AMCIS 2024 Proceedings

Americas Conference on Information Systems (AMCIS)

August 2024

Can Mental Health Affect InfoSec Behavior?

Naomi Woods
University of Jyväskylä, naomi.woods@jyu.fi

Hanna Paananen
University of Jyvaskyla, hanna.k.paananen@jyu.fi

Can Mental Health Affect InfoSec Behavior?

Emergent Research Forum (ERF) Paper

Naomi Woods
University of Jyväskylä
naomi.woods@jyu.fi

Hanna Paananen
University of Jyväskylä
hanna.k.paananen@jyu.fi

Abstract

Organizations have significant financial losses every year due to insider threats. These are caused by employees' malicious or accidentally weak information security (infosec) behavior, such as poor password security practices. Previous research has examined employees' insecure behaviors from many perspectives. However, individual factors such as employees' mental health have only been briefly considered in the infosec context. Depression and anxiety are very common within the global population, with a range of symptoms and severity of symptoms that could potentially affect an employee's infosec behavior. With little research in this area, it is important to understand the impact of these factors through empirical examination. A mixed-method study aims to examine depression and anxiety in the infosec context using psychological evaluation tools and interviews. The results will have important implications for research and practice, and especially for professionals who create and develop methods to improve infosec behavior within the organizational context.

Keywords

Information security behavior, Mental health, Depression, Anxiety, Security threats.

Introduction

Organizations spend sizable budgets every year in minimizing information security (infosec) threats (Hwang and Cha 2018). Infosec budgets are increasing every year due to a growing numbers of security breaches, with information being leaked and consequently leading to organizations' financial and reputational losses (Hwang and Cha 2018). Within an organization, employees are often considered the weakest link in the infosec chain (Warkentin and Willison 2009). Employees pose a serious threat to infosec (Warkentin and Willison 2009), with organizations finding it difficult to avoid or prevent security threats due to the complexity and difficulty in monitoring or controlling an employee's actions. Therefore, organizations make significant investments in protective infosec technology. However, to improve security awareness and improve infosec hygiene, organizations need to equally invest in the employees too (Hwang and Cha 2018). Previous researchers have approached these issues from several psychological perspectives to understand employees. However, there are still numerous gaps in this area of research.

Previous research and proposed study motivations

Previous research suggests that security threats comprise mainly of harm caused by employee malicious, negligent, or accidental poor security behaviors (Crossler et al. 2013). These behaviors can include, abusing privileges, using unauthorized devices, intentionally/unintentionally leaking sensitive information, not backing up data, clicking on suspicious links in emails, reusing the same password for organizational and personal accounts (Guo et al. 2011). Previous infosec researchers have examined organizational security threats, employees' infosec behavior, and factors that may influence it by applying psychological theories for example, to create persuasive messaging (Johnston et al. 2019), provide security behavior awareness training and education (Hu et al. 2022), and using deterrence (DT) as means to encourage users improve their security hygiene (Warkentin and Willison 2009). In more recent times, researchers have examined employees' individual factors/difference, such as, personality gender, age, and culture, and their effect on infosec behavior (e.g., Egelman and Peer 2015; Shropshire et al. 2015; Vance et al., 2022). One area of individual differences that has had very little consideration in the infosec context is employees' mental health. Mental health is an important factor as symptoms of mental health conditions are well-documented in affecting peoples' behavior (APA 2013). Addressing this research gap is even more critical when considering the number of people (and employees) that experience symptoms from mental health disorders (25% of global population (WHO 2001)), and more specially, some level of symptoms of anxiety and/or depression (the two most common conditions (WHO 2019)).

Depression and Anxiety

A high proportion of the world's population have experienced symptoms of a mental health condition (WHO 2001). These disorders have varying symptoms, with varying severities. However, a person can still experience symptoms without having the clinical condition (APA 2013).

Depressive disorder (depression) is one of the most common mood disorders. It can be generally characterized by a depressed mood and/or loss of interest or pleasure in activities for long periods of time (WHO 2019). Symptoms can include, sadness, emptiness, socially withdrawn, physically slow, and many more. Cognitive impairments, such as difficulties in concentration, learning and memory, thinking and making decision, are often accompany these affective symptoms. These symptoms can vary from person to person with varying degrees of severity (mild, moderate, and severe) and duration (experienced nearly every day for at least two weeks) (Black and Grant 2014).

Anxiety disorders include characteristics of excessive fear and anxiety, and related behavioral disturbances that significantly impact lives (APA 2013). There are several different anxiety disorders with generalized anxiety disorder (GAD) being one of the most prevalent with symptoms of persistent and excessive uncontrollable worry and anxiety. The experienced anxiety is often irrational or more excessive than the threat deserves (Black and Grant 2014). There are many emotional and cognitive impairment symptoms, include feelings of panic, paranoia, depression, and some can experience stimming, stuttering, loss of concentration and memory, and adopting avoidance behaviors as a coping strategy (Woods 2022).

Although the symptoms of depression and anxiety for many can be debilitating; there are many people whose symptoms cause difficulties and impact their daily routines and aspects of their lives (such as work) but are still able to continue with a relatively normal life (APA 2013; WHO 2019). Therefore, it is important to understand how anxiety and depression symptoms present themselves, and how they can manifest within the infosec context while employees enact infosec behaviors. For instance, symptoms experienced by an employee could potentially increase their vulnerability (and consequently, their organization's vulnerabilities), in becoming a victim of a data breach (Woods 2022).

How can depression and anxiety have an impact on information security?

Previous research has examined mental health and infosec from a limited number of perspectives. The majority of research has explored how technostress or security-related stress can impact infosec behavior and information security policies (ISPs) compliance (D'Arcy and Teh 2019; Hwang and Cha 2018; Nasirpouri et al. 2020), and vice versa (Ali and Dominic 2022; Lee et al. 2016).

Symptoms of depression and anxiety can be experienced by employees while in a working environment. People with depression can have slow cognitive processes, and find themselves distracted and consumed by their symptoms (Black and Grant 2014). Even with mild symptoms, depression could affect a person while working, which could affect their security behavior (not necessarily intentionally), and becoming passive towards or being unaware any signs of criminal activity or attack. A conceptual study by Woods (2022), theorized using a clinical psychological lens, how the symptoms of different mental disorders could affect users' vulnerabilities to cybercrimes, and affect their cybersecurity practices (summarized in Table 1). The study's observations could be extended to the organizational setting, and suggest that depression could cause employees to have poor security behaviors, such as clicking on suspicious links, and visit insecure websites due to impaired judgement and decision-making processes (Donalds and Osei-Bryson 2020). They may also adopt insecure password behaviors, such as reusing due to memory impairments and forgetting passwords. Moreover, memory, concentration, and decision-making impairments could also result in passive inactivity to software, application, and security patch updates, all resulting in increased vulnerability (Woods, 2022). Additionally, the findings of a large-scale study by Kyytsönen et al. (2022) led them to suggest that depression could negatively affect an individual's perceptions of their own infosec skills. However, they suggested that further research is needed to conclude if depression actually affected their skills, or whether the depression affected their perception of their skills.

Mental Disorder	Brief description, example symptoms	Vulnerabilities to cybercrimes	Cyber security behaviors: secure or insecure behaviors
Depressive disorder	Feeling of sadness. Loss of pleasurable feelings. Physical and cognitive slowness (inc. memory loss, poor decision making). Avoidance behaviors, social withdrawnness.	Social engineering: victim Online harassment: victim Identity-related crimes: victim Hacking: victim DoS attack: victim	Password management: insecure Oversharing info: secure /insecure Proactive security behaviors: insecure Backing-up info: insecure
Anxiety disorders	Excessive fear and anxiety. Feelings of worry, panic, paranoia. Cognitive slowness, inc. memory loss, and poor decision making. Avoidance behaviors. Depression.	Social engineering: victim Online harassment: victim Identity-related crimes: victim Hacking: victim DoS attack: victim	Password management: insecure Oversharing info: secure /insecure Proactive security behaviors: secure/insecure Backing-up info: insecure

Table 1. Summary of depression and anxiety symptoms, vulnerability to cybercrimes, and cybersecurity behaviors.

As anxiety disorders often cause increased attention and strong responses to potential threats, could a slight increase in hypervigilance be helpful? Woods (2022) suggested that this may not be the case within the organizational context (summarized in Table 1). Some people may develop phobias towards new technologies and feel paranoid towards technology monitoring and invading their privacy within the work setting. Due to anxiety, excessive worry could leave employees vulnerable to several cybercrimes, such as social engineering (Welk et al. 2015), where criminals could manipulate and prey upon their insecurities. As with depression, employees with anxiety disorders can often have loss of concentration, leading to errors in judgment such as clicking on suspicious links in emails, and through loss of memory, could adopt insecure password behaviors to cope. Employees with anxiety symptoms could also become easily overwhelmed by too much and too complex information to process, which may lead many to ignore communications and adopt avoidance behaviors. Being overwhelmed and therefore avoiding for instance, security messages, could result in employees not recognizing or responding to communications that their security (or that of the organization's) is being threatened (Woods 2022). Employees may become passive towards protecting their systems' and their organization's security while experiencing an anxiety disorder.

It is unclear how symptoms of depression and anxiety affect employees and interact with their infosec behavior. Therefore, the objective of this study is to gain an in-depth understand of how employees' mental health can affect the security of an organization, and how symptoms of depression and anxiety can affect employees' infosec behavior. In this study we will examine employees' attitudes towards their infosec behavior, their understanding and awareness of organization's infosec culture, and explore their experiences towards protecting their organization while experiencing depression and/or anxiety. We will conduct research that aims to answer these research questions:

- RQ1: What symptoms of depression and anxiety can lead to insecure infosec behavior?
- RQ2: How does the severity of the symptoms effect insecure infosec behavior and in what way?
- RQ3: How do employees with symptoms of depression and/or anxiety feel about protecting their organization when experiencing their symptoms?
- RQ4: Are there aspects of infosec procedures/technology/communication that can be adapted to ensure security when employees have symptoms of depression and/or anxiety?

Proposed research methods: Mixed-methods study

Participants will be recruited from a variety of organizations. The sample will include employees who undertake infosec behaviors within their organizational roles, and experience symptoms of depression and/or anxiety at some level of severity. Due to this mixed-methods study taking a more qualitative approach, we will aim to recruit 15-25 employees (or more until saturation has been reached).

Due to the sensitive nature of the factors being measured, ethical considerations will be taken into account, and ethical clearance from the institution's ethical committee will be sought. Participants' consent will be obtained, information including privacy policies are provided to the participants, and data collected is kept confidential and coded.

Quantitative data collection: the Hospital Anxiety and Depression Scale (HADS) (Zigmond and Snaith 1983) will be used to measure the participants' anxiety and depression levels. The HADS is a reliable and widely used tool, developed with the purpose of detecting and measuring anxiety and depression mainly for the clinical setting. However, in addition to measuring clinical levels of depression and anxiety, it also detects non-clinical severity levels (Crawford et al. 2001), and has been used in organizational contexts (Bocéréan and Dupret 2014). The HADS is a self-assessment scale with 14 items which form the questionnaire: seven items measuring depression and anxiety. HADS will be completed by all participants to understand what symptoms and severity of depression and/or anxiety they experience. After this study, the questionnaire responses will be coded, calculated, and analysed. Participants will be informed of their results, with support offered to those who require it. In addition to the HADS items, preliminary questions regarding the participants' infosec behaviours will help gauge the level of interaction the participants have within their daily organizational roles.

Qualitative data collection: semi-structured interviews will be conducted using questions that are based on the literature, and established guidelines (Myers 2013). Interviews are often chosen as means to collect data in qualitative research "since they enable researchers to step back and examine the interpretations of their fellow participants in some detail" (Walsham, 1995, p. 78). We will ask the participants to openly respond to questions regarding their symptoms of depression and/or anxiety, the severity, and their experiences guided by the previously answered questions from the HADS. Further questions will centre around their infosec behaviour, and attitudes towards securing their organization. We aim to use a laddering technique to encourage the participants to find any subconscious connections between their symptoms and their security behavior. After which, additional questions will focus on support for the participants, asking about if and what ways in which they feel their organizations could adapt to be more inclusive towards their needs, and whether there are any factors, e.g., procedures or technology that can support and improve their security practices within their organizations.

All interview data will be transcribed and coded by at least two coders guided by verified data analysis methods (Myers 2013). The data will be analyzed using content analysis due to having a background knowledge and understanding of the topic we are exploring.

Conclusion

Building on previous research, this study applies a clinical psychological lens, strives to understand what and how symptoms of employees' depression and/or anxiety affect infosec behavior. Due to the variety and severity of symptoms, it is difficult to predict how they will have an impact, without an empirical investigation. For example, symptoms of hypervigilance could result in improve infosec behaviors, however, when accompanied by other symptoms, e.g., paranoia, can lead to avoidance behavior. Although we can speculate some results, such as, employees with impaired judgement and memory loss may find it difficult to perform secure infosec behaviors, for example, clicking on suspicious links in emails (Woods 2022). Regardless of what is discovered, as one of the first empirical studies of this area, all results will have important implications. The findings will firstly, contribute to a growing body of research. Secondly, the results will provide a better understanding of employees and how their mental health affects their organization's infosec. This will have implications for finding ways to improve infosec behavior, and encouraging safer organizational practices. The results could also yield concrete suggestions of how to improve the content and communication of security awareness and practices. Finally, through improving employees' infosec behavior, this should lead to more secure organizations, with fewer security breaches.

REFERENCES

American Psychiatric Association. 2013. *Diagnostic and statistical manual of mental disorders: DSM-5* (5:5), Washington, DC: American Psychiatric Association.

Black, D. W., and Grant, J. E. 2014. *DSM-5® guidebook: the essential companion to the diagnostic and statistical manual of mental disorders*. Arlington, VA: American Psychiatric Pub.

Bocéréan, C., and Dupret, E. 2014. "A validation study of the Hospital Anxiety and Depression Scale (HADS) in a large sample of French employees," *BMC psychiatry* (14:1), pp. 1-11.

Crawford, J. R., Henry, J. D., Crombie, C., and Taylor, E. P. 2001. "Normative data for the HADS from a large non-clinical sample". *British Journal of Clinical Psychology* (40.4), pp. 429-434.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future directions for behavioral information security research," *Computers & Security* (3:2), pp. 90-101.

D'Arcy, J., and Teh, P. L. 2019. "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization," *Information & Management* (56:7), pp. 103151.

Donalds, C., and Osei-Bryson, K. M. 2020. "Cybersecurity compliance behavior: exploring the influences of individual decision style and other antecedents," *International Journal of Information Management* (51), pp. 102056.

Egelman, S., and Peer, E. 2015. "Scaling the security wall: developing a security behavior intentions scale (SeBIS)," in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pp. 2873–288

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding nonmalicious security
violations in the workplace: A composite behavior model," *Journal of management information systems* (28:2), pp. 203-236.

Hu, S., Hsu, C., & Zhou, Z. 2022. "Security education, training, and awareness programs: Literature review" *Journal of Computer Information Systems* (62:4), pp. 752-764.

Hwang, I., and Cha, O. 2018. "Examining technostress creators and role stress as potential threats to employees' information security compliance," *Computers in Human Behavior* (81), pp.282-293.

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. 2019. "Speak their language: Designing effective messages to improve employees' information security decision making," *Decision Sciences* (50:2), pp. 245-284.

Kyytsönen, M., Ikonen, J., Aalto, A. M., and Vehko, T. 2022. "The self-assessed information security skills of the Finnish population: A regression analysis," *Computers & Security* (118), pp. 102732.

Lee, C., Lee, C. C., and Kim, S. 2016. "Understanding information security stress: Focusing on the type of information security compliance activity," *Computers & Security* (59), pp. 60-70.

Myers, M. D. 2013. *Qualitative research in business and management*, London: Sage Publications.

Nasirpouri Shadbad, F., and Biros, D. 2022. "Technostress and its influence on employee information security policy compliance," *Information Technology & People* (35:1), pp. 119-141.

Shropshire, J., Warkentin, M., and Sharma, S. 2015. "Personality, attitudes, and intentions: predicting initial adoption of information security behavior," *Computers & Security* (49), 177–191.

Vance, A., Eargle, D., Eggett, D., Straub, D., and Ouimet, K. 2022. "Do security fear appeals work when they interrupt tasks? A multi-method examination of password strength," *MIS Quarterly* (46:3), pp.1721-1738.

Walsham, G. 1995. "Interpretive case studies in IS research: Nature and method," *European Journal of Information Systems* (4), pp. 74–81.

Warkentin, M., and Willison, R. 2009. "Behavioral and policy issues in information systems security: the insider threat," *European Journal of Information Systems* (18:2), pp.101-105.

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., and Mayhorn, C. B. 2015. "Will the "phisher-men" reel you in? Assessing individual differences in a phishing detection task," *International Journal of Cyber Behavior, Psychology and Learning* (5:4), pp.1–17.

Woods, N. 2022. "Users' Psychopathologies: Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior," in *Cyber Security: Critical Infrastructure Protection* Cham: Springer International Publishing, pp. 93-134.

World Health Organization (WHO). 2019. "Mental disorders," URL: https://www.who.int/news-room/fact-sheets/detail/mental-disorders.

Zigmond, A. S., and Snaith, R. P. 1983. "The hospital anxiety and depression scale," *Acta psychiatrica scandinavica* (67:6), pp.361-370.