Computers & Security 161 (2026) 104776

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Full Length Article

Technostress and information security – A review and research agenda of security-related stress

Antony Mullins *, Nik Thompson

Curtin University, Bentley, Western Australia, Australia

ARTICLE INFO

Keywords:
Technostress
Security-related stress
Information security
Information security behavior
Information security management
Information security policy
Compliance
Systematic literature review

ABSTRACT

Technostress is a growing concern for organisations, given the negative impacts of stress on employees' job satisfaction, productivity, and intention to comply with or violate policies. Security-related stress (SRS), a dimension of technostress, addresses how security-related activities, such as information technology compliance, can impact an individual's stress. Addressing security-related stress research is vital, given it can help identify factors that can both enhance employee well-being and strengthen an organisation's security posture. In this paper, we systematically review the literature from the past two decades addressing security-related stress and identify twenty-seven relevant studies for analysis. We make contributions in three areas. Firstly, we discover the predominant theoretical frameworks and models that address security-related stress while examining key factors and constructs that examine security-related stress. Secondly, we describe how security-related stress is measured and what interventions have proven effective in reducing it. Finally, based on our comprehensive analysis, we present a research agenda to inform future research directions of security-related stress.

1. Introduction

As individuals increasingly face technology demands, the potential for technostress is a growing concern. Security-related stress (SRS) has emerged as an essential field of study as researchers seek to understand its implications for operational and organisational strategies and mental health.

In recent years, the prevalence of security threats, coupled with heightened public awareness and scrutiny, has prompted organisations to prioritise the mental well-being of their employees while attempting to navigate these challenges (Malik et al., 2024). This focus on mental health is crucial, as prolonged exposure to security-related stress can lead to burnout, decreased productivity, and increased staff turnover rates (H. Chen et al., 2022). Recognising the signs of security-related stress and implementing effective support systems can help mitigate negative outcomes, promoting a healthier work environment and enhancing overall organisational and employee resilience (McCormac et al., 2018).

Investing in mental health resources, such as counselling services and stress management programs, supports employees and contributes to a more engaged and motivated workforce, ultimately strengthening the organisation's ability to respond to security challenges (Yazdanmehr et al., 2023). Prioritising mental health initiatives, organisations can create a culture of openness and support, encouraging employees to seek help when needed and reducing the stigma often associated with mental health issues.

Understanding the impacts of security-related stress is paramount. Operationally, information security initiatives can cause anxiety, diminishing the initiatives' effectiveness and potentially exposing an organisation to security breaches (Hwang and Cha, 2018). Although the implementation of security software and protocols provides some protection, insider threats remain a concern, given that measures typically focus on external threats (Hwang and Cha, 2018). The management of security-related stress is of organisational relevance as it has the potential to reduce internal risk. Thus, organisational security strategies should both increase security protection and help minimise any stress levels produced by these measures (Lee et al., 2016).

In this nascent field, we identify that there is an opportunity to extend the body of knowledge through a comprehensive analysis of extant research and to explain the key themes and propose research directions to support future work. To our knowledge, there is one related review of security-related stress (Aggarwal and Dhurkari, 2023), which meta-analysed the relationship between stress and compliance. We differentiate from this work by examining all aspects of mental

* Corresponding author at: Curtin University, Bentley, Western Australia, AUSTRALIA.
E-mail address: Antony.Mullins@cbs.curtin.edu.au (A. Mullins).

https://doi.org/10.1016/j.cose.2025.104776
Received 12 July 2025; Received in revised form 12 November 2025; Accepted 16 November 2025
Available online 17 November 2025

well-being and psychological aspects of security-related stress.

Later sections in this paper examine the theoretical background of security-related stress studies and the key factors that contribute to security-related stress in the workplace. Next, we consider how these factors can be measured and potential interventions that can mitigate security challenges and foster a more resilient workforce. Finally, we provide an agenda for future research detailing the opportunities we have identified through our analysis. We also share the systematic review protocol that we applied to this study, to find the data to answer the following research questions:

RQ1) What predominant theoretical frameworks and models address security-related stress?
RQ2) What key factors and constructs address security-related stress?
RQ3) How is security-related stress measured?
RQ4) What interventions have proven effective in reducing security-related stress?
RQ5) What are the future research directions of security-related stress?

2. Research methodology

To address the research questions, we conducted a systematic literature review (SLR) that involved a comprehensive search of academic databases, selection criteria for relevant studies, and an analysis of the findings to synthesise existing knowledge in the field. The review highlighted theories, models, factors, and gaps in the current literature, providing a foundation for future studies and contributing to a deeper understanding of security-related stress factors. This systematic approach ensures the research is grounded in empirical evidence, allowing for a thorough examination of how security-related stress impacts both individuals and organisations and enables future research to replicate and extend our findings. The systematic literature review adhered to the Preferred Reporting Items for Systematic and Meta-Analyses (PRISMA) statement process (Page et al., 2021), as shown in Fig. 1.

The first step involved searching the Scopus database, followed by the Web of Science, ACM Digital Library, IEEE Xplore, and PsycINFO databases for peer-reviewed articles published within the last two decades, focusing on keywords related to security stress and its

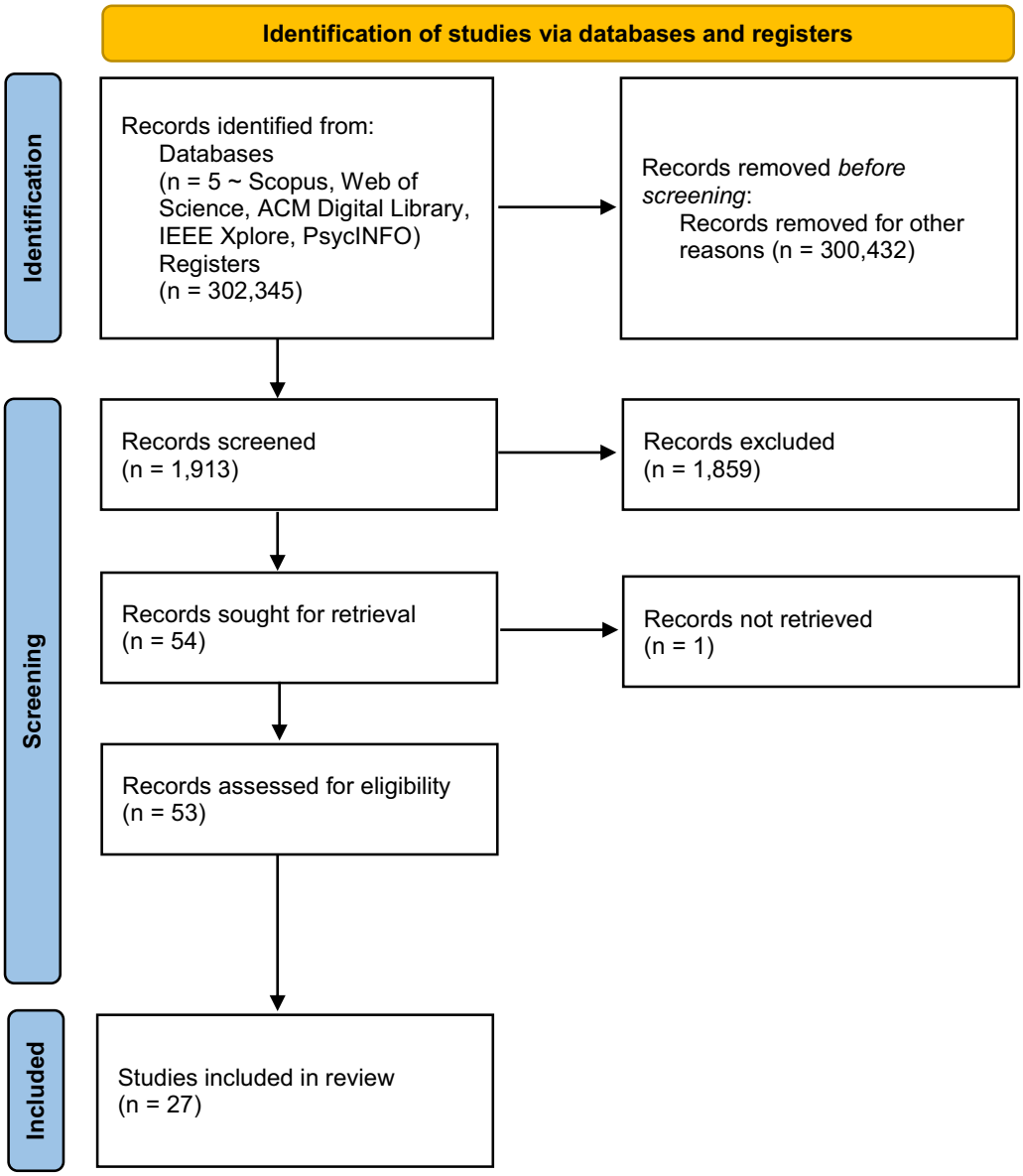

Fig. 1. Preferred Reporting Items for Systematic and Meta-Analyses (PRISMA) - SRS.

psychological effects. The initial search string included searching the database for titles, abstracts, and keywords that included the following terms: "information security" or "cyber security" or "cybersecurity", resulting in 302,345 articles (Scopus ~ 102,948, Web of Science ~ 81,764, ACM Digital Library ~ 16,887, IEEE Xplore ~ 100,270, PsycINFO ~ 476). Given the breadth of the search, further refinement included filtering the articles to include only titles and abstracts that matched the following terms: "technostress" or "techno stress" or "stress" or "strain" or "security-related stress" or "SRS" or "security strain" or "technostress creators", resulting in 1913 articles.

This extensive literature-gathering process strengthens the validity of the findings. The 1913 articles were screened by reading the title and abstract to ensure they were appropriate and covered security-related stress in various contexts, including its impact on individuals. The inclusion criteria are summarised in the following points: The article must be from a reputable journal or conference and address human behaviour and the information security perspectives of security-related stress. Initially, 54 articles met the inclusion criteria; however, one article could not be accessed. To ensure robustness, both members of the research team discussed and reviewed the articles until a consensus was reached, resulting in twenty-seven articles. Therefore, the final set of records provided in Table 1 contained twenty-seven articles (19 Journal Articles, 8 Conference Papers). The research team reviewed these articles in detail, allowing an in-depth examination of methodologies, outcomes, and theoretical frameworks employed across different research settings. The impact of SRS research was evident, given that nineteen of the twenty-seven articles appeared in leading journals, such as *Computers in Human Behavior* and *Computers and Security*.

Table 1
Theories and Models.

S. No	Study	Theoretical Foundation
1	Ali and Dominic (2024)	Security-Related Stress (SRS) Model, Coping Theory
2	Ament and Haag (2016a)	SRS Model, Person-Environment Fit Model
3	Ament and Haag (2016b)	SRS Model, Person-Environment Fit Model
4	L. Chen et al. (2022)	Challenge Hindrance Stress Model
5	H. Chen et al. (2022)	SRS Model, Psychological Capital
6	H. Chen et al., 2023	Challenge Hindrance Stress Model
7	D'Arcy and Teh (2019)	SRS Model, Affective Events Theory, Coping Theory
8	D'Arcy et al. (2014)	SRS Model, Moral Disengagement Theory, Coping Theory
9	Frank and Kohn (2021)	SRS Model and Psychological Capital
10	Hwang and Cha (2018)	SRS Model
11	Hwang et al. (2022)	SRS Model
12	Hwang and Seo (2025)	Person-Environment Fit Model
13	Jeon et al. (2023)	Coping Theory, Frustration, Emotional Coping
14	Lee et al. (2016)	SRS Model, Person-Environment Fit Model
15	Li and Huang (2020)	SRS Model, Coping Theory, Emotion-Focused Coping, Problem-Focused Coping
16	Lundgren and Bergstrom (2019)	SRS Model
17	McCormac et al. (2018)	Job Stress, Information Security Awareness, Resilience
18	Mizrak et al. (2025)	Burnout Theory
19	Pham et al. (2016)	Extended Job Demands Resources Model
20	Pham et al. (2019)	Extended Job Demands Resources Model
21	Posey and Shoss (2024)	Authors' own Model that includes Job Demands, Invasion, Insecurity, and Conflict
22	Savoli et al. (2017)	Coping Theory
23	Shadbad and Biros (2021)	Role Theory
24	Shadbad and Biros (2022)	Technostress Model
25	Yazdanmehr et al. (2023)	Transactional Model of Stress, Coping Theory
26	Yepuru and Hsu (2019)	Stressor Strain Outcome Model
27	Yepuru et al. (2018)	Stressor Strain Outcome Model

3. Results

Interestingly, though our search criteria included the last 20 years, the relevant articles only spanned the last 11 years, highlighting the more recent recognition of security-related stress in research. Given this relatively brief history, many research opportunities still exist, and further interdisciplinary collaboration is needed to address these challenges effectively. The insights from such studies can inform the development of targeted interventions and policies to mitigate security-related stress, enhancing individual well-being and organisational resilience. A timeline of the number of studies per year is provided below in Fig. 2.

3.1. What predominant theoretical frameworks and models address security-related stress?

To address research question 1 (RQ1), we identified key theoretical frameworks and models assessing security-related stress (Table 1). Identifying the most prominent theoretical framework used provided challenges, given that many researchers combine multiple approaches to comprehensively understand the factors influencing security-related stress and the relationship between individuals' and organisations' security demands.

The studies listed in Table 1 have explored the impact of technology on individuals' stress, emphasising the need for effective coping mechanisms and organisational support to mitigate its effects. Such work often applies or adapts the technostress model as a theoretical foundation, e.g., (D'Arcy et al., 2014; Shadbad and Biros, 2021).

3.1.1. Technostress

Technostress refers to the negative impact that excessive technology use can have on an individual's stress levels (Tarafdar et al., 2007). Ragu-Nathan et al. (2008) further conceptualised and validated five factors (techno-overload, techno-invasion, techno-complexity, techno-insecurity, and techno-uncertainty) within the technostress model. Furthermore, Hang et al. (2022) highlighted the five factors as stressors that can negatively impact a user's well-being. Techno-overload is characterised by individuals feeling overwhelmed by the increasing number of tasks due for completion; techno-invasion relates to the lack of boundaries between work and personal life, which can lead to increased time spent on work-related activities. Techno-complexity refers to the stressful situations that modern technology can bring about. Techno-insecurity highlights anxiety and concerns about job security due to the threat of technology replacing individuals. Finally, techno-uncertainty addresses the uncertain challenges individuals face in adapting to rapidly changing technologies (Hwang and Cha, 2018). These five dimensions of technostress recognise the need for effective strategies to manage the challenge of stress due to technology integration.

3.1.2. Security-related stress

D'Arcy et al. (2014) coined the term "Security-Related Stress" by applying the concept of technostress creators to the context of security; however, only overload, complexity, and uncertainty were proposed. In a security-related stress context, overload is one of the primary contributors. IT professionals often face a large number of information security demands, which can lead to users feeling overwhelmed with having to address security demands on top of their typical job role (D'Arcy et al., 2014). Furthermore, this may lead to decreased productivity within the job role and increased frustration and stress for the user (D'Arcy et al., 2014). Complexity is a factor that can exacerbate the issue of stress, especially within a security domain, as users attempt to navigate intricate systems and protocols that require specialised knowledge and skill, and again, impact the users' core job role (D'Arcy et al., 2014).

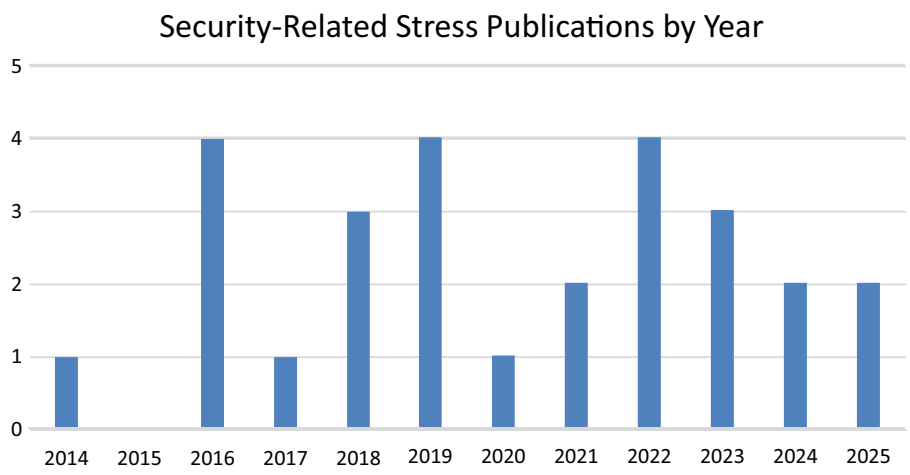

Fig. 2. SRS Publications by Year.

Finally, uncertainty can further contribute to the stress experienced by users, as they may struggle to understand evolving security policies and potential threats, leaving them unsure about how to protect sensitive information while fulfilling their primary responsibilities effectively (D'Arcy et al., 2014). Literature has shown that security-related stress can predict information security policy compliance (D'Arcy and Teh, 2019) and employee behaviours (Ali and Dominic, 2024), highlighting the need for organisations to implement more user-friendly security measures and provide adequate training to alleviate these pressures.

3.1.3. *Coping theory*

Technostress and security-related stress have been extended by other theories and models, such as coping theory, person-environment fit, and challenge-hindrance theory. Coping theory was most prominent in seven of the twenty-seven articles that addressed coping elements and how people handle stressful IT demands. Coping theory explores how individuals manage and respond to stressors, particularly in high-pressure environments (D'Arcy et al., 2014), and emphasises the importance of problem-focused and emotion-focused coping strategies, which can significantly influence an individual's ability to navigate security-related challenges effectively. Applying coping theory in this context not only aids in understanding individual responses but also informs the development of targeted interventions that can enhance resilience and reduce stress levels among those facing security threats. Understanding the various coping mechanisms can lead to more effective training programs and support systems designed to equip individuals with the skills necessary to manage security-related stress in both personal and professional settings.

D'Arcy and Teh (2019) identified that coping theory has evolved since its inception. It no longer focuses on appraisals of stress and coping mechanisms but also includes emotions based on recognising that stress, emotions, and coping are conceptually related. Emotion-focused coping (EFC) is generally described as a strategy that helps an individual manage their emotions to restore emotional stability and alleviate stress (Yazdanmehr et al., 2023). Inward and outward emotion-focused coping are often examined in tandem, given that inward EFC relates to internal self-reactions that help manage stress and emotions. In contrast, outward EFC involves seeking support from others or expressing emotions to external sources (Yazdanmehr et al., 2023), which can significantly influence overall well-being and resilience in the face of stress. Understanding the interplay between these two forms of emotion-focused coping can provide valuable insights into how individuals navigate challenging situations and enhance their emotional resilience (Li and Huang, 2020). Emotion-focused coping includes psychological avoidance, reinterpretation, and rationalisation (D'Arcy et al., 2014). These strategies help individuals regulate their emotions and restore emotional stability. Effective emotion-focused coping can also foster greater control over one's emotional responses, enabling individuals to adapt more successfully to stressors and maintain healthier relationships with others (Yazdanmehr et al., 2023).

Understanding coping theories that investigate emotions is vital, given that Yazdanmehr et al. (2023) showed that both inward and outward emotion-focused coping can increase an employee's intention to violate an information security policy. Furthermore, researchers should identify the strategies employed by IT security users and how these strategies impact their ability to manage stress and anxiety in high-pressure environments. This understanding can lead to the development of tailored interventions that support emotional well-being among IT professionals, enhancing their compliance and job satisfaction.

3.1.4. *Person-environment fit (PEF)*

Person-environment fit (PEF) is another concept that has been applied to security-related stress. The PEF model is relevant as it examines the relationship between an individual's capabilities and the demands of their environment, proposing that if the relationship is unbalanced, the individual's stress level and well-being may be affected (Ament and Haag, 2016b; Hwang and Seo, 2025; Yepuru and Hsu, 2019). Understanding the link between PEF and security stress can lead to more effective strategies for improving individuals' resilience and coping mechanisms in high-stress security environments, given that the social environment of individuals can positively influence security compliance; however, the work environment has the opposite effect (Ament and Haag, 2016a). Therefore, to increase security compliance, organisations must attempt to balance employee stress and anxiety (Hwang and Seo, 2025).

3.1.5. *Challenge-hindrance stressor (CHS)*

Challenge-hindrance stressor (CHS) is a theory that categorises job stressors into challenge and hindrance stressors to examine their effects on work-related outcomes (L. Chen et al., 2022). Challenge stressors, such as security responsibility, continuity demand, and learning demand, can lead to positive outcomes (Chen et al., 2023), while hindrances can have the opposite effect and impede performance (D'Arcy et al., 2014). Furthermore, differentiating between the two categories of stressors is valid, given Chen et al. (2023) demonstrated that challenge stressors could motivate employee compliance in promotion-focused individuals, whereas hindrance stressors, such as complexity, overload, and uncertainty, had an adverse effect on compliance. Managing the challenge and hindrance stress factors is essential to influence employee performance and well-being in demanding workplaces, such as those implementing security policies and compliance expectations.

3.2. What key factors and constructs address security-related stress

Researchers often extend established models to better explain the factors that influence the security behaviours of interest. To address RQ2, we sought to identify the core models and constructs that have formed the theoretical foundation of prior work. Given that Techno-stress and Security-Related Stress models were predominant in the literature, the primary constructs studied in prior work included technostress-complexity, insecurity, invasion, overload, and uncertainty, predominantly from a security compliance perspective. However, Lundgren and Bergstrom (2019) examined stressors (overload, uncertainty, and complexity) and the related stress inhibitors within an information security risk management process as opposed to security compliance to highlight the importance of tailoring security policies and training programs to support managerial and technical staff in managing their unique stressors. Frank and Kohn (2021) also examined SRS outside of security compliance, focusing on how psychological capital components, such as self-efficacy and resilience, can impact security-related stress. Furthermore, Mizrak et al. (2025) examined the relationship between cybersecurity fatigue and mental-health related stress and anxiety.

As the list of factors which have been examined along with security-related stress is considerable, we have extracted and summarised all these extensions below in Table 2, highlighting the variance in constructs that researchers have examined with security-related stress. We use this data to develop a single diagram providing a high-level view of the entire theoretical base to date and present this later in the section.

Our analysis reveals that a considerable number of constructs have been proposed and evaluated in the SRS literature to date. To better explain the findings, we have developed a mapping diagram to visualise the relationship paths between SRS and additional constructs. This mapping provides a high-level view of what the current literature has examined, highlights possibilities for future research, and demonstrates how authors have differed in their approach to investigating stress and the relationship between security compliance and non-compliance. The diagram is provided below in Fig. 3. Using this mapping of the expansive list of constructs, we have identified four predominant areas, and we use this grouping as the basis for our subsequent discussion. The four areas are: coping, emotion, regulatory focus/environment, and psychological capital constructs.

Table 2
Constructs addressed in the literature.

Construct Group	Constructs	S. No
SRS Creators	Overload, Uncertainty, Complexity, Insecurity, Invasion, Challenge, Hindrance, Job Stress, Burnout	All except 18, 22
SRS Inhibitors	Literacy Facilitation, Technical Support Provisioning, Involvement Facilitation	11, 14, 16
Coping	Coping Response, Procrastination, Neutralisation, Inward Emotion-Focused Coping, Psychological Detachment/Distancing, Denial, Wishful Thinking, Outward Emotion-Focused Coping, Emotional Support Seeking, Venting, Moral Disengagement, Reconstrue Conduct, Obscure or Distort, Devalue the Target, Problem-Focused Coping	1, 7, 8, 13, 15, 22, 25, 27
Emotion	Strain, Information Security Fatigue, Emotional Exhaustion, Cynicism, Frustration, Positive Emotions, Negative Emotions	4, 7, 12, 18, 24, 26
Regulatory Focus/ Environment	Promotion Focus, Prevention Focus, Compliance Effort, Work Impediment, Perceived Responsibility, Organisation Support, Organisation Commitment, Social Environment, Conflict, News	2, 3, 6, 10, 11, 13, 19, 20, 21, 23
Psychological Capital	Hope, Optimism, Self-Efficacy, Resilience, Autonomy	5, 9, 17, 20
Information Security Policy Intention	Violation, Compliance	All except 3, 10, 14, 16, 17, 22, 26, 27

3.2.1. Coping constructs

Individuals often employ strategies to assist in coping and managing stress. For example, Yazdanmehr et al. (2023) examined security stress creators (overload, complexity, and uncertainty) and their association with emotion-focused coping (inward and outward) and problem-focused coping. The researchers examined inward emotion-focused coping mechanisms, including denial, psychological distancing, wishful thinking, and outward emotion-focused coping mechanisms, such as seeking emotional support and venting. Their findings suggest that security-related stress can trigger emotional and problem-focused coping mechanisms and influence the intention to violate security policies. Similarly, Li and Huang (2020) proposed a model to address SRS and its association with emotional reactions, such as fatigue and frustration, and emotional coping responses, such as inward and outward emotion-focused coping strategies, when facing information security policy compliance in the workplace. D'Arcy et al. (2014) also examined security stress creators, their association with emotion-focused coping, and their impact on moral disengagement from information security policy violations. The authors showed that security-related stress and moral disengagement are the key factors that can influence and prevent information security policy violations. When employees experience heightened security stress, they may justify or rationalise their unethical behaviours, distancing themselves from the moral implications of their actions.

Ali and Dominic (2024) also examined coping responses such as procrastination, psychological detachment, and neutralisation, and their moderating effect on the association between SRS and the intention to violate security policies. Their findings suggest that employees often perceive security requirements as stressful and employ avoidance coping strategies, which can lead to security policy violations and emotional distress since emotions played a moderating role in the (SRS to neutralisation to ISP compliance) relationship path.

3.2.2. Emotion constructs

Individuals often express emotions in stressful situations, and the underlying mechanisms driving these emotions can provide insight into individuals' coping responses. D'Arcy and Tan (2019) examined emotional reactions, such as frustration and fatigue, and coping responses, including neutralisation, when investigating information security policy compliance. They recognised that frustration and fatigue increase information security policy non-compliance and pose significant challenges for organisations aiming to enhance their information security posture. They also note that negative emotions were associated with neutralisation coping strategies.

H. Chen et al. (2022) examined the impact of positive emotions (such as interest, excitement, pride, and enthusiasm) and negative emotions (such as hostility, irritability, distress, fear, and nervousness) on the relationship between challenge information security stress and ISP compliance. Challenge stress is a positive type of pressure, and the authors supported this by finding that positive emotions mediate the relationship between challenge information security stress and ISP compliance. This positive aspect can lead to improved compliance rates and a stronger organisational culture of security awareness, supporting the thought that employees may perceive security challenges as opportunities for personal and professional growth. However, negative emotions did not mediate the relationship between challenging information security stress and ISP compliance.

Further examining the emotional aspects, Shadbad and Biros (2022) recognised that the unpredictable nature of technology can lead to frustration and anxiety among individuals, emphasising how technological failures can result in reduced productivity. Building on their

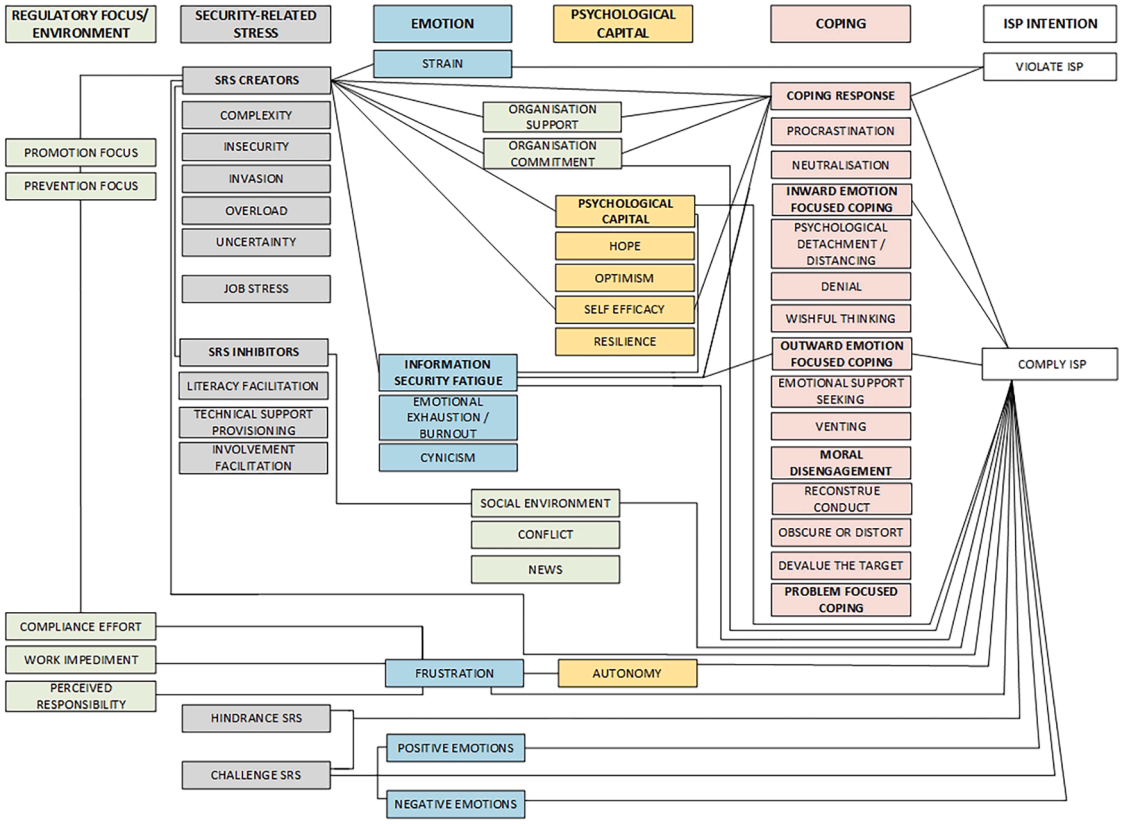

Fig. 3. Security-Related Stress Constructs.

previous work (Shadbad and Biros, 2021), the study also expanded the existing five constructs from the technostress framework to include an additional technostress construct, "techno-unreliability".

3.2.3. *Regulatory focus / environment*

Regulatory focus theory assumes that individuals are motivated by either a promotion or prevention focus, which influences their emotional behaviour (Brockner and Higgins, 2001). Examples of promotion-focused individuals include those seeking to advance in their careers or aiming to achieve a personal goal. At the same time, prevention-focused individuals strive to avoid loss and maintain a safe environment by adhering to rules and policies. Furthermore, the environment in which individuals operate, such as person-organisation fit, can impact their attitudes (Brockner and Higgins, 2001). Examining security stress, Hwang et al. (2022) distinguished between creators of stress (overload, complexity, and uncertainty) and inhibitors (literacy facilitation, technical support provisioning, and involvement facilitation). The research addressed regulatory focus by examining the impact of promotion and prevention focus on stress creators. The results varied, given that the prevention focus was not positively related to stress creators, and the promotion regulatory focus was negatively associated. The authors also addressed organisational commitment and highlighted a significant positive relationship between compliance intention and organisational commitment, thereby recognising that individuals who share organisational goals tend to have higher degrees of organisational commitment among employees.

Chen et al. (2023) examined the moderating regulatory mechanisms of promotion focus and prevention focus on the relationship between challenge SRSs and security policy compliance, and found that hindrance SRSs harmed the intent to comply with information security policies. While the prevention focus was found to positively moderate hindrance SRS and compliance intention, promotion focus positively moderated the relationship between challenge SRS and compliance intention. These findings highlight the complex interplay between security-related stressors and employee behaviour, suggesting that organisations should tailor their security awareness programs to foster a supportive environment that minimises hindrance stress while enhancing challenge stress.

Jeon et al. (2023) focused on frustration and its drivers, including compliance effort, work impediments, and perceived responsibility, as well as the implications for information system security policy compliance. However, they also examined the impact of allowing autonomy for an individual and its association with compliance. Interestingly, the results indicated that frustration negatively affected employees' intentions to comply; however, this relationship was moderated by the level of perceived autonomy that the respondents had. This suggests that employees are more likely to comply with security policy if given more autonomy and opportunities.

Ament and Haag (2016b) presented a multidimensional approach to SRS. They proposed three dimensions that highlight non-technical aspects in addition to the traditional SRS constructs: work environment (complexity, overload, uncertainty), personal environment (invasion, job insecurity, degree of freedom), and social environment (conflict, news). Although the research was theoretical, a subsequent study applied the model to examine how the factors influence compliance with information security policies (Ament and Haag, 2016a). Their research found that work-related SRS had an adverse effect on information security policy compliance, whereas the social environment had a positive impact. These insights underscore the complexity of human behaviour concerning information security, suggesting that organisations should consider both workplace dynamics and social influences when developing strategies to improve employee information security policy compliance.

Lee et al. (2016) examined how employees become stressed, the factors behind it, and the differences between managerial and technical security-oriented organisations. The constructs evaluated included prior

security knowledge, perceived security threat, mitigation adaptation, attitude to information security policy compliance, stressors (invasion of privacy, work overload), types of information security compliance, and information security stress. The study indicated that work overload and invasion of privacy can influence information security stressors, and work overload has a more significant effect in managerial security-oriented organisations. However, the invasion of privacy has a greater influence on stress in technical security-oriented organisations. These findings suggest that organisational context is crucial in shaping employees' experiences of information security-related stress.

Finally, Hwang and Seo (2025) investigated security compliance intention in relation to stress and anxiety. The study focused on role conflict and ambiguity as the main contributors of role stress, and anxiety and fatigue as the contributors of role strain. Similar to other studies, the results showed that role stress significantly increased strain and also reduced compliance intention. However, collaborative communication was shown to moderate the effect of strain on compliance.

3.2.4. Psychological capital

Psychological capital is an individual's psychological state that includes positive traits such as self-efficacy (individual belief to succeed), optimism (confidence to succeed), hope (expectation and desire), and resilience (adapting to changing environments) (Luthans and Youssef-Morgan, 2017).

Frank and Kohn (2021) examined whether a positive psychological state (Self-efficacy, Resilience) can reduce the unwanted outcomes of security-related stress (overload, complexity, uncertainty). Their findings indicated that fostering self-efficacy and resilience among employees may mitigate the adverse effects of security stress and enhance their commitment to adhering to information security policies. However, they also recognised that the positive impact diminishes once an individual has been a victim of cybercriminal behaviour, underscoring the importance of promoting psychological resilience and providing robust support systems to help employees recover from such traumatic experiences and reinforce their commitment to ethical practices in information security.

H. Chen et al. (2022) also examined psychological capital traits, hope, optimism, self-efficacy, and resilience, and their impact on information security fatigue as an emotion-based mediator in exploring the relationship between employees' information security-related stress (SRS) and information security policy compliance intention. Their research indicates that higher levels of psychological capital can mitigate the detrimental effects of information security fatigue, promoting greater adherence to security policies among employees. While SRS increases information security fatigue, reducing their intention to follow security policies.

3.3. How is security-related stress measured?

Our analysis of the methodological approaches in the literature showed that surveys are by far the most dominant approach to gathering data. All articles used surveys except one (Lundgren and Bergstrom, 2019), which interviewed participants and captured examples of stressors and stress inhibitors in practice. This is somewhat understandable, as surveys allow researchers to collect extensive datasets using quantifiable scales that can then be analysed using statistical methods. Some measures are also well-suited for the survey methodology. In particular, the difficulty in objectively assessing stress generally dictates the use of self-report surveys; however, the results can be biased due to low self-confidence, self-bias, and memory recall issues (Masood et al., 2012). On the other hand, Alshenqeeti's (2014) interview approach enabled a more detailed qualitative approach to capturing and analysing data, but it comes with its own validity and reliability concerns, given the potential for bias, such as interviewers introducing their own views and preconceived notions. Clearly examining stress measurement methods outside of the SRS scope could be beneficial, and we address some examples in Section 3.5.2.

Given our finding that most articles have employed surveys, we address Research Question 3 by identifying the specific scales and items used in these studies and examining their theoretical development and sources. Table 3 provides a summary of all studies, the scales that were employed, and the original source from which those scales were derived.

At the top level, we find that the security-related stress measures from Ayyagari et al. (2011) and D'Arcy et al. (2014) are the predominant instruments for measuring stress. Ayyagari et al. (2011) examined stressors such as work-home conflict, invasion of privacy, work overload, role ambiguity, and job insecurity. The scales used to assess work overload, role ambiguity, and strain were adapted from Moore (2000).

Table 3
How Security-Related Stress is Measured.

Stress Scales	Articles Authors	Scale Origin
Work Overload, Invasion of Privacy, Strain, Role Ambiguity, Role Conflict Scales Ayyagari et al. (2011)	Hwang and Cha (2018); L. H. Chen et al. (2022); D'Arcy and Teh (2019); Lee et al. (2016); Hwang and Seo (2025); Shadbad and Biros (2021); Shadbad and Biros (2022); Yepuru and Hsu (2019); Yepuru et al. (2018)	Moore (2000); Kreiner (2006); Netemeyer et al. (1996); Alge (2001); Eddy et al. (1999)
Work Impediment Scale Bulgurcu et al. (2010)	D'Arcy and Teh (2019); Jeon et al. (2023); Pham et al. (2019)	Original
Challenge Stress Scale Cavanaugh et al. (2000)	L. H. Chen et al. (2022)	Original
SRS Complexity, SRS Overload, SRS Uncertainty Scales D'Arcy et al. (2014)	Ali and Dominic (2024); Ament and Haag (2016a); H. H. Chen et al. (2022); H. Chen et al. (2023); Frank and Kohn (2021); Hwang et al. (2022); Li and Huang (2020); Yazdanmehr et al. (2023)	Ragu-Nathan et al. (2008)
Job Stress Scale (Role Stress Scale) Lambert et al. (2006)	McCormac et al. (2018)	Cullen et al. (1989)
Work Overload, Invasion of Privacy, Information Security Stress (Strain) Scales Lee et al. (2016)	L. H. Chen et al. (2022); Hwang and Seo (2025); Yepuru et al. (2018); Yepuru and Hsu (2019).	Ayyagari et al. (2011)
Perceived Workload, Work Exhaustion, Role Ambiguity Scales Moore (2000)	Yepuru and Hsu (2019); Shadbad and Biros (2022)	Caplan et al. (1975); Kahn et al. (1964); Schaufeli et al. (1995)
Techno Overload, Techno Invasion, Techno Complexity, Techno Insecurity, Techno Uncertainty Scales Ragu-Nathan et al. (2008)	Hwang and Cha (2018); Hwang et al. (2022); Shadbad and Biros (2022)	Original
Role Conflict Tarafdar et al. (2007)	Hwang and Cha (2018); Hwang and Seo (2025); Shadbad and Biros (2021)	Rizzo et al. (1970)
Stress Not Measured	Ament and Haag (2016b); Pham et al. (2016); Savoli et al. (2017)	
Observations / Interviews	Lundgren and Bergstrom (2019)	
Health Scales – Maslach Burnout Inventory	Mizrak et al. (2025)	
Job Insecurity Scale Vander Elst et al. (2014)	Posey and Shoss (2024)	De Witte (2000)

However, the questions refer explicitly to ICT and do not examine security-related aspects. D'Arcy et al. (2014) constructed survey items to address complexity, overload, and uncertainty; however, these items were adapted from Ragu-Nathan et al. (2008). The original technostress paper by Ragu-Nathan et al. (2008) is similar in some ways to Ayyagari et al. (2011) and addresses techno-overload, invasion, complexity, insecurity, and uncertainty from a technostress creator's perspective. Each item in the measurement addresses generalised technology, as opposed to security. Minor nuances exist between technostress and SRS items, for instance, when assessing techno-complexity, SRS items initially included a question to examine job pressure due to information security demands; however, the original technostress items do not address job pressure. Incidentally, the job pressure item was removed from the SRS items due to poor factor loadings. Appendix A includes a comparison of the nuances of complexity, overload, and uncertainty items in the technostress and SRS measurement items.

To address security-related stress, researchers often adapt survey items from multiple sources to address different constructs; for instance, D'Arcy and Teh (2019) adopted the work impediment item from Bulgurcu et al. (2010), which addresses security from a compliance perspective, but also includes the role ambiguity and role conflict scale items from Ayyagari et al. (2011). In several cases, these scales are derived from work in other disciplines. Although this is a relatively common practice in research, there is variance in the degree to which the scale has been contextualised to the security domain. This can be seen, for example, in the work of L. Chen et al. (2022) and McCormac et al. (2018) who addressed job stress using the challenge stress scale from Cavanaugh et al. (2000) and the job stress scale from Lambert et al. (2006). In both cases, the original scales are generalised and not directly related to security-related stress. For example, the challenge stress scale is centred around the time pressure of managers (Cavanaugh et al., 2000), while the job stress scale adopted by McCormac et al. (2018) addressed police and correctional officer stress (Cullen et al., 1989; Lambert et al., 2006), focusing on emotions such as anger, frustration, and tension. The context of both scales differs, and survey items may be misinterpreted in a traditional IT security setting where all employees must adhere to IT security policies regardless of their position. They may also face different stressors compared to police, correctional officers, and managers.

Upon reviewing the researchers' methods, it was evident that observational data is seldom collected, given that all but one of the articles administered questionnaires to gather responses. Lundgren and Bergstrom (2019) assessed stress by examining the familiar constructs of overload, complexity, and uncertainty. However, in contrast to all other studies, they interviewed respondents and directly observed behaviour instead of utilising survey instruments. Furthermore, the article did not address compliance but examined the impact of risk management tools.

3.4. What interventions have proven effective in reducing security-related stress?

To address Research Question 4, we highlight and categorise the interventions that have proven effective in reducing security-related stress, providing insight into how they can be implemented across various organisational contexts.

3.4.1. Organisational support interventions

Organisational support is a crucial coping resource that helps employees manage work-related stress effectively, enhancing their well-being and job performance. Peer support and feedback are essential components of organisational support, as they can alleviate the negative impacts of job demands on employees. Information security policy-related organisational support includes technology support, flexible work schedules, and training programs, which empower employees to perform their tasks more effectively and reduce stress. Research outside of security-related stress has indicated that higher levels of perceived organisational support correlate with lower burnout and psychological dysfunction levels, indicating employees are less likely to resort to emotional coping strategies when organisational support is available (Jawahar et al., 2007).

Organisations should create supportive environments to enhance employee commitment, given that the level of commitment can vary based on individual characteristics and the work environment (Hwang et al., 2022). Managing role stress is essential for commitment, given that role stress can negatively impact organisational commitment and affect employees' intention to comply with information security policies (Shadbad and Biros, 2021).

Research has shown that prioritising literacy facilitation, such as training programs, can act as a stress inhibitor related to security and support employees in feeling confident about compliance with security policies (Hwang et al., 2022). Technical support provisioning is essential for helping employees manage the demands of information security policies and security-related stress, as it provides the necessary resources, such as troubleshooting, help desk services, and training to address security-related concerns effectively (Yazdanmehr et al., 2023). Adequate technical support can also enhance employees' understanding of the rationale behind security measures, encouraging a sense of ownership and commitment to compliance.

Finally, involvement facilitation refers to the organisational strategies that encourage employees to engage with information technology (IT) systems, making it easier to implement and use them effectively and ultimately reducing the stress associated with adapting to modern technologies (Hwang et al., 2022). Employees should be encouraged to participate in training sessions and collaborative decision-making processes. Research has shown that the more involved employees feel in the implementation process, the less likely they are to experience security-related stress (Hwang et al., 2022). However, care should be taken, as there may be negative impacts if the involvement leads to overreliance on IT support services (Pham et al., 2016).

3.4.2. Psychological interventions

Employees are encouraged to develop and improve a positive mental state to help counter the negative impact of security-related stress. Psychological capital is a mental state encompassing four key components: hope, resilience, optimism, and self-efficacy. A level of perseverance characterises hope, while resilience refers to the ability to bounce back from challenges and utilise existing resources to overcome difficulties (Frank and Kohn, 2021). Optimism indicates that individuals expect events to go their way, and self-efficacy relates to their confidence in their ability. H. Chen et al. (2022) showed that higher levels of psychological capital are associated with improved information security behaviours. Therefore, employers should create an optimistic environment to assist with information security management. However, Frank and Kohn (2021) offered some caution and further noted that the positive aspect of psychological capital diminishes when an individual has been the victim of a cyberattack.

3.4.3. Social interventions

Although under-researched within the field of security-related stress, social aspects among employees, such as conflict, are important to consider, as employee disputes can occur, sometimes due to colleagues requesting to bypass existing policies and regulations. Ament and Haag (2016a) identified that social conflicts can positively influence an individual's intention to comply. They showed that if a peer instructs an individual to break company policy, they are more likely to comply with security compliance requirements. Certainly, companies would want to limit social conflict amongst their employees, given that it does not necessarily reduce security-related stress. However, it is interesting that some disputes may positively impact security compliance, possibly as the dispute causes employees to pause and consider their actions systematically in light of the organisational requirements.

News reports on security-related incidents were another social aspect

shown to cause security-related stress, but they also positively impacted the intention to comply (Ament and Haag, 2016a). Exposing the risks associated with cybersecurity incidents can positively influence users to comply and potentially safeguard them from cyberattacks. Indeed, social aspects and exposures can cause more stress for an individual, but they also assist companies in ensuring employees meet compliance requirements.

3.5. Future research directions and agenda

Our final research question considers future research directions, and we share an agenda for future work on security-related stress. Our review found that articles on this topic only spanned the past 11 years, with over half of the articles within the last five years. Security-related stress is still a relatively new concept with ample scope for further research in high-quality venues. We propose four central themes in our agenda for future research directions – the advancement of theoretical models, a move beyond survey methodologies, exploration of the role of behavioural coping mechanisms, and to consider home-users in future work. We elaborate on these themes in the following sections, with key research directions for each.

3.5.1. Advance theoretical and conceptual foundation models

Most security-related stress research used the security-related stress model as the basis of their work. Darcy (2014) introduced this model to differentiate stress caused by security-related demands from the general technostress construct. This was operationalised as a second-order construct comprising of overload, complexity, and uncertainty. In their study, the path from SRS to behavioural intention was mediated by moral disengagement, and their model provided an explanatory power of 46 %. Though significant, it is evident that the source of the other 54 % of unexplained variance must still be sought.

The original formulation of technostress included two additional dimensions, which were omitted from the SRS formulation (techno-insecurity and techno-invasion) (Ragu-Nathan et al., 2008). It may be worth revisiting these dimensions, especially the techno-invasion dimension, as it showed the highest loading in the original technostress construct.

More recent work has expanded on the SRS foundation by integrating other existing theories, models, and constructs, such as the person-environment fit model, coping response, and psychological capital, e.g., (Ament and Haag, 2016a; Chen et al., 2023; H. H. Chen et al., 2022; Frank and Kohn, 2021; Lee et al., 2016). However, existing literature lacks consistency in the theoretical development of the models and theories. In particular, emotion-focused coping response constructs lack consistency between authors. For instance, D'Arcy et al. (2014) justify the convergence of moral disengagement theory mechanisms and emotion-focused coping process to examine constructs such as reconstrue conduct, obscure or distort, and devalue the target constructs, while Yazdanmehr et al. (2023) addressed denial, psychological distancing and wishful thinking, and Ali and Dominic (2024) examined procrastination, psychological detachment and neutralisation. Certainly, emotion-focused coping is an important concept that needs to be addressed to further understand how security-related stress impacts a user's coping mechanism.

Another avenue for future work in this area includes considering temporal and frequency dimensions in the stress assessment. For example, the Job Stress Survey (Spielberger and Vagg, 1999) is commonly used to measure general sources of job stress. In this instrument, respondents report both the severity and frequency of stress-inducing events. Similarly, studies of organisational behaviour reveal that job stress is related to both anxiety and time stress in distinct ways (Parker and DeCotiis, 1983). As different dimensions of job stress may have different stressors, there is scope for future work to study the stressors and outcomes at a more granular level.

3.5.2. Move beyond survey approaches for data collection

Following on from the above, we find that research predominantly uses or adapts survey questions from D'Arcy et al. (2014), Ayyagari et al. (2011), and Lee et al. (2016). The items from D'Arcy et al. (2014) address complexity, overload, and uncertainty from a security aspect, while the constructs used in Ayyagari et al. (2011) are generalised to information communication technologies and address complexity, overload, conflict, invasion of privacy, role ambiguity, and strain. Though models have been refined and extended, we find that most articles in our review employed self-report measures to record stress. All but one of the articles employed surveys, with the one remaining paper employing interviews. Though surveys are a well-established and convenient methodology for behavioural research, the question remains whether self-report measures are the ideal means to measure something as hard to define as stress. Given that surveys are prone to numerous potential validity concerns as well as social desirability bias, an opportunity exists to apply an improved instrument to assess security stress.

To this end, observational data is a promising candidate which has not been explored in prior SRS research. Observational data has the advantage of promising objectivity, while also addressing the risk of common method bias, as the stress measurement and the outcome (e.g., compliance) are no longer measured using the same method.

Observation opens up the possibility to assess stress from a range of markers, including physical (eyelid movement, facial expressions, head movements), psychological (electrocardiogram, electroencephalogram), behavioural (mouse behaviour, application usage), and performance-based (accuracy and response) perspectives (Carneiro et al., 2019). Kim et al. (2022) used eye-tracking measures to determine that stressed individuals exhibit a larger number of blinks, longer scanpath length, and more complex gaze paths compared to less stressed individuals when interacting with service kiosks. Furthermore, biometric measurement methods, such as body media devices, can detect skin moisture, heat flux, and changes in near-body and skin temperature to indicate an individual's stress (Moody and Galletta, 2015). Physiological markers in particular have been accepted as indicators of underlying psychological state since the early research on stress, e.g. (Cannon, 1914). As these represent internal states, not under the conscious control of the respondent, they are also considered to be a stronger and more objective view than that provided by self-report (Fried et al., 1984).

3.5.3. Explore the role of emotion-focused vs problem-focused coping strategies

SRS research typically considers the actions that the users take in response to security threats, such as security policy compliance behaviours. This is consistent with the dominant theoretical approaches for behavioural information security, which are largely focused on the problem-focused responses of users. However, evidence from the psychological sciences shows that users may exhibit a wide range of approaches to coping with a threat, including emotion-focused strategies, which are aimed at addressing the internal state (Lazarus, 1966). Such

responses may be especially pertinent in the context of SRS, which is itself an internal state.

Some work has recognised the potential role of emotion-focused coping (EFC) in SRS. For example, Ali and Dominic (2024) considered the role of EFC responses, such as neutralisation, procrastination, and detachment, as possible mediators of the relationship between SRS and policy compliance. Similarly, other research has proposed similar links where the effect of SRS might be mediated by neutralisation (D'Arcy and Teh, 2019), problem devaluation (D'Arcy et al., 2014), or inwards and outwards EFC (Li and Huang, 2020) as a mediator. Recent behavioural security research has shown that the emotion-focused and problem-focused responses may be enacted in parallel, and this may delay the enactment of desirable security behaviours (Thompson et al., 2024). This is a perspective that has not yet been considered in SRS research.

Furthermore, as over 400 types of coping have been identified in prior literature (Skinner et al., 2003), this is an area of theoretical development which is ripe with opportunities for future work. Understanding the types of emotional responses, and the context in which they are enacted can provide insights into what issues cause stress and what kinds of problems hinder the success of information security.

3.5.4. Consider the home-user

Finally, researchers should examine the relationship between security-related stress and home-user security demands. Though prior research has emphasised the organisational context, with policy compliance behaviour as the dependent variable, much of the behavioural insight applies in the home too. While a home-user may not have formalised IT policies to comply with, they do still need to enact general security-related behaviours, and validated and established scales already exist to assess these. Furthermore, as home-users do not enjoy the support or infrastructure management offered to organisational users, it is likely that they may experience even greater stress when dealing with information security demands. Home or end-user security is an area that lacks considerable research, and interventions are especially challenging as end-users often prioritise convenience over security (Reuter et al., 2022). An opportunity thus exists to explore how security-related stress may prevent them from taking the necessary best-practice steps to secure their local networks and devices.

We summarise our research agenda with twelve (12) future study areas in Table 4.

Table 4
Research Agenda.

Goal	Steps
Advance theoretical and conceptual foundation models	1. Refine the security-related stress model to address the substantial unexplained variance in behaviour. 2. Revisit under-explored dimensions of the original technostress construct. 3. Consider temporal and frequency dimensions of stress assessment.
Move beyond survey approaches for data collection	1. Assess the validity of self-report measures for SRS. 2. Further explore and enhance the use of observational data collection approaches. 3. Investigate if physiological indicators of stress are exhibited in SRS.
Explore the role of emotion-focused vs problem-focused coping strategies	1. Consider user behaviours that are not directly addressing the security threat/compliance. 2. Further explore emotion-focused mechanisms that influence security behaviours. 3. Identify which of the types of coping responses are applicable to SRS.
Consider the home-user	1. Consider home-user security behaviour rather than "compliance" as the dependent variable. 2. Compare how the role of organisational IT support (or lack of) differs from home-users in SRS. 3. Develop SRS measurement instruments that are operationalised for the home context.

3.5.5. Limitations

Although a thorough literature search was conducted, other literature databases, such as ProQuest and the Computer Science Database, may have been considered for inclusion. Our original literature search began with Scopus, which was subsequently expanded to four additional databases (Web of Science, ACM Digital Library, IEEE Xplore, and PsycINFO), which only yielded an additional total of four articles for inclusion in our research. Thus, we expect that further database inclusions may yield only incremental gains. A further limitation arises in our inclusion of only articles written in English; therefore, there is an opportunity to further enhance this research and international representation by including non-English articles.

3.6. Conclusion

This article presents a systematic review of the field of security-related stress, based on five leading scientific databases, and identifies twenty-seven articles that examine how security-related stress impacts users primarily in a security policy compliance setting. Specifically, the elements of security uncertainty, overload, and complexity have been demonstrated to impact the user's decision-making process. To address the challenges in security-related stress, this study addresses four research questions, outlining the theoretical frameworks in extant research, key constructs that have been measured, methodological approaches, and finally, the interventions that have proven effective in reducing security-related stress. These findings will provide a robust primer and reference source for those who are interested in this growing area of research. A final and significant contribution of our work is the development of a research agenda to provide evidence-based recommendations and identify research gaps in this area. We discuss four primary research goals that we believe are pertinent and share twelve research topics, each of which has potential for further study. We hope that our efforts to distil the knowledge of this field motivate others to engage in this interesting avenue of research and to continue the research agenda that we have set forth.

CRediT authorship contribution statement

Antony Mullins: Writing – review & editing, Writing – original draft, Conceptualization. **Nik Thompson:** Writing – review & editing, Writing – original draft, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A

SRS - Complexity (D'Arcy et al. 2014)	Technostress – Complexity (Ragu-Nathan et al. 2008)
CX1. I sometimes feel pressure in my job due to information security requirements.	Not in the Technostress items
CX2. I find that new employees often know more about information security than I do.	I1–15. I find new recruits to this organization know more about computer technology than I do.
CX3. I do not know enough about information security to comply with my organization's policies in this area.	I1–12. I do not know enough about this technology to handle my job satisfactorily.
CX4. I often find it difficult to understand my organization's information security policies.	I1–16. I often find it too complex for me to understand and use new technologies.
CX5. It takes me awhile to understand my organization's information security policies and procedures.	I1–13. I need a long time to understand and use new technologies.
CX6. I sometimes do not have time to comply with my organization's information security policies.	I1–14. I do not find enough time to study and upgrade my technology skills.
Overload	
OL1. I am forced by information security policies and procedures to do more work than I can handle.	I1–2. I am forced by this technology to do more work than I can handle.
OL2. My organization's information security policies and procedures hinder my very tight time schedules.	I1–3. I am forced by this technology to work with very tight time schedules.
OL3. I have a higher workload due to increased information security requirements.	I1–5. I have a higher workload because of increased technology complexity.
OL4. I am forced to change my work habits to adapt to my organization's information security requirements.	I1–4. I am forced to change my work habits to adapt to new technologies.
	I1–1. I am forced by this technology to work much faster. (Author removed due to error correlation)
Uncertainty	
UC1. There are constant changes in information security policies and procedures in my organization.	I1–23. There are constant changes in computer software in our organization.
UC2. There are frequent upgrades to information security procedures in my organization.	I1–25. There are frequent upgrades in computer networks in our organization.
UC3. There are always new information security requirements in my job.	I1–22. There are always new developments in the technologies we use in our organization.
UC4. There are constant changes in security-related technologies in my organization.	I1–24. There are constant changes in computer hardware in our organization.

Comparison of SRS items (D'Arcy et al., 2014) and Technostress (Ragu-Nathan et al., 2008) – Item numbering from original sources

Data availability

No data was used for the research described in the article.

References

Aggarwal, A., Dhurkari, R.K., 2023. Association between stress and information security policy non-compliance behavior: a meta-analysis. Comput. Secur. 124, 102991. https://doi.org/10.1016/j.cose.2022.102991.

Alge, B.J., 2001. Effects of computer surveillance on perceptions of privacy and procedural justice. J. Appl. Psychol 86, 797–804. https://doi.org/10.1037/0021-9010.86.4.797.

Ali, R.F., Dominic, P.D.D., 2024. Investigation of information security policy violations among oil and gas employees: a security-related stress and avoidance coping perspective. J. Inf. Sci. 50, 254–272. https://doi.org/10.1177/01655515221087680.

Alshenqeeti, H., 2014. Interviewing as a data collection method: a. Crit. Rev. Engl. Linguist. Res. 3, 39. https://doi.org/10.5430/elr.v3n1p39.

Ament, C., Haag, S., 2016a. How information security requirements stress employees. Presented at the. In: 2016 International Conference on Information Systems. ICIS, 2016.

Ament, C., Haag, S., 2016b. Security-related stress - A neglected construct in information systems stress literature. Presented at the. In: 24th European Conference on Information Systems. ECIS, 2016.

Ayyagari, R., Grover, V., Purvis, R., 2011. Technostress: technological antecedents and implications. MIS. Q. 35, 831–858. https://doi.org/10.2307/41409963.

Brockner, J., Higgins, E.T., 2001. Regulatory focus theory: implications for the study of emotions at work. Organ. Behav. Hum. Decis. Process 86, 35–66. https://doi.org/10.1006/obhd.2001.2972.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information Security Policy compliance: an empirical study of rationality-based beliefs and Information security awareness. MIS. Q. 34, 523–548. https://doi.org/10.2307/25750690.

Cannon, W.B., 1914. The interrelations of emotions as suggested by recent physiological researches. Am. J. Psychol 25, 256–282. https://doi.org/10.2307/1413414.

Caplan, R.D., Cobb, S., French, J.R.P., Van Harrison, R., Pinneau, S., 1975. Job Demands and Worker health: Main Effects and Occupational Differences. U.S. Dept. of Health, Education, and Welfare, Public Health Service, Center for Disease Control, National Institute for Occupational Safety and Health, [Washington].

Carneiro, D., Novais, P., Augusto, J.C., Payne, N., 2019. New methods for stress assessment and monitoring at the workplace. IEEE. Trans. Affect. Comput 10, 237–254. https://doi.org/10.1109/TAFFC.2017.2699633.

Cavanaugh, M.A., Boswell, W.R., Roehling, M.V., Boudreau, J.W., 2000. An empirical examination of self-reported work stress among U.S. managers. J. Appl. Psychol. 85, 65–74. https://doi.org/10.1037/0021-9010.85.1.65.

Chen, H., Hai, Y., Tu, L., Fan, J., 2023. Not all information security-related stresses are equal: the effects of challenge and hindrance stresses on employees' compliance with information security policies. Behav. Inf. Technol. https://doi.org/10.1080/0144929X.2023.2295950.

Chen, H., Liu, M., Lyu, T., 2022a. Understanding employees' information security–related stress and policy compliance intention: the roles of information security fatigue and psychological capital. Inf. Comput. Secur. 30, 751–770. https://doi.org/10.1108/ICS-03-2022-0047.

Chen, L., Xie, Z., Zhen, J., Dong, K., 2022b. The impact of challenge information security stress on information security policy compliance: the mediating roles of emotions. Psychol. Res. Behav. Manag 15, 1177–1191. https://doi.org/10.2147/PRBM.S359277.

Cullen, F., Link, B., Wolfe, N., Frank, J., 1989. The social dimensions of police officer stress. Justice. Q. 2, 507–533.

D'Arcy, J., Herath, T., Shoss, M.K., 2014. Understanding employee responses to stressful information security requirements: a coping perspective. J. Manag. Inf. Syst. 31, 285–318. https://doi.org/10.2753/MIS0742-1222310210.

D'Arcy, J., Teh, P.-L., 2019. Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization. Inf. Manag. 56. https://doi.org/10.1016/j.im.2019.02.006.

De Witte, H., 2000. Work Ethic and Job insecurity: Assessment and Consequences For well-being, Satisfaction and Performance At work, in: From Group to Community. Garant, pp. 325–350.

Eddy, E.R., Stone, D., Eugene, E., 1999. The effects of information management policies on reactions to Human resource information systems: an integration of privacy and procedural justice perspectives. Pers. Psychol 52, 335–358. https://doi.org/10.1111/j.1744-6570.1999.tb00164.x.

Frank, M., Kohn, V., 2021. How to mitigate security-related stress: the role of psychological capital. Presented at the. In: Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 4538–4547. https://doi.org/10.24251/hicss.2021.550.

Fried, Y., Rowland, K.M., Ferris, G.R., 1984. The physiological measurement of work stress: a critique. Pers. Psychol 37, 583–615.

Hang, Y., Hussain, G., Amin, A., Abdullah, M.I., 2022. The moderating effects of technostress inhibitors on techno-stressors and employee's well-being. Front. Psychol 12. https://doi.org/10.3389/fpsyg.2021.821446.

Hwang, I., Cha, O., 2018. Examining technostress creators and role stress as potential threats to employees' information security compliance. Comput. Hum. Behav 81, 282–293. https://doi.org/10.1016/j.chb.2017.12.022.

Hwang, I., Kim, S., Rebman, C., 2022. Impact of regulatory focus on security technostress and organizational outcomes: the moderating effect of security technostress

inhibitors. Inf. Technol. People 35, 2043–2074. https://doi.org/10.1108/ITP-05-2019-0239.
Hwang, I., Seo, R., 2025. Mitigating security stress: exploring the contingent role of collaborative communication in enhancing information security compliance. Comput. Secur. 151, 104326. https://doi.org/10.1016/j.cose.2025.104326.
Jawahar, I.M., Stone, T.H., Kisamore, J.L., 2007. Role conflict and burnout: the direct and moderating effects of political skill and perceived organizational support on burnout dimensions. Int. J. Stress. Manag 14, 142–159. https://doi.org/10.1037/1072-5245.14.2.142.
Jeon, S., Son, I., Han, J., 2023. Understanding employee's emotional reactions to ISSP compliance: focus on frustration from security requirements. Behav. Inf. Technol. 42, 2093–2110. https://doi.org/10.1080/0144929X.2022.2109512.
Kahn, R.L., Wolfe, D.M., Quinn, R.P., Snoek, J.D., Rosenthal, R.A., 1964. Organizational stress: Studies in Role Conflict and ambiguity, Organizational stress: Studies in Role Conflict and Ambiguity. John Wiley, Oxford, England.
Kim, S.Y., Park, H., Kim, H., Kim, J., Seo, K., 2022. Technostress causes cognitive overload in high-stress people: eye tracking analysis in a virtual kiosk test. Inf. Process. Manag 59, 103093. https://doi.org/10.1016/j.ipm.2022.103093.
Kreiner, G.E., 2006. Consequences of work-home segmentation or integration: a person-environment fit perspective. J. Organ. Behav 27, 485–507.
Lambert, E.G., Hogan, N.L., Camp, S.D., Ventura, L.A., 2006. The impact of work–family conflict on correctional staff: a preliminary study. Criminol. Crim. Justice 6. https://doi.org/10.1177/1748895806068572.
Lazarus, R.S., 1966. Psychological Stress and the Coping Process. McGraw-Hill, New York, NY, US.
Lee, C., Lee, C.C., Kim, S., 2016. Understanding information security stress: focusing on the type of information security compliance activity. Comput. Secur. 59, 60–70. https://doi.org/10.1016/j.cose.2016.02.004.
Li, Y., Huang, X., 2020. Understanding employees' ISP compliance from the perspective of emotion-focused coping approaches. Presented at the. In: 26th Americas Conference on Information Systems, AMCIS 2020.
Lundgren, M., Bergstrom, E., 2019. Security-related stress: a perspective on information security risk management. Presented at the. In: 2019 International Conference on Cyber Security and Protection of Digital Services. Cyber Security. https://doi.org/10.1109/CyberSecPODS.2019.8884877, 2019.
Luthans, F., Youssef-Morgan, C.M., 2017. Psychological capital: an evidence-based positive approach. Annu. Rev. Organ. Psychol. Organ. Behav. 4, 339–366. https://doi.org/10.1146/annurev-orgpsych032516-113324.
Malik, A.S., Acharya, S., Humane, S., 2024. Exploring the impact of security technologies on mental health: a comprehensive review. Cureus 16, e53664. https://doi.org/10.7759/cureus.53664.
Masood, K., Ahmed, B., Choi, J., Gutierrez-Osuna, R., 2012. Consistency and validity of self-reporting scores in stress measurement surveys. In: 2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society. Presented at the 2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 4895–4898. https://doi.org/10.1109/EMBC.2012.6347091.
McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., Lillie, M., 2018. The effect of resilience and job stress on information security awareness. Inf. Comput. Secur. 26, 277–289. https://doi.org/10.1108/ICS-03-2018-0032.
Mizrak, F., Demirel, H.G., Yasar, O., Karakaya, T., 2025. Digital detox: exploring the impact of cybersecurity fatigue on employee productivity and mental health. DISCOV. MENT. HEALTH 5. https://doi.org/10.1007/s44192-025-00149-x.
Moody, G.D., Galletta, D.F., 2015. Lost in cyberspace: the impact of information scent and time constraints on stress, performance, and attitudes online. J. Manag. Inf. Syst. 32, 192–224. https://doi.org/10.1080/07421222.2015.1029391.
Moore, J.E., 2000. One road to turnover: an examination of work exhaustion in technology professionals. MIS. Q. 24, 141–168. https://doi.org/10.2307/3250982.
Netemeyer, R.G., Boles, J.S., McMurrian, R., 1996. Development and validation of work–family conflict and family–work conflict scales. J. Appl. Psychol. 81, 400–410. https://doi.org/10.1037/0021-9010.81.4.400.
Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P., Moher, D., 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. https://doi.org/10.1136/bmj.n71.
Parker, D.F., DeCotiis, T.A., 1983. Organizational determinants of job stress. Organ. Behav. Hum. Perform 32, 160–177. https://doi.org/10.1016/0030-5073(83)90145-9.
Pham, H.C., Brennan, L., Furnell, S., 2019. Information security burnout: identification of sources and mitigating factors from security demands and resources. J. Inf. Secur. Appl. 46, 96–107. https://doi.org/10.1016/j.jisa.2019.03.012.
Pham, H.-C., El-Den, J., Richardson, J., 2016. Stress-based security compliance model - an exploratory study. Inf. Comput. Secur. 24, 326–347. https://doi.org/10.1108/ICS-10-2014-0067.
Posey, C., Shoss, M., 2024. Employees as a source of security issues in times of change and stress: a longitudinal examination of employees' security violations during the COVID-19 pandemic. J. Bus. Psychol 39, 1027–1048. https://doi.org/10.1007/s10869-023-09917-4.
Ragu-Nathan, T.S., Tarafdar, M., Ragu-Nathan, B.S., Tu, Q., 2008. The consequences of technostress for end users in organizations: conceptual development and empirical validation. Inf. Syst. Res. 19, 417–433. https://doi.org/10.1287/isre.1070.0165.
Reuter, C., Iacono, L.L., Benlian, A., 2022. A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead. Behav. Inf. Technol 41, 2035–2048. https://doi.org/10.1080/0144929X.2022.2080908.
Rizzo, J.R., House, R.J., Lirtzman, S.I., 1970. Role conflict and ambiguity in complex organizations. Adm. Sci. Q 15, 150–163. https://doi.org/10.2307/2391486.
Savoli, A., Addas, S., Fagnot, I., 2017. Coping with information security stressors in healthcare. In: Presented at the AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation.
Schaufeli, W.B., Leiter, M.P., Kalimo, R., 1995. The General Burnout Inventory: A Self-Report Questionnaire to Assess Burnout At the Workplace.
Shadbad, F.N., Biros, D., 2022. Technostress and its influence on employee information security policy compliance. Inf. Technol. People 35, 119–141. https://doi.org/10.1108/ITP-09-2020-0610.
Shadbad, F.N., Biros, D., 2021. Understanding employee information security policy compliance from role theory perspective. J. Comput. Inf. Syst. 61, 571–580. https://doi.org/10.1080/08874417.2020.1845584.
Skinner, E.A., Edge, K., Altman, J., Sherwood, H., 2003. Searching for the structure of coping: a review and critique of category systems for classifying ways of coping. Psychol. Bull 129, 216–269. https://doi.org/10.1037/0033-2909.129.2.216.
Spielberger, C.D., Vagg, P.R., 1999. Job Stress Survey: Professional Manual. Psychological Assessment Resources.
Tarafdar, M., Tu, Q., Ragu-Nathan, B.S., Ragu-Nathan, T.S., 2007. The impact of technostress on role stress and productivity. J. Manag. Inf. Syst. 24.
Thompson, N., McGill, T., Narula, N., 2024. No point worrying" – The role of threat devaluation in information security behavior. Comput. Secur. 143, 103897. https://doi.org/10.1016/j.cose.2024.103897.
Vander Elst, T., De Witte, H., De Cuyper, N., 2014. The job insecurity Scale: a psychometric evaluation across five European countries. Eur. J. Work. Organ. Psychol. 23, 364–380. https://doi.org/10.1080/1359432X.2012.745989.
Yazdanmehr, A., Li, Y., Wang, J., 2023. Employee responses to information security related stress: coping and violation intention. Inf. Syst. J. 33, 598–639. https://doi.org/10.1111/isj.12417.
Yepuru, P., Hsu, J.S.-C., 2019. Exploring the role of mindfulness on easing the negative impacts of information security stress. Presented at the. In: Proceedings of the 23rd Pacific Asia Conference on Information Systems: Secure ICT Platform for the 4th Industrial Revolution. PACIS, 2019.
Yepuru, P., Hsu, J.S.-C., Li, Y., 2018. Dealing with security related stress: mindfulness on countermeasures. Presented at the. In: Proceedings of the 22nd Pacific Asia Conference on Information Systems - Opportunities and Challenges for the Digitized Society: Are We Ready? PACIS, 2018.