applied sciences

MDPI

Article

We are not Equipped to Identify the First Signs of Cyber-Physical Attacks: Emotional Reactions to Cybersecurity Breaches on Domestic Internet of Things Devices

Sanja Budimir[1], Johnny R.J. Fontaine[1], Nicole M.A. Huijts[2,3], Antal Haans[3], Wijnand A. IJsselsteijn[3], Anne-Marie Oostveen[4], Frederic Stahl[5], Ryan Heartfield[6], George Loukas[6] Anatolij Bezemskij[6], Avgoustinos Filippoupolitis[6], Ivano Ras[7, 8] and Etienne B. Roesch[8,9]

[1] Department of Work, Organisation and Society, Faculty of Psychology and Educational sciences, Ghent University, Gent, Belgium; Sanja.Budimir@UGent.be; Johnny.Fontaine@UGent.be
[2] Psychology of Conflict, Risk and Safety, University of Twente, Enschede, the Netherlands; n.m.a.huijts@utwente.nl
[3] Department of Industrial Engineering & Innovation Sciences, Eindhoven University of Technology, the Netherland; A.Haans@tue.nl; W.A.IJsselsteijn@tue.nl
[4] Centre for Robotics and Assembly. Faculty of Engineering and Applied Sciences (FEAS). Cranfield University, Cranfield, United Kingdom; j.m.oostveen@cranfield.ac.uk
[5] German Research Center for Artificial Intelligence GmbH (DFKI), Marine Perception Research Department, Germany; frederic_theodor.stahl@dfki.de
[6] School of Computing and Mathematical Sciences, University of Greenwich, London, United Kingdom; G.Loukas@greenwich.ac.uk; Anatolij.Bezemskij@greenwich.ac.uk; avgoustinos.f@gmail.com; ryan.heartfield@exalens.com
[7] D-INFK, ETH Zurich, Switzerland; ivano.ras@gmail.com
[8] Centre for Integrative Neuroscience and Neurodynamics, University of Reading, Reading, United Kingdom; e.b.roesch@reading.ac.uk
[9] School of Psychology and Clinical Language Sciences, University of Reading, Reading, United Kingdom

* Correspondence: Sanja.Budimir@UGent.be

Featured Application: This research offers insights into how cybersecurity breaches impact users of household Internet of Things (IoT) devices on a psychological level. Through the Component Process Model (CPM) framework, the study uncovers the nuanced emotional responses evoked by different cybersecurity breach scenarios, ranging from security cameras to smart speakers. These findings provide a deeper understanding of users' psychological vulnerabilities in the face of cyber threats, paving the way for more effective cybersecurity strategies tailored to domestic IoT environments. By integrating these insights, stakeholders, including device manufacturers and policymakers, can reinforce security protocols, address user concerns resulting from cybersecurity breaches, and strengthen resilience against cyber intrusions within households.

Abstract: The increasing number of domestic Internet of Things (IoT) devices in our lives leads to numerous benefits, but also comes with an increased risk of cybersecurity breaches. These breaches have psychological consequences for the users. We examined the nature of the psychological impact of cybersecurity breaches on domestic IoT by investigating emotional experiences in a scenario study (Study 1) and a field experiment (Study 2), using the five emotion components of the Component Process Model (CPM) and emotion regulation as a framework. We replicated a three-dimensional structure for emotional experiences found in a previous study, with an addition of an ancillary fourth dimension in the second study. The first dimension represents emotional intensity. The second bipolar dimension describes constructive vs unconstructive action tendencies. On the third dimension, also bipolar, cognitive and motivational emotion features are opposed to affective emotion features. The fourth dimension, labeled distress symptoms, mainly reflected negative

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Lastname

Received: date
Revised: date
Accepted: date
Published: date

emotions. In Study 2, most of the introduced frequent irregularities on IoT devices have not been noticed, and the intensity of emotional reactions and tendencies to react in a constructive way decreased throughout the phases of the experiment. These findings reveal that we are not emotionally equipped to identify potential threats in the cyber world.

Keywords: cybersecurity breach; IoT devices; emotions; Componential Process Model

1. Introduction

The number of Internet of Things (IoT) devices and their integration in the workplace as well as in private lives has exponentially increased over the past years, with the global number surpassing 16 billion in 2023, and it is expected to reach 18.8 billion by the end of 2024 and, continuing to expand rapidly towards 30 billion by 2030 [1,2]. Moreover, with the introduction and application of 5G technology, the diversity of their use is expected to increase even more. The number of devices that can be connected to the Internet and controlled wirelessly has already expanded from light bulbs, security doors, locks, speakers, vacuum cleaners, security cameras to washing machines, smart toys, smart fridges, air quality monitors, domestic robots, and more.

Applications of IoT devices include various environments, from work offices and public spaces to homes. When these devices are used in the privacy of the household, specific issues need to be addressed. The ISO 25010 framework, which focuses on product quality, also identifies critical security attributes such as confidentiality, integrity, non-repudiation, accountability, authenticity and resistance [3,4].These attributes are particularly relevant for ensuring the secure use of IoT devices in the home. Furthermore, the protection of home IoT networks from external threats falls under the information security management guidelines outlined in ISO 27000 [5].

The home should be a private space for members of the household, but this privacy may be challenged with the introduction of IoT devices that enable remote control. Despite the clear benefits of remote control (e.g., appliances such as washing machines, vacuum cleaners, to the automatic remote activation of lights, speakers, and locks), these advantages can easily transform into threats if the control is taken over by a third party. Potentially it could open the front door to wrongdoers without an actual physical burglary and give access to private activities through compromised cameras and microphones, as well as interfere with numerous settings that can cause discomfort or damage to household members. For example, attackers could manipulate smart thermostats, leading to energy waste or health risks, disable security systems to facilitate unauthorized access (using similar sounding phrases to trigger the device to perform unintended actions), listen to private conversations, deploy malicious applications, or access sensitive data, exposing the household to privacy violations or identity theft and potentially leading to economic losses and safety concerns [6]. According to the mid-year update to the 2023 SonicWall Cyber Threat Report, IoT malware globally increased by 37% in the first half of 2023, with a total of 77.9 million attacks compared to 57 million in the first half of 2022 [7]. IoT devices are increasingly targeted by sophisticated malware that exploit weak passwords, outdated firmware, and insecure interfaces, highlighting the importance of proactive measures [8].

1.1. Cyber security breach

A cybersecurity breach poses a threat for any connected device by compromising confidentiality through unauthorized access, integrity through unauthorized manipulation of data, availability through denial of service and jamming, and non-repudiation by offering evidence that a specific activity was not legitimate [9]. Most attacks in 2022 exploited known common vulnerabilities and exposures (CVEs) often used in automated attack toolkits. Despite being aware of these vulnerabilities, IoT and firmware service

providers may take time to assess and release patches, leaving smart homes exposed to cybercriminals during this period [10]. This delay allows attackers to continuously exploit these weaknesses, undermining the security and privacy of IoT environments.

In the event of a cybersecurity breach involving an IoT device, the consequences can extend beyond cyberspace to impact physical environments. These physical effects may include breaches of privacy, such as eavesdropping through a baby monitor; unauthorized actuation, like a smart speaker playing loud music unexpectedly during the night; incorrect actuation, such as a camera rotating in the wrong direction; and delayed or obstructed actuation, for example, preventing a smart door from locking [11]. However, the main issue with IoT is that traditional cyber risk management systems may not be effective due to the growing demands and capabilities of IoT technology [12]. Apart from the direct consequences that the breach can have, such as a loss of control, inconvenience, or financial, vocational, health and safety impacts, it can also cause damage to the users' psychological wellbeing. Depending on the nature of the attack and its consequences, some of these impacts can be instantly noticeable, while others only become apparent over time. Little is known about how users experience cybersecurity breaches, and it is important to gain a better understanding of users' needs and consequently adjust the manufacturers' security standards as well as legal regulations to protect cybersecurity in households. This domain lacks scientific, targeted, and theoretically grounded research. First attempts to explore the psychological aspects of cyber aggression indicate victim's distress through reports of anxiety, stress, anger, sadness, insecurity, annoyance, frustration and even a suicide [13]. Reported emotional reactions to threatening events in cyberspace indicate the importance of exploring the emotion processes in reaction to cybersecurity breaches.

1.2. Emotion processes resulting from cybersecurity breaches / Component Process Model

Cybersecurity breaches can impact victims emotionally by making them feel vulnerable and distressed, especially when they lose control over personal information at home. Losses in confidentiality, integrity, and availability of data play a major role in these reactions. Traditionally, emotions are studied by using emotion terms representing a specific emotion or an emotional dimension, such as anger, fear, or positive and negative affect [14]. As this approach examines only one aspect of the emotion process (i.e., the feeling as experienced by the person), it provides limited insights into the underlying emotion process that is elicited by the cybersecurity breach. An approach for studying the whole emotion process is offered by the Component Process Model (CPM) [15]. CPM defines emotions as processes elicited by goal-relevant events that consist of five components, namely appraisals (cognitive evaluation of the event), action tendencies (preparation for the action and directed action), bodily reactions (physiological reaction), expressions (expressive behavior in face, voice, and gestures) and subjective feeling (awareness of the occurrence of an emotion process). From an evolutionary perspective emotions are designed to be adaptive, enabling us to respond effectively to our environment. However, they can also lead to psychopathology and mental dysfunction.

Using the CPM [15], one can go beyond merely observing the positive and negative feelings, and look at the unfolding emotion process. In turn, this enables a much better understanding of both the adaptive and constructive, as well as the possible maladaptive and unconstructive aspects of these processes.

Previous studies [16–18], have addressed emotional responses to cybersecurity incidents, primarily focusing on broader cyber threats like cyberterrorism and cyberbullying, concentrating mainly on basic emotions and immediate emotional reactions. Our study, however, takes a different approach by focusing specifically on emotional responses to cybersecurity breaches in domestic IoT environments. By applying the Component Process Model (CPM) framework, we explore not only the subjective feeling dimension of emotions but also the unfolding of the emotional process. Unlike existing research, which primarily focuses on broad categories of cyber threats and the basic emotions, our approach goes beyond these by considering a specific context. This allows us to provide a

more detailed understanding of how different IoT devices and breach intensities elicit varying emotional reactions, thus contributing to a clearer theoretical framework within the existing body of cybersecurity research.

Recently, the emotional impact of cybersecurity breaches on victims, focusing on a range of connected devices (e.g., computers, smartphones) and accounts (e.g., email, social media, and bank accounts) have been explored in two studies [19,20]. In the specific context of cybersecurity breaches, this approach allowed not only for the identification of negative emotions, but also of how emotions can be constructive or unconstructive. The first study analyzed anticipated emotion processes through presenting participants with cybersecurity breach situations [21]. The second study analyzed the experiences of victims of actual cybersecurity breaches [20]. Both studies used the lens of the Component Process Model and found the same well-interpretable three-dimensional structure of emotion processes experienced in cybersecurity breach situations. The first dimension reflects the intensity of negative emotional experiences in general with high positive loadings of all negative emotion features. The second dimension differentiates between two types of "action tendencies." One pole represents constructive tendencies, which aim to resolve the distressing situation, while the opposite pole reflects unconstructive tendencies, such as withdrawing or attacking. A third bipolar dimension describes cognitive motivational emotional reactions on one side (with highest loadings for appraisals and action tendencies), versus affective emotion reactions on the other side (with highest loadings for subjective feelings, expressions, and bodily reactions). Previous studies [20,21] explored emotional reactions to cybersecurity breaches but focused on general connected devices, such as smartphones, computers, and online accounts. Our study diverges by specifically targeting a wider range of domestic IoT devices, including smart cameras, smart speakers, and other home-based technologies. Additionally, we combine both a scenario-based survey study and a real-life field experiment to capture emotional responses in more realistic home environments. This dual approach provides deeper insights into how users emotionally respond to cybersecurity breaches in their own homes, making our study unique compared to prior works.

1.3. Research aims and hypothesis

In two studies, we aim to increase our understanding of the complexity of emotion processes—both maladaptive and adaptive—triggered by cybersecurity breaches on IoT devices located in the home, and how these vary between different types of IoT devices and attack intensities.

For these purposes, participants were presented with different cybersecurity breaches. In Study 1—the online scenario study—written descriptions of these breaches were presented to participants, and they were asked to imagine as if it was happening to them. In Study 2—the field experiment—the same breaches were simulated to occur to actual IoT devices installed in the participant's own home. In the field experiment, self-report data were collected during various phases: before participants were exposed to the simulated attacks, during attacks of which the participants were not notified by the experimenter, and during attacks but being informed about these being executed to their IoT devices. We had the following research questions and hypothesis:

1.3.1.Research question and hypothesis 1

What is the structure of emotional experiences elicited by domestic IoT cybersecurity breaches, through scenarios (Study 1) and simulations (Study 2)?

Based on previous scenario studies, the hypothesis is that a three-dimensional structure will be identified, consisting of an intensity dimension, a constructive vs. unconstructive action tendency dimension, and a cognitive-motivational vs. affective orientation dimension.

1.3.2.Research question and hypothesis 2

How does the type of IoT devices and the intensity of cybersecurity breaches affect the emotional experiences of users, through scenarios (Study 1) and simulations (Study 2)?

We hypothesize that more intense cybersecurity breaches will elicit more intense negative emotions. The effects of the type of IoT devices and other emotion dimensions will be explored.

1.3.3. Research question and hypothesis 3

Do emotional experiences change throughout the phases of cybersecurity breaches in the experiment (Study 2)?

We hypothesize that the most intense emotional reactions will occur during the phase of the field experiment, when participants are exposed to simulated cybersecurity breaches without being informed. The effects of the type of IoT devices and other emotion dimensions will be explored.

2. Study design

The objective of the study was to examine individuals' emotional experiences of cybersecurity breaches on their IoT devices. This objective applies to both the online scenario study (Study 1) and the field experiment (Study 2). For this purpose, we constructed cybersecurity breach scenarios for five different IoT devices within the home namely: a security camera, a smart scale, a smart light, a digital photo frame plugged into a smart socket, and a smart speaker. The selection of the five IoT devices is strategic; these devices are prevalent in contemporary households and serve different functions that raise distinct privacy and security concerns. Our aim is to provide a comprehensive understanding of how users perceive security threats across various devices. Since we used the same devices in Study 1 as in Study 2, we were constrained in our selection by ethical considerations, including that the devices should not directly lower home security (e.g., no smart door lock) and should be non-medical. To minimize potential harm, we implemented strict controls over simulated breaches. For instance, activities were designed to avoid severe privacy violations, such as recording participants through the smart camera. Scenarios focused on less intrusive actions, like opening or closing the camera's shutter or triggering moderate-volume sounds from the smart speaker. Device use was limited to a dedicated tablet within the home. Participants were chosen for the study based on their psychological resilience, with their responses closely tracked using an online diary and questionnaires (details not included in this study). This approach allowed the research team to quickly identify and address any concerning situations as they arose. The cybersecurity breach on each device included two or three different cybersecurity breach intensity levels (independent variable; see Table A2 in Appendix A). The intensity increased by manipulating the duration, frequency, or volume of irregular device activity. The nature and the intensity of these breaches were influenced by ethical considerations, and all were approved by ethical committees of the involved research partners. Emotional reactions to a total of 18 cybersecurity breach scenarios (3 to 4 per device) were measured across two separate studies (independent variable; an online scenario-based study and a field experiment). For both studies, the independent variables included the type of IoT device (e.g., camera, smart scale) and the breach intensity (mild, moderate, severe). The dependent variables measured were emotional reactions; appraisals, action tendencies, bodily responses, expressions, subjective feelings.

For Study 1, the objective was to investigate how emotional responses vary across different IoT devices when participants imagine cybersecurity breaches of varying intensity. Study 1 was an online scenario study in which participants were presented with detailed descriptions of cybersecurity breaches. They were asked to imagine themselves experiencing the described situation (exposure). Then participants were provided ample time to read, reflect (context) and report their emotions using the Cybersecurity GRID questionnaire (dependent variable), which probes into all emotion components. In Study 1 no real device was involved, and the emotion reactions were based on imagining the breach scenario (exposure). The objective of Study 2 was to observe how actual exposure

to cybersecurity breaches in real-life settings impacts emotional responses, also across different IoT devices with varying intensities of simulated cybersecurity breaches.

Study 2 was a field experiment in which participants experienced cybersecurity breaches on their actual IoT devices in their households. The intensity of the breaches increased progressively (e.g., the frequency of a smart light turning on/off) (context). Real, staged cybersecurity breaches on household IoT devices were implemented (exposure). Each household had a variable experimental duration depending on their start and the number of experimental phases, with an average study period of 7 weeks. Emotional reactions were similarly measured using the Cybersecurity GRID questionnaire (dependent variable). The Component Process Model (CPM) serves as a foundational framework in our research. It allows us to dissect the emotional responses elicited by cybersecurity breaches, focusing on how users perceive threats based on their experiences with household IoT devices. This model aids in understanding the interplay between emotional reactions and contextual factors that influence user behavior.

3. Study 1

3.1. Materials and Methods

3.1.1. Participants

Study 1 involved 544 participants, aged 18-65, with equal gender representation. They were recruited by the research team from Qualtrics experience management company [22] and represented a range of professions and technological familiarity levels. To better understand user emotional responses to security breaches, we classified the selected IoT devices and corresponding types of intrusions. Table 1 below outlines the devices.

Table 1. Overview of Number of Participants (N=544) Exposed to Specific Scenario for Different IoT Devices and Conditions in Study 1.

Conditions		CAMERA	SCALE	LIGHT	PHOTO FRAME	SPEAKER
1	A	35	34	26	26	22
	B			24	26	28
2	A	36	37	27	26	27
	B					26
3		37	30	26	26	
Total		108	101	103	104	103

3.1.2. Procedure

Each participant was presented with one randomly assigned scenario of a cybersecurity breach on a household IoT device and was asked to imagine finding oneself in that scenario. Subsequently, they were asked to report their expected emotional experience on five emotion components plus emotion regulation features measured by the Cybersecurity GRID questionnaire [19,20]. In total there were 18 scenarios of cybersecurity breaches on 5 different IoT devices (security camera, scale, light, digital photo frame and speaker). Each scenario had two or three different intensity levels, with higher levels being more intensive and more intrusive; for some levels there were two scenarios described (see Appendix A, Table A1). Each participant was assigned randomly to only one scenario (Table 1)

3.1.3. Instrument

The Cybersecurity GRID questionnaire examines five emotion components plus emotion regulation in the specific setting of cybersecurity breaches. It includes a total of

73 emotion features (16 appraisals, 16 action tendencies, 11 bodily reactions, 8 expressions, 14 subjective feelings, and 8 emotion regulations). An overview of all items is available in the Appendix A Table A3- table (including all the factor loadings).

3.2. Results

3.2.1. Underlying Structure of the Interindividual Differences in Emotion Processes in the Situation of Cybersecurity Breaches of Domestic IoT Devices

To identify the major dimensions that can represent the interindividual variability among 73 emotion features, a Principal Component Analysis was applied. The components will be referred to as dimensions in the remainder of this manuscript to avoid confusion with the concept of emotion components. Based on previous research [19,20] we expected a three-dimensional structure, and the Scree plot in this study indeed clearly indicated a replication of this number of dimensions (Appendix A, Figure A1). Orthogonal Procrustes rotation towards the a priori expected dimensions of 'General', 'Constructive vs unconstructive reactions' and 'Affective vs cognitive-motivational reactions' found in the previous study [19] was applied on the unrotated factor loading matrix (Table 2). A very good congruence for all three dimensions (proportionality coefficient per factor, Tucker's phi: .99 .93 .92) point to a replication of the previous study working only with a cybersecurity breach of a security camera [19]. The three-dimensional structure accounted for 48% of total variance (see Table 2 for the ten highest loading features per dimension, see Table A3 in Appendix A for a full loading matrix and the loadings for second and third dimension are plotted in the Figure A3).

On the first dimension all emotion features had a positive loading, indicating an emotional reaction to the scenario of a cybersecurity breach, and with the highest loadings for subjective experiences (e.g., I would feel worried, I would feel afraid). The highest loadings on this dimension indicated more intensive negative emotion processes elicited by the cybersecurity breach scenarios on IoT devices. This dimension is labeled 'emotional intensity'.

The second dimension had high loadings of appraisals and action tendencies indicating constructive reactions on the one side, and unconstructive action tendencies, bodily reactions, and subjective feelings on the other side. This bipolar dimension is labeled 'constructive vs unconstructive.' Positive loadings reflected unconstructive action tendencies (e.g., I would want to destroy whatever was close, I would want to take revenge) as well as bodily reactions indicated distress (e.g., I would have pain in the chest, I would be dizzy), while negative loadings reflected constructive tendencies (e.g., I would think "I wonder whether something is wrong with the device/account", I would want to find a solution and fix the problem). The second dimension reflected the specific nature of cybersecurity breaches in which either withdrawing from the use of connected devices or wanting to attack or punish the often invisible and unreachable attacker can be considered unconstructive.

The third dimension is also replicated. The cognitive-motivational pole is represented by positive loadings of appraisal and action tendency emotion features (e.g., I would think "Someone may have access to my private information", I would think "Someone could destroy my data."). The affective pole of this dimension is represented by negative loadings of subjective feelings, bodily reactions, expressions, and emotion regulation features (e.g., I would be restless, slouched, frustrated, sad).

Table 2. Principal Component Loadings of the Cybersecurity GRID Items in Study 1 After Orthogonal Procrustes Rotation Towards the a Priori Theoretically Expected Dimensions

	Dimension Loading

Emotion Feature Item	**D1**	**D2**	**D3**
General Emotion Dimension			
SF7 I felt/ I would feel worried.	.79	.02	-.18
SF4 I felt/ I would feel afraid.	.76	.27	-.20
SF3 I felt/ I would feel anxious.	.75	.10	-.25
SF5 I felt/ I would feel panic.	.73	.23	-.31
SF14 I felt/ I would feel uncomfortable.	.72	.07	-.16
SF6 I felt/ I would feel upset.	.71	.07	-.26
A17 I thought/ I would think “Someone could use my data to harm me."	.69	.11	.52
SF1 I was/would be in an intense emotional state.	.68	.37	-.29
BR8 My muscles were/would be tense.	.67	.28	-.34
E8 I was/ would be walking around nervously.	.67	.29	-.34
Constructive			
AT9 I wanted to/would want to find a solution and fix the problem.	.28	-.60	-.14
A2 I thought/ I would think “I wonder whether something is wrong with the device/account."	.27	-.55	.00
AT2 I wanted to/would want to regain control over the device/account.	.46	-.53	.00
AT1 I wanted to/would want to stop what was happening.	.47	-.50	.03
AT11 I wanted to/would want to reset my device.	.33	-.47	-.07
Unconstructive			
BR4 I had/would have pain in the chest.	.56	.55	-.14
BR2 I was/would be dizzy.	.58	.54	-.14
AT14 I wanted to/would want to destroy whatever was close.	.37	.53	.07
SF10 I felt/ I would feel ashamed.	.49	.53	-.13
AT5 I wanted to/would want to isolate myself physically.	.50	.52	.19
Cognitive-Motivational			
A16 I thought/ I would think “Someone could destroy my data."	.65	.12	.57
A15 I thought/ I would think “Someone may have access to my private information."	.66	.06	.57
A8 I thought/ I would think “My security could be jeopardized."	.64	-.02	.55
A17 I thought/ I would think “Someone could use my data to harm me."	.69	.11	.52
A14 I thought/ I would think “I could lose personal information, data and documents."	.60	.07	.52
Affective			
E7 I was/would be restless (touching face, hair, biting nails, nervously kicking with legs).	.64	.22	-.40
E5 I slouched/ would slouch (shoulders down, head down, hands down).	.44	.26	-.39
E3 I spoke/would speak louder.	.45	.13	-.36
SF9 I felt/ I would feel sad.	.56	.15	-.36
SF12 I felt/ I would feel frustrated.	.56	-.21	-.36

Note. For the full table with loadings, see supplemental material Table S3.

We showed that the internal structure of emotion features reported for the scenarios describing cybersecurity breaches on different domestic IoT devices is comparable to the structure that was found for cybersecurity breaches on a smart camera in another scenario study [19], as well as on smart phones, computers, and different online accounts (email, bank, and social network accounts) in a survey study [20]. It can thus be concluded, based on all these studies, that the internal structure of emotional experiences of cybersecurity breaches includes three dimensions where the first one reflects the intensity of negative emotional experience. A second dimension differentiates constructive versus unconstructive action tendencies. On the third-dimension cognitive motivational reactions are opposed to affective (bodily) reactions.

3.2.2. Differences across Five IoT Devices in Households

Separate univariate ANOVAs with a nested design were performed to compare the effect of type of device (5 devices: camera, scale, light, photo frame, and speaker), and different conditions (3 to 4 conditions with varying levels of intensity in terms of noticeability) on the three identified emotion dimensions (emotional intensity, constructive/unconstructive, cognitive motivational/affective).

A univariate ANOVA revealed that there was a statistically significant difference in the emotional intensity dimension (F (4, 501) = 13.43, p=.000, η^2= .10). Tukey's HSD Test for multiple comparisons indicated that the mean value of the emotional intensity dimension was significantly different between the smart camera and the other devices, namely the smart scale (p=.000, 95% C.I. = [.39, 1.11]), the smart light (p=.000, 95% C.I. = [.40, 1.11]), the smart digital photo-frame (p=.000, 95% C.I. = [.34, 1.05]), and the smart speaker (p=.000, 95% C.I. = [.41, 1.12]). Reactions to the smart camera cybersecurity breach scenario triggered the most intensive emotional reaction (Figure 1). There was no statistically significant difference between the other IoT devices (p > .05).

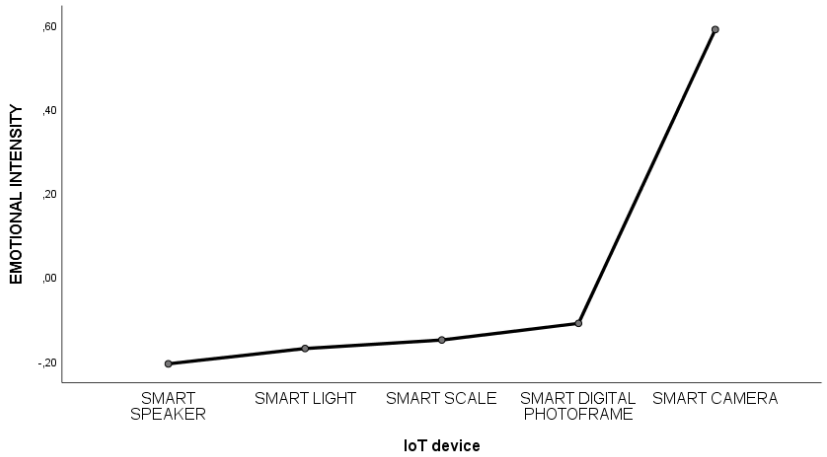

Figure 1. Estimated Marginal Means of The Emotional Reactions on the First Dimension for IoT Devices.

A univariate ANOVA revealed that there was a statistically significant difference in the Constructive vs Unconstructive dimension (F (4, 501) = 4.21, p=.002, η^2= .03). Tukey's HSD Test for multiple comparison indicated that the mean value was significantly different between the smart light and the smart scale (p=.029, 95% C.I. = [.03, .78]), and between the smart light and the smart speaker (p=.016, 95% C.I. = [-.80, -.05]). Reactions to the cybersecurity breach scenario on a smart light triggered more anticipated constructive action tendencies compared to breaches on the smart scale and smart speaker, which triggered more anticipated unconstructive action

tendencies (Figure 2). There was no statistically significant difference between the other IoT devices ($p > .05$).

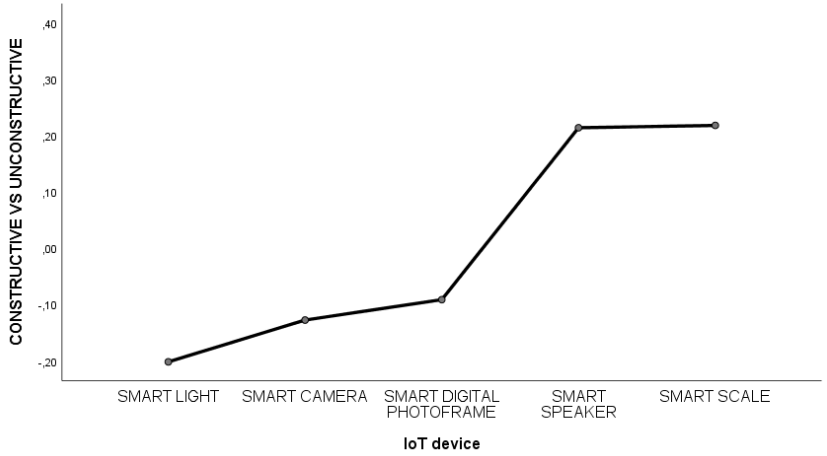

Figure 2. Estimated Marginal Means of the Emotional Reactions on The Second Dimension for IoT Devices.

A univariate ANOVA revealed that there was a statistically significant difference in the Cognitive-Motivational vs Affective dimension ($F(4, 501) = 5.55$, $p=.000$, $\eta^2= .04$). Tukey's HSD Test for multiple comparison indicated that the mean value of the Cognitive-Motivational vs Affective dimension was significantly different between the smart camera and the smart scale ($p=.001$, 95% C.I. = [.18, .90]), the smart camera and the smart light ($p=.008$, 95% C.I. = [.08, .80]), the smart camera and the smart digital photo frame ($p=.035$, 95% C.I. = [.02, .74]), the smart scale and the smart speaker ($p=.026$, 95% C.I. = [-.77, -.03]). Reactions to the cybersecurity breach scenario on the smart camera triggered more anticipated cognitive motivational reactions compared to more affective reactions on the smart scale, smart light, and smart digital photo frame. Also, reactions to cybersecurity breaches on the smart speaker triggered more anticipated cognitive motivational reactions compared to more affective reactions for the breach on the smart scale (Figure 3). There was no statistically significant difference between the other IoT devices ($p > .05$).

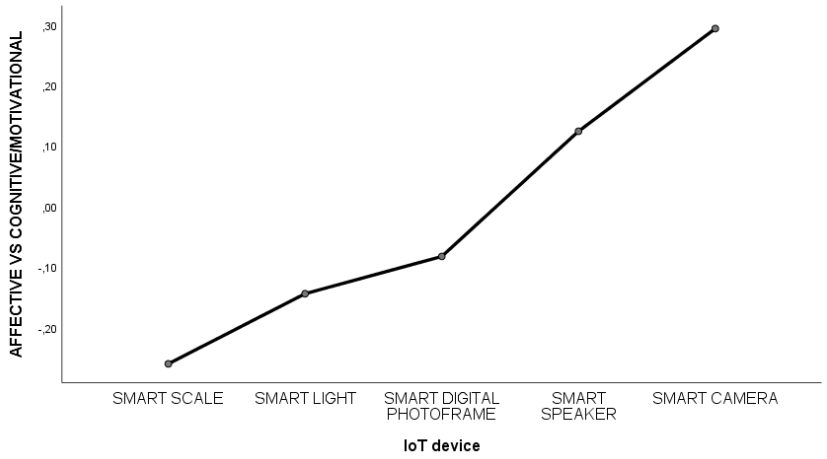

Figure 3. Estimated Marginal Means of the Emotional Reactions on the Third Dimension for IoT Devices.

By comparing how emotional reactions to cybersecurity breaches on domestic IoT devices differ, we found the largest effects of cybersecurity breaches on the smart security camera. One of the explanations could be that cybersecurity breaches on the smart security camera have the strongest expected negative effect on privacy. In an interview study conducted parallel to this one, participants specifically expressed concern about the camera recording them.[23]

3.2.3. Comparison Across Different Conditions/Intensities Across Five IoT Devices

A univariate ANOVA revealed that there was a statistically significant difference in the Emotional intensity dimension on the smart speaker (F (3, 99) = 4.17, p=.008, η^2= .11). Tukey's HSD Test for multiple comparison indicated that the mean value of the Emotional intensity dimension was significantly different between conditions 1a and 1b (p=.013, 95% C.I. = [-1.72, -.15]), and conditions 1a and 2a (p=.013, 95% C.I. = [-1.70, -.14]). Reactions to the cybersecurity breach scenario on condition 1b and 2a triggered a more anticipated intense emotional reaction compared to condition 1a (Figure 4). Conditions 1b and 2a were intended to be more intrusive and included starting a radio on low volume without instruction and a decrease in volume of the smart speaker, compared to condition 1a which informed the user that the radio is not available anymore. There was no statistically significant difference between the other conditions (p > .05).

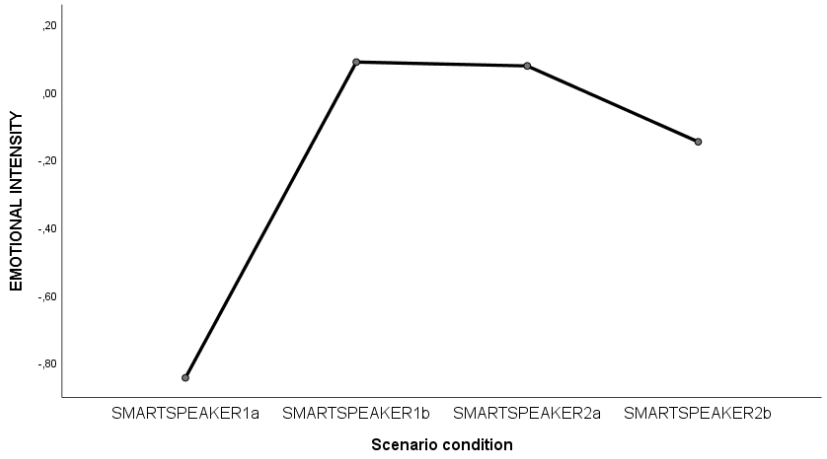

Figure 4. Estimated Marginal Means of the Emotional Reactions on The First Dimension for Different Conditions Within the Smart Speaker.

There were no differences between the different conditions for any of the IoT devices on the second dimension (p > .05).

A univariate ANOVA revealed that there was a statistically significant difference in the Cognitive-Motivational vs Affective dimension for the smart scale (F (2, 98) = 10.23, p=.000, η^2= .17). Tukey's HSD Test for multiple comparison indicated that the mean value of the Cognitive-Motivational vs Affective dimension was significantly different between conditions 1 and 2 (p=.007, 95% C.I. = [.16, 1.22]), and 1 and 3 (p=.000, 95% C.I. = [.48, 1.60]). Participants anticipated more cognitive motivational emotion reactions to the smart scale cybersecurity breach scenario in condition 1 (previous weight measurements deleted) vs the more affective reactions in conditions 2 (3 kg higher measures) and 3 (9 kg higher measures) (Figure 5). There was no statistically significant difference between the other conditions (p > .05).

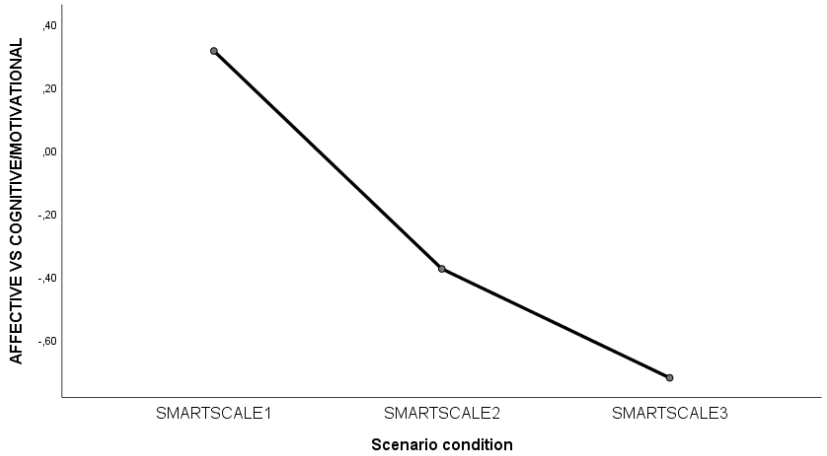

Figure 5. Estimated Marginal Means of the Emotional Reactions on The Third Dimension for Different Conditions Within the Smart Scale.

A univariate ANOVA revealed that there was a statistically significant difference in the Cognitive-Motivational vs Affective dimension for the smart speaker ($F(3, 99) = 5.35$, $p=.002$, $\eta^2= .14$). Tukey's HSD Test for multiple comparison indicated that the mean value of the Cognitive-Motivational vs Affective dimension was significantly different between conditions 1a and 1b ($p=.031$, 95% C.I. = [-1.31, -.04]), 1a and 2a ($p=.030$, 95% C.I. = [-1.30, -.05]), and 1a and 2b ($p=.001$, 95% C.I. = [-1.55, -.30]).

Reactions to the cybersecurity breach scenario on a smart speaker in condition 1a (radio becoming unavailable during use) triggered more anticipated affective reactions compared to the more cognitive motivational reactions in conditions 1b (starts playing the radio at low volume without instruction), 2a (decreases the radio volume), and 2b (turning the radio on without intention) (Figure 6). A possible reason could be that interruption of the radio use was perceived more as losing something (enjoyment of the radio) while the other conditions might not have been perceived as such. There was no statistically significant difference between the other conditions ($p > .05$).

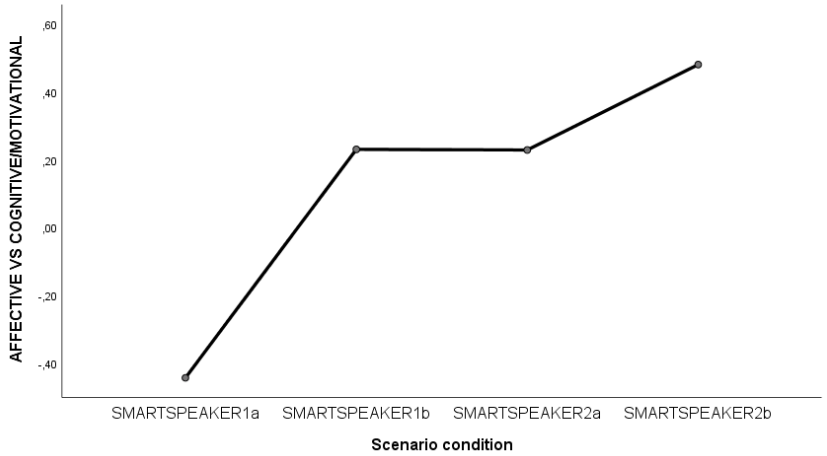

Figure 6. Schemes follow the same formatting Estimated Marginal Means of the Emotional Reactions on the Third Dimension for Different Conditions Within the Smart Speaker

To summarize, a comparison across different devices revealed that the most intensive emotional reactions (the highest scores on the first dimension) were found for cybersecurity breaches on the smart camera. The most unconstructive action tendencies were found for cybersecurity breaches on the smart scale and the smart speaker, while the most

constructive action tendencies were for breaches on the smart light. The most affective (as compared to cognitive) reaction was found for cybersecurity breaches on the smart scale, light, and digital photo frame while the most cognitive motivational reaction was found for the smart camera breach. We found different reactions to different levels of cybersecurity breaches for the smart speaker and the smart scale, which reflected different levels of intrusion (e.g., by duration, increase in measures, intensity of speaker volume, full overview of scenarios in Appendix A, Table A1). Differences for the smart speaker were found on the first dimension and third dimension. On the first dimension, 'emotional intensity', reactions were emotionally more intensive in conditions that were representing more intrusive breaches (without instruction decreasing the volume or turning on the radio). On third dimension, a more affective reaction was found for the least intrusive condition (turning off the radio), compared to more cognitive motivational reactions in more intrusive conditions (turning on the radio, decreasing the volume, playing without an instruction). Different conditions for a smart scale resulted in differences in scores on the third dimension, indicating more affective reactions (and less cognitive-motivational) for more intrusive conditions where a higher increase in the values was recorded on the smart scale (an increase of 3 or 9 kg compared to the actual weight measures).

4. Study 2

4.1. Materials and Methods

4.1.1. Participants

The field experiment took place in the Netherlands and United Kingdom with an initial aim to recruit 10 households per country.

The recruitment process included an initial screening of potential participants for psychopathological problems by using the Achenbach System of Empirically Based Assessment (ASEBA)[1]. Participants whose results were in the borderline or pathological range on the scales for internalizing and externalizing problems were excluded from participation in the experiment. The additional requirements for participation in the experiment were as follows: (i) all household members had to be above 18 years old and give informed consent for participation, (ii) they had to agree to collaborate during the 3 month period of the experiment by using the provided devices, participating in interviews, and filling in online questionnaires, (iii) they had to spend a substantial amount of time in the house and use the installed IoT devices, (iv) they could not have any pets in the household, and (v) could not have medical problems, which would require them to have a reliable weighing scale (as one of the IoT devices was a smart scale on which irregularities were introduced).

Due to difficulties in the recruitment phase of the experiment and to the premature withdrawal from the participation by a few households, a total of 16 households participated in the experiment. In the Netherlands, there were 9 households with 18 members (9 men and 9 women, M_{age}=54 years old), which consisted of students or employed people in their twenties (8 participants within age range from 23-26 years), employed and unemployed people (6 participants, within age range from 55-66 years), and retired people (6

[1] ASEBA

The Achenbach System of Empirically Based Assessment (ASEBA) [24] offers a comprehensive approach to assessing adaptive and maladaptive functioning. Developed through decades of research and practical experience to identify actual patterns of functioning, the ASEBA provides professionals with user-friendly tools. For screening the participants for the home experiment, we applied The Adult Self-Report for ages 18-59 (ASR 18-59) to obtain their perception of their adaptive functioning, substance use, and other problems. We analyzed the Syndrome Scale Scores, a scale used to measure internalizing problems (anxious/depressed, withdrawn, somatic complaints), thoughts problems, attention problems, and externalizing problems (aggressive behavior, rule-breaking behavior, intrusive).

participants, within age range from 68-75 years old). In the United Kingdom, there were a total of 7 households with 13 members (7 men and 6 women, M_{age}=40), which were mostly employed (12 participants, within the age range of 23-59) and one retired person in their seventies). At the end of the experiment, all participants were gifted with the installed devices (estimated worth of 1000 EUR for each household). Ethical approval for this study was provided by each of the participating universities of the authors of this paper.

4.1.2. Design

The smart IoT devices installed in each household included a smart security camera, a smart scale, smart speaker, smart light and smart socket with a plugged-in digital photo frame. These devices were targeted with a set of irregularities to simulate cybersecurity breaches. The list of irregularities on IoT devices that were included in the household field experiment is presented in Table A2 in the Appendix A. Irregularities were introduced at increasing levels of intensity and were executed remotely by the Research Team through computer scripts, automated pipelines, and a precise schedule. Using the participant's login credentials was intended to mimic a plausible real-life scenario in which the attacker had gained access to login credentials illegally. In addition to the 5 main IoT devices, participants were given a few more IoT gadgets (a motion sensor, a door-window sensor, two keychain presence sensors) and a tablet to use for running the apps of the devices and to access the online questionnaires through the links placed on the desktop screen.

The experiment was divided into four phases (0, 1, 2, and 3). The duration of each phase varied per household due to necessary adjustments to the schedule and the availability of the participants in their households. Phase 0 was the phase corresponding to the IoT devices installation in the household, phase 1 (duration between 13-59 days, M=35 days) was a phase of uninterrupted use of the installed devices, phase 2 (duration between 12-31 days, M=23 days) was a phase in which the research team remotely executed irregularities on the installed IoT devices unbeknown to the participants and in which we expected most of the emotional reactions because of the introduced irregularities, and phase 3 (duration between 5-13 days, M=12 days) included the execution of the same irregularities, but this time with the participant's knowledge. This knowledge consisted of participants being aware that deliberate irregularities on the IoT devices were introduced by the research team, but they were not informed about the nature, timing, and description of such irregularities.

4.1.3. Procedure

Before the beginning of the experiment, each participant received a list of the devices to be installed in the household with links to user agreements of the manufacturers of those devices. During the first meeting they were additionally briefed about the experiment, which included details about the devices and the participants' required collaboration in the interviews as well as in daily and weekly questionnaires. The signing of a consent form was followed by the first interview and the installation of all the planned IoT devices. Participants were provided with contact information of a member of the research team that they could use in case of encountering issues with the IoT devices and apps, which resulted in several visits to the households for logging in to apps for IoT devices. The research team kept the login code of the devices for the execution of the simulated attacks (via automation by means of IFTTT and Stringy). It also wanted to prevent participants from changing the passwords or installing additional apps on their phones.

During the experiment, participants had access to the link for an online questionnaire where they could report any positive or negative experience that they encountered with an IoT device, as well as estimate the valence, intensity, novelty, and dominance of the emotional experience triggered by irregularities in their IoT devices. Each dimension was estimated on a seven-point Likert scale. The research team analyzed the reported experiences in real-time on a weekly basis. Every week, the most intense negative emotional experience which was reported by each individual participant was chosen for a deeper

evaluation through the online Cybersecurity GRID questionnaire. The research team would send participants individualized emails repeating their own description of the reported experience and a link to the Cybersecurity GRID questionnaire (see Instrument), instructing them to report on their emotional experience in that specific instance. A reported experience would be considered relevant for the Cybersecurity GRID questionnaire based on the following two criteria: (i) The reported event was an irregularity introduced by the research team. This was checked by comparing the time of the event as reported by the participant against the time of execution of the irregularity by the research team. (ii) The reported event did not match an irregularity executed by the research team, but the chosen event was estimated as the most intensive weekly negative experience based on the emotional valence of the event.

4.1.4. Instrument

In Study 2, the Cybersecurity GRID questionnaire was also employed to assess five emotional components, along with emotion regulation, within the specific context of cybersecurity breaches[19,20]. It includes a total of 71 emotion features (16 appraisals, 14 action tendencies, 11 bodily reactions, 8 expressions, 14 subjective feelings and 8 emotion regulations). For the current study, two action tendency features were removed (AT15: 'I wanted to/would want to take revenge', AT16: 'I wanted to/would want to find and punish the attacker'), as they did not fit the setting of the field experiment in which participants were uninformed about, and thus very likely unaware of, the cybersecurity breaches until phase 3.

4.2. Results

4.2.1. Underlying Structure of the Inter-Individual Differences in Emotion Processes in the Situation of Cybersecurity Breaches of IoT Devices in the Household

For the analyses, we integrated phase 0 (8 reports) and phase 1 (14 reports) and analyzed them as one phase (total of 22 reports) as there was no introduction of any irregularities in these first two phases. In phase 2 irregularities were introduced without informing the participants (144 reports, out of which 7 were reports of the irregularities introduced by a team), while in phase 3 the participants were made aware of possible irregularities (73 reports, out of which 16 were reports of the irregularities introduced by a team). In total we analyzed 239 reports (out of which 23 were reports of the irregularities introduced by a team. Thus, only 9.6% of reports deal with actual irregularities introduced by the research.

Principal Component Analysis was applied to the emotion features from the Cybersecurity GRID questionnaire, which represented reactions to the reported negative experiences with domestic IoT devices and simulated cybersecurity breaches in the field experiment. Based on the Scree Plot (Appendix A, Figure S3), we identified not three, but four dimensions. Then, we applied Orthogonal Procrustes rotation towards the three-dimensional structure as identified in Study 1. A very good congruence was found for the first dimension, while for the second and third dimensions the congruence coefficient fell just below the criteria cut-off point of .85 for a fair congruence (proportionality coefficient per factor, Tucker's phi: .97,.83, .83)[2]. The first dimension pointed to a replication of previous findings of cybersecurity breach of Study 1 and previous studies [19,20]. While not identical, there was a quite substantial overlap for the second and the third dimension. Given the fact that just the small sample size in the field experiment could reasonably account for the small deviations from the structure of Study 1, we adopted the same

[2] We also did an analysis for internal structure for the participants' reports only in the second phase and those who make sufficient discrimination for their answers (who made the same score in maximally 70% of cases). The structure of only the second phase was very comparable with the structure across all episodes in all phases (proportionality coefficient per factor, Tucker's phi: .97, .89, .92)

interpretation of the second and a third dimension as in the previous studies (see Table 3 for the ten highest loading features per dimension, see in Appendix A Table A4 for a full loading matrix and for the loadings for second and third dimension are plotted in the Figure A4).

The first dimension was comparable to those in previous studies, with all features loading positively and reflecting a general tendency to react emotionally to an irregularity. The emotion features for subjective experiences and bodily reactions (e.g., ″I was shaking″, ″I had goosebumps″) had the highest loading, which indicates more intensive negative emotion processes elicited by the irregularities of IoT devices. This factor is labelled emotional intensity.

On the second dimension positive loadings concerned unconstructive reactions in the form of distressing bodily reactions (e.g., ″I had a pain in the chest″, ″I sweated″), while negative loadings reflected constructive reactions (e.g., "I wanted to regain control over the device/account", "I wanted to find a solution and fix the problem").

The third dimension was not completely replicated but showed a clear tendency of differentiating appraisals and action tendencies on one side and an affective part with subjective feelings, bodily reactions, and expressions on the other side. The highest positive loadings included appraisal emotion features (e.g., I thought "It is not safe that this device is connected to the Internet, I thought "Someone could destroy my data.") and are interpreted as the cognitive-motivational pole of dimension. The opposite pole of this dimension was represented by negative loadings on subjective feelings and bodily reactions features (e.g., ″I felt frustrated″, ″My heartbeat was faster″) and is described as the affective pole of the dimension.

The fourth dimension was bipolar with mostly negative loadings on items representing distress symptoms (″I felt worried″, ″I felt uncomfortable″). With only two positive loadings which are equal or higher than .30 (″I wanted to/would want to reset my device″. ″I wanted to/would want to swear and curse. ″) the other pole of the fourth dimension was not well defined. This dimension is labeled distress symptoms.

Table 3. Results From Principal Component Analysis of the Cybersecurity GRID Questionnaire from Study 2 After Orthogonal Procrustes Rotation

Emotion Feature Items	**Dimension Loading**			
	D1	**D2**	**D3**	**D4**
Emotional Intensity				
BR3 I was/would be shaking.	.76	.55	.06	.08
BR9 I had/would have goosebumps.	.76	.54	-.02	.10
BR2 I was/would be dizzy.	.74	.54	.09	.11
SF2 I experienced/ I would experience the emotional state for a long time.	.74	.39	-.17	.02
SF4 I felt/ I would feel afraid.	.74	.39	-.10	-.11
AT5 I wanted to/would want to isolate myself physically.	.73	.45	.07	.03
BR4 I had/would have pain in the chest.	.73	.57	.04	.11
BR5 I sweated/would sweat (whole body).	.73	.57	.04	.11
BR11 My body became/would become hot (puff of heat. cheeks or chest).	.73	.49	-.10	.11
E4 I had/would have a trembling voice.	.73	.49	-.07	.05
Constructive				

AT2 I wanted to/would want to regain control over the device/account.	.34	-.56	-.08	.04
AT9 I wanted to/would want to find a solution and fix the problem.	.44	-.55	-.18	.04
A2 I thought/ I would think "I wonder whether something is wrong with the device/account."	.40	-.54	.03	.17
A18 I thought/ I would think "Similar situations might happen again in the future."	.39	-.45	-.08	.00
AT10 I wanted to/would want to report the situation (e.g. to the police or to the internet provider).	.41	-.44	.19	-.14
Unconstructive				
BR4 I had/would have pain in the chest.	.73	.57	.04	.11
BR5 I sweated/would sweat (whole body).	.73	.57	.04	.11
BR3 I was/would be shaking.	.76	.55	.06	.08
BR2 I was/would be dizzy.	.74	.54	.09	.11
BR10 I had/would have a dry mouth.	.71	.54	-.03	.08
Cognitive motivational				
A19 I thought/ I would think "It is not safe that this device is connected to the Internet."	.47	.02	.47	-.12
A16 I thought/ I would think "Someone could destroy my data."	.69	.37	.39	.10
A15 I thought/ I would think "Someone may have access to my private information."	.57	.23	.38	-.13
A17 I thought/ I would think "Someone could use my data to harm me."	.66	.39	.38	.05
A8 I thought/ I would think "My security could be jeopardized."	.64	.26	.34	.14
Affective				
SF12 I felt/ I would feel frustrated.	.49	-.34	-.46	.15
SF11 I felt/ I would feel angry.	.57	-.13	-.43	.07
SF6 I felt/ I would feel upset.	.63	.03	-.42	.06
E1 I frowned/would frown.	.33	-.29	-.37	-.02
BR6 My heartbeat was/would be faster.	.58	.23	-.35	.30
Distress symptoms				
SF7 I felt/ I would feel worried.	.57	.01	-.15	-.55
SF14 I felt/ I would feel uncomfortable.	.57	-.08	-.14	-.53
BR1 I had/would have stomach discomfort.	.58	.07	-.15	-.52
SF10 I felt/ I would feel ashamed.	.48	.24	-.30	-.48
SF3 I felt/ I would feel anxious.	.60	-.02	-.24	-.48
Oppositional tendencies				
AT11 I wanted to/would want to reset my device.	.59	-.29	.04	.39
AT13 I wanted to/would want to swear and curse.	.58	.00	-.25	.30

To summarize, the first dimension was comparable to the previously found structure, and in this study also reflected emotional intensity. Small deviations for the second (constructive vs unconstructive action tendencies) and third dimension (affective vs cognitive motivational) are most likely to be accounted for by the small sample size of the field study. However, it could also be explained by differences in the conditions that people underwent. In the field study, participants were less likely to interpret the irregularities as an intentional activity of somebody else or a cybersecurity breach than in the scenario study. This could be attributed to the fact that in the scenario study the scenario descriptions indicated that they do not have control of the IoT devices. Therefore, participants were more likely to attribute the irregularities to intentional activity of a third party. Future research can explore if there are subtle differences in the meaning of these factors or whether these differences are random deviations because of the small sample.

4.2.2. Differences on the Dimensions across the Three Phases of the Field Experiment

Separate univariate ANOVA's were performed to compare the effect of the different field experimental phases on the three identified emotion dimensions. As the number of reports varied between different household members, we included the participants as a random factor in the design.

A univariate ANOVA revealed that there was a statistically significant difference in the Emotional intensity dimension ($F(2, 204) = 16.02$, $p=.000$, $\eta^2= .14$). Tukey's HSD Test for multiple comparison indicated that the mean value of the Emotional intensity dimension was significantly different between phases 1 and 2 ($p=.025$, 95% C.I. = [.04, .73]), and phases 1 and 3 ($p=.000$, 95% C.I. = [.48, 1.22]), and between phases 2 and 3 ($p=.000$, 95% C.I. = [.25, .68]). Reactions to the irregularities of IoT devices were most intense at the beginning of the field experiment, lower in the second phase, and the lowest in the third phase (Figure 7).

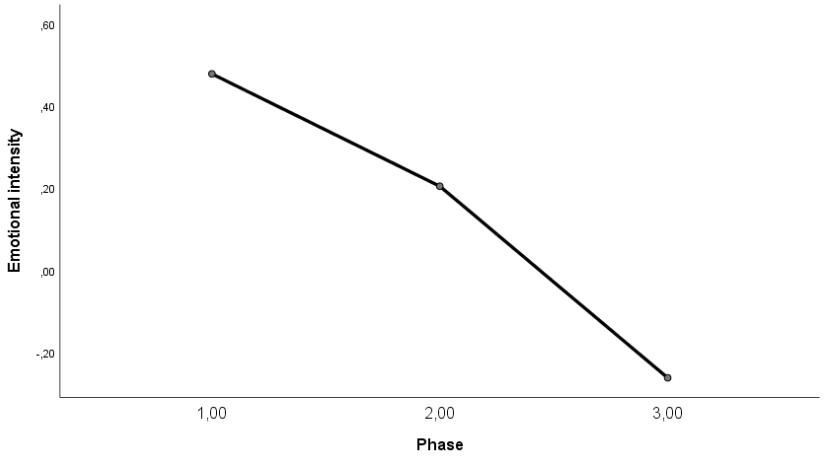

Figure 7. Schemes follow the same formatting Estimated Marginal Means of the Emotional Reactions on the First Dimension for Different Phases of the Household Experiment.

A univariate ANOVA revealed that there was a statistically significant difference in the Constructive vs Unconstructive dimension ($F(2, 204) = 26.78$, $p=.000$, $\eta^2= .21$). Tukey's HSD Test for multiple comparison indicated that the mean value of Constructive vs unconstructive dimension was significantly different between phases 1 and 2 ($p=.001$, 95% C.I. = [-.94, -.22]), between phases 1 and 3 ($p=.000$, 95% C.I. = [-1.5, -.73]), and between phases 2 and 3 ($p=.000$, 95% C.I. = [-.76, -.31]).

The emotional reactions reported in phase 1 were the most constructive and became less constructive in phase 2 and phase 3 (see Figure 8).

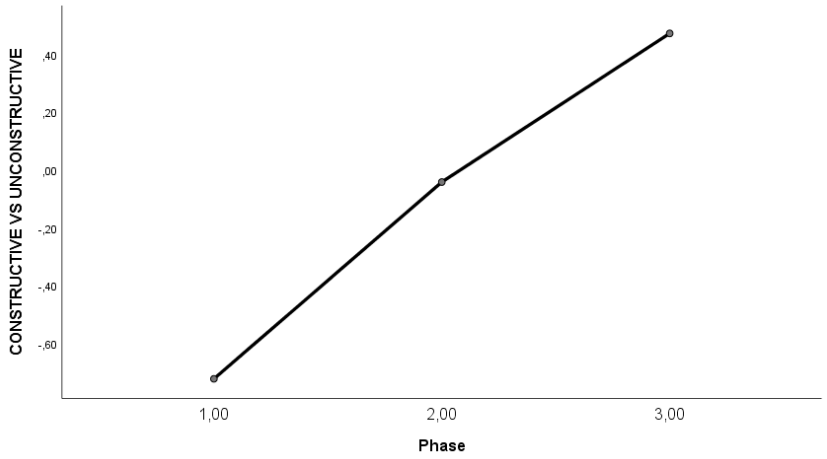

Figure 8. Mean Emotional Reactions on the Second Dimension for Different Phases of the Household Experiment.

A univariate ANOVA revealed that there was a statistically significant difference in the Cognitive-Motivational vs Affective dimension (F (2, 204) = 7.57, p=.001, η^2= .07). Tukey's HSD Test for multiple comparison indicated that the mean value of Cognitive-Motivational vs Affective dimension was significantly different between phase 2 and phase 3 (p=.001, 95% C.I. = [-.70, -.15]). Reactions to the reported irregularities of IoT devices triggered more affective reactions in phase 2 (in which they were not aware of possible cybersecurity breaches on their IoT devices) and more cognitive motivational reactions in phase 3 (in which they were aware of the possibility of breaches) (Figure 9). There was no statistically significant difference between other phases (p > .05).

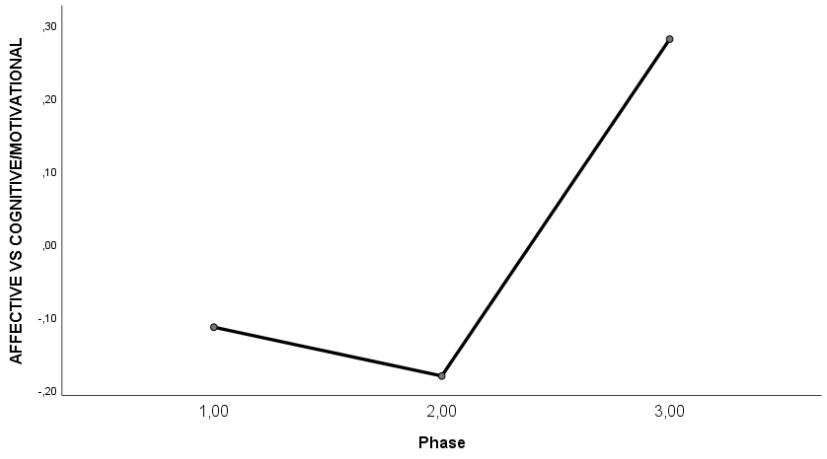

Figure 9. Estimated Marginal Means of the Emotional Reactions on the Third Dimension for Different Phases of the Household Experiment.

There were no significant differences in the fourth dimension (Distress Symptoms vs Oppositional Tendencies) between different phases or between different IoT devices.

Additionally, we analyzed variation in the dimensions for the different devices but found no statistically significant differences (see statistical tests in the Appendix B). For this analysis we included only participants' reports from the second phase of the field experiment as in this phase participants were exposed to simulated irregularities on the IoT devices installed in their house. Initially, we introduced a balanced design, comparable to the ones in Study 1. However, the number of reported irregularities between

different devices varied and was unevenly distributed (from 8 reports for smart camera to 40 for the smart speaker). The reasons for this uneven distribution are partially that the participants were often not aware of the simulated cybersecurity attacks and therefore did not report them. Instead, they reported on other negative experiences they had with the devices. While still interesting, this created an obstacle for the comparison of experiences between the different devices, as was done in the scenario study.

In the field experiment the most emotionally intensive reports were found at the beginning of the experiment, and emotional intensity decreased systematically during the experiment, with the lowest scores on the emotional intensity dimension observed at the end of experiment, in the third phase.

The fact that the participants reported more unconstructive and more cognitive reactions during the third phase could be attributed to the fact that they were informed of possible cybersecurity breaches in this phase. This might have introduced less need to intervene (represented by less constructive action tendencies on the second dimension) and an attempt to cognitively understand what was happening (represented by the more cognitive reactions on the third dimension).

To summarize, in phase 1 there were more intense emotional processes, as well as more constructive and more affective reactions to experienced issues with domestic IoT devices. In phase 2, there were less intense emotional processes, less constructive and as many affective reactions. In phase 3, the intensity of the reactions went further down, and the emotional reactions became less constructive, but they became more cognitive in nature.

5. Discussion

This is the first time that a scenario study (Study 1) was complemented by a real-life field experiment (Study 2) for studying behavior and emotional reactions to cybersecurity breach situations of IoT devices.

For the broad range of situations presented in both studies—scenarios of cybersecurity breaches and a simulation of the same scenarios in the household field experiment—we found that the elicited experiences were clearly emotional, with individual differences in the reported responses. These emotional aspects confirm the need to explore the psychological perspective of cybersecurity breaches.

The findings indicate that emotional responses vary significantly based on the type of device involved, aligning with previous research that suggests emotions can be pivotal in shaping user behavior and attitudes toward IoT security. These insights emphasize the need for further research into tailored security measures for different IoT devices and highlight the importance of designing user-friendly security solutions that account for emotional reactions.

Application of the Component Process Model [15] and the GRID framework [25],going beyond using only emotion terms, allowed us to detect and explore aspects of emotion processes which would not have been identified by using standard approaches. The emotion perspective is relevant in cybersecurity breach situations, as all the emotion components representing the whole emotion process (appraisals, action tendencies, bodily reactions, expressions, subjective feelings) plus emotion regulation vary systematically across persons, devices, field experiment phases, and scenarios. We found a replicable structure of these emotion processes in both studies, which allows a description of the individual differences through the emotion lens as well as studying of the behavior in different cybersecurity breach situations. In both studies we found a comparable three-dimensional structure for the emotion features, which by and large confirms emotion structures that were found in recent studies on cybersecurity breaches using the Component Process Model (Budimir et al., 2020, 2021) . The three-dimensional structure consists of a general intensity dimension, a constructive vs unconstructive reaction dimension, and an affective vs cognitive-motivational dimension.

When looking at the quantitative differences on the identified emotion dimensions, the main finding of the first scenario study is that an anticipated cybersecurity breach of a security camera evokes significantly more intense emotions than cybersecurity breaches of other IoT devices. While cybersecurity breaches on all IoT devices have both an impact in cyberspace and a direct physical impact (e.g., unauthorized activation of lights), the security camera has the greatest potential to affect our privacy.

This could explain why people had the strongest reactions to the security camera scenarios. The key finding from the second study, a household field experiment, is that people appear to have difficulty detecting subtle irregularities that may indicate cybersecurity breaches. During the second phase all households have been frequently confronted with mild irregularities. Despite this objective exposure, less than 10% of the reported emotional experiences were due to these experimentally introduced irregularities. Moreover, we observe that the intensity of the emotional reactions as well as the tendencies to react constructively systematically decrease across the three phases. The expected increase in the second phase, when participants were exposed to a variety of irregularities, was thus not observed. One of the reasons for these unexpected results in the field experiment, is the failure to notice and to interpret the irregularities in the functioning of IoT devices installed at their home as a threat for cybersecurity breach (which was also apparent from the qualitative interviews) [23]. Participants had no expectations of any form of cybersecurity breaches in the first two phases of the experiment. They were only informed about the likelihood of cybersecurity breaches caused by the research team in the third phase of the experiment. Even then the participants did not consistently identify the nature of the breaches, or which devices were targeted by the simulated breaches. An explanation could be that the breaches were not intense enough to be noticed. However, the low noticeability of cybersecurity breaches on IoT devices is a realistic scenario in everyday life, as most breaches are not intended to be noticed (unless the attacker aims to intimidate the victim).

In general, it can be concluded that IoT devices and connected systems can be breached without users noticing and knowing it, which poses a major threat to them. Individuals intending to carry out cybersecurity breaches can easily execute minor interventions that go unnoticed by users, enabling them to gain control of the entire system and inflict harm on a larger scale. Our results indicate that we are not emotionally equipped to identify small forms of dysfunction in IoT devices. Evolutionarily, emotions have been developed to make us aware of the presence of positive or negative goal relevant events happening in the environment in order to react to them in an adaptive way (e.g., [26]). There is thus a strong need to increase awareness of threats in the cyber world so that we can take appropriate actions to avoid damaging consequences.

Grounded in the Component Process Model (CPM) of emotion, our analysis enhances the understanding of how users emotionally respond to cybersecurity threats, particularly during breaches. The CPM integrates cognitive, physiological, and behavioral aspects of emotions, providing a comprehensive view of user reactions. By recognizing that emotions change over time, we can better assess how user perceptions shift in response to emerging threats. Overall, studying emotions in the context of cybersecurity breaches is crucial for understanding user vulnerabilities and developing strategies that encourage emotional resilience, ultimately leading to a more secure environment for IoT users.

The results of this study point to significant practical implications for the field of cybersecurity, particularly when it comes to IoT devices used in domestic settings. A key takeaway is the need to improve users' ability to recognize subtle cybersecurity threats. Often, minor irregularities in IoT devices go unnoticed by users, yet these could indicate the early stages of a cyberattack. Enhancing awareness and preparedness in handling such risks is therefore crucial. In addition, manufacturers should prioritize reinforcing the security features of these devices, not only to prevent potential breaches, but also to reduce the psychological impact on users when such incidents occur.

Addressing both the technical and emotional vulnerabilities highlighted in this study, allows a more user-centered approach to cybersecurity to be developed, which helps reduce the wide-ranging risks posed by cyberattacks. By following the ISO 27000 guidelines, manufacturers can improve the security of IoT devices, reducing the chances of unauthorized access and helping to ease users' concerns. These measures are crucial for maintaining trust in IoT systems, especially in homes, where security breaches can cause emotional and psychological harm. The findings from both studies highlight the emotional dimensions of cybersecurity breaches, such as intensity, constructive versus unconstructive reactions, and the interplay between affective and cognitive-motivational components. These insights can directly influence IoT security protocols by guiding the development of security measures that align with users' emotional responses. This approach enables the creation of more sensitive and adaptable features, such as real-time alerts that match users' emotional states, user-friendly interfaces that reduce panic and confusion during a breach, and proactive educational programs that build emotional resilience. By addressing these dimensions, security protocols can enhance user awareness, facilitate timely detection of threats, and improve overall security compliance, thereby reducing the psychological impact of cybersecurity breaches.

In conclusion, our study contributes valuable insights into the psychological implications of cybersecurity breaches. Based on a comprehensive study of the emotion processes using the Component Process Model, we suggest that developers and policymakers should prioritize user education and awareness programs regarding IoT device security. This could mitigate psychological distress following privacy breaches and enhance overall user confidence.

6. Limitations and Future Perspectives

The studies presented in this paper, including both the scenario-based study (Study 1) and the field experiment with simulated cybersecurity breaches (Study 2), encountered several challenges and limitations. Study 1 was designed to explore participants' emotional responses to hypothetical scenarios involving clear cybersecurity breaches. This controlled approach allowed us to introduce breaches in a clear and straightforward manner, offering insights into emotional reactions that may be difficult to capture in real-time situations. The use of simulated scenarios is grounded in behavioral research [27–29], which indicates that participants can provide accurate emotional responses in controlled environments. These simulations are designed to replicate real-world situations, thereby offering valid insights into user experiences. However, the hypothetical nature of these scenarios means there may have been a gap between how participants imagined they would feel and how they would react in a live situation.

In contrast, Study 2 was designed to simulate real-world cybersecurity breaches in a field setting, capturing participants' emotional reactions in a more realistic environment. One major limitation of Study 2 was that the intensity and consequences of the breaches were intentionally kept at a relatively low level for ethical reasons. While these low-intensity breaches often went undetected by participants, they reflect real-world situations where attackers aim to keep breaches concealed. Noticeability played a key role in the differences between the two studies: Study 1, where irregularities clearly indicated cybersecurity breaches, elicited stronger emotional responses, whereas Study 2, where most simulated breaches went unnoticed, resulted in more subdued emotional reactions. This aspect of noticeability is critical for understanding the emotional processing differences between hypothetical and real-world breach scenarios. Future research should address the limitations by exploring a wider range of breach intensities, using more diverse samples, and comparing both hypothetical and real-world scenarios to better understand the gap between perceived and actual emotional responses.

Sampling formed another limitation of this study. Partly different types of samples were used in Study 1 and Study 2. While Study 1, which used hypothetical scenarios, only included a UK sample, Study 2 was conducted in both the Netherlands and the UK.

Including samples from different countries enhances the robustness and generalizability of our findings, but the differences in the populations of the two studies complicate direct comparisons, as any observed differences may result from sample variation rather than the nature of the task itself.

Our findings emphasize the need to raise awareness about the threat that cybersecurity breaches pose to household privacy. Breaches may occur more frequently than people realize. Increasing awareness can help users recognize the signs of potential breaches. In addition to raising awareness, it is crucial to educate users on how to protect their IoT devices and respond effectively when attacks occur. Offering psychological support for those affected by cybersecurity breaches is also important, as these incidents can have significant emotional impacts, potentially leading to long-term psychological difficulties, similar to what is seen in cases of physical breaches, like burglary [30,31]. The findings of this study not only advance theoretical understanding of user emotional responses in cybersecurity contexts, but also provide actionable insights for manufacturers and policymakers. Enhanced device security measures and user education initiatives are essential to address the psychological impacts of breaches. Regulators should focus on enforcing stricter security standards for IoT devices, particularly in terms of transparency and accountability. For example, manufacturers should be required to disclose potential vulnerabilities and provide timely security updates. Regulators should also encourage consumer education programs that help users identify and respond to early signs of a breach.

From a risk management perspective, organizations and users should implement strategies that encompass both technical safeguards and psychological support. Understanding the emotional impact of cybersecurity breaches enables companies to create comprehensive risk management approaches that mitigate not only technical vulnerabilities, but also the emotional and psychological stress these incidents cause. Addressing both aspects fosters a more user-centered approach to cybersecurity, reducing the broad range of risks associated with cyberattacks. Following ISO 27000 guidelines can help manufacturers enhance the security of IoT devices, decreasing the likelihood of unauthorized access and alleviating users' concerns. These measures are essential for maintaining trust in IoT systems, particularly in homes where security breaches can lead to significant emotional and psychological harm.

Author Contributions: Conceptualization, S.B., J.R.J.F., N.M.A.H., A.H., G.L., and E.B.R.; methodology, S.B., J.R.J.F., N.M.A.H., A.H., and E.B.R.; software, F.S., R.H., A.B., A.F., I.R., and E.B.R.; validation, E.B.R.; formal analysis, S.B.; investigation, S.B., J.R.J.F., N.M.A.H., A.H., W.A.I., A.M.O., G.L., F.S., R.H., A.B., A.F., I.R., and E.B.R.; resources, S.B., J.R.J.F., N.M.A.H., A.H., A.M.O., G.L., F.S., R.H., A.B., A.F., I.R., and E.B.R.; data curation, S.B., J.R.J.F., N.M.A.H., A.H., G.L., F.S., R.H., A.B., A.F., I.R., and E.B.R.; writing—original draft preparation, S.B., J.R.J.F., G.L., and E.B.R.; writing—review and editing, N.M.A.H., A.H., A.M.O., F.S., G.L., and E.B.R.; supervision, J.R.J.F., A.H., G.L., and E.B.R.; project administration, S.B., J.R.J.F., N.M.A.H., A.H., G.L., and E.B.R.; funding acquisition, J.R.J.F., A.H., and E.B.R.

Funding: This research was funded by EU FP7 CHIST-ERA funding scheme (European Coordinated Research on Long-term Challenges in Information and Communication Sciences & Technologies ERA-NET, corresponding to grant: FWO project G0H6416N (FWOOPR2016009701) and NWO project 651.002.002).

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and approved by the Ethical committees of all involved partners for this research project (Ghent University, University of Reading, Eindhoven University of Technology and University of Greenwich).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: In this section, you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A Detailed Scenarios and Emotional Response Measures for Study 1

Appendix B Statistical Analysis of Device-Specific Emotional Responses in Study 2

References

1. IoTAnalytics Connected IoT Device Market Update—Summer 2024 Available online: https://iot-analytics.com/number-connected-iot-devices/.
2. Statista Number of Internet of Things (IoT) Connections Worldwide from 2022 to 2023, with Forecasts from 2024 to 2033 Available online: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.
3. ISO 25000, Software and Data Quality Available online: https://iso25000.com/index.php/en/iso-25000-standards/iso-25010.
4. Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — Product Quality Model.
5. ISO/IEC 27000 Family Information Security Management Available online: https://www.iso.org/standard/iso-iec-27000-family.
6. Vardakis, G.; Hatzivasilis, G.; Koutsaki, E.; Papadakis, N. Review of Smart-Home Security Using the Internet of Things. *Electronics* **2024**, *13*, 3343, doi:10.3390/electronics13163343.
7. Marton, A. IoT Malware Attacks up by 37% in the First Half of 2023 Available online: https://iotac.eu/iot-malware-attacks-up-by-37-in-the-first-half-of-2023/.
8. Kaspersky Unveils an Overview of IoT-Related Threats in 2023 Available online: https://www.kaspersky.com/about/press-releases/kaspersky-unveils-an-overview-of-iot-related-threats-in-2023.
9. Heartfield, R.; Loukas, G.; Budimir, S.; Bezemskij, A.; Fontaine, J.R.J.; Filippoupolitis, A.; Roesch, E. A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home. *Comput. Secur.* **2018**, *78*, 398–428, doi:10.1016/j.cose.2018.07.011.
10. Bitdefender THE 2023 IOT SECURITY LANDSCAPE REPORT 2023.
11. Loukas, G. *Cyber-Physical Attacks: A Growing Invisible Threat*; Butterworth-Heinemann, 2015; ISBN 978-0-12-801463-9.
12. Parsons, E.K.; Panaousis, E.; Loukas, G.; Sakellari, G. A Survey on Cyber Risk Management for the Internet of Things. *Appl. Sci.* **2023**, *13*, 9032, doi:10.3390/app13159032.
13. Baraniuk, C. Ashley Madison:'Suicides' over Website Hack. Available online: https://www.bbc.com/news/technology-34044506 (accessed on 10 December 2019).
14. Watson, D.; Clark, L.A.; Tellegen, A. Development and Validation of Brief Measures of Positive and Negative Affect: The PANAS Scales. **1988**, 8.
15. Scherer, K.R. Appraisal Considered as a Process of Multilevel Sequential Checking. In *Appraisal processes in emotion: Theory, methods, research*; Series in affective science; Oxford University Press: New York, NY, US, 2001; pp. 92–120 ISBN 978-0-19-513007-2.
16. Gross, M.L.; Canetti, D.; Vashdi, D.R. Cyberterrorism: Its Effects on Psychological Well-Being, Public Confidence and Political Attitudes. *J. Cybersecurity* **2017**, doi:10.1093/cybsec/tyw018.
17. Gross, M.L.; Canetti, D.; Vashdi, D.R. The Psychological Effects of Cyber Terrorism. *Bull. At. Sci.* **2016**, *72*, 284–291, doi:10.1080/00963402.2016.1216502.
18. Kopecký, K.; Szotkowski, R. Cyberbullying, Cyber Aggression and Their Impact on the Victim – The Teacher. *Telemat. Inform.* **2017**, *34*, 506–517, doi:10.1016/j.tele.2016.08.014.

19. Budimir, S.; Fontaine, J.R.J.; Huijts, N.M.A.; Haans, A.; Loukas, G.; Roesch, E.B. *Emotional Reactions on Cybersecurity Breach Situations: A Scenario-Based Survey Study (Preprint)*; Journal of Medical Internet Research, 2020;
20. Budimir, S.; Fontaine, J.R.J.; Roesch, E.B. Emotional Experiences of Cybersecurity Breach Victims. *Cyberpsychology Behav. Soc. Netw.* **2021**, *24*, 612–616, doi:10.1089/cyber.2020.0525.
21. Budimir, S.; Fontaine, J.R.J.; Huijts, N.M.A.; Haans, A.; Loukas, G.; Roesch, E.B. Emotional Reactions to Cybersecurity Breach Situations: Scenario-Based Survey Study. *J. Med. Internet Res.* **2021**, *23*, e24879, doi:10.2196/24879.
22. Qualtrics, P.U. Qualtrics 2019.
23. Huijts, N.M.A.; Haans, A.; Budimir, S.; Fontaine, J.R.J.; Loukas, G.; Bezemskij, A.; Oostveen, A.; Filippoupolitis, A.; Ras, I.; IJsselsteijn, W.A.; et al. User Experiences with Simulated Cyber-Physical Attacks on Smart Home IoT. *Pers. Ubiquitous Comput.* **2023**, doi:10.1007/s00779-023-01774-5.
24. Achenbach, T.M. *The Achenbach System of Empirically Based Assessemnt (ASEBA): Development, Findings, Theory, and Applications.*; Burlington, VT: University of Vermont Research Center for Children, Youth, & Families, 1966;
25. *Components of Emotional Meaning: A Sourcebook*; Fontaine, J.R.J., Scherer, K.R., Soriano, C., Eds.; Oxford University Press, 2013; ISBN 978-0-19-959274-6.
26. Frijda, N.H. *The Emotions*; Cambridge University Press, 1986; ISBN 978-0-521-31600-2.
27. Riquelme, H.E.; Alqallaf, A. Anticipated Emotions and Their Effects on Risk and Opportunity Evaluations. *J. Int. Entrep.* **2020**, *18*, 312–335, doi:10.1007/s10843-019-00262-3.
28. Kaplan, S.; Winslow, C.; Craig, L.; Lei, X.; Wong, C.; Bradley-Geist, J.; Biskup, M.; Ruark, G. "Worse than I Anticipated" or "This Isn't so Bad"?: The Impact of Affective Forecasting Accuracy on Self-Reported Task Performance. *PLOS ONE* **2020**, *15*, e0235973, doi:10.1371/journal.pone.0235973.
29. Kutt, K.; Nalepa, G.J. Emotion Prediction in Real-Life Scenarios: On the Way to the BIRAFFE3 Dataset. In *Artificial Intelligence for Neuroscience and Emotional Systems*; Ferrández Vicente, J.M., Val Calvo, M., Adeli, H., Eds.; Lecture Notes in Computer Science; Springer Nature Switzerland: Cham, 2024; Vol. 14674, pp. 465–475 ISBN 978-3-031-61139-1.
30. Beaton, A.; Cook, M.; Kavanagh, M.; Herrington, C. The Psychological Impact of Burglary. *Psychol. Crime Law* **2000**, *6*, 33–43, doi:10.1080/10683160008410830.
31. Chung, M.C.; Stedmon, J.; Hall, R.; Marks, Z.; Thornhill, K.; Mehrshahi, R. Posttraumatic Stress Reactions Following Burglary: The Role of Coping and Personality. *Traumatol. Int. J.* **2014**, *20*, 65–74, doi:10.1037/h0099374.