes. In a passive attack, the attacker seeks to observe and gather sensitive data or information without disrupting the normal operation of the system or network (Ali, Dustgeer, Awais & Shah, 2017; Olawumi, Väänänen & Haataja, Toivanen, 2017).

Cybersecurity incidents can have severe consequences for a smart home company, leading to potential crises and significant reputational damage (Knight & Nurse, 2020). These incidents not only damage the reputation of an organisation, but also affect the trust of stakeholders and their interactions with the company (Coombs, 2007). It is essential for IoT manufacturers to understand the specific impact of such crises on their industry. Effective communication after a crisis is crucial to restore stakeholder trust (Sen & Borle, 2015). Moreover, research has shown that trust plays a crucial role in consumers' decision to adopt

IoT technologies and services (AlHogail, 2018). Trust helps consumers to overcome perceptions of uncertainty and risk associated with smart home devices and enhances the consumers' level of acceptance and ultimately intent to use these technologies. By addressing concerns about cybersecurity incidents and emphasising trustworthiness, IoT manufacturers can increase the level of trust among potential consumers.

The impact of crisis situations on consumers' attitudes towards organisations has been extensively researched. Coombs (2007) provides a framework called the Situational Crisis Communication Theory (SCCT) that outlines how organisations can minimise reputational damage through post-crisis communication. However, Coombs' study primarily focused on more traditional crisis situations, such as natural disasters, product recalls, and corporate scandals. The SCCT framework has been widely applied in various context, however, as cyberattacks on smart home devices are a relatively new phenomenon it is relatively unexplored. This study builds on Coombs' work by investigating appropriate crisis communication strategies in a new context with specific characteristics.

Therefore, the aim of this study is to investigate the effect of different types of security attacks on consumers' feelings of trust, perceived threat, crisis responsibility, and intention to use smart home devices, with the goal of filling the gap in the literature on the impact of cyberattacks on smart home devices in the context of crisis communication. Taking this all into account, the following research question can be formulated:

RQ: *To what extent do type of smart home device (high intrusiveness vs. low intrusiveness) and type of security attack (passive vs. active) affect crisis responsibility, trust towards the organisation, trust towards the device, perceived threat, and intention to use smart home devices?*

First, a theoretical framework will be outlined from which hypotheses will be derived to contribute to answering the research question. Subsequently, a detailed explanation of the research methodology and instrument will be presented, followed by the research results. Lastly, the report will be concluded with a discussion that summarises the results, limitations, and recommendations for future research.

2. Theoretical framework

2.1 Internet of Things (IoT) and smart home devices

2.1.1 Internet of Things (IoT)

In 1999 British technology pioneer Kevin Ashton first used the term "Internet of Things" (IoT). Ashton described this term as "objects in the physical world that could be connected to the Internet by sensors" (Rose, Eldridge & Chapin, 2015). The concept of the IoT refers to a system of interconnected physical objects, including devices, vehicles, buildings, and other items. These objects are embedded with electronics, software, sensors, and network connectivity, which enable them to collect and exchange data (Gokhale, Bhat & Bhat, 2019). Through the IoT, objects can be remotely sensed and controlled using existing network infrastructure. This opens possibilities for more seamless integration of the physical world into computer-based systems, leading to increased efficiency and accuracy.

2.1.2 Smart home devices

The smart home, which refers to a household that is furnished with information and communication technology to enable the interoperability of various household products and services, is considered to be a notable example of an Internet of Things (IoT) service that has garnered significant attention in recent times (Peine, 2008, as cited in Hong, Nam & Kim, 2020). A broad definition of a Smart Home is provided by Aldrich (2003, as cited in Solaimani, Keijzer-Broers & Bouwman, 2013, p. 2):

> A Smart Home can be defined as a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment through the management of technology within the home and connections to the world beyond.

However, there are also industry-specific definitions for a smart home. For example, in the home automation industry (also called Domotica), a Smart Home refers to a residence or living space equipped with technology that enables automated control of devices and systems (Hu, Wei, Cong, 2013).

The market for smart homes has witnessed remarkable growth, with prominent global information technology (IT) companies such as Google, Amazon and Apple actively involved in this sector and leading the sales of smart home devices (Hong, Nam & Kim, 2020). Recent research shows that over 4.8 million households (59%) in the Netherlands own at least one smart home product (Multiscope, 2023). Dutch households have a total of about €4.1 billion worth of smart home products in their homes, with smart lighting or switches being the most common devices, accounting for 36 percent. Approximately 28 percent of homes are equipped with smart security or safety devices, while the remaining smart home products fall into categories such as energy and heating, smart speakers, and household and comfort.

2.2 Security attacks

The development of the Internet of Things (IoT) has led to the growth of smart home environments, which offer users a wide range of benefits, such as temperature monitoring, smoke detection, automatic lighting control and smart locks (Touqeer et al., 2021). However, as Ali, Dustgeer, Awais and Shah (2017) noted, the Internet-connected nature of these environments also creates new challenges in terms of security, authentication, and privacy. In particular, IoT devices and sensors can exchange data over networks, which enables them to solve different issues and provide new services (Touqeer et al., 2021). Unfortunately, that same connectivity also exposes smart homes to various types of security attacks, which can put users' private data at risk.

Such security attacks are classified into two main categories, active and passive (Ali, Dustgeer, Awais & Shah, 2017; Olawumi, Vaananen, Haataja & Toivanen, 2017; Panigrahi, 2022; GeeksforGeeks, 2023). First, an active security attack involves an attacker trying to modify or introduce fraudulent data into a system's internal network. Attacks of this type alter or destroy data intentionally, disrupting the normal operation of the system (Olawumi et al., 2017; Geeksforgeeks, 2023). The activities of active attackers may include the modification of transmitted or stored data or the injection of new data streams into the internal network of the system (Olawumi et al., 2017). Active attacks can take various forms, including denial of service (DoS), malware, masquerade, change of the message's content, repudiation, replay, and password cracking (Ali et al., 2017; Geeksforgeeks, 2023). These types of attacks can harm the integrity and availability of a system's resources Active attacks are rather easy to detect as the victims are usually getting notified about active attacks (Panigrahi, 2022). This is mainly because active attacks involve direct interaction with the victim's system or network, leaving visible traces or provoking responses that can be easily detected.

On the other hand, passive security attacks are attempts by an attacker to gain unauthorized access to private information by monitoring or listening to its transmission without modifying it (Olawumi et al., 2017). Passive attacks attempt to obtain information from a system without affecting its resources, unlike active attacks (Geeksforgeeks, 2022). In passive attacks, transmissions are monitored or eavesdropped on. They are not altered or destroyed.

Examples of passive attacks include eavesdropping, sniffing, and monitoring transmissions, where the attacker captures and analyses data packets to steal sensitive information (Ali et al., 2017; Geeksforgeeks, 2023). Passive attacks are particularly harmful to the confidentiality of the message since they do not alter the original message and can be difficult to detect as the victim is not notified about the attack and the attacker does not modify the transmitted messages (Olawumi et al., 2017; Ali et al., 2017; Panigrahi, 2022). Detecting passive attacks can be challenging since they do not leave direct visible traces. They are often detected through network monitoring and traffic analysis, identifying suspicious patterns and anomalies.

The perception of the system's security and reliability can be undermined by security attacks, which can negatively affect users' trust in the device. As a result, trust in the device can be reduced and the perceived threat associated with the device can be raised.

Furthermore, it can be argued that passive attacks are more severe than active ones because passive attacks remain undetected for longer periods, allowing attackers to gather sensitive data or spy on the users' behaviour without their knowledge, causing greater harm and privacy violations.

From this, the following hypothesis can be drawn up for this study:

H1: A passive security attack (in contrast to an active security attack) results in a (a) higher degree of perceived threat, (b) greater decrease in trust towards the device.

Moreover, it is important to consider the different levels of intrusiveness since users' trust in particular devices can be affected by their level of intrusiveness. When devices have high intrusiveness, they often collect and store extensive amounts of personal information, raising concerns and decreasing trust in the device. Further, higher privacy and security concerns arise from the collection and storage of more personal information by high intrusive devices. These concerns, in turn, may influence the perceived threat associated with the devices.

Based on this, the following is hypothesised:

H2: High intrusive devices (in contrast to low intrusive devices) are associated with (a) a higher degree of perceived threat, (b) a greater decrease in trust towards the device.

2.3 Managing crisis situations

A crisis situation not only affects users' perceptions towards the device, but it also affects perceptions towards the organisation behind it. As Coombs (2007) already found in his study, crisis situations affect the reputation of organisations. First, a theoretical understanding of a crisis will be provided, with a specific definition of its characteristics and components. This lays the foundation for further exploration of Coombs' Situational Crisis Communication Theory.

2.3.1 What is a crisis?

The term crisis has been defined or explained in many ways. The term "crisis" originates from the Greek word "*krisis*" which denotes "a time of great danger, difficulty or doubt when problems must be solved or important decisions must be made" (Oxford University Press, n.d.). Several authors have widely explored the term crisis according to their specific discipline, including public relations, management, and organisational communication (Coombs & Holladay, 2010).

A crisis can cause a threat to corporate reputation. Coombs (2007) described crisis as "a sudden and unexpected event that threatens to disrupt an organisation's operations and poses both a financial and a reputational threat" (p. 164). During a crisis, the organisation's reputation is at risk, as it can give people a reason to view it negatively. The news media and the internet are influential in shaping perceptions during such times. The majority of stakeholders rely on news reports to learn about a crisis (Coombs, 2007). Therefore, communication is essential in time of a crisis (Seeger, Sellnow & Ulmer, 1998).

2.3.2 Managing a crisis

Extensive research has already been performed on crisis communication. Crisis communication is defined as "the collection, processing, and dissemination of information required to address a crisis situation" (Coombs, 2012, p. 20). As mentioned above, communication is essential in times of a crisis. Crises damage organisations' reputation and such threat affects the stakeholders' interaction with the organisation (Barton, 2001; Dowling, 2002, in Coombs 2007a). The Situational Crisis Communication Theory (SCCT) of Coombs (2007b) provides a framework for understanding how organisations can maximize their reputational protection by post-crisis communication.

The SCCT of Coombs predicts the level of reputational damage caused by a crisis, based on the type of crisis, the severity, and prior reputation (Coombs, 2007a). The SCCT draws upon the principles of Attribution Theory, which suggests that people tend to attribute causes or responsibility to events, particularly negative events such as a crisis. The crisis responsibility in SCCT refers to the extent to which stakeholders hold the organisation responsible for the crisis. During a crisis, stakeholders tend to designate a responsible party to take the blame and at the same time try to limit the damage caused (Brown & Ki, 2013). The degree to which an organisation is blamed is an integral part of an organisation's degree of crisis responsibility, which can also be interpreted as the degree of blame attributed to the organisation (Millar & Heath, 2004). The level of responsibility can have a significant impact on how stakeholders perceive and respond to the crisis (Coombs, 2007b). According to Coombs (2007), if stakeholders perceive a higher level of crisis responsibility on the part of the organisation, it can lead to greater reputation damage. Eventually, this can lead to several negative outcomes, including a damaged image, legitimacy, and reputation for the organisation, as well as financial and legal liability (Sellnow & Seeger, 2013). Security attacks may affect the perception of crisis responsibility, with users holding the organisation responsible for the effects of the attack on their privacy and safety.

Next to crisis responsibility, security attacks may influence the users' trust in the organisation behind the system. Since the organisation has the responsibility to protect the users' privacy and security, security attacks can be seen as a failure in fulfilling this responsibility. Failing to protect the users' privacy and security affects the trust in the organisation behind the system, which in turn can determine the perceived safety and reliability of the system.

Furthermore, it may be argued that passive security attacks have a greater impact on users' trust in the organisation behind the system and crisis responsibility than active attacks. Considering that passive attacks are difficult to detect, leaving the organisation unaware that attackers are, for example, eavesdropping on users undetected. Resulting users to feel helpless and lose trust in the organisation. Moreover, due to the invisible and undetected nature of passive attacks, it may be more challenging for an organisation to take responsibility for the attack, leading to greater user uncertainty and further eroding trust in the organisation. From this, the following hypothesis can be drawn up for this study:

H3: A passive security attack (in contrast to an active security attack) results in (a) a higher level of crisis responsibility, and (b) a greater decrease in trust towards the organisation.

Furthermore, devices with high intrusiveness are more sensitive in nature and if something goes wrong with a device with high intrusiveness, users will feel more insecure and assign a high degree of crisis responsibility to the organisation behind the system. Since an attack on a high intrusiveness device result in an invasion of users' privacy, it will also lead to a large decrease in trust in the organisation. Thus, the following hypothesis is proposed:

H4: High intrusive smart devices (in contrast to low intrusive smart devices) are associated with (a) a higher level of crisis responsibility, and (b) a greater decrease in trust towards the organisation.

In addition to assessing the direct effects of the independent variables on the four dependent variables, an investigate will be conducted to determine the presence of a possible interaction effect between the type of smart home device (high intrusiveness vs. low intrusiveness) and the type of security attack (passive vs. active). The following hypothesis can be proposed:

H5: There is an interaction effect between the type of smart home device (high intrusiveness vs. low intrusiveness) and the type of security attack (passive vs. active) on (a) perceived threat, (b) crisis responsibility, (c), trust towards the organisation, and (d) trust towards the device.

2.4 Intention to use smart home devices

2.4.1 Perceived threat

The perception of consumer risks related to product adoption and usage has been studied for many years (Bauer 1967, Dowling & Staelin 1994). Perceived threat (i.e., perceived risk or concern) is described as uncertainty about possible negative consequences of using a product or service. Research has shown that perceived threat can reduce the acceptance and adoption of technology (Chen & Barnes, 2007). Concerns about privacy, which also shape attitudes to purchases, have been an important consideration in studies of consumer purchase intent and behaviour for decades (George, Chen & Yuan, 2021). Perceived threat can reduce users' intention to use smart home devices, as users may be concerned about the security of their devices and their privacy. Therefore, the following can be hypothesised:

H6: Perceived threat will have a negative effect on the intention to use.

2.4.2 Trust towards the device

Next to perceived threat, earlier research has also concluded that trust plays a significant role in accepting Internet technologies (Gefen, 2000). When users trust a technology, they will intuitively adopt a positive attitude towards using that technology (Shuhaiber & Mashal, 2019). Luor et al. (2015) found that residents' perception of trust in smart homes is positively related to their attitudes toward smart homes. Park et al. (2018) also reported that trust in smart homes was positively related to users' intention to use smart homes. Therefore, there can be concluded that trust towards smart home devices, can strengthen users' intention to use smart home devices, as users have more confidence in the safety and reliability of the devices. From this reasoning, the following hypothesis follows:

H7: Trust towards the device will have a positive effect on the intention to use.

2.4.3 Crisis responsibility

Brands or organisations' reputations may be negatively impacted by crises, which may affect consumers' intentions to buy or use their products or services. This perception is known as "crisis responsibility" and refers to the extent to which the organisation can be held accountable for the occurrence of the event (Coombs & Holladay, 2002). It relates to how stakeholders perceive the organisation's actions or inactions prior to and during a crisis (Coombs, 2007). Crisis responsibility is a key indicator of the potential reputational damage a crisis might cause (Coombs & Schmidt, 2000). Coombs & Holladay (2007) indicate that stakeholders may have lower purchase intent if they perceive that the brand or organisation has not acted responsibly to protect them. As opposed to this, stakeholders who perceive the crisis was not intentional will be more likely to purchase (Coombs, 2007b).

Following this, crisis responsibility of the smart home device manufacturer influences the intention to use, as the organisation's sense of responsibility for managing security incidents and restoring users' trust can play an important role in whether people will use smart home devices. The following will be hypothesised:

H8: Crisis responsibility will have a negative effect on the intention to use.

2.4.4 Trust towards the organisation

Trust is essential to a successful buyer-seller relationship. A study by Luor et al. (2015) found that attitudes toward smart home services and perceptions of trust were positively correlated. Users who trust the organisation that develops and produces the specific smart home devices, are more likely to use and continue using them. Lacking this trust, users may be reluctant to share personal information or use the smart home devices for their intended purpose if they are concerned about the security or reliability of the organisation behind the devices. The hypothesis can be stated as follows:

H9: Trust towards the organisation will have a positive effect on the intention to use.

2.5 Research model

The research model that follows from these hypotheses is visualised in Figure 1. The full list of hypotheses is presented in Appendix B.

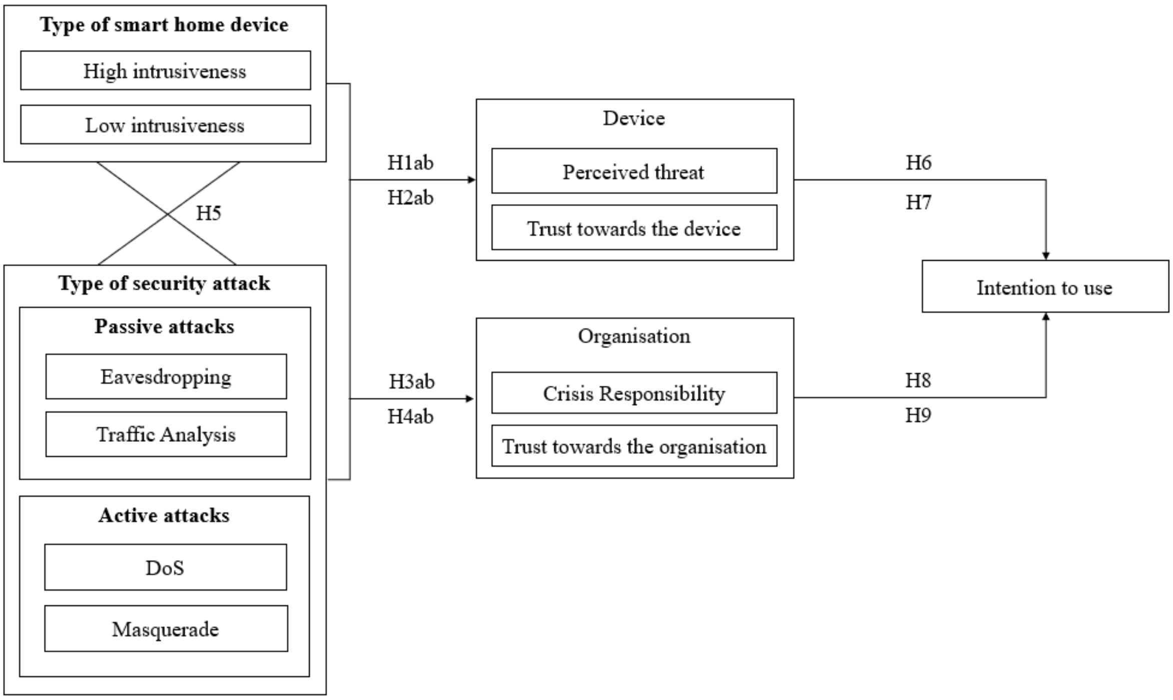


Figure 1. Research model

3. Method

3.1 Design

To address the research question proposed for this study, a scenario-based 2 (type of smart home device: high intrusiveness vs. low intrusiveness) x 2 (type of security attack: passive vs. active) experimental design was executed (Table 1). A fictitious company NexaHome, which sells smart home devices, was used in the scenario to evaluate the hypotheses. A fictional organisation was used to rule out any associations with the brand, such as former reputation or brand preferences, which could lead to any bias (Laufer & Jung, 2010). A pre-test was conducted before the main study was designed.

Table 1

Overview of 2 x 2 design

		Type of smart home device	
		High intrusiveness	Low intrusiveness
Type of security attack	Passive	Eavesdropping Traffic analysis	Eavesdropping Traffic analysis
	Active	DoS Masquarade	DoS Masquarade

3.2 Pre-test

Prior to the main study, a pre-test was conducted to determine which stimulus materials and manipulations to use. The pre-test involved a scenario-based between-subjects experiment with a 2 (smart home device: smart camera vs smart thermostat) x 2 (type of security attack: passive vs active) factorial design, resulting in four experimental conditions. This was intended to determine whether respondents can distinguish passive from active security attacks. Additionally, the respondents' the associated privacy risks of different smart home devices have been examined. In total, 51 respondents participated.

3.2.1 Privacy risks smart home devices

Firstly, the respondents were presented a total of eight most popular smart home devices in the Netherlands according to an online study from Statista (2022). Current literature gave no clear description of which smart home devices are perceived as most risky to use. Therefore, respondents were asked to what extent they assess the privacy risks associated with the use of smart home devices on a 7-point Likert scale ranging from "No risk at all" to "Extreme risk".

Table 2 shows the associated privacy risks for the different smart home devices. The list of smart home devices was randomly ordered for every respondent.

The lowest scores were assigned to the bluetooth speaker without a virtual assistant (*M* = 2.37), smart bulbs (*M* = 2.41) and smart thermostats (*M* = 2.73). On the other hand, smart speakers with an integrated virtual assistant (*M* = 5.27) and smart security cameras (*M* = 5.94), received the highest scores. However, t-test results revealed no significant difference between the scores of bluetooth speakers and smart thermostats (*t*(50) = -1.66, p = .104). Similarly, there was no significant difference observed between the scores of smart bulbs and the smart thermostat (*t*(50) = -2.22, p = .031). Therefore, based on the non-significant differences observed among the scores of the devices it can be concluded that all three devices can be seen as equally low in terms of intrusiveness. While there is no significant difference between device scores, a smart thermostat was also chosen as the 'low intrusiveness' device based on other factors. Smart thermostats may pose unique privacy risks as they access sensitive information such as energy consumption and presence in the home. Therefore, the choice of smart thermostat was based not only on the pre-test results, but also on the potential for collecting more sensitive data compared to the other devices.

The mean score for the privacy risks associated with smart security cameras (*M* = 5.94, *SD* = 1.35) was found to be significantly higher than the mean score for smart thermostats (*M* = 2.73, *SD* = 1.65), *t*(50) = -12.73, p < .001, two-tailed, suggesting that participants perceived smart security cameras to be more risky in terms of privacy compared to smart thermostats. With all this in mind, the smart thermostats were chosen as the low intrusiveness smart devices and the smart security camera as the high intrusiveness devices.

Table 2

Mean scores and standard deviations of the associated privacy risks of different smart home devices

Smart home device		Privacy risks	
		M	*SD*
1.	Bluetooth speaker without a virtual assistant	2.37	1.51
2.	Smart bulbs	2.41	1.60
3.	Smart thermostats	2.73	1.65
4.	Smart plugs	2.86	1.47
5.	Smart TVs	3.10	1.87
6.	Streaming devices (e.g. Amazon Fire TV stick, Google Chromecast)	4.08	1.41
7.	Smart speakers with an integrated virtual assistant (e.g. Google Home, Amazon Echo)	5.27	1.13
8.	Smart security cameras	5.94	1.35

Note: measured on a 7-point Likert scale

3.2.2 Identifying type of security attack

Next, respondents were shown stimulus material (full list in Appendix C) with manipulated security attacks and smart home devices. After being briefed on the types of security attacks (passive vs. active), respondents read the stimulus material. After reading the text, they were asked to identify the type of security attack and what type of smart home device had been impacted.

As part of the manipulation check, respondents were asked to assess the extent to which they believed the attacker attempted to (1) observe the system, (2) gather information, (3) change the system's content, and (4) damage the system. Statements 1 and 2 refer to passive security attacks, while statements 3 and 4 refer to active security attacks. Each item was scored on a 7-point Likert scale, from "Totally disagree" to "Totally agree".

As Table 3 shows, the results of the manipulation check showed that respondents were able to distinguish between passive and active security attacks. The t-test results indicate that there is a significant difference between the mean scores for passive and active statements in the stimulus material including the passive security attack. The mean score for the passive statements (*M* = 6.63, *SD* =.555) was significantly higher than the mean score for the active statements (*M* = 2.14, *SD* = 1.32), t(50) = 20.30, p < .001, two-tailed. The mean score for the active statements in the stimulus material including the active attack also indicate a significant difference. The mean score for the active statements (*M* = 5.94, *SD =1*.29) was significantly higher than the mean score for the passive statements (*M* = 3.24, *SD* = 2.20), t(50) = -6.32, p < .001, two-tailed, indicating that the manipulation was successful.

Table 3

Mean scores, standard deviations and t-tests of the manipulations

	Passive security attack					*Active security attack*				
	M	*SD*	*df*	*Sig.*	*t*	*M*	*SD*	*df*	*Sig.*	*t*
Passive statements	6.63	.555	50	<.001	85.22	3.24	2.20	*50*	<.001	10.50
Observe the system	6.55	.702				3.20	2.21			
Gather information	6.71	.576				3.27	2.34			
Active statements	2.14	1.32	50	<.001	11.54	5.94	1.29	50	<.001	32.77
Change the system content	2.06	1.39				5.86	1.58			
Damage the system	2.22	1.57				6.02	1.61			

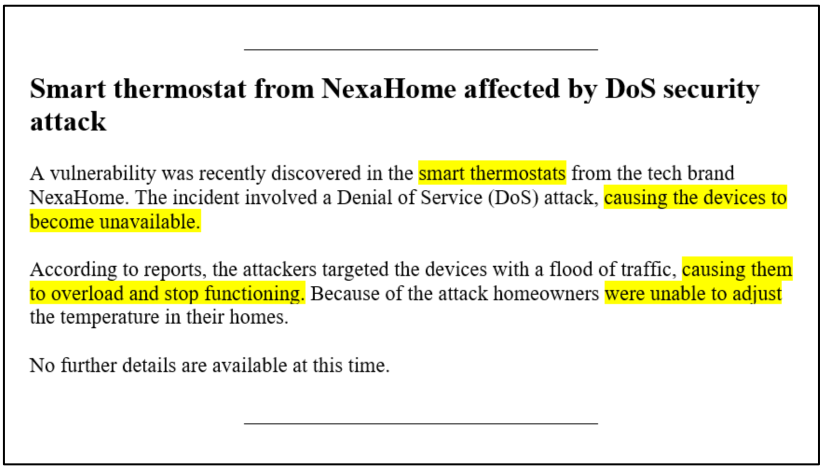
Note: measured on a 7-point Likert scale

Table 4
Experimental conditions type of smart home device, type of security attack

Condition 1 High intrusiveness: smart camera; passive attack: eavesdropping	Condition 5 Low intrusiveness: smart thermostat; passive attack: eavesdropping
Condition 2 High intrusiveness: smart camera; passive attack: traffic analysis	Condition 6 Low intrusiveness: smart thermostat; passive attack: traffic analysis
Condition 3 High intrusiveness: smart camera; active attack: DoS	Condition 7 Low intrusiveness: smart thermostat; active attack: DoS
Condition 4 High intrusiveness: smart camera; active attack: masquerade	Condition 8 Low intrusiveness: smart thermostat; active attack: masquerade

3.3 Stimulus materials and procedure

Following the pre-test, stimuli were developed for the main study. The experiment was administered by an online questionnaire, whereby participants were randomly assigned to one of the eight different scenarios (Table 4). For all eight conditions, the independent variables type of smart home device and the type of security attack were manipulated. Respondents were asked to imagine that they are a user of a NexaHome branded smart device and that one day they discover a news article on a prominent news site that catches their attention. The scenarios presented to the respondents included a text which revealed that a certain smart home device from NexaHome was facing a security attack. Figure 2 shows two examples of the scenarios.



Smart thermostat from NexaHome affected by DoS security attack

A vulnerability was recently discovered in the smart thermostats from the tech brand NexaHome. The incident involved a Denial of Service (DoS) attack, causing the devices to become unavailable.

According to reports, the attackers targeted the devices with a flood of traffic, causing them to overload and stop functioning. Because of the attack homeowners were unable to adjust the temperature in their homes.

No further details are available at this time.

Figure 2. Example of condition with an active, DoS attack and low intrusive device.

In the images, the different manipulations are highlighted. These highlights were absent in the actual study and is now purely added for clarification. After reading the scenario, respondents were asked to answer statements regarding the dependent variables.

Respondents were notified that they would need to answer a question about the content of the text at the end of the survey, to ensure that respondents read the scenarios thoroughly. These questions were asked as a manipulation check.

3.4 Participants

To reach participants, a convenience sampling approach was used. Next to that, a snowballing technique was used by asking participants to share the questionnaire within their network. In total, 340 respondents participated in this study. Yet, data of 125 respondents had to be discarded, as they did not complete the questionnaire fully, or clicked through the page with the stimulus material too quickly, implying that they did not read the scenario sufficiently. Therefore, data from 215 responses were used for the analyses. Of these 215 participants, 44% were male (*N* = 85) and 56% were female (*N* = 116). The respondents' age ranged from 18 to 76, with a mean of 33.11 (*SD* = 12.70). A total overview of the respondents' demographics per condition can be found in Table 5 on the next page.

Table 5

Overview of respondents' demographics per condition

	Age		Gender				Educational level		User smart home devices		Total	
			Male	Female	Other	PNTS						
Conditions	*M*	*SD*	*N*	*N*	*N*	*N*	*M*	*SD*	*M*	*SD*	*N*	*%*
1. SC-P-ED	31.04	11.19	10	18			6.18	1.06	4.00	1.19	28	13.0
2. SC-P-TA	34.75	15.88	13	15			5.57	1.40	3.75	1.40	28	13.0
3. SC-A-DO	35.33	12.80	18	6			5.67	1.58	4.04	1.27	24	11.2
4. SC-A-M	31.92	12.85	9	14	2		5.64	1.41	3.44	1.58	25	11.6
5. ST-P-ED	35.46	13.70	10	16			5.65	1.29	3.46	1.42	26	12.1
6. ST-P-TA	32.66	11.54	12	16		1	5.41	1.50	3.38	1.32	29	13.5
7. ST-A-DO	33.04	13.11	12	14			5.62	1.50	3.85	1.41	26	12.1
8. ST-A-M	31.14	10.85	11	17	1		5.79	1.45	3.62	1.24	29	13.5
Total	33.11	12.70	95	116	3	1	5.69	1.40	3.69	1.35	215	100

Note: SC = Smart camera; ST = Smart thermostat; P = Passive; A = Active; ED = Eavesdropping; TA = Traffic analysis; DO = DoS; M = Masquerade; PNTS = Prefer not to say; Educational level: 1 = Primary education, 7 = Scientific education; User smart home devices: 1 = Never heard of it, 5 = Use at home.

3.5 Measures

The dependent variables were measured using previously validated scales. All questions in the questionnaire were measured on 7-point Likert scales, ranging from “Strongly disagree” to “Strongly agree”. The full list of used constructs and items in the main study can be found in Appendix A.

3.5.1 Dependent measures

Crisis responsibility was measured using seven items from Coombs and Holladay (2002). Examples of items are: “The cause of the crisis was something the organisation could control” and “The blame for the crisis lies in the circumstances, not the organisation.”

The variable trust was divided into two parts: 1) *trust towards the organisation* and 2) *trust in the device*. Both constructs were adapted from Yang, Lee and Zo (2017) and consisted of four items each. An example of an item measuring trust in an organisation is “I think the organisation is reliable” and “I think the organisation keep customers’ best interest in mind”. In order to measure trust in the device, Yang, Lee, and Zo (2017) scales have been adjusted. This scale includes items such as “I feel confidence in smart home devices” and “I think smart home devices meet their expectations”.

Five items to measure perceived threat have been adopted from the research of Duezguen et al., 2020). Examples of items in this scale are: “Smart home devices pose a threat to my security and privacy” and “It is terrible, when my security and privacy is violated by smart home devices.”

Intention to use was measured by the scale from Klobas, McGill and Wang (2019). This scale consists of three items, such as: “I would like to use smart home devices” and “I can see myself using smart home devices.”

3.5.2 Validity and reliability

To establish the validity of the questionnaire, a factor analysis was conducted (Table 6, on the previous page). Upon examining the results, it was evident that all items converged to their respective scales. There was a factor loading of over .7, indicating that the items and their underlying constructs are strongly related. Next to that, the reliability of the different scales used in this study was calculated by determining the Cronbach's alpha of each individual scale. Here, the rule of thumb of George and Mallery (2003) was observed: $\alpha > .9$ - excellent, $\alpha > .8$ - good, $\alpha > .7$ - acceptable, $\alpha > .6$ - questionable, $\alpha > .5$ - not good, $\alpha > .4$ - unacceptable. When

Table 6

Factor analysis for the dependent variables

Scales with associated items	*1*	*2*	*3*	*4*	*5*
1. Crisis responsibility					
The blame for the crisis lies with NexaHome	.643				
The cause of the crisis was something NexaHome could control	.504				
The cause of the crisis is something over which NexaHome had no power *	.710				
The cause of the crisis is something that was manageable by NexaHome	.674				
The cause of the crisis is something over which NexaHome had power	.794				
2 Trust towards the organisation					
I think NexaHome is reliable		.855			
I think NexaHome keeps promises and commitments		.608			
I think NexaHome keeps customers' best interests in mind		.671			
I feel confidence in brand NexaHome		.713			
3. Trust towards the device					
I think smart home devices are reliable.			.879		
I think smart home devices meet their expectations			.655		
I think smart home devices serve users' interests			.433		
I feel confidence in smart home devices.			.566		
4. Perceived threat					
Smart home devices pose a threat to my security and privacy				.906	
The trouble caused by smart home devices threaten my security and privacy				.702	
Smart home devices are a danger to my security and privacy				.777	
Using smart home devices is a risk to my security and privacy				.729	
5. Intention to use					
I would like to use smart home devices					.805
I expect to use smart home devices.					.970
I can see myself using smart home devices					.968
Eigenvalue	3.49	3.82	4.04	3.89	4.3
% of variance	15.44	3.03	5.65	10.03	26.58
Cronbach's alpha *(α)*	.81	.86	.85	.88	.95
Deleted items	2	0	0	1	0

Note: * = Reversed scored item

the Cronbach's alpha is lower than .5, the scale will have to be found as not reliable.

To increase the reliability, it was decided to remove two items in the crisis responsibility scale. The two deleted items (“Circumstances, not NexaHome, is responsible for the crisis” and “The blame for the crisis lies in the circumstances, not NexaHome”) showed low correlation with the other items in the scale and did not contribute significantly to the internal consistency of the scale, as measured by the Cronbach's alpha. In addition, one item (“It is terrible when my security and privacy is violated by smart home devices”) was removed from the perceived threat scale to significantly increase the Cronbach's alpha value, indicating improved reliability of this scale. After the removal of some items, the Cronbach's alpha for all scales is above .80 and can therefore be considered reliable.

4. Results

4.1 Manipulation checks

To test whether the stimulus materials were correctly manipulated, a manipulation check was conducted. All items were measured on a 7-point Likert scale ranging from “Strongly disagree” to “Strongly agree”. The passive security attack was tested with two items (“I think the attacker tried to observe the system” and “I think the attacker tried to gather information”, α = .86). T-test results (Table 7) show that in the stimulus materials including passive security attacks, the mean score for the passive statements (*M* = 5.76, *SD* =1.41) was significantly higher than the mean score for the active statements (*M* = 3.13, *SD* = 1.42), *t*(110) = -13.64, *p* < .001, two-tailed. This indicates that the manipulation was successful.

Furthermore, the active security attack was tested with two items (“I think the attacker tried to change the system content” and “I think the attacker tried to damage the system”, α = .82). T-test results show that in the stimulus materials including active security attacks, the mean score for the active statements also indicate a significant difference. The mean score for the active statements (*M* = 5.17, *SD* =1.24) was significantly higher than the mean score for the passive statements (*M* = 3.12, *SD* = 1.56), *t*(103) = 8.56, *p* < .001, two-tailed, indicating that the manipulation was successful.

Table 7
Mean scores, standard deviations and t-tests of the manipulations

	Passive security attack					*Active security attack*				
	M	*SD*	*df*	*Sig.*	*t*	*M*	*SD*	*df*	*Sig.*	*t*
Passive statements	5.76	1.41	110	<.001	56.91	3.12	1.56	103	<.001	20.41
Observe the system	5.48	1.39				3.14	1.67			
Gather information	6.04	1.10				3.09	1.75			
Active statements	3.13	1.42	110	<.001	23.33	5.17	1.24	103	<.001	42.38
Change the system content	3.01	1.53				4.95	1.65			
Damage the system	3.24	1.60				5.38	1.23			

Note: Measured on a 7-point Likert scale

4.2 Descriptive statistics

4.2.1 Mean scores and standard deviations dependent variables

Table 8 provides an overview of the mean scores for each dependent variable with the corresponding standard deviations. A 7-point Likert scale was used to measure the dependent variables. The dependent variable perceived threat has a mean of 4.72 (*SD* = 1.16) and intention to use also has a mean of 4.72 (*SD* = 1.61) and thus both have relatively assigned the highest mean scores. Following that, crisis responsibility was assigned a mean score of 4.67 (SD = 1.11) and trust towards the device has a mean of 4.55 (SD = 1.07). Finally, trust towards the organisation has a mean score of 3.60 (*SD* = 1.07), making it the lowest scoring variable.

Table 8

Descriptive statistics for the dependent variables

	Type of security attack				*Type of smart home device*			
Dependent variable	*Passive attack*		*Active attack*		*High intrusiveness*		*Low intrusiveness*	
Crisis responsibility	*M* = 4.81	*SD* = 1.12	*M* = 4.52	*SD* = 1.09	*M* = 4.78	*SD* = 1.09	*M* = 4.56	*SD* = 1.12
Trust towards the organisation	*M* = 3.36	*SD* = .969	*M* = 3.85	*SD* = 1.12	*M* = 3.51	*SD* = 1.10	*M* = 3.68	*SD* = 1.04
Trust towards the device	*M* = 4.41	*SD* = 1.09	*M* = 4.70	*SD* = 1.03	*M* = 4.51	*SD* = 1.14	*M* = 4.56	*SD* = 1.00
Perceived threat	*M* = 4.80	*SD* = 1.02	*M* = 4.63	*SD* = 1.28	*M* = 4.75	*SD* = 1.09	*M* = 4.69	*SD* = 1.22
Intention to use	*M* = 4.62	*SD* = 1.62	*M* = 4.82	*SD* = 1.62	*M* = 4.76	*SD* = 1.62	*M* = 4.68	*SD* = 1.62

Note: Measured on a 7-point Likert scale.

4.3 Main effects

A multivariate analysis of variance (MANOVA) analysis has been conducted to test the hypothesised main effects of the independent variables type of security attack and type of smart home device on the dependent variables crisis responsibility, trust towards the organisation, trust towards the device, and perceived threat. Both independent variables included two levels, security attack type consisted of passive security attack and active security attack. and smart home device type consisted of high intrusiveness and low intrusiveness. An overview of the MANOVA effects of the independent variables can be found in Table 9.

Table 9

MANOVA effects of the independent variables

	Df	F	p	η^2	*Wilks' Λ*
Type of security attack	4, 208	2.915	.022*	.053	.947
Type of smart home device	4, 208	.601	.662	.011	.989
Type of security attack x type of smart home device	4, 208	.747	.561	.014	.986

Note: * p < .05; ** p < .01.

An examination of the results MANOVA analysis reveals a significant effect of the type of security attack on the dependent variables (*F*(4, 208) = 2.915, *p* < .05; Wilks' Λ = .947). Furthermore, the effects of the type of smart home device on the dependent variables turned out to be statistically insignificant (*F*(4, 208) = .601, *p* = .662; Wilks' Λ = .989). Also, the results indicate that there is no significant interaction effect (*F*(4, 208) = .747, *p* = .747; Wilks' Λ = .986).

4.3.1 The main effect of the type of security attack

The results MANOVA analysis reveals a significant effect of the type of security attack on the dependent variables (F(4, 208) = 2.915, p < .05; Wilks' Λ = .947). The results of the ANOVA analysis (Table 10) show a significant direct effects of type of security attack on trust towards the organisation (*F*(1, 211) = 11.040, *p* ≤ .001; Wilks' Λ = .050). Results show that trust towards the organisation were significantly lower among respondents who were exposed to stimulus material including a passive security attack (*M* = 3.36; *SD* = .969) than among respondents who were exposed to stimulus material including an active security attack (*M* = 3.85; *SD* = 1.12). These results indicate that hypothesis 3b is supported. The mean scores and standard deviations of the dependent for each of the conditions are summarised in Table 11.

In addition, the main effect of type of security attack on trust towards the device gave an F ratio of F(1, 211) = 4.007, *p* = < . 05; Wilks' Λ =, showing that there is a significant difference between the passive security attack (*M* = 4.41, *SD* = 1.09) and the active security attack (*M* = 4.70, *SD* = 1.03). Therefore, it can be assumed that a passive security attack, compared to an active security attack, does indeed reduce trust in the organisation. This means that hypothesis 1b is supported.

Furthermore, the results show that the type of security attack has no significant effect on perceived treat (*F*(1, 211) = 1.085, *p* = .299). Therefore, hypotheses 1a is not supported. Also the effect of type of security attack on crisis responsibility was found to be insignificant, although there is an indication that there exists a trend effect (*F*(1,211) = 3.337, *p* =.069).

Table 10

ANOVA effects of the type of security attack

	Df	F	p	η^2	*Wilks' Λ*
Crisis responsibility	1, 211	3.337	.069	.016	.016
Trust towards the organisation	1, 211	11.040	.001**	.050	.050
Trust towards the device	1, 211	4.007	.047*	.019	.019
Perceived threat	1, 211	1.085	.299	.005	.005

Note: * p < .05; ** p < .01.

Participants that were exposed to a passive security attack (*M* = 4.81; *SD* = 1.12) have assigned higher scores to crisis responsibility, than participants that were exposed to an active security attack (*M* = 4.52; *SD* = 1.09). However, the observed p-value is below the threshold of significance (*p* < 0.05), therefore hypothesis 3a is not supported.

Besides, passive and active security attacks consisted of two different sorts of attacks. Passive was divided into eavesdropping and traffic analysis, and active consisted of DoS and masquerade. Therefore, there is also tested whether effects exist between these different sorts of passive and active attacks. The results of an independent t-test (Table 11) show that there was a significant effect of the type of active attack on crisis responsibility (*t*(102) = -2.115, *p* = < .05). Participants in the masquerade group (M = 4.73, SD = 1.07) had slightly higher mean scores on crisis responsibility compared to those in the DoS group (M = 4.29, SD = 1.08). It can thus be concluded that participants exposed to stimulus material including a masquerade attack attributed higher levels of crisis responsibility to the smart home device manufacturer compared to participants exposed to a DoS attack.

Results also show that the direct effect of type of active attack on trust towards the organisation (*t*(102) = 2.403, *p* = < .05) is statistically significant. The mean score for trust towards the organisation in the DoS group was *M* = 4.12 (*SD* = 1.21), while the mean score in the masquerade group was *M* = 3.60 (*SD* = .986). Thus, it can be concluded that participants exposed to stimulus material including a masquerade attack feel less trust towards the smart home device manufacturer compared to participants exposed to a DoS attack. Furthermore, the direct effect of type of active security attack on trust towards the device (*t*(102) = 3.943, *p* = <

Table 11
Independent t-tests results of the different sorts of active and passive security attacks

	Df	t	p
Type of active security attack (DoS vs. masquerade)			
Crisis responsibility	102	-2.115	.037*
Trust towards the organisation	102	2.403	.018*
Trust towards the device	102	3.943	<.001**
Perceived threat	102	-1.090	.279
Type of passive security attack (eavesdropping vs. traffic analysis)			
Crisis responsibility	109	.867	.388
Trust towards the organisation	109	-1.144	.255
Trust towards the device	109	.737	.463
Perceived threat	109	.802	.424

Note: * p < .05; ** p < .01.

Table 12

Descriptive statistics for the dependent variables

	Type of active attack		*Type of passive attack*	
	DoS	*Masquerade*	*Eavesdropping*	*Traffic analysis*
Dependent variables	M (SD)	M (SD)	M (SD)	M (SD)
Crisis responsibility	4.29 (1.08)	4.73 (1.07)	4.90 (1.19)	4.72 (1.04)
Trust towards the organisation	4.12 (1.21)	3.60 (.986)	3.25 (1.06)	3.46 (.870)
Trust towards the device	5.09 (.958)	4.34 (.973)	4.49 (1.06)	4.33 (1.12)
Perceived threat	4.49 (1.31)	4.76 (1.25)	4.88(1.03)	4.73 (1.02)

Note: Measured on a 7-point Likert scale.

. 001) also turned out to be statistically significant. Trust towards the device were significantly lower among participants who were exposed to stimulus material including a masquerade attack (*M* = 4.34*; SD* = .973*)* than among participants who were exposed to stimulus material including a DoS attack (*M* = 5.09*; SD* = .958*)*

However, the direct effect of type of active security attack on perceived threat (*t*(102) = -1.090, *p* = .278) is found to be insignificant. Besides, there were no significant effects of type of passive security attack on crisis responsibility (*t*(109) = .867, *p* = .388), trust towards the organisation (*t*(109) = -1.144, *p* = .255), trust towards the device (*t*(109) = .737, *p* = < .463), and perceived threat (*t*(109) = .802, *p* = .424). A full overview of the mean scores and standard deviations of the dependent variables can be found in Table 12.

4.3.2 The main effect of the type of smart home device

The MANOVA analysis shows that there is an insignificant overall effect of the type of smart home device on the dependent variables (*F*(4, 208) = .601, *p* = .011; Wilks' Λ =.989). An ANOVA analysis (Table 13) shows that the effects of type of smart home device on crisis

Table 13

ANOVA effects of the type of smart home device

	Df	F	p	η^2	*Wilks' Λ*
Crisis responsibility	1, 211	2.121	.147	.010	.010
Trust towards the organisation	1, 211	1.172	.280	.006	.006
Trust towards the device	1, 211	.013	.909	.000	.000
Perceived threat	1, 211	.184	.668	.001	.001

Note: * p < .05; ** p < .01.

responsibility (*F*(1, 211) = 2.121, *p* = .147; Wilks' Λ =.010), trust towards the organisation (*F*(1, 211) = .1.172, *p* = .280; Wilks' Λ =.006), trust towards the device (*F*(1, 211) = .013, *p* = .909; Wilks' Λ =.000), and perceived threat (*F*(1, 211) = .184, *p* = .668; Wilks' Λ =.001) are all found insignificant. Therefore, hypotheses 2a, 2b, 4a and 4b are all not supported.

4.4 Interaction effects

The results of the MANOVA analysis indicate that the interaction effect is insignificant (*F*(4, 208) = .747, *p* = .747; Wilks' Λ = .986). In addition, a ANOVA analysis (Table 14) was used to examine whether there is an interaction effect between type of security attack and type of smart home device on the dependent variables crisis responsibility(*F*(2, 211) = 1.205, *p* = .274; Wilks' Λ =.006), trust towards the organisation(*F*(2, 211) = 1.141, *p* = .287; Wilks' Λ =.005), trust towards the device(*F*(2, 211) = .426, *p* = .515; Wilks' Λ =.002), perceived threat (*F*(2, 211) = 1.819, *p* = .179; Wilks' Λ =.009). However, none of these interaction effects are significant. Therefore, hypotheses 5a, 5b, 5c and 5d are not supported.

Table 14

ANOVA analysis for the interaction effect

	Df	F	p	η^2	*Wilks' Λ*
Crisis responsibility	1, 211	1.205	.274	.006	.006
Trust towards the organisation	1, 211	1.141	.287	.005	.005
Trust towards the device	1, 211	.426	.515	.002	.002
Perceived threat	1, 211	1.819	.179	.009	.009

4.5 Correlations

A Pearson correlation analysis was conducted to measure the strength of the underlying relationship between the dependent variables. The results are summarised in Table 15, revealing significant correlations between various variables. Regarding demographic information, gender demonstrated significant correlations with user smart home device (*r* = -.292, *p* = <.001), crisis responsibility (*r* = -.142, *p* = <.05), trust towards the device (*r* = -.215, *p* = <.001) and the intention to use (*r* = -.213, *p* = <.001). On the other hand, age was only found to have a significant correlation with crisis responsibility (*r* = -.162, *p* = <.05). Educational level exhibited significant correlations with user smart home device (*r* = .263, *p* = <.001), trust towards the device (*r* = -.137, *p* = <.05), and intention to use (*r* = .153, *p* = <.05).

Table 15

Mean, standard deviation and Pearson correlation

	Descriptives		Correlations								
	Mean	SD	1	2	3	4	5	6	7	8	9
1. Gender	-	-	1								
2. Age	33.11	12.70	.080	1							
3. Educational level	5.70	1.39	.004	-.011	1						
4. User smart home device	3.69	1.36	-.297**	-.125	.263**	1					
5. Crisis responsibility	4.67	1.11	-.142*	-.162*	.118	.157*	1				
6. Trust towards the organisation	3.60	1.07	.002	.084	-.019	.002	-,561**	1			
7. Trust towards the device	4.55	1.07	-.215**	-.012	.137*	.357**	-,142*	,387**	1		
8. Perceived threat	4.72	1.16	.088	-.055	.015	-.298**	,124	-,142*	-,489**	1	
9. Intention to use	4.72	1.61	-.213**	.018	.153*	.445**	-,104	,224**	,624**	-,387**	1

Note: Mean score for Age is self-reporting. Other variables measured on a 7-point Likert scale. * p < .01; ** p < .001.

Furthermore, user smart home device, was significantly correlated with crisis responsibility (*r* = .157, *p* = <.05), trust towards the device (*r* = .357, *p* = <.001), perceived threat (*r* = -.298, *p* = <.001), and intention to use (*r* = .445, *p* = <.001).

In addition, the results show that the variable crisis responsibility has a correlation of *r* = -.561 with the variable trust towards the organisation. In other words, there is a strong, negative relationship between these variables. The analysis shows that this correlation is significant with a p-value <.001. In addition, there was found to be a significant negative correlation between crisis responsibility and trust towards the device (*r* = -.142, p < .05). However, no significant correlation was found between crisis responsibility and perceived threat (*r* = .124) and between crisis responsibility and intention to use (*r* = -.104).

Next to that, trust towards the organisation has a significant correlated with trust towards the device (*r* = .387, p < .001), perceived threat (r = -.142, p < . 05) and intention to use (*r* = .224, p < .001). Trust towards the device negatively correlates with perceived threat (*r* = -.489, p < .05) and an correlate positively with intention to use (*r* = .624, p < .001). Subsequently, perceived threat correlates negatively with the intention to use (*r* = -.387, p < .001).

4.6 Regression analysis

A hierarchical regression analysis has been performed to determine the amount of variance each independent variable adds. This type of regression involves a systematic inclusion of variables into the model, and at each step, the change in R^2 is calculated. The analysis was carried out in three sequential steps. In the first step, demographic information was entered as the independent variables. The second step involved adding the device-related variables, specifically perceived threat, and trust towards the device. Lastly, in the third step, organisation-related variables, namely crisis responsibility and trust towards the organisation, were introduced. Table 16 provides an overview of the regression model, listing the variables included at each step.

Table 16

Overview of regression model

Model	Variables
1	Demographics
	Gender
	Age
	Educational level
	User smart home device
2	Device-related variables
	Perceived threat
	Trust towards the device
3	Organisation-related variables
	Crisis responsibility
	Trust towards the organisation

Note: Dependent variable is intention to use.

The results of the hierarchical regression analysis (Table 17) indicated that Model 1 accounted for 21.1% of the variance in the intention to use (R^2 = .211, $F(4, 210) = 13.739$, $p <$ .001). This model included only the demographic information as predictors. The significant contribution of the demographic variables suggests that individual characteristics were important in explaining the variation in the intention to use smart home devices.

In Model 2, the device-related variables were added to the analysis. As a result, the explained variance increased substantially by 24.3% ($\triangle R^2$ = .243). The overall R^2 for Model 2 was .453, meaning that Model 2 is accounted for a total of 45.3% of the variance in the intention to use. The F-test indicated that the model was highly significant ($F(6, 210) = 28.199$, $p < .001$).

Table 17

Regression model summary

Model	R^2	SE	$\triangle R^2$	F	Df	*p*
1	.211	1.461	.211	13.739	4,210	< .001**
2	.453	1.223	.243	28.199	6,210	< .001**
3	.458	1.223	.005	21.343	8,210	< .001**

Note: Dependent variable is intention to use

This indicated that the device-related factors, such as perceived threat and trust towards the device played a crucial role in understanding the variation in the intention to use smart home devices.

In the final Model 3, organisation-related variables were introduced. Model 3 accounted for 45.8% of the variance in the intention to use ($R^2 = .458$, $F(8, 210) = 21.343$, $p < .001$). The addition of organisation-related variables contributed to a slight increase in the explained variance by 0.5% ($\triangle R^2 = .005$) compared to Model 2. This suggests that factors related to the organisation offering the smart home devices, such as crisis responsibility and trust towards the organisation, added minimal predictive power to the overall model.

To summarise, the hierarchical regression analysis showed that demographic information, device-related variables, and organisation-related variables collectively contributed to the prediction of the intention to use, with Model 3 accounting for the highest amount of explained variance at 45.8%.

4.6.1 Regression coefficients

Table 18 contains the regression coefficients of all the tested variables within Model 3. As the results show, the demographic variable user smart home device is the only demographic variable that is a significant predictor of the intention to use smart home devices ($\beta = .244$, $t(207) = 3.971$, $p < .001$). The p-value is less than 0.001, indicating that the relationship between 'user smart home device' and the intention to use smart home devices is highly statistically significant. However, it is worth noting that the other demographic variables, including gender ($\beta = -.044$, $t(207) = -.797$, $p = .427$), age ($\beta = .042$, $t(207) = .800$, $p = .425$), and educational level ($\beta = .030$, $t(207) = .548$, $p = .584$), did not demonstrate statistically significant associations with the intention to use smart home devices in Model 3.

Furthermore, the relationship between the variable trust towards the device and the intention to use smart home devices was found to be statistically significant ($\beta = .493$, $t(207)$

= 7.225, *p* < .001). The positive coefficient for trust towards the device indicates that it has a positive effect on the intention to use smart home devices. In other words, higher levels of trust towards the device are associated with higher levels of intention to use smart home devices. Therefore, hypothesis 7 is supported. However the predictive value of perceived threat (β = -.062, *t*(207) = -1.002, *p* = .318), crisis responsibility (β = -.083, *t*(207) = -1.268, *p* = .206), and trust towards the organisation (β = -.025, *t*(207) = -.362, *p* = .718) towards the intention to use are found to be insignificant. These results indicate that perceived threat, crisis responsibility, and trust towards the organisation do not have a significant impact on the intention to use smart home devices. Therefore hypotheses 6, 8 and 9 are not supported.

Table 18

Regression coefficients

	B	SE	β	*t*	*p*
Gender	-.145	.182	-.044	-.797	.427
Age	.005	.007	.042	.800	.425
Educational level	.035	.064	.030	.548	.584
User smart home device	.293	.074	.244	3.971	<.001**
Perceived threat	-.087	.087	-.062	-1.002	.318
Trust towards the device	.748	.104	.493	7.225	<.001**
Crisis responsibility	-.122	.096	-.083	-1.268	.206
Trust towards the organisation	-.037	.103	-.025	-.362	.718

Note: Dependent variable is intention to use. * *p* < .05; ** *p* < .01.

To summarise the above-tested hypotheses Table 19 provides an overview of the hypotheses that were formulated and the outcomes.

Table 19

List of hypotheses and the outcomes

Hypothesis		Outcome
H1a	A passive security attack (in contrast to an active security attack) results in a higher degree of perceived threat.	Not supported
H1b	A passive security attack (in contrast to an active security attack) results in a greater decrease in trust towards the device.	Supported
H2a	High intrusive smart devices (in contrast to low intrusive smart devices) are associated with a higher degree of perceived threat.	Not supported
H2b	High intrusive smart devices (in contrast to low intrusive smart devices) are associated with a greater decrease in trust towards the device.	Not supported
H3a	A passive security attack (in contrast to an active security attack) results in a higher level of crisis responsibility.	Not supported
H3b	A passive security attack (in contrast to an active security attack) results in a greater decrease in trust towards the organisation.	Supported
H4a	High intrusive smart devices (in contrast to low intrusive smart devices) are associated with a higher level of crisis responsibility.	Not supported
H4b	High intrusive smart devices (in contrast to low intrusive smart devices) are associated with a greater decrease in trust towards the organisation.	Not supported
H5a	There is an interaction effect between the type of smart home device and the type of security attack on perceived threat	Not supported
H5b	There is an interaction effect between the type of smart home device and the type of security attack on trust towards the device	Not supported
H5c	There is an interaction effect between the type of smart home device and the type of security attack on crisis responsibility	Not supported
H5d	There is an interaction effect between the type of smart home device and the type of security attack on trust towards the organisation	Not supported
H6	Perceived threat will have a negative effect on the intention to use	Not supported
H7	Trust towards the device will have a positive effect on the intention to use	Supported
H8	Crisis responsibility will have a negative effect on the intention to use	Not supported
H9	Trust towards the organisation will have a positive effect on the intention to use	Not supported

5. Discussion

The purpose of this study was to experimentally investigate the extent to which the type of smart device (high intrusiveness vs. low intrusiveness) and the type of security attack (passive vs. active) affect crisis responsibility, trust towards the organisation, trust towards the device, perceived threat and intention to use smart devices in the home.

5.1 Discussion of the results

5.1.1 Type of security attack

First, the study revealed a significant effect of the type of security attack on the dependent variables trust towards the organisation and trust towards the device. Results indicate that trust towards the organisation and the device were significantly lower in response to a passive security attack compared to an active security attack. This finding is consistent with the expectation that people may perceive passive attacks as having a greater impact on their trust in the organisation behind the system and in the device itself. This derives from the reasoning that passive attacks are difficult to detect, leaving the organisation unaware that attackers for instance are eavesdropping on users undetected (Olawumi et al., 2017; Ali et al., 2017; Panigrahi, 2022). Passive attacks, in which sensitive data is gathered secretly or users are monitored without their knowledge, may be perceived as more severe than active attacks and lead to greater damage and privacy violations. Due to this unnoticeable nature and the difficulties in detecting and taking responsibilities for them, users often feel helpless and insecure resulting in the loss of trust in the device and organisation. Acknowledging this increased severity associated with passive attacks affects users' trust in the device, as the perceived violation of privacy and feeling unaware of such activities erodes trust in both the device and the responsible organisation.

Secondly, the results indicate that there were no significant effects found for the type of security attack on perceived threat and crisis responsibility. In other words, the lack of significant effect suggests that the type of attack may not directly influence participants' perception of threat or their attribution of crisis responsibility. This result aligns with the observation made by Gerber, Reinheimer and Volkamer (2019), who highlighted that most users are unaware of certain negative consequences that could arise from the usage of privacy-threatening technologies. Therefore, the insignificant effect could be explained by participants limited overall awareness and understanding of the specific threats of different security attacks. It could be that many participants were not well informed about the nuances and potential severity of different types of security attacks, forming general perceptions of perceived threat and crisis responsibility regardless of the specific attack presented in the study.

Interestingly, the study revealed that participants exposed to a masquerade attack, a type of passive security attack, tended to attribute higher levels of crisis responsibility to the smart home device manufacturer compared to participants exposed to a DoS attack, another type of passive security attack. While these unexpected findings are fascinating, it is important to emphasise that the research design did not foresee the need for specific sources to support this observation. This discovery came as a surprise during the analysis phase. A possible explanation for this difference in attributions could be that users perceive a DoS attack, where the system is flooded with excessive traffic to disrupt the normal operation of the device, as more of a technical error, rather than a direct threat to their privacy and security. In contrast, masquerade attacks, involving unauthorised access by attackers, may be seen as more dangerous by users because an attacker has gained unauthorised access to their smart home device. This would result in a higher degree of crisis responsibility being assigned to the manufacturer, compared to a DoS attack. Although, it is important to interpret this understanding cautiously, as the absence of literature to confirm the findings limits the strength of this claim.

5.1.2 Type of smart home device

Additionally, the study examined the impact of different types of smart home devices on users' perceptions. However, the type of smart home device had no significant effect on the dependent variables. This nonsignificant effect suggests that the level of intrusiveness did not impact the participants' perceptions of crisis responsibility, perceived threat, trust towards the organisation and the device.

A reason for this could be that the participants in this study may have had generally positive perceptions of both high- and low-intrusive smart home devices, leading to similar levels of trust, perceived threat, and crisis responsibility, regardless of the level of intrusiveness. Furthermore, explanation for this might be found in the Technology Acceptance Model (Davis, 1989). This model suggest that perceived usefulness and perceived ease of use are key determinants of user acceptance of technology. This means that if participants view both high and low levels of intrusiveness in smart home devices as equally useful and user-friendly, their attitudes and intentions will be less influenced by their intrusiveness level. Perhaps this explains why this study did not find a significant effect of smart home device type.

5.1.3 Interaction effects smart home device and security attack

Besides examining the main effects of security attack type and smart home device type on the dependent variables, the study also investigated potential interaction effects between these two factors. However, no significant interaction effects were found, indicating that the relationship between security attack type and smart home type did not have a combined effect on the dependent variables (trust in the organisation and device, perceived threat and crisis responsibility).

The absence of significant interaction effects indicates that the influence of the type of security attack and the type of smart home device on the dependent variables is largely independent of each other. In other words, the influence of the type of security attack (passive or active) on the dependent variables does not vary depending on the specific type of smart home device used (low or high intrusiveness), and the other way around.

5.1.4 Intention to use

The results of this study also indicated that trust towards the device was a significant predictor of intention to use. This outcome aligns with the previous expectations from Shuhaiber and Mashal's (2019) research in which they argued that users who trust a technology have a positive attitude towards using that technology. This significance of trust indicates that trust is crucial for consumers who remain positive about using and maintaining smart home devices for the long term due to their confidence in their reliability, security, and overall performance. Users develop their perceptions of technology's capabilities and security based on trust. A trusting relationship with smart home devices will allow users to integrate them more comfortably and confidently into their daily lives. The positive association between trust and the intention to use smart home devices highlights the need to create and maintain trust within the smart home industry. By providing reliable product performance and strong security measures, manufacturers can build consumer trust. By doing so, they can encourage users to continue using their smart home devices over the long term and reinforce their positive attitude towards them.

On the other hand, this study initially hypothesised that trust towards the organisation behind the smart home devices would positively affect the intention to use smart home devices. However, this effect turned out to be insignificant. In other words, consumer’s trust in the organisation did not significantly affect their intention to use smart home devices. A possible explanation for this insignificant result could be related to the use of a fictious organisation. Research from Adebesin and Mwalugha (2019) suggests that trust acts as a mediator between organisational reputation and the intention to use. Meaning that the impact of trust on the intention to use is influenced by the consumers’ perception of the organisation’s reputation. Consequently, higher organisational reputation contributes to greater trust, which in turn positively impacts consumers' intention to use its products and services. In this line of reasoning, it might be possible that the absence of a significant effect of trust on intention to use may be due to the organisation's lack of a true reputation. Moreover, organisational reputation is also an important predictor of behavioural intentions in Coombs' (2007a) SCCT model, which further supports the idea that reputation plays a crucial role in the consumer decision-making process. The absence of real organisational reputation in the study may have contributed to the observed insignificant effect of trust towards the organisation on the intention to use smart home devices.

Furthermore, the study aimed to explore the effect of perceived threat on the intention to use smart home devices. Despite initial expectations, the results revealed a lack of direct significance between perceived threat and intention to use. One possible explanation for this insignificant effect is that individuals' intentions regarding technology usage are more strongly influenced by the perceived benefits rather than their perceived risks (Al Nawayseh, 2020). Elaborating on this, the self-determination theory provides valuable insights, suggesting that individuals' perception of enjoyment and satisfaction plays a crucial role in driving consumer behaviour (Rouibah, Lowry & Hwang, 2016). According to this theory, when individuals perceive technology as enjoyable, useful, and fulfilling their needs, they are more likely to adopt it, even in the presence of potential risks or threats, contributing to the privacy paradox. Therefore, the influence of perceived benefits and the fulfilment of user needs might overshadow the impact of perceived threat on the intention to use smart home devices, leading users to prioritise the benefits and convenience of technology use over their concerns about potential risks to their privacy and security.

Additionally, it was expected that crisis responsibility would negatively affect the intention to use smart home devices. However, the effects turned out to be insignificant, indicating that crisis responsibility did not significantly predict the intention to use. A possible explanation for this insignificant effect could be that the participants did not perceive crisis responsibility as an important factor in their decision-making process and focused more on the perceived benefits and risks of the smart home devices themselves. It is possible that crisis responsibility might not be a prominent consideration for individuals when evaluating their intention to use smart home devices. Building on this, Trkman, Popovič and Trkman (2021) found in their study that the perceived crisis severity is positively mediated by personal and societal benefits. In other words, when consumers perceive a crisis of high severity, they may weigh the personal and societal benefits they gain from using smart home devices more heavily, resulting in a greater likelihood of continued use. A consumer's decision-making process consists of a combination of factors, which means that crisis responsibility, while important in crisis communication, may not always be the primary determinant of the consumer's decision-making process. This implies that companies can maintain consumer trust and continued use of smart home devices even when security attacks or crises occur by highlighting the benefits of smart home devices and their contribution to personal and societal well-being.

However, the study revealed a significant negative correlation between crisis responsibility and trust in the organisation. This indicates that when users perceive a crisis or security attack, their trust in the smart home manufacturer decreases. Previous studies have already shown that when customers perceive an organisation as trustworthy, this positively influences their evaluation and rating of the company (Edinger-Schrons et al., 2019). Moreover, Zhao et al. (2021) conducted a study that further supports the idea that trust has a positive impact on corporate reputation. This implies that when trust is established between users and an organisation, it improves the organisation's overall reputation. Moreover, a positive reputation of an organisation has been shown to have a beneficial effect on consumers' behavioural intentions (Coombs, 2007a). Thus, trust not only plays a crucial role in consumers' perception of an organisation's trustworthiness, but also influences their intention to use the company's products or services.

5.2 Implications

In theoretical perspectives, this research represents a valuable first attempt to integrate the phenomenon of security attacks into current crisis communication theories, such as Coombs' Situational Crisis Communication Theory (SCCT). Building on this, future researchers can extend this exploration to other settings, such as AI-powered systems and various other IoT applications.

Furthermore, the study contributed to the understanding of how different type of security attacks influence the user perceptions of trust towards the device. The finding that passive security attacks lead to lower levels of trust is consistent with the reasoning that these attacks are difficult to detect, leaving users unaware of potential privacy breaches. This insight can provide information for future research on user behaviour in response to security incidents.

In addition, the study found no significant effect associated with security attack types on perceived threat or crisis responsibility. Considering the general lack of awareness and understanding that participants have of different types of attacks, this suggests that their overall knowledge and awareness may be limited. A deeper exploration of user perceptions and knowledge of cybersecurity threats could provide researchers and organisations with valuable insights.

From a practical standpoint, several implications can be drawn from these findings for smart home device manufacturers. It is crucial for organisations in the smart home industry to understand how different security attacks affect trust. Users' trust in their devices appears essential, which is why smart home device manufacturers should invest in robust security measures that address the potential severity of security attacks. Manufacturers can foster stronger brand loyalty and consumer satisfaction by taking proactive steps towards securing their devices.

5.3 Limitations and directions for further research

It is important to note that the present study has certain limitations and suggestions for future research can be identified based on the study's objectives, methods, and results.

First, in this study, a fictitious organisation and crisis were used to avoid influencing results based on previous crises or the organisation's reputation. This decision was made to avoid bias caused by previous reputation or brand preferences. However, using these simulated scenarios, rather than real-life situations, may have limited respondents' ability to empathise. The utilisation of a real-world context may provide a more precise depiction of consumers' responses to security attacks. Furthermore, future research might consider using an existing organisation, since reputation and brand preferences might influence the relationship between perceived threat, trust in the device, trust in the organisation, and crisis responsibility. Further exploring these dynamics would be valuable for future research.

Another limitation lies in the design of the study, specifically the use of a 2x2 experimental design. While the design provides a structured framework for examining the effects of different variables, it may not fully reflect the complexity and nuances of real-life cyber security attacks. As the results of the study show, only 45.8% of the variance in intention to use smart home devices could be explained by means of this study. In other words, the factors manipulated and measured in the study could only explain a portion of the variation in participants' intention to use smart home devices after a cybersecurity attack. The remaining 54.2% of the variance remains unexplained, indicating the need for further research to test the boundaries of the model and identify more of the variances to explain the concept of behavioural intention fully.

Furthermore, a significant and controversial finding of this study was the lack of perceived threat effect on the intention to use smart home devices. Prior research has consistently reported that perceived threat or risk is a key factor in obstructing the adoption of technologies and shows a negative relationship with intention to use technologies. The results of this study conflict with these established findings. A potential explanation is that respondents in this study have a great understanding of smart home technologies and were therefore more aware of the risk perceptions. To better understand consumers' attitudes toward cybersecurity attacks, it is recommended that qualitative methods be used in future research. Qualitative research can provide insightful and in-depth information about consumers' psychological and emotional reactions to security attacks, which can contribute to a better understanding of the phenomenon.

Finally, the primary focus of this research was to examine how security attacks affect consumer perceptions to provide input for deploying appropriate post-crisis communications. Despite finding no significant effects on crisis responsibility in this study, previous research has underlined the importance of addressing post-crisis communication methods. To better understand effective crisis communication strategies, it would be useful to directly test various post-crisis communication approaches from the Situational Crisis Communication Theory (SCCT) (Coombs, 2007a) in future studies. This direct testing approach would provide valuable insights into which response strategies are most successful in restoring consumer confidence and encouraging continued use of smart home devices after a security attack. By understanding the impact of these strategies, organisations can better tailor their crisis communication efforts and effectively address consumer concerns, ultimately enhancing their reputation and credibility.

5.4 Conclusion

This study aimed to investigate the effects of cyber security attacks on consumers' feelings of trust, perceived threat, crisis responsibility, and intention to use smart home devices. The findings highlight the crucial role of trust in the context of smart home technologies. Specifically, trust towards the organisation was found to be insignificant in predicting the intention to use smart home devices. Instead, trust towards the device showed to be the only significant predictor of consumers' intention to use it. This underscores the importance of building and maintaining trust towards the smart home devices themselves, rather than solely rely on the consumer’s trust towards the manufacturers behind the smart home devices. Manufacturers must prioritise the importance of gaining consumer trust by ensuring reliable product performance and strong security measures. By doing so, they can encourage users to keep using their smart home devices eventually and reinforce their positive attitude towards them.

Moreover, the study found that the type of security attack had different effects on consumer perceptions. Passive security attacks had a greater impact on trust towards both the organisation and the device compared to active security attacks. Surprisingly, the type of security attack had no significant effect on perceived threat or crisis responsibility attributed to the smart home device manufacturer. Several factors may influence consumers' perception of responsibility, such as their understanding of the incident or their overall perception of the benefits and risks of the device. Therefore, understanding consumers' emotional reactions and perceptions of incidents can be vital in shaping effective crisis communication strategies.

Lastly, the level of intrusiveness of smart home devices did not significantly affect consumers' trust in the organisation or device, perceived threat, or crisis responsibility. This suggests that consumers showed similar levels of trust and crisis responsibility regardless of the degree of intrusiveness of the device. Other factors, such as an overall positive perception of smart home devices, or perceived usefulness and ease of use, may have played a more significant role in shaping consumers' attitudes towards these devices.

Overall, this study provides valuable insights into the effects of cyber security attacks on consumers' perceptions and intentions regarding smart home devices. The findings contribute to the understanding of crisis communication in the context of smart home technologies and can guide the development of effective post-crisis communication strategies. As the digital landscape continues to evolve, these insights become even more relevant in shaping effective and proactive responses to digital crises and strengthening consumer trust when security incidents arise.

References

Aldrich, F.K. (2003). Smart Homes: Past, Present and Future. In: Harper, R. (eds) *Inside the Smart Home* (pp. 17-39). London, England: Springer. doi:10.1007/1-85233-854-7_2

Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). IoT based smart home: Security challenges, security requirements and solutions. *Proceedings of the International Conference on Automation and Computing* (pp. 1-6). Huddersfield, England: IEEE. doi:10.23919/iconac.2017.8082057

AlHogail, A. (2018). Improving IoT technology adoption through improving consumer trust. *Technologies, 6*(3), 1-17. doi:10.3390/technologies6030064

Al Nawayseh, M. K. (2020). Fintech in COVID-19 and beyond: what factors are affecting customers' choice of fintech applications. *Journal of Open Innovation: Technology, Market, and Complexity, 6*(4), 153. doi:10.3390/joitmc6040153

Bauer, R. A. (1967). Consumer behavior as risk taking, In: Cox, D. F. (ed.) *Risk Taking and Information Handling in Consumer Behavior* (pp. 23-33). Boston, MA: Harvard University Press

Brown, K. A., & Ki, E. J. (2013). Developing a valid and reliable measure of organizational crisis responsibility. *Journalism & Mass Communication Quarterly, 90*(2), 363-384. doi:10.1177/1077699013482911

Coombs, W. T., & Holladay, S. J. (2007). The negative communication dynamic. *Journal of Communication Management, 11*(4), 300–312. doi:10.1108/13632540710843913

Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets: initial tests of the situational crisis communication theory. *Management Communication Quarterly, 16*(2), 165–186. doi:10.1177/089331802237233

Coombs, W. T., & Holladay, S. J. (2010). *The Handbook of Crisis Communication*. Oxford, England: Blackwell Publishing Ltd.

Coombs, W. T. (2007a). Protecting organization reputations during a crisis: The development and application of Situational Crisis Communication Theory. *Corporate Reputation Review, 10*(3), 163-176. doi:10.1057/palgrave.crr.1550049

Coombs, W. T. (2007b). Attribution Theory as a guide for post-crisis communication research. *Public Relations Review, 33*(2), 135-139. doi:10.1016/j.pubrev.2006.11.016

Coombs, W. T., & Schmidt, L. (2000). An empirical analysis of image restoration: Texaco's racism crisis. *Journal of Public Relations Research, 12*(2), 163-178. doi:10.1207/S1532754XJPRR1202_2

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3), 319-340. doi:10.2307/249008

Dowling, G., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research, 21*(1), 119–134. doi:10.1086/209386

Duezguen, R., Mayer, P., Berens, B., Beckmann, C., Aldag, L., Mossano, M., Volkamer, M., & Strufe, T. (2020). How to increase smart home security and privacy risk perception. *Proceedings of IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 997-1004). Shenyang, China: IEEE. doi:10.1109/TrustCom53373.2021.00138.

Edinger-Schons, L. M., Lengler-Graiff, L., Scheidler, S., and Wieseke, J. (2019). Frontline employees as corporate social responsibility (CSR) ambassadors: a quasi-field experiment. *J.Bus. Ethics 157*, 359–373. doi:10.1007/s10551-018-3790-9

Geeksforgeeks. (2023). Active and passive attacks in information security. Retrieved from https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/

George, D., & Mallery, P. (2003). *SPSS for Windows step by step: A simple guide and reference. 11.0 update* (4th ed.). Boston: Allyn & Bacon

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IoT. International Advanced Research Journal in Science, Engineering and Technology, 5(1), 41-44. doi:10.17148/IARJSET.2018.517

Gerber, N., Reinheimer, B., & Volkamer, M. (2019). Investigating people's privacy risk perception. *Proceedings on Privacy Enhancing Technologies, 3,* 267-288. doi:10.2478/popets-2019-0047

Hong, A., Nam, C., & Kim, S. (2020). What will be the possible barriers to consumers' adoption of smart home services? *Telecommunications Policy, 44*(2), 1-15. doi: 10.1016/j.telpol.2019.101867

Hu, M. D., Wei, Z. Q., & Cong, Y. P. (2013). A smart home architecture based on concept ontology. *Applied Mechanics and Materials*, 303–306, 1559–1564. doi:/10.4028/www.scientific.net/amm.303-306.1559

Jacobsson, A., & Davidsson, P. (2015). Towards a model of privacy and security for smart homes. *Proceedings of IEEE 2nd World Forum on Internet of Things (WF-IoT).* doi:10.1109/WF-IoT.2015.7389144

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security, 99,* 1-18. doi:10.1016/j.cose.2020.102036.

Klobas, J. E., McGill, T., & Wang, X. (2019). How perceived security risk affects intention to use smart home devices: A reasoned action explanation. *Computers & Security, 87*. doi:10.1016/j.cose.2019.101571

Laufer, D., & Jung, J. M. (2010). Incorporating regulatory focus theory in product recall communications to increase compliance with a product recall. *Public Relations Review, 36*(2), 147-151. doi:10.1016/j.pubrev.2010.03.004

Luor, T., Lu, H. P., Yu, H., Lu, Y. (2015). Exploring the critical quality attributes and models of smart homes, *Maturitas, 82*(4), 377–386. doi:10.1016/j.maturitas.2015.07.025.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy (IUIPC). The Construct, the Scale and a Causal Model. *Information System Research, 15*(4), 336-355. doi:10.1287/isre.1040.0032

Mani, Z., & Chouk, I. (2017). Drivers of consumers' resistance to smart products. *Journal of Marketing Management, 33*(1-2), 76-97. doi:10.1080/0267257X.2016.1245212

Millar, D. P., & Heath, R. L. (2004). *Responding to Crisis. A Rhetorical Approach to Crisis Communication.* Mahwah, NJ: Lawrence Erlbaum Associates

Multiscope. (2023). Smart home producten in 59% huishoudens. Retrieved from https://www.multiscope.nl/persberichten/smart-home-producten-in-59-procent-huishoudens/

Olawumi, O., Väänänen, A., Haataja, K., & Toivanen, P. (2017). Security issues in smart home and mobile health system: threat analysis, possible countermeasures and lessons learned. *International Journal of Information Technologies & Security, 9*(1), 31-51.

Oxford University Press (n.d.). *Oxford dictionary* [Online]. Retrieved from: https://www.oxfordlearnersdictionaries.com/definition/english/crisis_1

Panigrahi, K. K. (2022). Difference between active attack and passive attack. Retrieved from https://www.tutorialspoint.com/difference-between-active-attack-and-passive-attack

Park, E., Kim, S., Kim, Y., Kwon, S. J. (2018). Smart home services as the next mainstream of the ICT industry: determinants of the adoption of smart home services. *Universal Access in the Information Society, 17,* 175–190. doi:10.1007/s10209-017-0533-0

Peine, A. (2008). Technological paradigms and complex technical systems—The case of smart homes. *Research Policy, 37*(3), 508-529. doi:10.1016/j.respol.2007.11.009.

Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The Internet Society, 80,* 1-50. Retrieved from: https://www.semanticscholar.org/paper /THE-INTERNET-OF-THINGS-%3A-AN-OVERVIEW-Understanding-Rose-Eldridge/be5012a06734594bf3d06a0563c9c7619e5d906e

Rouibah, K., Lowry, P. B., & Hwang, Y. (2016). The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: *New perspectives from an Arab country. Electronic Commerce Research and Applications, 19,* 33-43. doi:10.1016/j.elerap.2016.07.001.

Sears, A. (2019). ‘Felt so violated:’ Milwaukee couple warns hackers are outsmarting smart homes. *Fox6 news.* https://www.fox6now.com/news/felt-so-violated-milwaukee-couple-warns-hackers-are-outsmarting-smart-homes

Seeger, M. W., Sellnow, T. L., & Ulmer, R. R. (1998). Communication, organization, and crisis. *Annals of the International Communication Association, 21*(1), 231-276. doi: 10.1080/23808985.1998.11678952

Sellnow, T. L., & Seeger, M. W. (2013). *Theorizing Crisis Communication.* West Sussex, England: Wiley.

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems, 32*(2), 314–341. doi:10.1080/07421222.2015.1063315

Shuhaiber, A., & Mashal, I. (2019). Understanding users' acceptance of smart homes. *Technology in Society, 58*. doi:10.1016/j.techsoc.2019.01.003

Solaimani, S., Keijzer-Broers, W., & Bouwman, H. (2015). What we do – and don't – know about the smart home: an analysis of the smart home literature. *Indoor and Built Environment 24*(3), 370-383. doi:10.1177/1420326X13516350

Statista. (2022). Smart home device ownership in the Netherlands in 2022 [Graph]. In Statista. Retrieved from https://www.statista.com/global-consumer-survey/tool/10/gcs_nld_202204?bars=0&index=0&absolute=0&missing=0&heatmap=0&rows%5B0%5D=v0530b_smar_usagesmarthome&tgeditor=0&pendo=0

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing, 77,* 14053–14089. doi:10.1007/s11227-021-03825-1

Trkman, M., Popovič, A., & Trkman, P. (2021). The impact of perceived crisis severity on intention to use voluntary proximity tracing applications. *International Journal of Information Management, 61,* 1-16. doi:10.1016/j.ijinfomgt.2021.102395

Uckelmann, D., Harrison, M., & Michahelles, F. (2011). *Architecting the Internet of Things.* Berlin, Germany: Springer-Verslag

Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: an extension of the theory of planned behavior. *Industrial Management & Data Systems, 117*(1), 68–89. doi:10.1108/imds-01-2016-0017

Zhao, Y., Abbas, M., Samma, M., Ozkut, T., Munir, M., & Rasool, S. F. (2021). Exploring the Relationship Between Corporate Social Responsibility, Trust, Corporate Reputation, and Brand Equity. *Frontiers in Psychology, 12,* 1-10. doi:10.3389/fpsyg.2021.766422

Zlatolas, L. N., Feher, N., & Hölbl, M. (2022). Security perception of IoT devices in smart homes. *Journal of Cybersecurity and Privacy, 2*(1), 65-73. doi:10.3390/jcp2010005

Appendices

Appendix A: Overview of the used constructs and items in the main study

Table A1

Overview of the used constructs and items in the main study

Construct (Cronbach's α in parentheses)	Items	Source
Crisis Responsibility (α = .90)	Circumstances, not NexaHome, is responsible for the crisis. The blame for the crisis lies with NexaHome. The blame for the crisis lies in the circumstances, not NexaHome. The cause of the crisis was something NexaHome could control. The cause of the crisis is something over which NexaHome had no power. The cause of the crisis is something that was manageable by NexaHome. The cause of the crisis is something over which NexaHome had power.	Coombs and Holladay (2002)
Trust towards the organisation (α = .92)	I think NexaHome is reliable. I think NexaHome keeps promises and commitments. I think NexaHome keeps customers' best interests in mind. I feel confidence in brand NexaHome.	Yang, Lee and Zo (2017)
Trust towards the device (α = .92)	I think smart home devices are reliable. I think smart home devices meet their expectations I think smart home devices serve users' interests I feel confidence in smart home devices.	Adjusted scale from Yang, Lee and Zo (2017)
Perceived threat (α = .94)	Smart home devices pose a threat to my security and privacy. The trouble caused by smart home devices threaten my security and privacy. Smart home devices are a danger to my security and privacy. It is terrible when my security and privacy is violated by smart home devices. Using smart home devices is a risk to my security and privacy.	Duezguen et al. (2021)
Intention to use (α = .96)	I would like to use smart home devices. I expect to use smart home devices. I can see myself using smart home devices.	Klobas, McGill and Wang (2019)

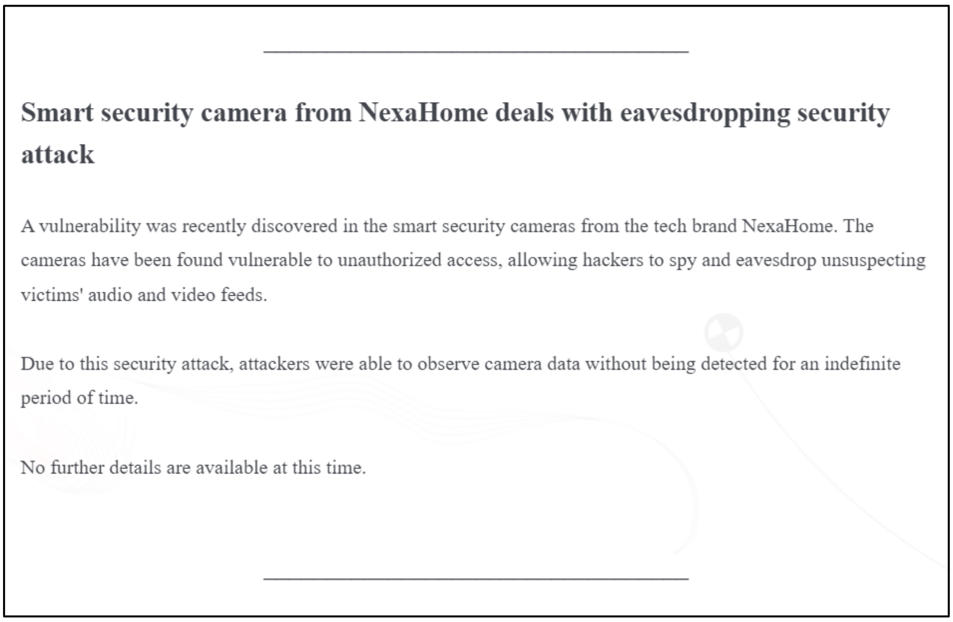
Appendix B: List of all the hypothesis

Table B1
List of hypothesis

Hypothesis	
H1a	A passive security attack (in contrast to an active security attack) results in a higher degree of perceived threat.
H1b	A passive security attack (in contrast to an active security attack) results in a greater decrease in trust towards the device.
H2a	High intrusive smart devices (in contrast to low intrusive smart devices) are associated with a higher degree of perceived threat.
H2b	High intrusive smart devices (in contrast to low intrusive smart devices) are associated with a greater decrease in trust towards the device.
H3a	A passive security attack (in contrast to an active security attack) results in a higher level of crisis responsibility.
H3b	A passive security attack (in contrast to an active security attack) results in a greater decrease in trust towards the organisation.
H4a	High intrusive smart devices (in contrast to low intrusive smart devices) are associated with a higher level of crisis responsibility.
H4b	High intrusive smart devices (in contrast to low intrusive smart devices) are associated with a greater decrease in trust towards the organisation.
H5a	There is an interaction effect between the type of smart home device and the type of security attack on perceived threat
H5b	There is an interaction effect between the type of smart home device and the type of security attack on trust towards the device
H5c	There is an interaction effect between the type of smart home device and the type of security attack on crisis responsibility
H5d	There is an interaction effect between the type of smart home device and the type of security attack on trust towards the organisation
H6	Perceived threat will have a negative effect on the intention to use
H7	Trust towards the device will have a positive effect on the intention to use
H8	Crisis responsibility will have a negative effect on the intention to use
H9	Trust towards the organisation will have a positive effect on the intention to use

Appendix C: Full list of experimental conditions

Condition 1: High intrusiveness: smart camera; passive attack: eavesdropping



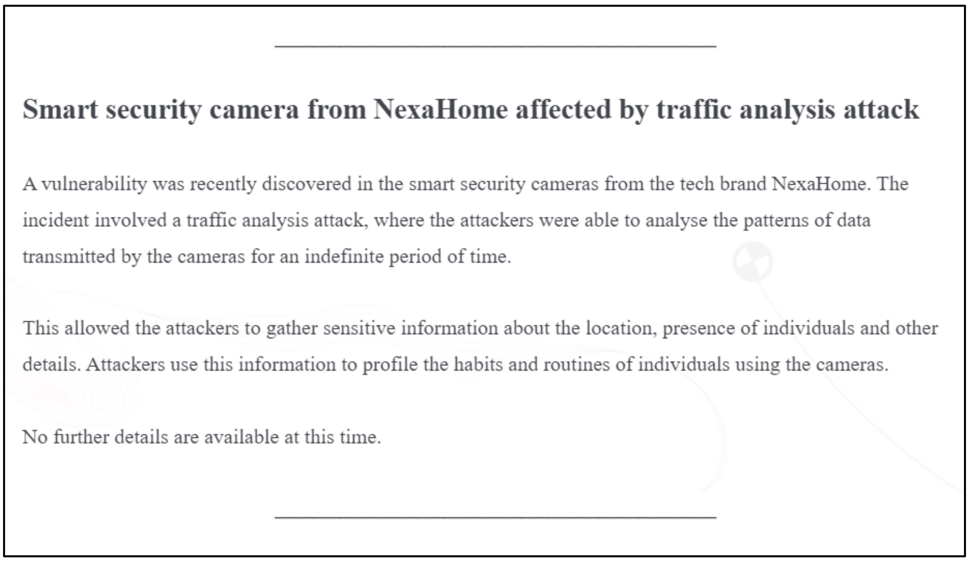
Smart security camera from NexaHome deals with eavesdropping security attack

A vulnerability was recently discovered in the smart security cameras from the tech brand NexaHome. The cameras have been found vulnerable to unauthorized access, allowing hackers to spy and eavesdrop unsuspecting victims' audio and video feeds.

Due to this security attack, attackers were able to observe camera data without being detected for an indefinite period of time.

No further details are available at this time.

Condition 2: High intrusiveness: smart camera; passive attack: traffic analysis



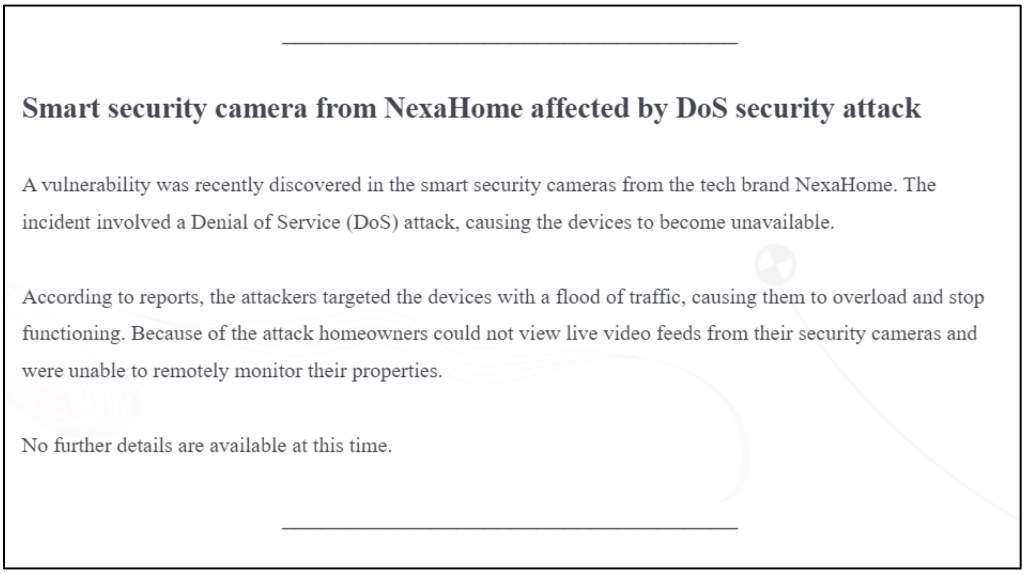
Smart security camera from NexaHome affected by traffic analysis attack

A vulnerability was recently discovered in the smart security cameras from the tech brand NexaHome. The incident involved a traffic analysis attack, where the attackers were able to analyse the patterns of data transmitted by the cameras for an indefinite period of time.

This allowed the attackers to gather sensitive information about the location, presence of individuals and other details. Attackers use this information to profile the habits and routines of individuals using the cameras.

No further details are available at this time.

Condition 3: High intrusiveness: smart camera; active attack: DoS



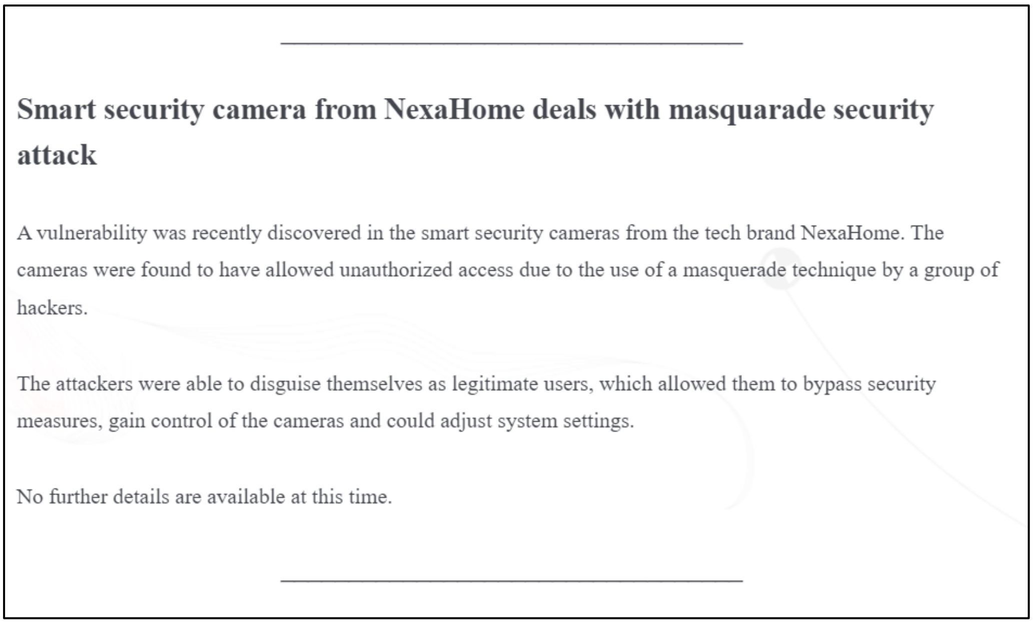
Smart security camera from NexaHome affected by DoS security attack

A vulnerability was recently discovered in the smart security cameras from the tech brand NexaHome. The incident involved a Denial of Service (DoS) attack, causing the devices to become unavailable.

According to reports, the attackers targeted the devices with a flood of traffic, causing them to overload and stop functioning. Because of the attack homeowners could not view live video feeds from their security cameras and were unable to remotely monitor their properties.

No further details are available at this time.

Condition 4: High intrusiveness: smart camera; active attack: masquerade



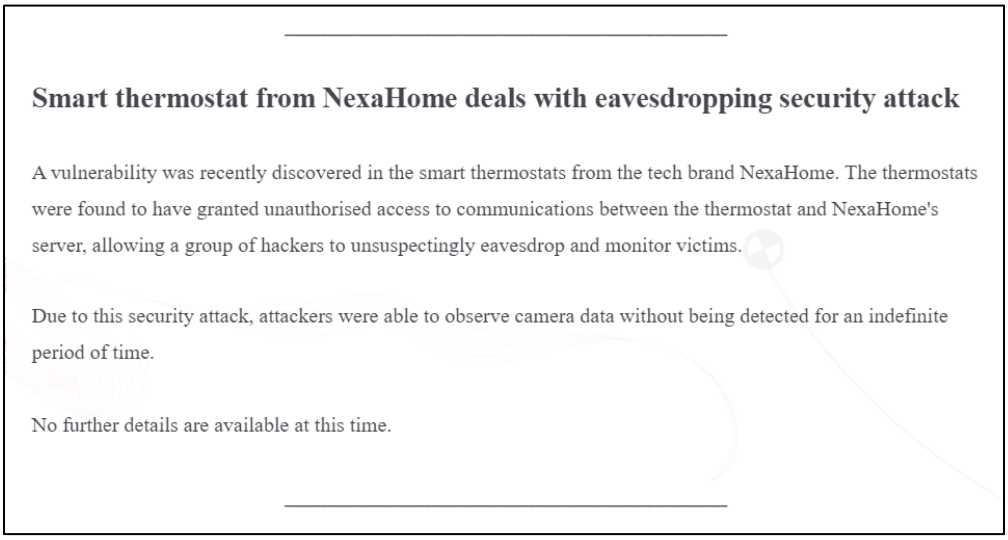
Smart security camera from NexaHome deals with masquarade security attack

A vulnerability was recently discovered in the smart security cameras from the tech brand NexaHome. The cameras were found to have allowed unauthorized access due to the use of a masquerade technique by a group of hackers.

The attackers were able to disguise themselves as legitimate users, which allowed them to bypass security measures, gain control of the cameras and could adjust system settings.

No further details are available at this time.

Condition 5: Low intrusiveness: smart thermostat; passive attack: eavesdropping



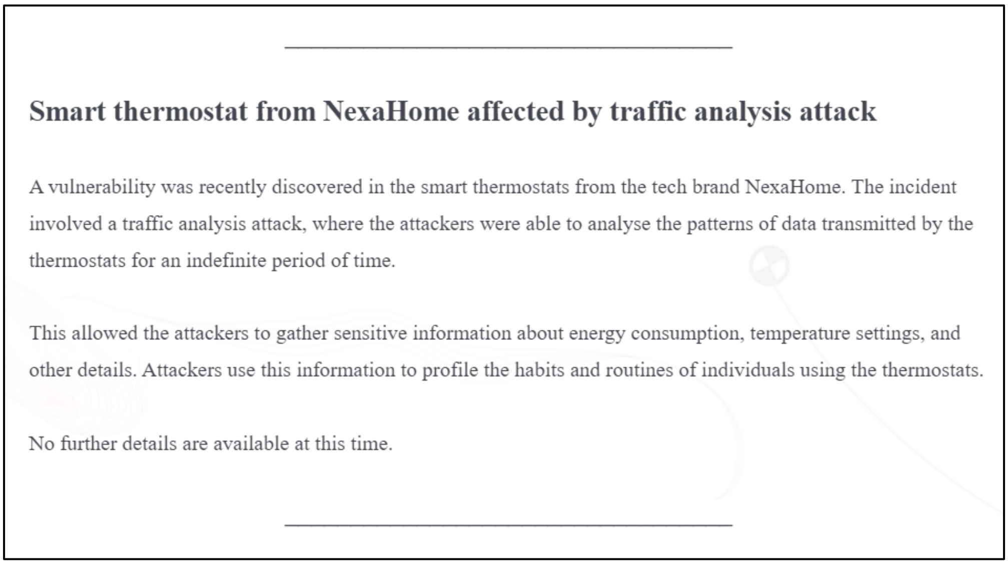
Smart thermostat from NexaHome deals with eavesdropping security attack

A vulnerability was recently discovered in the smart thermostats from the tech brand NexaHome. The thermostats were found to have granted unauthorised access to communications between the thermostat and NexaHome's server, allowing a group of hackers to unsuspectingly eavesdrop and monitor victims.

Due to this security attack, attackers were able to observe camera data without being detected for an indefinite period of time.

No further details are available at this time.

Condition 6: Low intrusiveness: smart thermostat; passive attack: traffic analysis



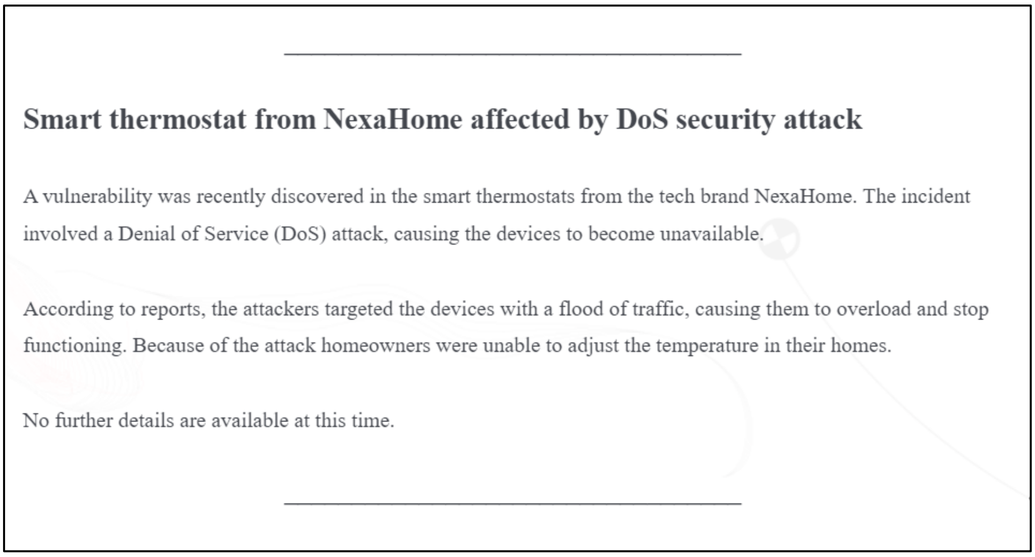
Smart thermostat from NexaHome affected by traffic analysis attack

A vulnerability was recently discovered in the smart thermostats from the tech brand NexaHome. The incident involved a traffic analysis attack, where the attackers were able to analyse the patterns of data transmitted by the thermostats for an indefinite period of time.

This allowed the attackers to gather sensitive information about energy consumption, temperature settings, and other details. Attackers use this information to profile the habits and routines of individuals using the thermostats.

No further details are available at this time.

Condition 7: Low intrusiveness: smart thermostat; active attack: DoS



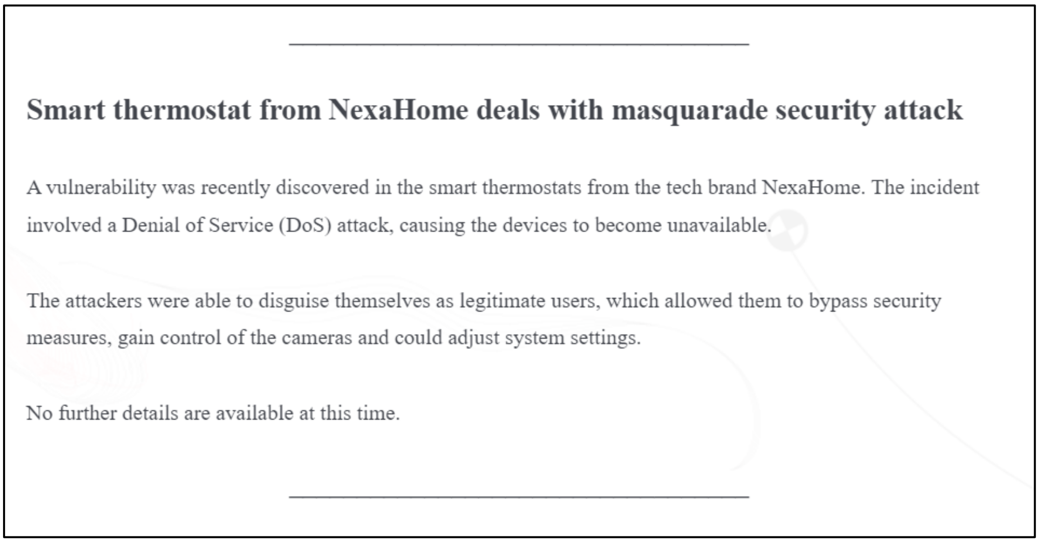
Smart thermostat from NexaHome affected by DoS security attack

A vulnerability was recently discovered in the smart thermostats from the tech brand NexaHome. The incident involved a Denial of Service (DoS) attack, causing the devices to become unavailable.

According to reports, the attackers targeted the devices with a flood of traffic, causing them to overload and stop functioning. Because of the attack homeowners were unable to adjust the temperature in their homes.

No further details are available at this time.

Condition 8: Low intrusiveness: smart thermostat; active attack: masquerade



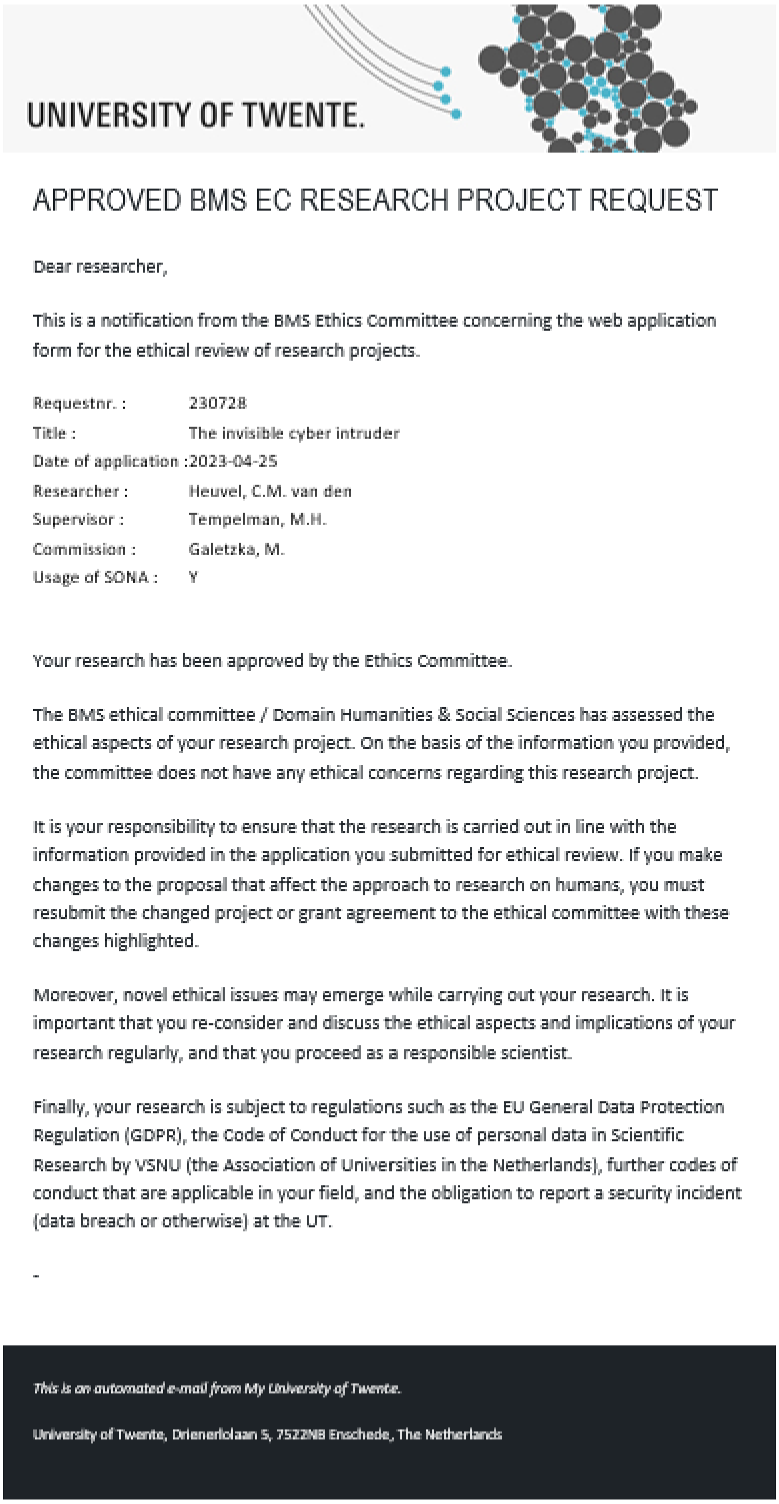
Smart thermostat from NexaHome deals with masquarade security attack

A vulnerability was recently discovered in the smart thermostats from the tech brand NexaHome. The incident involved a Denial of Service (DoS) attack, causing the devices to become unavailable.

The attackers were able to disguise themselves as legitimate users, which allowed them to bypass security measures, gain control of the cameras and could adjust system settings.

No further details are available at this time.

Appendix D: Approval form of ethics committee



UNIVERSITY OF TWENTE.

APPROVED BMS EC RESEARCH PROJECT REQUEST

Dear researcher,

This is a notification from the BMS Ethics Committee concerning the web application form for the ethical review of research projects.

Requestnr. :	230728
Title :	The invisible cyber intruder
Date of application :	2023-04-25
Researcher :	Heuvel, C.M. van den
Supervisor :	Tempelman, M.H.
Commission :	Galetzka, M.
Usage of SONA :	Y

Your research has been approved by the Ethics Committee.

The BMS ethical committee / Domain Humanities & Social Sciences has assessed the ethical aspects of your research project. On the basis of the information you provided, the committee does not have any ethical concerns regarding this research project.

It is your responsibility to ensure that the research is carried out in line with the information provided in the application you submitted for ethical review. If you make changes to the proposal that affect the approach to research on humans, you must resubmit the changed project or grant agreement to the ethical committee with these changes highlighted.

Moreover, novel ethical issues may emerge while carrying out your research. It is important that you re-consider and discuss the ethical aspects and implications of your research regularly, and that you proceed as a responsible scientist.

Finally, your research is subject to regulations such as the EU General Data Protection Regulation (GDPR), the Code of Conduct for the use of personal data in Scientific Research by VSNU (the Association of Universities in the Netherlands), further codes of conduct that are applicable in your field, and the obligation to report a security incident (data breach or otherwise) at the UT.

-

This is an automated e-mail from My University of Twente.

University of Twente, Drienerlolaan 5, 7522NB Enschede, The Netherlands