Victim's negative emotion processes in cybersecurity breach situations: a testimony of anger and fear related emotion processes

Sanja Budimir [1], Johnny R.J. Fontaine [1], Antal Haans[2], Nicole M.A. Huijts [2,3], George Loukas [4] and Etienne B. Roesch [,5,6]

[1]Department of Work, Organization and Society, Faculty of Psychology and Educational sciences, Ghent University, Gent, Belgium

[2]Department of Industrial Engineering & Innovation Sciences, Eindhoven University of Technology, the Netherlands

[3]Psychology of Conflict, Risk and Safety, University of Twente, Enschede, the Netherlands

[4]Internet of Things and Security Centre, University of Greenwich, Greenwich, United Kingdom

[5]Centre for Integrative Neuroscience and Neurodynamics, University of Reading, Reading, United Kingdom

[6]School of Psychology and Clinical Language Sciences, University of Reading, Reading, United Kingdom

Abstract

The numerous benefits of increased internet connection are accompanied by a growing number of cybersecurity breaches. The successful protection of users' wellbeing and their security, premised on preventative training and effective care of victims, requires an understanding of their experiences. To map this landscape, we explored a spectrum of emotional experiences in cyber security breach situations from the victim's perspective. Participants (N=130) were asked to describe a cybersecurity breach on an Internet of Things device, computer, smartphone, email, or social network account they experienced themselves or heard about from friends or the media. They were asked to report their personal or anticipated emotional experiences in that situation, based on Scherer's Components Process Model (Scherer, 2001) of emotions and emotion regulation. Answers were qualitatively analyzed by coding them into categories of emotion processes components within the GRID framework (Fontaine et al., 2013) and for emotion regulation within the Conceptual Integration Model (Connor-Smith & Flachsbart, 2007). The most frequently reported emotion processes in cybersecurity breach situations include: (i) the appraisals privacy intrusion, unknown and no control, (ii) the action tendencies intervention, defensive and attack, (iii) the expressions high vocal energy, abrupt movement, eyes closed/tears, (iv) the bodily responses high autonomic arousal, distress, high temperature, (v) the subjective feelings fear, anger and anxiety and (vi) the emotion regulations instrumental support, relaxation and suppression. This profile of reactions is similar to the emotional experiences of victims of physical security breaches (e.g. burglary), but with specific characteristics of uncertainty, unknown consequences and absence of punishment.

Keywords: Cybersecurity breach victims; Emotion processes; Componential emotion model

Introduction

The internet eased many aspects of life, facilitating the global availability, sharing and trading of information and products. Unfortunately, it also gave rise to new forms of crime, namely cyber-crime. An understanding of the risks and consequences of cyber-crime from the victim's perspective is absent from the literature, but is very much needed to improve security, resilience and wellbeing of victims.

Indeed, as we grow more dependent on technology, devices connect in tighter meshes, from computers and smart phones to Internet of Things (IoT) devices, such as smart speakers or smart door locks. Adapting to these changes thus requires an unremitting process that involves the user's abilities, as well as strategies to react to the challenges that stem from the constant and dynamic development of technology and new applications.

The merging of our physical and virtual worlds by means of such devices is supposed to support and enhance wellbeing, but without adequate security and protection, and non-existent provisions to support resilience, this wellbeing may in fact be very much under threat (Heartfield et al., 2018). Notably, typical users of the internet seem to be overconfident in the security of the devices they use, with more than 978 million adults in 20 countries reporting having experienced cyber-crime or knowing someone who did; an impressive 53% of users globally (Symantec, 2018). Not only has vulnerability to cyber threat been exposed in devices and mechanisms typical to sectors of business and the confidential transaction of data, but the increased variety of devices that now connects to the internet led to a new generation of threat, in devices that span all aspects of modern society, such as medical devices, most modern cars and household appliances.

We posit that this new landscape of technology requires adaptive security strategies centered on users, who, obviously, have extremely varied expertise and experience of technology(Williams et al., 2020). To date, the scientific literature on cyber-crime has mostly focused on technological consequences (Loukas, 2015) and on guidelines for dealing with security issues (Vishwanath et al., 2020), with little focus on the psychology of the user experience. The psychological consequences of an attack, however, can far outlast and be more significant than any disturbance caused to the technology, since harm to the user may have deep ramifications, which will depend on the motivations of the perpetrator (socioeconomic, psychosocial or geopolitical; Ibrahim, 2016) and will always involve a level of distress (Heartfield et al., 2018). In the present work, we describe a first step in the investigation of the structure of psychological experience of cybersecurity breach victims.

Psychological consequences of cyber security breaches

Results from the few available studies (Canetti et al., 2017; Gross et al., 2016, 2017) are indicating increased anxiety and stress as a reaction to simulated cyber-terrorism, and anger, anxiety, sadness and insecurity as common responses to cyber-aggression (Kopecký & Szotkowski, 2017). Although some findings highlight the negative impact of cyber-crime victimization on subjective wellbeing (Kaakinen et al., 2018), to our knowledge there is no systematic study of the psychological experience of cybersecurity breach victims. A cybersecurity breach can be expected to have a psychological impact on the victim, because it creates situations for the user that contravene their goals. Understandably, the more a user relies on technology, the more powerful the ripples of an attack: Work and livelihood can be disturbed, and personal and social spheres can be altered, sometimes irrevocably. When such an event is perceived as relevant to one's personal concerns, it will drive an emotional response (Frijda, 1986; Scherer, 2001).

Short term consequences: emotions

Depending on the perceived importance, nature and magnitude of the breached integrity of the system and devices, we can expect short-term psychological consequences that can develop into long-term, far-reaching psychological turmoil.

A leading security company reported such short-term consequences to lead to anger, annoyance, the feeling of being cheated, upset, frustration, and other negative emotions (Symantec, 2010). Recently published scientific research investigating affective reactions to hypothetical cyber-attack scenarios reported that high negative emotional valence and arousal are found for attacks (Pyke et al., 2021). Also, it has been argued that more severe consequences of cybersecurity breaches can even lead to suicide (Baraniuk, 2015). Overall, there is little in-depth understanding of emotional responses to cyber-attacks.

Goal relevant situations are typically considered prime triggers of emotions (Scherer, 2001) and, in this study, we conceive of emotions as the short-term psychological effects that may stem from the perception and understanding that one has become a cybersecurity breach victim. In this research we aimed to confirm and understand the nature of these emotions. Due to the fact that there are few insights on emotion responses to

cyber breaches, we rely on well-validated the theoretical framework about emotions (Componential emotion approach, Scherer, 2001) to explore emotional experiences.

Componential emotion approach

While emotions have traditionally been studied through the semantics of emotion terms or emotion dimensions (e.g. anger and fear, or emotional valence (positive and negative affect), and dominance), leading to limited insights, the componential emotion appreach provides a more detailed insights into the emotion process. It holds that the whole emotion process, yielding a full-blown emotional experience, can be described as encompassing five components: appraisal of the situation, action tendencies, bodily responses, expressions and subjective feelings (Scherer, 2001) Each component has a function: the appraisal component supports the cognitive evaluation of the eliciting event. Action tendencies refer to the preparation and direction action, which then yields physiological (body responses) and behavioral outcomes (expressions). Subjective feelings ensue, grounding and signaling to the individual the occurrence of the emotion process. This decomposition in components is particularly useful for emotion psychologists, for it allows the elaboration of hypotheses and measurements, and for applied psychologists as it permits the construction of targeted interventions to assist emotion regulation.

Psycholinguistic GRID research

Based on the Component Process Model (Scherer, 2001), the GRID framework (Fontaine et al., 2013) was developed. According to this framework, each emotion component can be described with several factors. The framework was originally developed to assess the semantic spaces of emotion terms based on the cross-cultural comparison of emotion terms in 27 countries (24 languages). This led to the reliable definition of a four-dimensional structure, comprising valence, power, arousal, and novelty, which encompasses 142 emotion features spanning the five components. Additionally, each emotion component can be described through additional factors (Fontaine et al., 2013).

Appraisals can be described with six factors: (i) novelty/chance (unexpected and unpredictable events that occur by chance and require urgent action), (ii) coping ability (resources to avoid or modify the consequences, if the consequences are avoidable and modifiable, and ability to live with the consequences), (iii) expected/familiar (estimation of familiarity of the event, predictability of the consequences, if the expectations are confirmed and if the event is caused intentionally), (iv) goal relevance (importance and relevance for person's or somebody else's goals), (v) norm violation (violation of laws or socially accepted norms and incongruences with own standards and ideals), (vi) self vs other cause (caused by person's own or somebody else's behavior).

Action tendencies can be described through three factors: (i) defensive vs appetitive (wanting to flee and to oppose versus wanting to show off, to be tender, sweet and kind vs wanting to flee and to oppose), (ii) disengagement vs intervention (apathy, withdrawal and fleeing tendencies opposed to taking initiative to change the situation), and (iii) submit vs attack (tendencies to be with others and submit oneself to others versus aggressive and opposition tendencies).

Bodily responses can be described through three factors: (i) distress symptoms (non-sympathetic, non-adrenergic arousal), (ii) autonomic arousal (high arousal of autonomic nervous system) and (iii) body temperature (temperature factor).

The expression component is represented with three categories: (i) facial expressions (1. frown vs smile, 2. jaw drop/eyebrows up, and 3. eyes closed/tears.), (ii) vocal expressions (1. vocal energy, 2. firm vs perturbed speech), and (iii) body movement (1. moving toward vs withdrawing, and 2. no vs abrupt movement).

Subjective feelings can be described through 24 emotion terms categories in six main categories: (i) joy (joy, happiness, pleasure, pride, love, interest), (ii) fear (fear, anxiety, stress, disgust), (iii) sadness (sadness, disappointment, being hurt, despair), (iv) anger (anger, irritation, hate, jealousy), (v) surprise, and (vi) compassion.

Lazarus appraisal model

In addition to appraisal within GRID framework (Fontaine et al., 2013), more detailed approach to appraisals in the emotion process is offered by Lazarus' model of core relational themes (Lazarus, 1993) by interpreting appraisals in reference to the environment. The concept of appraisal is seen as a cognitive mediator of the stress reaction, a universal process of evaluating the significance of the event for one's personal wellbeing. According to this model, emotions are always a response to relational meaning (i.e., a person's sense of the harm and benefits in a specific relationship between person and environment). Each emotion involves a different core

relational theme. Anger reflects a demeaning offense against me and mine, anxiety includes facing uncertain, existential threat, and shame is about having failed to live up to an ego ideal. Compassion includes being moved by another's suffering and wanting to help, disgust refers to taking in or being too close to an indigestible object or idea, while fright includes facing an immediate, concrete, and overwhelming physical danger. Happiness is about making reasonable progress toward to realization of a goal, hope includes fearing the worst but yearning for the better, relief represents a distressing goal-incongruent condition that has changed for the better or gone away, while sadness is about having experienced an irrevocable loss. This approach to appraisals can offer more detailed insight into appraisals of victims in interaction with the cybersecurity breach in their environment.

Definitions of Specific Coping Strategies and Organization into Higher Level Categories

According to the Component Process Model (Scherer, 2001), emotions are dynamic processes driven by all emotion components and regulatory processes. Regulation (coping) as a part of emotion process can affect all components (Fontaine et al., 2013). Coping strategies can be organized into higher level categories with the highest level of distinction between engagement and disengagement coping (Connor-Smith & Flachsbart, 2007). Depending on the coping goals, engagement coping can be defined as being an engagement strategy with the primary goal of changing the stressor or regulating and appropriately expressing related emotions (problem solving, instrumental support, mixed social support, emotional regulation) or a secondary control with adaptation to stress (distraction, cognitive restructuring and acceptance). Disengagement coping is characterized with strategies such as avoidance, denial, wishful thinking, and withdrawal. This approach offers a detailed overview of a range of possible coping strategies that can be applied to any of the components that are part of the emotion process.

The current study

In this study, a combination of exploratory and theory-driven research within the framework of the componential emotion approach was applied, to study the emotion process in cybersecurity breach situations, from situation to regulation, by answering the following research questions:

1. What emotion processes are generated as a reaction to cybersecurity breaches?
2. Which emotion regulation mechanisms are employed in situations of cybersecurity breaches?

To understand the user's experience to cyber security threats, we surveyed the reactions that people who experienced, first or second hand (via friends, acquaintances or media) recall and/or anticipate a cybersecurity breach, with open questions, that were structured though the lens of emotion theories and the five components of the emotion process. We included questions about a wide range of devices, including IoT devices, smartphone and computers, as well as questions about a wide range of applications, including email, social media networks, which are common cybersecurity breach targets. This exploratory study is an important first step in the design of a comprehensive theoretical framework of the experience of cybersecurity breach victims.

Method

Sample

Undergraduate students and professionals, from different backgrounds and countries (N=130), were recruited in the period between June and December 2017, from the University of Zagreb (N=102), Eindhoven University of Technology (N=12), and social networks (N=16). Students (of which most were studying psychology) received course credits for their participation, whereas the general population did not receive any compensation. Only people that had direct or indirect experience with cyber-attacks were invited to complete our survey. The sample included participants who reported experiences of cyber-attacks first-hand (N=12), through hearing from experiences of friends and acquaintances (N=81), or in the media (N=37). Participants were mostly females (N=105) with an average age of 22.28 years (SD=6.261, range from 18-53 years old).

Procedure

We used an online platform, Qualtrics (Qualtrics, 2017) to ask participants to describe a cybersecurity breach experience on an IoT device, computer, smartphone, email, or social network account, that they experienced themselves or heard about from friends or the media. Subsequently, they were asked to describe their personal or anticipated emotional experiences in that situation. It took an average of 20 minutes to fill in the questionnaire, which comprised questions on all five components of the emotion process and questions about emotion regulation.

Instrument

Participants were first asked basic information about their usage of connected devices. Subsequent questions were related to their experience of cybersecurity breach, whether they had first-hand experience, they had friends who had a cybersecurity breach, or they learned about cyber-attacks from the media. They were instructed to remember and describe in detail an occurrence of such cybersecurity breach situation. Depending on their answers, participants were directed to tailored sections of the questionnaire, related to cyber-attacks on IoT devices, computers, smartphones, social networks or email accounts. The participants were then asked using open questions to describe in their own words their emotional experiences of the cybersecurity breach, or to anticipate how they would have felt in the case they were themselves the victims of the attack they reported. These open questions followed the GRID framework (Fontaine et al., 2013), to probe dimensions related to the five components of the emotion process being appraisals, action tendencies, bodily reactions, expressions and subjective feelings. Finally, they were asked to describe how they regulated or would have regulated their emotions in that situation.

Analysis

Answers from questions about emotion processes in relation to the five components (appraisals, action tendencies, bodily reactions, expressions and subjective feelings) were analyzed and coded in categories within the GRID framework (Fontaine et al., 2013), while emotion regulation was coded within the Conceptual integration model (Connor-Smith & Flachsbart, 2007) using QSR International's NVivo 11 Software. An iterative process of coding was applied. During this process, it became clear that other emotion theories and new categories would be helpful in understanding the emotion process and were therefore included. Therefore, in addition to coding within the GRID framework (Fontaine et al., 2013), several appraisals in cybersecurity breach situations were coded within the Lazarus appraisal model (Lazarus, 1993) When analyzing the text it became clear that, apart from appraisals coded within GRID framework (Fontaine et al., 2013) and Lazarus appraisal model (Lazarus, 1993), specific appraisals like privacy intrusion, unknown cause or consequence, insecurity, and 'other cause' were important for cybersecurity breach situation, therefore we added those codes. Furthermore, in addition to emotion regulation categories within the Conceptual integration model, several other emotion regulation strategies specific for this study, were found to be a good fit within categories of rumination from Watkins, Moulds & Mackintosh model (2005), and suppression from Gross model (Gross, 2002). Also, several new categories were added within the subjective feelings (panic, shock, worried, depressed, embarrassment, frustration, furious and rage) for the cases which did not fit any of the categories proposed by applied models. These new categories are marked within the result section.

Results

Participants reported emotional experiences due to the cybersecurity breaches of social media or an email account (58.5%), computer (22.3%), smartphone (11.5%), and IoT devices (7.7%). Descriptions of their anticipated emotional processes are based on the cybersecurity breach scenario that they reported (90.8%), as well as on first-hand experiences (9.2%). Descriptions of emotional processes were analyzed and coded within the GRID framework into the categories that are empirically identified in the research (Fontaine et al., 2013) on Component Process Model of emotion (Scherer, 2001) and described in the section: Analysis. Coded categories include description on the five components, namely: appraisal, action tendencies, bodily response, expression, subjective feeling, and additionally emotion regulation, and we coded experiences within each category depending on the meaning of described experiences regardless under which question category experience was described (in some cases participants gave information about one component when replying to another questions). In total, 4008 meaning units were detected, out of which 3864 (96.4%) were coded within the above listed emotion and emotion regulation models. Only 144 meaning units could not be coded as meaning units within the described models, (as they were not semantically associated with the topics or they were random entries) and were thus not included in the further analyses.

We present the number of references for each coded meaning unit as well as a number of participants that reported on a specific emotion process. Additionally, we present examples of first-hand, and examples of anticipated emotion experiences, as the analysis of those experiences contributed to the scope expansion of reported experiences. Results are presented for each emotion component and emotion regulation separately in respect to subcomponents within each component.

Appraisals

Coding of responses in the emotion component appraisal was based on appraisal categories within the original GRID framework (Fontaine et al., 2013) (see list of categories in Table 1) and on categories within Lazarus (Lazarus, 1993) appraisal model (see list of categories in Table 2). In addition to categories within these frameworks, several additional categories were used, as they were found to be prevalent and specific for cybersecurity breach situations, namely: privacy intrusion, unknown cause or consequence, other cause, and insecurity.

We found that the most salient appraisals in the cybersecurity breach situations are negative, with most frequently reported appraisals of privacy intrusion (N_P = 80, e.g., ˝ My privacy being attacked and someone having full control over my personal messages, accounts, passwords.˝), and unknown cause or consequence (N_P = 78, e.g., ˝I would be wondering who is responsible.˝). They are followed by appraisals of having no control (N_P = 55, e.g., ˝Knowing I am no longer in control of the things happening under my name.˝), fright (N_P = 39, e.g., ˝They may find something they shouldn't and may use it against me. ˝, ˝I thought he would harm me˝), insecurity (N_P = 32, e.g., ˝I would think about the fact that internet is not a safe place to keep your personal information.˝, ˝Other people have gained access to your devices without you knowing.˝), norm violation (N_P = 31, e.g., ˝Probably the theft of my data.˝, ˝It is in some way the same as a criminal that enters your house.˝, Anger as a demeaning offense against me and mine (N_P = 27, e.g., Whether the hacker would use my account to target friends and family.˝, ˝Suddenly a tool used against you.˝), and self-cause (N_P = 20, e.g., ˝I would start thinking what have I done wrong˝; Table 1-2).

Table 1. *Categories within the GRID framework for Appraisal Component*

Category	N_R	N_P	Examples of references
NOVELTY_CHANCE CAUSE	5	3	I always think things like that won't happen to you, and when they do happen you just can't believe it.
COPING ABILITY	18	14	How nice would it be to posses certain skills to track down the hackers! (A)
NO CONTROL[1]	82	55	Knowing I am no longer in control of the things happening under my name. (A) You cannot find the actual offender. (P)
EXPECTED _FAMILIAR[1]	1	1	That it was a common situation for such a company. (A)
GOAL RELEVANCE[1]	23	16	Your computer is your life (A) I would be stressed because there are many important files that I would probably need. (P)
NORM VIOLATION[1]	45	31	Probably the theft of my data. (A) It is in some way the same as a criminal that enters your house. (P)
SELF CAUSE[1]	27	20	I would start thinking what have i done wrong (A).
OTHER CAUSE[2]	21	16	Person behind a cyber-attack is often someone close to you (A)
UNKNOWN CAUSE OR CONSEQUENCE[2]	206	78	I would be wondering who is responsible. (A) What kind of damage the hacker caused (P).

Note: [1]Categories within Scherer's Component Process Model of emotions (Scherer, 2001) and the GRID framework (Fontaine et al., 2013), [2]Categories specificly added for cybersecurity breach situations, N_R: number of references reporting experience, N_P: number of participants which reported experience A: anticipated cybersecurity breach experience. P: personal cybersecurity breach experience.

Table 2. *Categories within Lazarus appraisal mode for Appraisal Component*

Category	N_R	N_P	Examples of references
ANGER a demeaning offense against me and mine[1]	38	**27**	Whether the hacker would use my account to target friends and family. (A) Wonder if someone has offended other people using my identity. (A) The probability that the files that were stored on that computer were destroyed-(A) An attack on my safety and trust. (A) Suddenly a tool used against you (P). Quite indignant that this happened to me and someone made this cyber-attack. (P)
ANXIETY facing uncertain, existential threat[1]	14	12	Anxiety would probably arise because I would start thinking about what all could happen in the future. (A) I just wanted to know if everything was ok, so I kept asking questions that asked over safety and the situation at the moment (P)
SHAME having failed to live up to an ego-ideal[1]	15	12	My colleagues have seen this. I'm a joke now. I would also be ashamed if some material was visible to anyone other than me, let alone made public. (A) How could I be so stupid? (P)
COMPASSION being moved by another's suffering and wanting to help[1]	5	4	I can only imagine what it is like when inexplicable things happen for a long period of time (A) Who's also being attacked? (A)
DISGUST taking in or being too close to an indigestible object or idea[1]	1	1	And most certainly i would feel disgust toward the intruder. (A)
FRIGHT facing an immediate, concrete, and overwhelming physical danger[1]	59	39	I would've been afraid cause of possible identity theft. (A) They may find something they shouldn't and may use it against me. (A) I thought he would harm me (P)
HAPPINESS making reasonable progress toward to realization of a goal[1]	1	1	On the other hand, I would be happy because I know I'd never do such thing to another human being. (A)
HOPE fearing the worst but yearning for the better	3	3	Hoping my friends wouldn't be in danger. (A)
RELIEF a distressing goal-incongruent condition that has changed for the better or gone away[1]	3	3	The problem will be solved quickly, I don't have to worry. (A)
SADNESS having experienced an irrevocable loss[1]	13	10	I would realise that my computer would not be in function for a period of time and then I would become sad. (A)
PRIVACY intrusion[2]	129	80	My privacy being attacked and someone having full control over my personal messages, accounts, passwords. (A) Something of your own just got obtained by some anonymous person from the outside and that idea is horrifying. (P)
INSECURITY[2]	43	32	I would think about the fact that internet is not a safe place to keep your personel informations. (A) Other people have gain access to your devices without you knowing (P)

Note: [1]Categories within Lazarus appraisal model (Lazarus, 1993), [2]Categories specificly added for cybersecurity breach situations, N_R : number of references reporting experience, N_P: number of participants which reported experience A: anticipated cybersecurity breach experience. P: personal cybersecurity breach experience. * The following categories from the Lazarus appraisal mode were not included as they had zero coded references : ENVY wanting what someone else has, GUILT having transgressed a moral imperative, JEALOUSY resenting a third party for loss or threat to another's affection, LOVE desiring or participating in affection, usually but not necessarily reciprocated, PRIDE enhancement of one's ego-identity by taking credit for a valued object or achievement, either our own or that of someone or group with whom we identify.

Action tendencies

Coding within the category of action tendencies is based on the GRID framework (Fontaine et al., 2013), and the extracted factors are presented in Table 3. The most prevalent action tendencies in cybersecurity breach situations include a tendency for intervention (N_P = 96, e.g., ″I would probably feel an inner drive to undertake all possible actions to resolve the issue″ and ″I changed all my passwords, so he couldn't get in anymore″), followed by a tendency to act defensive (N_P = 39, e.g., ″To shut down as much as unnecessary accounts and applications as possible″ and ″I wanted to run away I wanted to be safe I wanted to undo this.″, to attack (N_P = 35, e.g., ″ I would have desire to punish a person who did that.″ or ″Probably throw some things around.″), and to disengage (N_P = 21, e.g., ″Probably using internet less.″ or ″I didn't talk to anyone about that at that specific moment.″; Table 3).

Table 3. *Categories within Action Tendency Component**

Category[1]	**N_R**	**N_P**	**Examples of references**
DEFENSIVE	60	39	To shut down as much as unnecessary accounts and applications as possible. I would probably feel the need to stop what is going on. I would like to protect myself in any way I can (A) I wanted to be safe I wanted to undo this. (R)
DISENGAGEMENT	29	21	get rid of all social networks. I would turn off the computer / cell phone and go to bed. Probably using interent less. (A) I didn't talk to anyone about that at that specific moment. (R)
INTERVENTION	250	96	I would probably feel an inner drive to undertake all possible actions to resolve the issue. (A) , Try to change password or anything to save/protect my documents if can Focus all my energy into trying to make things right Wanted to call my provider I would feel the urge to turn off the cyber attack apparatus as soon as possible how to protect myself from it in the future (A)I changed all my passwords, so he couldn't get in anymore (R) I began trying to recover my email Asap and continued doing so until I was successful. (R)
ATTACK	48	35	Probably would behave in an angry way. (A) I would have desire to punish a person who did that. (A) Probably throw some things around. (A) Hitting things (R)

Note: [1]Categories within Scherer's Component Process Model of emotions (Scherer, 2001) and the GRID framework (Fontaine et al., 2013), N_R : number of references reporting experience, N_p: number of participants which reported experience, A: anticipated cybersecurity breach experience, P: personal cybersecurity breach experience.

Expressions

Coding within the category expressions is based on the GRID framework (Fontaine et al., 2013) and several additional categories which were found in the reported emotion processes about the cybersecurity breach situations. The categories within the expression components are presented in Table 4.

The most often reported expressions in cybersecurity breach situations include high vocal energy (N_P = 51, e.g., ″My voice would be loud.″ and ″I yelled a bit.″), abrupt movement (N_P = 45, e.g., ″I was nervously kicking with legs)″, and ″I was walking around nervously.″), eyes closed/tears (N_P = 41, e.g., ″My eyes would be filled with tears.″, and ″I cried/ teared up″), withdrawing (N_P = 32, e.g., ″Standing slouched.″, and ″Your posture is minimized, you become very small.″), perturbed speech (N_P = 27, e.g., ″My talk would be discontinuous and abrupt.″, and ″I had a trembling voice.″), and frowning (N_P = 27, e.g., ″I would probably have my eyebrows down.″ and ″I frowned.″; Table 4).

Table 4. *Categories and Subcategories within the Expression Component*

	Category	N_R	N_P	Examples of references
Facial expression	FROWN[1]	37	**27**	I would probably have my eyebrows down. (A) I frowned. (P)
	NO SMILE[2]	3	3	Unsmiling (A)
	JAW DROP[1]	11	11	I would be shocked with my mouth open (A)
	EYEBROWS UP[1]	8	7	Raised eyebrows (A)
	EYES OPEN[2]	18	18	I would open my eyes widely (A)
	EYES CLOSED_TEARS	54	41	My eyes would be filled with tears. (A) I cried/ teared up. (P)
	ANGRY FACE[2]	6	5	Have an angry facial expression (A)
	CONFUSED FACE[2]	2	2	I think I would have a confused expression on my face (A)
	PAIN FACE[2]	1	1	Would grimace in pain (A)
	SAD FACE[2]	9	9	I would look sad (A)
	SCARED FACE*[2]	10	10	My face would look scared (A)
	SURPRISED FACE[2]	5	5	Surprise on my face (A)
	UPSET FACE[2]	2	1	Upset (A)
	WORRIED FACE[2]	12	12	Face probably concerned (A)
	NORMAL FACE EXPRESSION[2]	5	5	Dont think my facial expression would change that much (A)
Vocal expression	LOW VOCAL ENERGY[1]	13	13	I would be quiet (A)
	HIGH VOCAL ENERGY[1]	77	51	My voice would be loud. (A) I yelled a bit. (P)
	PERTURBED SPEECH[1]	26	27	My talk would be discontinuos and abrupt. (A) I had a trembling voice. (P)
	GENERAL VOICE EXPRESSION[2]	14	14	Not being able to sound comprehensive due to strong emotions (A)
	NORMAL VOCAL EXPRESSION[2]	4	3	Think my voice wouldn't be raising (A)
Body movement	MOVING TOWARD[1]	3	3	I would also try to get the body moving (A)
	WITHDRAWING[1]	41	32	Standing slouched. (A) Your posture is minimized, you become very small. (P)
	ATTACK POSTURE[2]	17	8	The fists would clench (A)
	NO MOVEMENT[1]	19	14	Standing still (A)
	ABRUPT MOVEMENT[1]	63	45	I would start walking nervously all over the room. (A) Running my hand through my hair. (P)
	NORMAL BODY EXPRESSION[2]	4	3	There would be no change in posture (A)

Note: [1]Categories within Scherer's Component Process Model of emotions (Scherer, 2001) and the GRID framework (Fontaine et al., 2013), [2]Added categories based on the coding of cybersecurity breach situations, N_R : number of references reporting experience, N_p: number of participants which reported the experience, A: anticipated cybersecurity breach experience. P: personal cybersecurity breach experience. The following categories from the GRID framework that were not included as they had zero coded references are SMILE and FIRM SPEECH.

Bodily response

Coding within the category bodily response is based on the GRID framework (Fontaine et al., 2013), and coded categories are presented in Table 5. The most salient bodily response in cybersecurity breach situation is high autonomic arousal, distress (N_P = 71, e.g., ˝I would feel heaviness in my stomach.˝, ˝ I probably would have a headache.˝) and a high temperature (N_P =31, e.g., ˝Heat in my head, chest and abdomen.˝ and ˝Feeling hot.˝; Table 5).

Table 5. *Categories within Bodily Response Component*

Category[1]	N_R	N_P	Examples of references
DISTRESS GENERAL	113	**71**	I would feel heaviness in my stomach (A). Maybe a little shaky. (R)
CHEST PAIN	4	4	Pressure in the chest (A)
HIGH AUTONOMIC AROUSAL	151	84	I would sweat, faster heart rate, faster breathing. My body would be tense. Dry mouth. (A) tickling and goosebumps because of the creepiness (R) I Started sweating (R)
LOW AUTONOMIC AROUSAL	4	4	Breathing deeply and slowly (A) so my body would be slow (P)
HIGH TEMPERATURE	33	31	Heat in my head, chest and abdomen. (A) Feeling hot. (P)
LOW TEMPERATURE	11	10	My hands cold (A)
USUAL BODILY RESPONSE	3	2	I think my body would not react differently while experiencing a cyber-attack (A)

Note: [1]Categories within Scherer's Component Process Model of emotions (Scherer, 2001) and GRID framework (Fontaine et al., 2013)

Subjective feeling

Coding within the category subjective feelings is based on the 24 basic emotion terms (Fontaine et al., 2013) and several additional categories that were found to be relevant during the analyses of reported subjective feelings in cybersecurity breach situations.

The most salient reported subjective feelings include negative emotions such as fear (N_P = 101), anger (N_P =90), anxiety (N_P =58), sad (N_P =49), panic (N_P =37), powerless (N_P =35), worried (N_P =30), uncomfortable (N_P =25), upset (N_P =22), ashamed (N_P =21), and frustrated (N_P =21; Table 6).

Table 6. *Categories within Subjective Feeling Component*

	Category	N_R	N_P	Examples of references
FEAR	ANXIETY[1]	92	58	Anxious. (A/P)
	DISGUST[1]	6	4	Disgust (A)
	FEAR[1]	221	101	Fear. Terrified. (A/P)
	PANIC[2]	54	37	Panic. (A/P)
	SHOCK[2]	27	19	Shocked (A)
	STRESS[1]	32	18	I would be really stressed (A) I started feeling stressed (P)
	UPSET[2]	27	22	Upset. (A/P)
	WORRIED[2]	49	30	Worried. (A/P)
SADNESS	BEING HURT[1]	25	16	I would feel hurt and vulerable (A)

	DEPRESSED[2]	20	13	I would be depressed (A). Weak, numb, exhausted (P)
	DESPAIR[1]	57	35	Helpless. Powerless, Despair (A)
	DISAPPOINTMENT[1]	12	9	i would feel disappointed (A)
	EMBARRASSMENT[2]	13	8	I would feel embarrassed (A)
	GUILT[1]	11	9	Guilt (A/P)
	SADNESS[1]	74	49	Sad. (A/P)
	SHAME[1]	30	21	Shame. (A/P)
ANGER	ANGER[1]	194	90	Angry. (A/P)
	FRUSTRATION[2]	36	21	Frustrated. (A/P)
	FURIOUS, RAGE[2]	22	14	Furious, rage (A)
	HATE[1]	3	3	Hateful (A)
	IRRITATION[1]	7	7	I would feel irritated (A). I would be annoyed as well at first, because claiming accounts back can be such a hassle (P)
SURPRISE[1]	SURPRISE[1]	24	20	Unpleasantly surprised. (A)
GENERALY UNPLEASANT[1]	GENERALY UNPLEASANT[1]	31	25	I wouldn't feel comfortable at all. (A) First time you get the notification you're feeling bad. (P)

Note: [1]Categories within 24 basic emotion terms (Fontaine et al., 2013), [2]Categories specificly added for cybersecurity breach situation are N_R : number of references reporting experience, N_p: number of participants which reported experience, A: anticipated cybersecurity breach experience, P: personal cybersecurity breach experience. The following categories from the original 24 basic emotion terms were not included as they had zero coded references: HAPPINESS, INTEREST, JOY, LOVE, PLEASURE, PRIDE, CONTEMPT, JEALOUSY and COMPASSION.

Emotion regulation

Emotion regulation strategies were mostly coded within categories of the Conceptual integration model (Connor-Smith & Flachsbart, 2007) and two additional emotion regulation strategies, rumination (Watkins et al., 2005) and suppression (Gross, 2002).

In the cybersecurity breach situation, the most frequently reported emotion regulation strategy was instrumental support (N_P = 71, e.g., ˝I would contact all the services that I could. ˝, ˝I should go to the police and hope for the best.˝), relaxation (N_P = 54, e.g., ˝I would try to calm down. ˝, ˝By taking deep breaths.˝), suppression (N_P = 50, e.g., ˝I would not let my anger get to me completely. ˝, and ˝I tried to minimize my nervousness when typing, to avoid making my friend nervous.˝), cognitive restructuring (N_P = 41, e.g., ˝Convince myself that it really isn't that bad and that I can make things right.˝, and ˝I decided to focus on positive things again (my work, family and friends).˝), emotional support (N_P = 32, e.g., ˝I would tell my friends and family. ˝, and ˝ I would ask for a comfort from other people.˝) and rumination (N_P = 23, e.g., ˝I would overthink about possible things he/she could've read or do with my personal info.˝, and ˝Trouble concentrating on work.˝; Table 7).

Table 7. *Categories within Emotion Regulation*

Category	N_R	N_P	Examples of references
NEGATIVE EMOTION FOCUSED[1]	13	11	Probably nervous which would affect the people around me. (A)
ENGAGEMENT COPING[1]	3	3	Try to stop putting my self in simmilar positions in the future (A)
INSTRUMENTAL SUPPORT[1]	117	71	I would contact all the services that I could. (A) I should go to the police and hope for the best.(P)
EMOTIONAL SUPPORT[1]	43	32	I would tell my friends and family. (A). I would ask for a comfort from other people. (A)
PHYSICAL ACTIVITY[1]	2	2	I WOULD go to the training which reduce my level of stress and anger (A)
RELAXATION[1]	81	54	I would try to calm down. (A) By taking deep breaths. (P)
SUPPRESSION[3]	65	50	I would not let my anger get to me completely. (A) I tried to minimize my nervousness when typing, to avoid making my friend nervous. (P)
SECONDARY CONTROL[1]	13	10	it would be hard for me to trust the online type of communication again, i.e. dating. (A) you do lose your trust at least for a while. (P)
DISTRACTION[1]	8	5	I would try to distract my thoughts by watching something or going out with friends. (A)
COGNITIVE RESTRUCTURING[1]	54	41	Convince myself that it really isn't that bad and that I can make things right. (A) I decided to focus on positive things again (my work, family and friends). (P)
ACCEPTANCE[1]	7	7	the realization that there is nothing I can do and that I have to start over (A) so you just have to accept the loss /R)
AVOIDANCE[1]	3	3	If it becomes to hard to live with it I would try not to think about it. It would not help me to solve anything but it would be easier to live this way. (A)
DENIAL[1]	5	4	I would not want to believe that it was cyber attack (A)
WISHFUL THINKING[1]	7	7	Maybe to turn back time and not to have contact with website or something that caused that (A)
WITHDRAWAL[1]	13	8	Maybe I would avoid tehnology for a while because of fear (A)
RUMINATION[2]	24	23	I would overthink about possible things he/she could've read or do with my personal info. (A) Trouble concentrating on work. (P)

Note: [1] Categories within Conceptal integration (Connor-Smith & Flachsbart, 2007). The following categories from this model were not included as they had zero coded references: MIXED EMOTION FOCUSED PRIMARY CONTROL, PROBLEM SOLVING, MIXED SOCIAL SUPPORT, RELIGIOUS COPING, BROAD DISENGAGEMENT, NARROW DISENGAGEMENT and SUBSTANCE USE, [2]Categories within Watkins, Moulds & Mackintosh (Watkins et al., 2005), [3] Categories within Gross (Gross, 2002) [4] Items are matched as much as possible to the items of the original GRID instrument (Fontaine et al., 2013), $N_{R:}$ number of references reporting experience, $N_{p:}$ number of participants which reported experience, A: anticipated cybersecurity breach experience. P: personal cybersecurity breach experience.

Discussion

In this study, we took an explorative stance to probe the scope of the experiences that ensue from cyber-security breach situations of connected technology, including IoT devices, smartphones, computers, and communication technology (social networks, email). Although largely exploratory, we used a theory-driven approach, by structuring the open questions and analyzing the responses using categories from emotion theories (Connor-Smith & Flachsbart, 2007; Fontaine et al., 2013; Scherer, 2001) While previous studies explored only one component of emotion experiences towards cyber-security breach situations, namely subjective feelings such as anger or emotion dimension such as emotional arousal (Canetti et al., 2017; Oulasvirta et al., 2012; Pyke et al., 2021; Symantec, 2011), we went further by also exploring appraisals, bodily reactions, expressions and action tendencies. This approach allowed us to explore all facets of emotion experiences in cybersecurity breach situations. First, a description of the coding process will be presented, followed by a discussion about central emotion processes in cybersecurity breach situations. Finally, implications, limitations and suggestions for future research are discussed.

Coding process: especially issues for appraisals

All the reported personal and anticipated emotion processes for the situation of cybersecurity breaches have been coded against the GRID framework (Fontaine et al., 2013) based on the Component Process Model (Scherer, 2001), namely appraisals, action tendencies, bodily responses, expressions and subjective feelings. However, particularly for the appraisal component, we found that many reported appraisals did not fit the GRID framework, but were found to be a better fit within the additional appraisal categorization based on Lazarus model (Lazarus, 1993). Emotion regulation was coded within categories based on several models: Conceptual integration model by Connor-Smith and Flachsbart (Connor-Smith & Flachsbart, 2007), and by two added emotion regulation strategies, rumination (Watkins et al., 2005) and suppression (Gross, 2002).

Cyber-security breaches are clearly emotional, with a focus on fear and anger

Overall, the most reported experiences in cybersecurity breach situations on each of the components reflect negative emotional experiences, which indicates that a cybersecurity breach situation is a negative emotional experience for the victim. Our results are in line with the limited literature that exists on the emotional experience of victims of cyber-crime (Canetti et al., 2017; Oulasvirta et al., 2012; Symantec, 2011) which also finds that negative emotions are associated with such an event. Subjective feelings found in our study are also reported in other sources on cyber-crime, such as fear, anger, annoyance, sadness, despair, shame, betrayal (Symantec, 2011), anxiety, annoyance, concern, and rage (Oulasvirta et al., 2012). However, while those studies were limited to reporting these subjective feelings, our study using the component emotion approach additionally explored the appraisals, bodily reaction, expressions and action tendencies. We find a lot of these features in participants' reporting of cyber-breach experiences, indicating that experiencing or anticipating the experience of a cybersecurity breach clearly elicits emotions in their broadest sense. If we look at the subjective feelings, there are two categories that are much more often reported than others, and those are subjective feelings of fear and anger. These two central emotions are also reflected throughout other emotion components.

Appraisals: threat and being unjustly treated and powerlessness

Analysis of the appraisal component of emotion processes revealed aspects of emotion experiences which are specific for cybersecurity breach situations, such as privacy intrusion, appraisals of the unknown cause or consequences of the breach situation and insecurity. Other frequently reported appraisals for this specific situation for victims of cybersecurity breach reflect perceptions of having no control, fright appraisals as result of perceiving immediate, concrete and overwhelming physical danger, insecurity, norm violation, demeaning offense against themselves or theirs, or blaming themselves. This list of the most salient appraisals are reflections of the breach happening without physical presence of the perpetrator but bringing privacy intrusion through an unauthorized access of the unknown perpetrator and involving vagueness of the cause and consequences. Appraisals of threat, of being treated unjustly, of privacy violation, and of powerlessness describe victims' appraisals in the cybersecurity situation.

Bodily expressive: highly aroused and expressive

Reported bodily responses and expressions such as a general high level of autonomic arousal and distress symptoms, abrupt movements, yelling, frowning, crying, shaking of the voice and withdrawal emphasize that the experience of falling victim of cybersecurity breach is stressful. In line with that. a rise in cortisol level due to cyber-attacks was reported in another study (Canetti et al., 2017). These highly aroused and expressive reactions can be related to the two main reported subjective feelings of fear and anger.

Action tendencies: constructive, but also many unconstructive especially withdrawal and aggression

Our participants also reported both active and passive action tendencies, either in the form of an intervention, attack or defense, or in the form of passive disengagement from the situation respectively. This latter finding is in line with lack of actions taken by victims of actual cybercrimes, as reported by a leading cyber-security company (Symantec, 2011). They reported that individuals who experience cyber-crime mostly do not report a crime, call their financial institutions or the police, or contact the website owner or email provider.

The reported action tendencies can be interpreted as both constructive and unconstructive. Interventions in the context of cybersecurity breaches present constructive action tendencies when they are focused on solving the situation. They include a tendency to stop the breaching behavior or to call the police. In this context, emotions serve the purpose of preparing us for adequate action (Frijda, 1986). Disengagement and withdrawal from activities that require connectedness (i.e., emailing, using social media, etc.) in the situation of cybersecurity breach presents unconstructive action. Disengagement, withdrawal and disconnection from the internet in a world in which most activities rely on digital connectedness, do not bring a solution for this specific situation and could potentially bring more difficulties to one's work or personal activities. Research shows that these unconstructive action tendencies are associated with subjective feelings of fear (e.g., Achenbach, 1966; Fontaine et al., 2013), which was indeed one of the main reported subjective feelings in our sample. Another unconstructive action tendency is a tendency to attack or retaliate. As the attacker is mostly unknown and hard to track, the attack tendency reflects the anger emotion (e.g., Achenbach, 1966; Fontaine et al., 2013) without a space in which a related action could take place.

Regulation: both constructive and unconstructive (suppressive / relaxation: need to get the emotion under control)

Additionally, emotion regulation strategies in cybersecurity breach situations refer to both external sources like reaching for instrumental and emotional help, and internal sources like relaxation, suppression, cognitive restructuring, and rumination. Most emotion regulation mechanisms reflect active attempts to deal with the situation, such as asking others for help, to calm or control themselves and not to show signs of distress. Participants also reported an inability to deal with the situation in the form of overthinking and analyzing the situation. This reported rumination could be seen either as intrusive thinking, which can perturb sleep or concentration, or as a means to solve the situation by analyzing the factors and outcomes of the hacking situation.

The reported emotion regulation strategies can also be interpreted with respect to their constructive and unconstructive nature. In the cybersecurity breach situation, the two most frequently reported regulations, suppression and relaxation, can be seen as both constructive and unconstructive as they reflect that people feel overwhelmed and have the need to bring an emotion process under control.

In conclusion it can be said that dominant emotion processes can be interpreted in terms of fear and anger that require regulation. Psychological effects of physical security breaches such as burglary, have similarly been found to be associated with similar negative subjective feelings, such as anger, fear, anxiety, shock, guilt, confusion, stress, embarrassment, and appraisals such as concerns for the future and self-blame (Beaton et al., 2000; Chung et al., 2014). This suggests that reactions to cybersecurity breaches are akin to the experience of physical security breaches. However, what specifically characterizes cybersecurity breaches, and what is different from physical security breaches, is the powerlessness experienced by users due to knowing neither the attacker nor the scale of the consequences (Heartfield et al., 2018). In case of data breach and loss of data, it is not known who is behind the breach as well as what will happen to the data and the extent of the damage, which brings a victim in a fearful state. These specific characteristics of cybersecurity breach situations make a victim more vulnerable. Additionally, as the attacker is often anonymous, the attack is unlikely to be punished which is reflected in victims' reported powerless anger. The combination of fear and powerless anger is likely to make the situation of cybersecurity breach especially psychologically charging and it could create a risk for the development of psychopathology. In the interaction with existing vulnerabilities, withdrawal could lead to risk for depression (e.g., Alfano et al., 1994; Elmer & Stadtfeld, 2020; Katz et al., 2011) and suicide, while powerless anger

and undirected aggression could lead to suspicion and complot thinking (e.g., Inesi et al., 2012; Schaerer et al., 2021).

Implications and future research

The strong negative emotions, e.g., anger and fear, which result from the experience of cyber-security breaches can have significant consequences that may unfold over time, and themselves create and sustain more distress. Such consequences may include increased distrust, suspicion and antisocial behavior (externalization), as well as depression and anxiety (internalization) (Achenbach, 1966). To prevent the development of psychological difficulties, there is a need to analyze the underlying components of the emotion process, to assert opportunities for intervention. To be successful, such an intervention should focus on the short-term consequences and individual components of the emotion process, the proximal cause of distress.

Very different reactions can, of course, be expected, depending on the nature of the threat, the remit of the situation, the original intent of the cybersecurity breach, the cyber-physical effects of the attack, and whether the victims have any control over the situation. The five components of the emotion process has been very insightful to gain insights into cybersecurity breaches reported in this study and is expected to also be insightful for disentangling the effects of different types of attacks and their consequences for the user.

Another factor to consider are inter-individual differences, such as personality and psychopathological traits. It can be expected that the stressful experiences of cyber-security breach would increase any existing tendencies or traits. It is thus paramount to protect potentially vulnerable users and prevent the short-term (negative emotion processes followed with aggressive or withdrawing behaviors) or long-term consequences (anxiety, depression, and antisocial behaviors) of a security breach.

A successful framework to support users should involve strategies for dealing with cybersecurity breach situations. The experiences that ensue will be in reaction to a violation or the anticipation of a violation, and supportive strategies may thus include the development of mechanisms and ways to help a user mitigate the situation, by providing sources of help, to get information and psychological support, before helping the user acquire new skills, to grow confidence and resilience.

We put forward that any effort to increase the security of technology must be centered on users, and that users should be an integral element of the security chain. The present study is a first step in that direction. With a view to contributing to the description of the psychology of users and victims of cyber-crime, our work highlights the kinds of experiences and behaviors that are likely to take place. Future work should focus on specific aspects of this experience.

Limitations

Our work has several limitations. One such limitation is related to the sample consisting mainly of students and women who may only be partially representative of the huge pool of users of the internet. Recruitment of victims of cyber-crime was a challenge for the current study but is likely a challenge for any study due to several reasons. First, considering the nature of cyber-crime, it is very likely that users are often not aware of the cyber-attack itself (de Bruijn & Janssen, 2017). Second, victims may be reluctant, fearful and suspicious to share their experiences through the online media through which they have been hacked. Third shame due to the failure of not protecting themselves or their families from hacking can also make a user not willing to share their experiences. However, students form an interesting group to start exploratory research, especially also in this domain (Pyke et al., 2021).

One could also argue that the anticipated and personal emotion experiences in cybersecurity breach situations might not be comparable, or that actual and anticipated behavior may similarly be qualitatively different. However, a strong support for convergence of anticipated and experienced emotion can be expected, as shown in other work (Robinson & Clore, 2001), which concludes that vignette methodologies can play a useful role in theory construction. This indicates that emotion dynamics in both anticipated and personal experience of cybersecurity breach situation can be expected to be equivalent and sufficient for the adjustment of the GRID questionnaire for specific cybersecurity breach situations. Short of being able to interview victims of hacking *in situation*, or inducing an attack in a controlled environment, researchers will have no other choice but using vignettes studies, imagined scenarios, or rely on the fallible memory of emotional reactions to having been hacked.

Conclusions

A security breach on devices that are connected to the Internet is a negative emotional experience. Emotional experiences reflect subjective feelings of fear, anxiety, despair, sadness, shame, anger, and frustration. Additional description of emotion experiences is offered by appraisals of privacy intrusion, unknown intentions

of perpetrator or the precise nature of the consequences that could follow, no control over the outcome of the situation, fright, facing danger and insecurities. Regardless of experienced action tendencies to actively solve the situation or to withdraw and disengage, a victim is faced with the inability to act upon the experienced emotions, either due to a lack of knowledge or due to the invisibility of the intruder. The results can be used as a starting point for the further development of an instrument which can be used to examine emotion experiences of users in the cybersecurity breach domain by assessing the whole emotion process through five emotion components and emotion regulation.

Author Contributions: Conceptualization, S.B., J.R.J.F., N.M.A.H., A.H. and E.B.R.; methodology, S.B., and J.R.J.F.; formal analysis, S.B., and J.R.J.F.; investigation, S.B. and J.R.J.F; data curation, S.B.; writing—original draft preparation, S.B. and J.R.J.F; writing—review and editing, S.B., J.R.J.F., N.M.A.H., A.H., E.B.R; project administration, S.B., J.R.J.F., N. M.A.H., A.H. and E.B.R.; funding acquisition, E.B.R. J.R.J.F. and A.H. All authors have read and agreed to the published version of the manuscript.

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 according to the guidelines of the Declaration of Helsinki, and approved by the Ethics Committee of Ghent University, Faculty of psychology and educational sciences number 2016/67, date of approval: 26.10.2016, and the Ethical Research Board of Eindhoven University of Technology number 641, date of approval: 06,10.2017.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.
Data Availability Statement: Data is available upon reasonable request.

Acknowledgments: N/A

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

References

Achenbach, T. M. (1966). *The Achenbach System of Empirically Based Assessemnt (ASEBA): Development, Findings, Theory, and Applications.* Burlington, VT: University of Vermont Research Center for Children, Youth, & Families.

Alfano, M. S., Joiner, Jr., Thomas E., & Perry, M. (1994). Attributional Style: A Mediator of the Shyness–Depression Relationship? *Journal of Research in Personality*, *28*(3), 287–300. https://doi.org/10.1006/jrpe.1994.1021

Baraniuk, C. (2015). *Ashley Madison:'Suicides' over website hack.* BBC News. https://www.bbc.com/news/technology-34044506

Beaton, A., Cook, M., Kavanagh, M., & Herrington, C. (2000). The psychological impact of burglary. *Psychology, Crime & Law*, *6*(1), 33–43. https://doi.org/10.1080/10683160008410830

Canetti, D., Gross, M., Waismel-Manor, I., Levanon, A., & Cohen, H. (2017). How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks. *Cyberpsychology, Behavior, and Social Networking*. https://doi.org/10.1089/cyber.2016.0338

Chung, M. C., Stedmon, J., Hall, R., Marks, Z., Thornhill, K., & Mehrshahi, R. (2014). Posttraumatic stress reactions following burglary: The role of coping and personality. *Traumatology: An International Journal*, *20*(2), 65–74. https://doi.org/10.1037/h0099374

Connor-Smith, J. K., & Flachsbart, C. (2007). Relations between personality and coping: A meta-analysis. *Journal of Personality and Social Psychology*, *93*(6), 1080–1107. https://doi.org/10.1037/0022-3514.93.6.1080

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2017.02.007

Elmer, T., & Stadtfeld, C. (2020). Depressive symptoms are associated with social isolation in face-to-face interaction networks. *Scientific Reports*, *10*(1), 1444. https://doi.org/10.1038/s41598-020-58297-9

Fontaine, J. R. J., Scherer, K. R., & Soriano, C. (Eds.). (2013). *Components of Emotional Meaning: A sourcebook*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199592746.001.0001

Frijda, N. H. (1986). *The Emotions*. Cambridge University Press.

Gross, J. J. (2002). Emotion regulation: Affective, cognitive, and social consequences. In *Psychophysiology*. https://doi.org/10.1017/S0048577201393198

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*. https://doi.org/10.1080/00963402.2016.1216502

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyw018

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R. J., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, *78*, 398–428. https://doi.org/10.1016/j.cose.2018.07.011

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*. https://doi.org/10.1016/j.ijlcj.2016.07.002

Inesi, M. E., Gruenfeld, D. H., & Galinsky, A. D. (2012). How power corrupts relationships: Cynical attributions for others' generous acts. *Journal of Experimental Social Psychology*, *48*(4), 795–803. https://doi.org/10.1016/j.jesp.2012.01.008

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. *Cyberpsychology, Behavior, and Social Networking*. https://doi.org/10.1089/cyber.2016.0728

Katz, S. J., Conway, C. C., Hammen, C. L., Brennan, P. A., & Najman, J. M. (2011). Childhood Social Withdrawal, Interpersonal Impairment, and Young Adult Depression: A Mediational Model. *Journal of Abnormal Child Psychology*, *39*(8), 1227–1238. https://doi.org/10.1007/s10802-011-9537-z

Kopecký, K., & Szotkowski, R. (2017). Cyberbullying, cyber aggression and their impact on the victim – The teacher. *Telematics and Informatics*. https://doi.org/10.1016/j.tele.2016.08.014

Lazarus, R. S. (1993). From Psychological Stress to the Emotions: A History of Changing Outlooks. *Annual Review of Psychology*, *44*(1), 1–22.

Loukas, G. (2015). Cyber-Physical Attacks: A Growing Invisible Threat. In *Cyber-Physical Attacks*. https://doi.org/10.1016/B978-0-12-801290-1.00008-4

Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., Vainio, N., & Myllymäki, P. (2012). Long-term effects of ubiquitous surveillance in the home. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*. https://doi.org/10.1145/2370216.2370224

Pyke, A., Rovira, E., Murray, S., Pritts, J., Carp, C. L., & Thomson, R. (2021). Predicting individual differences to cyber attacks: Knowledge, arousal, emotional and trust responses. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *15*(4). https://doi.org/10.5817/CP2021-4-9

Qualtrics. (2017). *Qualtrics*. Qualtrics.

Robinson, M. D., & Clore, G. L. (2001). Simulation, scenarios, and emotional appraisal: Testing the convergence of real and imagined reactions to emotional stimuli. *Personality and Social Psychology Bulletin*. https://doi.org/10.1177/01461672012711012

Schaerer, M., Foulk, T., du Plessis, C., Tu, M.-H., & Krishnan, S. (2021). Just because you're powerless doesn't mean they aren't out to get you: Low power, paranoia, and aggression. *Organizational Behavior and Human Decision Processes*, *165*, 1–20. https://doi.org/10.1016/j.obhdp.2021.03.005

Scherer, K. R. (2001). Appraisal Considered as a Process of Multilevel Sequential Checking. In *Appraisal process in emotion: Theory, Methods, Research*. https://doi.org/10.1007/s10566-008-9057-3

Symantec. (2010). *The Norton Online Family Report*. https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/nofr/Norton_Family-Report-USA_June9.pdf

Symantec. (2011). CYBERCRIME REPORT 2011. *World*.

Symantec. (2018). *2017 Norton Cyber Security Insights Report—Global Results*. 30.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160. https://doi.org/10.1016/j.dss.2019.113160

Watkins, E., Moulds, M., & Mackintosh, B. (2005). Comparisons between rumination and worry in a non-clinical population. *Behaviour Research and Therapy*, *43*(12), 1577–1585. https://doi.org/10.1016/j.brat.2004.11.008

Williams, E., Slade, E., & Hodges, D. (2020). *Individual differences in the adoption and secure use of smart home technology*. In British Academy of Management Conference: BAM2020 Conference In The Cloud, Online.