

Emotional Experiences of Cybersecurity Breach Victims

Sanja Budimir, PhD,^{1,2,i} Johnny R.J. Fontaine, PhD,¹ and Etienne B. Roesch, PhD³

Abstract

This study investigated emotional reactions to cybersecurity breaches. Based on prior research, a context-specific instrument was developed. This new instrument covered all five emotion components identified by the componential emotion approach. In total, 145 participants that experienced a cybersecurity breach reported on their appraisals, action tendencies, bodily reactions, expressions, subjective feelings, and regulation attempts. A principal component analysis on a total of 75 emotion reactions revealed a clear three-dimensional structure. The first dimension represented the extent to which the person was generally emotionally affected. The second dimension revealed constructive action tendencies and subjective feelings that were opposed to unconstructive action tendencies, expressions, and bodily reactions. The third dimension revealed cognitive motivational reactions that were opposed to affective reactions. This study clearly indicated that cybersecurity breaches do not only form a challenge for engineers, but also have important psychological ramifications that need to be addressed. Although some people have a tendency to react with constructive and proactive actions that are likely to limit the negative consequences of the cybersecurity breach, others experience a strong negative affective stress reaction and are unlikely to take the appropriate steps to deal with the security breach situation. These people, especially, can be expected to be vulnerable to psychological complaints and possibly psychopathology. The newly developed instrument uses a comprehensive approach to assess emotional reactions to cybersecurity threats and provides an efficient way to identify potentially problematic reactions.

Keywords: cybersecurity breach victims, emotion processes, componential emotion approach

Introduction

IN 2019, THE 50TH ANNIVERSARY of the Internet was celebrated.¹ For a long time, its invention has been welcomed with unbridled enthusiasm, as it created unprecedented possibilities for the interconnectedness of people. However, the increasing interconnectedness also entails an increasing vulnerability to cybersecurity breaches (unauthorized access and manipulation of information through the cyberspace). Governments have identified cybersecurity as one of the main challenges of our connected society, with the possibility for substantial negative economic impact (e.g., Eur Lex²).

The challenges, though, are not only technological, societal, or economical, but also psychological. Cybersecurity breaches can prevent the pursuit of individual goals in many areas of life. They can, therefore, be considered to be pow-

erful situational antecedents for negative emotions.^{3–5} Negative emotions, such as anxiety, anger, sadness, and insecurity, have in a few studies already been found to be associated with cybersecurity attacks.^{6–10} However, the emotional experiences themselves have not yet been the focus of scientific research, although they can be considered to be the first psychological reaction to these breaches and play a key role in possible long-term consequences. In this study, we investigate the structure of emotion processes in the context of cybersecurity breaches. We go beyond studying feelings, such as negative affectivity, and also take into account appraisals (cognitive), action tendencies (motivational), expressions (face, voice, and gestures), and bodily reactions (physiological), as well as regulation mechanisms people can use to deal with their emotional processes that jointly make up the emotion process

¹Department of Work, Organisation and Society, Ghent University, Ghent, Belgium.

²Department for Psychotherapy and Biopsychosocial Health, Danube University Krems, Krems an der Donau, Austria.

³Centre for Integrative Neuroscience and Neurodynamics, School of Psychology and Clinical Language Sciences, University of Reading, Reading, United Kingdom.

ⁱORCID ID (<https://orcid.org/0000-0002-4110-9112>).

Portions of these findings were presented as an oral presentation at the 15th European Conference on Psychological Assessment in Brussels, Belgium.

© Sanja Budimir *et al.* 2021; Published by Mary Ann Liebert, Inc. This Open Access article is distributed under the terms of the Creative Commons Attribution Noncommercial License [CC-BY-NC] (<http://creativecommons.org/licenses/by-nc/4.0/>) which permits any non-commercial use, distribution, and reproduction in any medium, provided the original author(s) and the source are cited.

(componential emotion approach^{4,5,11}). Moreover, we investigate how these emotion processes are affected by age, gender, and type of hacking experience.

Materials and Methods

Sample

As the internal structure is investigated with principal component analysis (PCA), for which a sample size of 150 observations is recommended,¹² 150 victims of cyberattacks were recruited through a Qualtrics panel in the United Kingdom.

Five participants were excluded from further analyses because they frequently used the same response category to an exceptional degree (75% or more across all items). This was done because nondifferentiation is one of the strongest indicators for lack of validity in responses.¹³ In the remaining sample, there were 49.7% females, the mean age was 35.47 years and ranged from 18 to 65 years old, 79% were employed, 8% were studying, 7% were unemployed, 5% were unable to work, and 1% were retired.

Instrument

To assess the emotion features that characterize emotion processes in the context of cybersecurity breaches, we constructed the Cybersecurity GRID, which is an adjusted version of the GRID questionnaire¹¹ (Supplementary Data S1). In total, 18 appraisals, 16 action tendencies, 8 bodily reactions, 11 expressions, 14 feelings, and 8 regulation strategies were selected for the questionnaire. Participants rated the degree to which each emotion feature described their own experience on a 7-point scale ranging from 1 (strongly disagree) to 7 (strongly agree).

Procedure

Members of the Qualtrics panel¹⁴ received a screening question about whether they had been a victim of a cybersecurity breach in the past (related to a device or an account). If this was the case, participants were asked to briefly describe the cybersecurity breach they experienced and to report on all components of their emotional reaction using the Cybersecurity GRID questionnaire.

Ethical approval

Ethical approval for studies run in the EU FP7 CHIST-ERA project “Cocoon: Emotion psychology meets cyber security,” of which this study is a part, was obtained from the ethical committee of Ghent University, Faculty of Psychology and Educational Science, number 2016/67.

Results

Emotion features of the Cybersecurity GRID questionnaire were found to be relevant for describing the actual experiences of cybersecurity breaches. Across all reported types of cybersecurity breaches, the average score for all items was 4.64 on a scale from 1 to 7 (Supplementary Data S2). On average, across items, 38.98% of the victims selected a response of 6 or 7, indicating that the items described their emotional experiences well in general (for more information see Table S1 in Supplementary Data S2).

Since this was an exploratory study in an uncharted area of emotional experiences, PCA was used to identify the major dimensions of variability among the 75 emotion reactions. Bartlett’s test of sphericity was significant [$\chi^2(2,775)=9630.68, p<0.001$] and the Kaiser–Meyer–Olkin was high (KMO=0.86), both indicating adequacy of PCA. Based on the CHull criterion, which offers a new method for identifying the number of dimensions in PCA that optimally balances goodness of fit/misfit and model complexity,^{15,16} three components were selected (Supplementary Data S3). A well interpretable structure was identified (see Table 1 for the 10 highest loading features on each principal component, Fig. 1 for the plot of the loadings on the second and third dimension, Supplementary Data S4 for a justification of the selected rotation, and Table S2 in Supplementary Data S5 for the full loading matrix).

To avoid confusion between “emotion components” from a substantive point of view and “principal components” in the PCA, the principal components will be referred to as dimensions in the remainder of the text.

On the first dimension, all emotional reactions loaded positively. This dimension can be interpreted as an emotional intensity dimension and accounted for 24.14% of the variance. The second dimension was a bipolar dimension with one pole being characterized by tendencies to solve the problem and subjective experiences and the opposite pole being characterized by tendencies to withdraw or attack as well as bodily reactions and expressions. It accounted for 8.15% of the variance. On the third—also bipolar—dimension, a distinction was observed between subjective experiences, bodily reactions, and expressions on the one hand, and appraisals and action tendencies on the other hand. It accounted for 5.34% of the variance. Only emotion regulation strategies, which loaded positively on the first dimension, were neither well differentiated on the second nor on the third dimension.

Victims reported a set of heterogeneous cybersecurity breaches with respect to their social network accounts (30.3%), email accounts (29.0%), computer (20.0%), financial accounts (11.0%), smartphone (6.2%), and tablet (3.4), which makes a total of 29.7% breaches on devices and 70.3% on accounts.

We examined the effects of types of cybersecurity breaches, age, and gender on the three identified dimensions. It was found that older participants reported more emotional reactions in general [$F(1, 8)=4.756, p=0.031$], and that breaches on a social network account generated the most emotional reactions in general, whereas breaches on an email account generated the least [$F(1, 8)=3.063, p=0.030$]. Women reported more constructive reactions than men [$F(1, 4)=5.135, p=0.025$], and more constructive reactions were reported when accounts were involved compared with devices [$F(1, 4)=7.257, p=0.008$].

Discussion

Although it is the first time that not only feelings, but also all components of the emotion process, were investigated exploratively in the context of cybersecurity breaches, highly systematic and well-interpretable results were observed. Both the mean scores and the coherent correlational structure indicated that the emotion features from all components

TABLE 1. RESULTS FROM PRINCIPLE COMPONENT ANALYSIS OF THE CYBERSECURITY GRID QUESTIONNAIRE

Emotion feature item	Dimension loading		
	D1	D2	D3
General emotion dimension			
ER8 I had trouble concentrating.	0.75	-0.07	-0.25
ER7 I could not stop thinking and analyzing the situation.	0.74	-0.06	-0.17
A9 I thought: "The security of people close to me could be jeopardized."	0.73	0.00	0.30
SF2 I experienced the emotional state for a long time.	0.73	0.21	-0.37
SF4 I felt afraid.	0.72	-0.11	-0.37
SF1 I was in an intense emotional state.	0.71	0.08	-0.46
SF5 I felt panic.	0.70	-0.24	-0.38
SF7 I felt worried.	0.69	-0.45	-0.22
A7 I thought, "My trust is betrayed."	0.69	-0.06	0.17
A16 I thought, "Someone could destroy my data."	0.68	-0.14	0.36
Unconstructive action tendencies			
AT14 I wanted to destroy whatever was close.	0.48	0.65	0.07
AT5 I wanted to isolate myself physically.	0.45	0.60	0.04
BR4 I had pain in the chest.	0.47	0.59	-0.32
AT4 I wanted to stop using devices that are connected to the Internet.	0.39	0.47	0.31
AT15 I wanted to take revenge.	0.48	0.47	0.02
Constructive action tendencies			
AT7 I wanted to change my privacy settings.	0.37	-0.51	0.16
AT9 I wanted to find a solution and fix the problem.	0.23	-0.64	0.20
AT1 I wanted to stop what was happening.	0.27	-0.65	0.05
AT3 I wanted to protect myself.	0.32	-0.66	0.17
AT2 I wanted to regain control over the device/account.	0.20	-0.71	0.20
Cognitive and motivational			
A2 I thought, "I wonder whether something is wrong with the device/account."	0.53	-0.02	0.45
A14 I thought, "I could lose personal information, data and documents."	0.52	-0.42	0.42
A4 I thought "My data are not available anymore"	0.53	0.25	0.42
A19 I thought, "It is not safe that this device is connected to the Internet."	0.58	0.18	0.40
A1 I thought, "I do not know what is happening."	0.53	-0.04	0.37
Affective			
BR11 My body became hot.	0.62	0.19	-0.45
BR6 My heartbeat was faster.	0.67	-0.14	-0.45
BR8 My muscles were tense.	0.61	0.11	-0.48
E4 I had a trembling voice.	0.57	0.11	-0.49
BR7 My breathing was faster.	0.63	0.06	-0.52

Bold values are the highest loading features on each dimension.

Loadings of the 10 emotional reactions that each defines best the general emotion dimension (D1), the constructive versus unconstructive dimension (D2), and the cognitive/motivational versus affective dimension (D3).

A, appraisal; AT, action tendencies; BR, bodily response; E, expression; SF, subjective feeling, and numbers indicate number of the items in the GRID questionnaire. All labeled items are listed in the Supplementary Data S5 and Supplementary Table S2.

included in the Cybersecurity GRID are relevant to describe emotion processes in this domain. Moreover, the identified structure can be very well interpreted based on existing research in other domains of emotions, affect, and coping.

On the first dimension, features from all emotion components loaded positively. Features from the feeling component were among the highest loading ones. This means that the first dimension strongly resembles the negative affectivity dimension of the well-known positive affect negative affect scale¹⁷, which exclusively relies on feeling and affect items. The contribution of studying all emotion components to represent the full emotion process^{5,11} can be found, however, in the two additional dimensions that give insight into the nature of the negative emotion processes during cybersecurity breaches.

On the second dimension, solution-oriented action tendencies were opposed to attack and withdrawal action tendencies. In the context of cybersecurity breach, solution-

oriented action tendencies can be considered constructive, as they help to deal with the situation and its consequences. Attack and withdrawal action tendencies can be considered unconstructive as the perpetrator often is not known in this context. Aggressive-oppositional action tendencies cannot lead to meaningful action. In addition, since an important part of our lives is now taking place online, withdrawing would imply a substantial loss of social contacts and/or work efficiency. The prominent role for action tendencies for differentiating emotional experiences is in line with the theoretical claim that action tendencies form the most important emotion component from a functional evolutionary perspective.³ The function of emotion processes is to prepare for action. At first glance, it might seem surprising that solution-oriented action tendencies and negative subjective experiences jointly characterize the same pole of this dimension. This observation, however, can be interpreted in the light of recent research on emotional competences and

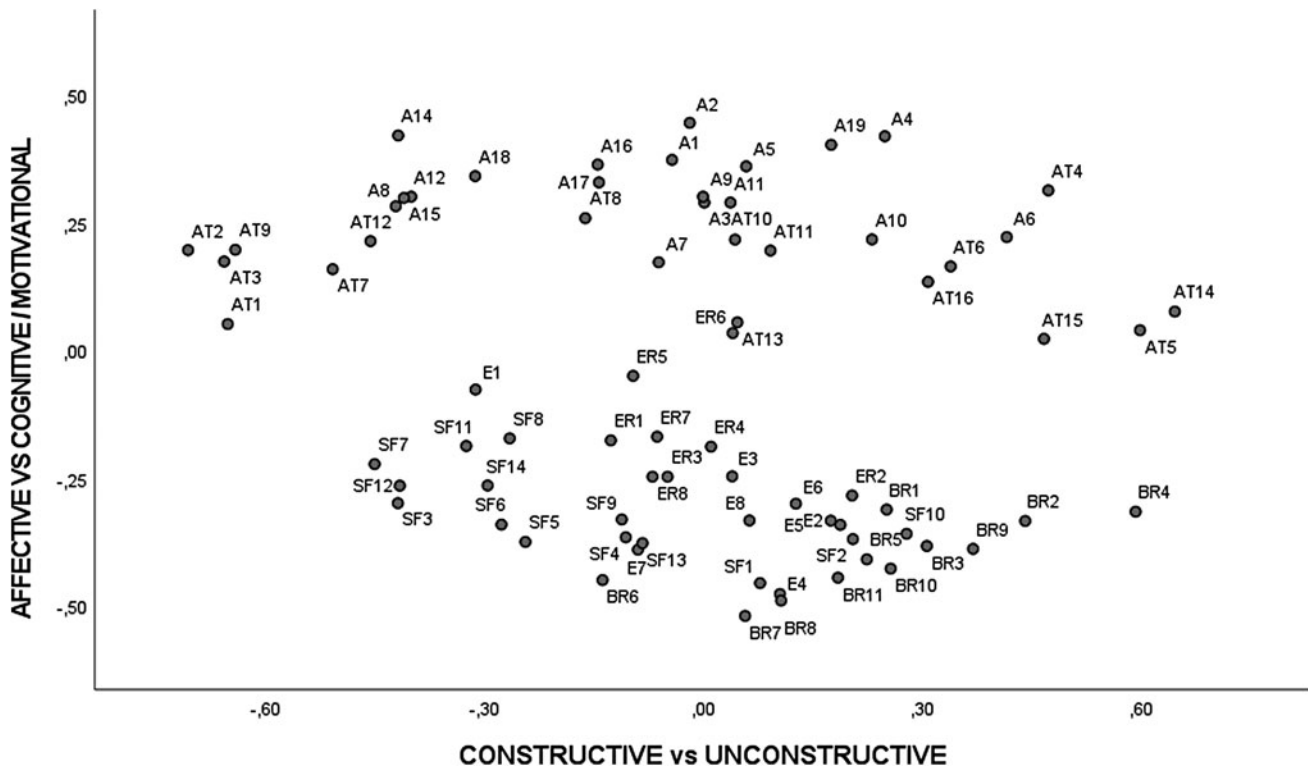


FIG. 1. Plot of the emotional reactions on the second and third dimensions as a function of the emotional component they belong to.

emotional intelligence. There it has been demonstrated that emotional awareness¹⁸ and understanding¹⁹ have positive effects on emotional functioning.^{20,21} Awareness of one's own negative emotional reactions might help to strengthen constructive solution-oriented action tendencies. The observation that the pole of unconstructive action tendencies matches with expressions and bodily reactions can be interpreted in terms of a strong stress reaction that demonstrates the lack of coping possibilities of the victim.^{22,23}

On the third dimension, cognitive and motivational reactions are opposed to affective reactions. When the second and the third dimension are taken together, the opposition of the left upper quadrant (characterized by constructive action tendencies), and the lower right quadrant (characterized by expressions and bodily reactions), can be interpreted by the distinction that is made in the coping literature between problem-focused and emotion-focused coping.²⁴ Based on previous findings in the stress and coping research that demonstrated positive psychological outcomes for problem-focused coping, and negative outcomes for emotion-focused coping, it can be predicted that people who react with strong expressions and bodily reactions to cybersecurity breaches are at risk to develop long-term consequences, and that those who react with constructive action tendencies can be expected to be buffered from these effects.

The relationships with age, gender, and type of security breach indicate that the nature of emotional reactions in this domain is sensitive to personality characteristics and the precise nature of the breach situation one is experiencing. Interestingly, participants reported the strongest emotional

reactions to the hacking of social network accounts. Apparently, an important issue in this domain is not only being hampered in one's daily activities or the privacy intrusion itself, but also the possibility of one's privacy being exposed to a large group of people. The observation that more constructive reactions were observed when accounts were hacked compared with devices could be accounted for by differences in how feasible constructive actions are perceived. Although social accounts have a procedure to deal with security breaches that are rather easily available, it is much less clear who to contact and what to do in case of a security breach of one's device.

It can be concluded that dealing with cybersecurity threats not only requires technological innovations by engineers, but also necessitates the development of emotional support systems that can avoid negative long-term psychological consequences. This study clearly demonstrates that cybersecurity breach situations elicit negative emotional reactions. With the Cybersecurity GRID, emotional reactions to cybersecurity breaches can now be comprehensively assessed, and this can help us in the future to identify who is at risk of developing negative psychological outcomes, as well as which personality characteristics and which context factors can help to buffer these effects.

Authors' Contributions

S.B., J.R.J.F., and E.B.R. have substantially contributed to the conception and design of the study, analysis, and interpretation of data for the study. J.R.J.F. and S.B. drafted the

article and E.B.R. revised it critically for important intellectual content. All three authors have approved the final version to be published and agree to be accountable for all aspects of the study in ensuring that questions related to the accuracy or integrity of any part of the study are appropriately investigated and resolved.

Acknowledgment

Many thanks to native speaker Arpine Hovasapian, PhD for English proofreading the article and for her valuable contribution to the article.

Author Disclosure Statement

No competing financial interests exist.

Funding Information

This study is part of a larger research project: Emotion psychology meets cybersecurity in IoT smart homes, 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 GOH6416N).

Supplementary Material

Supplementary Data S1
Supplementary Data S2
Supplementary Data S3
Supplementary Data S4
Supplementary Data S5

References

1. Abbruzzese J. (2019) On the 50th anniversary of the birth of the internet, technologists balance optimism and warnings. NBC news. <https://www.nbcnews.com/tech/tech-news/50th-anniversary-birth-internet-technologists-balance-optimism-warnings-n1073206> (accessed Nov. 5, 2019).
2. Eur Lex. (2017) Report from the commission to the European Parliament and the Council. EUROPA EUR-Lex home EUR-Lex—52017DC0474—EN. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017DC0474> (accessed May 7, 2021).
3. Frijda NH. (1986) *The emotions*. Cambridge: Cambridge University Press.
4. Frijda NH. Impulsive action and motivation. *Biological Psychology* 2010; 84:570–579.
5. Scherer KR. (2001) Appraisal considered as a process of multilevel sequential checking. In Scherer KR, Schorr A, Johnstone T, eds. *Series in affective science. Appraisal processes in emotion: Theory, methods, research*. Oxford: Oxford University Press, pp. 92–120.
6. Canetti D, Gross M, Waismel-Manor I, et al. How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. *Cyberpsychology Behavior, and Social Networking* 2017; 20:72–77.
7. Gross ML, Canetti D, Vashdi DR. The psychological effects of cyber terrorism. *Bulletin of the Atomic Science* 2016; 72:284–291.
8. Gross ML, Canetti D, Vashdi DR. Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity* 2017; 3: 49–58.
9. Kopecký K, Sztokowski R. Cyberbullying, cyber aggression and their impact on the victim—The teacher. *Tele-matics and Informatics* 2017; 34:506–517.
10. Symantec. (2010) The Norton Online Family Report. <https://www.broadcom.com/404-symantec> (accessed Mar. 30, 2018).
11. Fontaine JRJ, Scherer KR, Soriano C, eds. (2013) *Components of emotional meaning: A sourcebook*. New York: Oxford University Press
12. Guadagnoli E, Velicer WF. Relation of sample size to the stability of component patterns. *Psychological Bulletin* 1988; 103:265–275.
13. Roberts C, Gilbert E, Allum N, et al. Research synthesis. *Public Opinion Quarterly* 2019; 83:598–626.
14. Qualtrics PU. (2018) Qualtrics. <https://www.qualtrics.com>
15. Ceulemans Eva, Kiers HAL. Selecting among three-mode principal component models of different types and complexities: a numerical convex hull based method. *British Journal of Mathematical and Statistical Psychology* 2006; 59:133–150.
16. Wilderjans TF, Ceulemans E, Meers K. CHull: a generic convex-hull-based model selection method. *Behavior Research Methods* 2013; 45:1–15.
17. Watson D, Clark LA, Tellegen A. Development and validation of brief measures of positive and negative affect: The PANAS Scales. *Journal of Personality and Social Psychology* 1988; 54:1063–1070.
18. Rosenberg M, Chopra D. *Nonviolent communication: A language of life, 3rd Edition: Life-changing tools for healthy relationships*. Encinitas, CA: PuddleDancer Press, 2015.
19. Izard CE, Woodburn EM, Finlon KJ, et al. Emotion knowledge, emotion utilization, and emotion regulation. *Emotion Review* 2011; 3:44–52.
20. Izard CE, King KA, Trentacosta CJ, et al. Accelerating the development of emotion competence in Head Start children: effects on adaptive and maladaptive behavior. *Development and Psychopathology* 2008; 20:369–397.
21. Lane RD, Quinlan DM, Schwartz GE, et al. The levels of emotional awareness scale: A cognitive-developmental measure of emotion. *Journal of Personality Assessment* 1990; 55:124–134.
22. Chrousos GP. Stress and disorders of the stress system. *Nature Reviews Endocrinology* 2009; 5:374–381.
23. Wang X, Shangguan C, Lu J. Time course of emotion effects during emotion-label and emotion-laden word processing. *Neuroscience Letters* 2019; 699:1–7.
24. Lazarus RS, Folkman S. (1984) *Stress, appraisal, and coping*. New York: Springer Publishing Company.

Address correspondence to:

Dr. Sanja Budimir

Faculty of Psychology and Educational Sciences

Department of Work, Organisation and Society

Ghent University

Henri Dunantlaan 2

Ghent 9000

Belgium

E-mail: sanja.budimir@ugent.be