American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Cybersecurity Fatigue and Protective Behavior Among Remote Employees

Dr. Emily R. Carter

Associate Professor, University of Melbourne, Australia

Abstract

Remote work has transformed organizational cybersecurity from a predominantly infrastructure-centered concern into a distributed behavioral challenge in which employees routinely make security decisions while managing deadlines, digital interruptions, domestic distractions, authentication requirements, security warnings, software updates, and multiple communication platforms. Repeated exposure to these demands may produce cybersecurity fatigue, a state characterized by mental weariness, frustration, reduced perceived control, and disengagement from security-related decisions. This study examines the relationship between cybersecurity fatigue and protective behavior among remote employees through a simulation-based analytical design.

The manuscript synthesizes established evidence on security fatigue, information-security stress, cybersecurity awareness, remote-work security, and employee security behavior and develops a reproducible synthetic dataset representing 240 hypothetical remote employees. The simulated analysis evaluates whether increasing cybersecurity fatigue is associated with deterioration in protective behaviors such as suspicious-message verification, secure authentication, policy adherence, use of approved access mechanisms, and timely security action.

The simulated results demonstrate a strong negative association between cybersecurity fatigue and protective behavior ($r = -0.763$), while a simple regression model explains approximately 58.3% of the simulated variance in protective behavior. Employees represented in the high-fatigue condition exhibit substantially weaker protective-behavior scores than those represented in low- and moderate-fatigue conditions. These results are illustrative rather than empirical population estimates, but they demonstrate a theoretically credible mechanism through which excessive security friction may undermine organizational protection. The paper argues that effective cybersecurity governance should reduce unnecessary cognitive burden rather than depend exclusively on additional warnings, mandatory training, and employee responsibility.

Keywords: cybersecurity fatigue; remote employees; protective behavior; information security; security compliance; remote work; human factors; cybersecurity awareness

1. Introduction

The expansion of remote and hybrid work has altered the environment in which organizational cybersecurity decisions are made. Employees who previously operated within comparatively standardized office networks now interact with corporate applications through home networks, cloud

services, mobile devices, collaboration platforms, virtual private networks, multifactor authentication systems, and geographically distributed information environments. Remote working therefore extends cybersecurity beyond the technical perimeter of the organization and places greater responsibility on individual employees to recognize threats and maintain secure routines. Nwankpa and Datta specifically demonstrated that cybersecurity awareness and policy conditions are important to precaution-taking among remote workers, emphasizing that distributed work arrangements require behavioral as well as technological security capabilities.

The increased responsibility placed on employees can, however, create a paradox. Cybersecurity controls are intended to reduce organizational risk, yet continuously requiring users to evaluate warnings, create and update credentials, approve authentication requests, distinguish legitimate messages from sophisticated phishing attempts, complete repetitive training, follow complex access procedures, and respond to security notifications may impose a considerable cognitive burden. Stanton, Theofanos, Prettyman, and Furman identified this phenomenon as security fatigue and found that affected users expressed resignation, loss of control, fatalism, risk minimization, and decision avoidance. Their work established that cybersecurity failure cannot always be explained by ignorance or deliberate negligence; it can also emerge when individuals perceive security demands as excessive, repetitive, or difficult to integrate into their primary activities.

Remote working can intensify this problem because cybersecurity requirements coexist with non-security demands. Employees may be responding to deadlines, online meetings, family interruptions, digital communication overload, performance monitoring, and expectations of rapid availability while simultaneously being asked to exercise careful security judgment. Trang and Nastjuk experimentally showed that time-pressure-induced stress can increase information-security-policy non-compliance, while Posey and Shoss later found in a longitudinal work-from-home study that competing security demands and other daily stressors were associated with employee security violations. These findings make cybersecurity fatigue especially relevant to remote-work governance because protective action often occurs under conditions of divided attention rather than in isolated security situations.

Protective behavior in the present study refers to voluntary or required employee actions that reduce the probability or potential consequences of a cybersecurity incident. Such behavior includes scrutinizing suspicious messages, protecting credentials, using approved authentication and network-access procedures, applying updates, reporting incidents, protecting sensitive information, and complying with organizational security requirements. The effectiveness of these actions depends not only on knowledge but also on employee motivation, perceived usability, self-efficacy, workload, organizational support, and the degree to which cybersecurity procedures interfere with primary job tasks. Research on gamified workforce training has shown that appropriately designed learning interventions can strengthen security-related self-efficacy and behavioral outcomes, suggesting that the manner in which security demands are delivered can be as important as the amount of security information provided.

Against this background, the present paper examines cybersecurity fatigue as a behavioral risk factor in remote employment. Because no original respondent dataset was supplied, the study does not present invented employee survey findings as factual evidence. Instead, it combines verified scholarly literature with a transparent simulation of 240 hypothetical remote employees to demonstrate how a

fatigue–behavior relationship can be tested quantitatively. The simulation is intended to support methodological development, hypothesis formation, and future empirical validation. Its central proposition is that cybersecurity programs become less sustainable when protective responsibility is transferred to employees without corresponding attention to cognitive workload, usable security, contextual training, and organizational resources.

2. Objectives of the Study

2.1 Assessment of the Fatigue–Behavior Relationship

The first objective is to examine the theoretical and simulated relationship between cybersecurity fatigue and protective cybersecurity behavior among remote employees. The study evaluates the proposition that higher fatigue is associated with weaker security-protective behavior because cognitive depletion, frustration, and perceived security friction can reduce employees' willingness or ability to undertake effortful security actions.

2.2 Comparison Across Cybersecurity-Fatigue Levels

The second objective is to compare protective-behavior patterns across low, moderate, and high levels of simulated cybersecurity fatigue. This comparison is intended to determine whether deterioration in secure behavior appears progressively as fatigue increases rather than being restricted only to employees represented at extreme levels of exhaustion.

2.3 Development of Human-Centered Organizational Responses

The third objective is to translate the fatigue–behavior relationship into practical cybersecurity-governance implications. Particular attention is given to reducing unnecessary security friction, strengthening employee self-efficacy, improving awareness and training design, simplifying routine security processes, and building organizational environments in which secure behavior remains feasible during periods of workload and time pressure.

3. Review of Literature

3.1 Security Fatigue, Stress, and Cognitive Burden

Security fatigue emerged as an important human-centered cybersecurity concept through research showing that users can become psychologically exhausted by repeated security requirements. Stanton and colleagues' foundational qualitative study involved 40 participants and found that more than half spontaneously described experiences associated with security fatigue even though fatigue was not the direct focus of the original interview protocol. Participants reported resignation, diminished control, avoidance, and cost–benefit reasoning that could discourage protective action.

Pham, Brennan, and Furnell subsequently approached the issue through information-security burnout and the job demands–resources perspective. Their study examined how security demands could contribute to burnout and how organizational and personal resources might mitigate this condition. The work reinforced the proposition that employees possess finite psychological and operational resources for meeting security demands and that continually increasing those demands can eventually become counterproductive.

Trang and Nastjuk expanded this line of reasoning by experimentally investigating occupational stress and information-security-policy compliance. Their in-basket experiment demonstrated that time pressure can generate stress that increases policy non-compliance. Importantly, the findings suggest that cybersecurity behavior is influenced by the broader work environment rather than solely by an employee's security knowledge. A technically reasonable security procedure can therefore become behaviorally ineffective when employees must perform it while experiencing severe task pressure.

Chen, Liu, and Lyu provided further evidence by studying 488 employees and examining information-security-related stress, fatigue, psychological capital, and policy compliance intention. Their analysis indicated that information-security fatigue mediated the relationship between security-related stress and compliance intention, while psychological capital functioned as a beneficial personal resource. This evidence is particularly relevant because it treats fatigue not merely as an unpleasant emotional state but as a mechanism through which organizational demands may influence security behavior.

3.2 Training Quality, Advice Fatigue, and Protective Capability

Security Education, Training, and Awareness programs are among the most common organizational responses to employee cyber risk. Their effectiveness, however, depends on relevance and design. Reeves, Calic, and Delfabbro interviewed employees about organizational cybersecurity training and found that programs could be perceived as boring or poorly aligned with employees' working realities. Participants' reactions were influenced by content, delivery, organizational practices, colleague behavior, and pre-existing beliefs about cybersecurity threats.

Reeves and colleagues later developed the concept of advice-related cybersecurity fatigue, showing that poorly implemented training and repeated generic security advice may generate fatigue rather than sustainable engagement. Their 2023 study explicitly examined employee perceptions of cybersecurity training and developed a measure of SETA advice-related fatigue. This finding challenges the assumption that increasing training frequency automatically produces stronger security behavior. Training that is repetitive, generic, excessively long, or poorly timed may add another layer of cognitive demand.

The implication is not that security training should be reduced indiscriminately, but that training should be designed around behavioral usability. Bitrián, Buil, Catalán, and Merli found that gamified e-training could improve employee self-efficacy and information-security and data-protection behavior, including improvements in phishing-related outcomes. Their evidence supports an alternative to compliance-heavy awareness programs: interventions can strengthen protective behavior by increasing confidence, engagement, contextual relevance, and opportunities for active learning.

More recent work has continued to emphasize variation among employees rather than treating the workforce as a uniform security population. Baltuttis, Teubner, and Adam developed a typology of cybersecurity behavior among knowledge workers, demonstrating that behavioral characteristics differ meaningfully across employee groups. Such heterogeneity suggests that uniform awareness campaigns may be less effective than interventions adapted to actual employee behavior and risk conditions.

3.3 Remote Work as a Context for Security Fatigue

Remote work creates a distinctive context because cybersecurity controls are performed within a less standardized and more personally managed digital environment. Nwankpa and Datta's study of remote workers found that cybersecurity awareness was associated with greater use of security precautions. Their work establishes that remote employees are not inherently less security-conscious; rather, behavior depends on how organizational policies, awareness, and perceived risk interact within remote-working conditions.

Posey and Shoss provide especially important evidence regarding stress. Their longitudinal study followed 333 employees working from home over ten working days and identified several stressors associated with daily security violations. Competing demands caused by security were particularly important, demonstrating that behavioral security risk may rise when cybersecurity requirements conflict with employees' immediate work obligations.

The literature therefore indicates a clear research opportunity. Existing studies have established security fatigue, burnout, training fatigue, policy stress, and remote-work cybersecurity behavior, but these literatures are often examined separately. The present study connects them through a focused fatigue–protective-behavior framework. Its novelty lies not in claiming new empirical population evidence but in demonstrating a transparent simulation model that can be used as a foundation for a properly powered future field study of remote employees.

4. Research Methodology

4.1 Research Design and Analytical Logic

The study adopts a simulation-based quantitative research design supported by scholarly literature. No human participants were recruited, no questionnaire was administered, and no personal employee data were processed. A synthetic dataset containing 240 hypothetical remote-employee observations was generated solely to demonstrate the expected statistical behavior of the proposed relationship.

Cybersecurity fatigue was represented on a continuous five-point scale ranging from 1 to 5. Protective behavior was also represented on a five-point scale, with higher scores indicating more consistent cybersecurity precautions. The simulation imposed a theoretically plausible negative relationship between fatigue and protective behavior and added random individual variation so that observations would not lie on a deterministic line.

4.2 Proposed Measurement Framework

A future empirical investigation should preferably employ established multi-item instruments for cybersecurity fatigue and employee security behavior. However, consistent with the study's concise survey-development objective, the following five questions are proposed as an initial screening battery. Responses may be measured using a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Table 1: Proposed Five-Item Questionnaire for Future Empirical Validation

Item	Proposed Questionnaire Statement	Primary Construct
Q1	I feel mentally exhausted by the number of cybersecurity decisions I must make while working remotely.	Cybersecurity fatigue
Q2	Cybersecurity procedures frequently interrupt or complicate my main work responsibilities.	Security friction
Q3	I verify suspicious senders, links, or attachments before responding or providing information.	Protective verification behavior
Q4	I consistently use organization-approved authentication, access, update, and network-security procedures while working remotely.	Protective compliance behavior
Q5	I remain confident that I can follow important cybersecurity practices even when I am busy or under time pressure.	Security self-efficacy

Source: Proposed by the author for future empirical testing. These questions were not administered in the present simulation.

The five-item battery is intentionally concise and should be treated as a preliminary screening instrument rather than a fully validated psychometric scale. A subsequent empirical study should test internal consistency, convergent and discriminant validity, measurement invariance, and criterion validity and should expand each latent construct with multiple items where appropriate.

4.3 Statistical Procedure, Transparency, and Ethical Position

The simulated analysis uses descriptive statistics, fatigue-level comparisons, Pearson correlation, and simple linear regression. For interpretive comparison, cybersecurity fatigue was categorized as low, moderate, or high. Low fatigue included simulated scores up to approximately 2.33, moderate fatigue covered approximately 2.34 to 3.66, and high fatigue represented scores above approximately 3.66.

Pearson's correlation coefficient was used to estimate the direction and strength of association between fatigue and protective behavior. Simple regression was used to estimate the change in simulated protective behavior associated with a one-unit change in fatigue and the proportion of simulated variance explained.

Because the dataset is entirely synthetic, institutional ethical approval and participant consent were not applicable to the present simulation. Nevertheless, any future empirical extension involving actual employees should obtain appropriate institutional ethics approval or exemption, provide informed-consent information, minimize collection of identifiable employment data, protect respondents from managerial retaliation, and ensure that participation or non-participation cannot affect employment

evaluation. Security-behavior research is particularly sensitive because employees may reasonably fear that disclosure of mistakes or policy deviations could be interpreted as misconduct.

5. Analysis

5.1 Distribution of Simulated Fatigue and Protective Behavior

The synthetic sample contains 240 observations. Mean cybersecurity fatigue across the simulated cases was approximately 2.99, while mean protective behavior was approximately 3.31 on the five-point scale. Categorical comparison reveals a pronounced behavioral gradient. The low-fatigue group recorded an average protective-behavior score of approximately 4.10. This declined to approximately 3.30 in the moderate-fatigue group and approximately 2.50 in the high-fatigue group.

Table 2: Simulated Protective Behavior Across Cybersecurity-Fatigue Levels

Fatigue Category	Simulated n	Mean Fatigue	SD Fatigue	Mean Protective Behavior	SD Protective Behavior
Low	55	1.87	0.35	4.10	0.48
Moderate	134	3.01	0.37	3.30	0.50
High	51	4.14	0.43	2.50	0.51

Source: Author-generated synthetic data; n = 240. Values are illustrative and do not represent surveyed employees.

The difference between the low- and high-fatigue conditions is approximately 1.60 scale points, indicating that the simulated model produces a substantial deterioration in protective behavior as cybersecurity fatigue increases. This pattern represents the central theoretical proposition of the study: security behavior can weaken not because employees reject security as a goal, but because sustained security demands become increasingly difficult to perform alongside primary work obligations.

5.2 Correlation and Regression Pattern

Pearson correlation analysis produced a simulated coefficient of:

$r = -0.763$, $p < .001$

The association is negative and strong within the generated dataset. Higher cybersecurity-fatigue values therefore correspond to lower levels of protective behavior in the simulation.

Simple linear regression produced an estimated slope of approximately:

$B = -0.660$

The simulated model explains approximately:

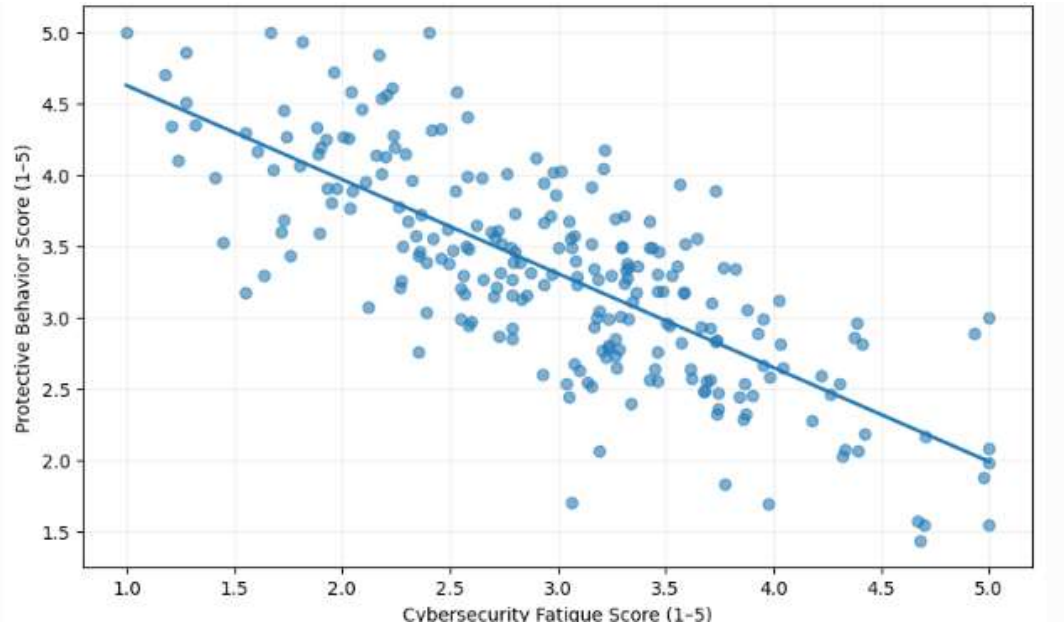
$R^2 = 0.583$

Thus, roughly 58.3% of variation in the synthetic protective-behavior scores is statistically associated with cybersecurity fatigue under the imposed simulation structure. This percentage must not be generalized to real organizations because the dataset was created specifically to represent a theoretically meaningful fatigue effect.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Graph 1: Simulated Relationship Between Cybersecurity Fatigue and Protective Behavior



Source: Author-generated simulation based on 240 synthetic observations.

Interpretation: The downward-sloping regression line demonstrates the simulated negative association. Cases toward the lower end of the fatigue scale tend to exhibit stronger protective behavior, whereas observations characterized by high fatigue tend to cluster at lower protective-behavior values.

Key Finding: The simulation supports the proposed hypothesis that rising cybersecurity fatigue can meaningfully erode consistent protective behavior when other conditions are held within the synthetic analytical framework.

5.3 Behavioral Meaning of the Simulated Findings

The simulated results should be interpreted as a methodological demonstration rather than a discovered population parameter. Nevertheless, the pattern is theoretically consistent with previous empirical evidence showing that stress, conflicting security demands, security burnout, and advice fatigue can weaken engagement with organizational cybersecurity requirements.

The analysis also demonstrates why cybersecurity metrics should not be restricted to knowledge-test scores or training-completion percentages. An employee may understand a rule but still fail to follow it when the procedure is cognitively demanding, disrupts an urgent task, appears repetitive, or is perceived as unlikely to generate a meaningful security benefit. Protective behavior should therefore be investigated as the outcome of both security competence and the conditions under which that competence must be exercised.

6. Discussion

6.1 Cybersecurity Fatigue as a Behavioral Security Risk

The central implication of this study is that cybersecurity fatigue should be treated as an organizational risk variable rather than simply as an employee attitude problem. The simulated negative relationship

between fatigue and protective behavior reflects mechanisms already identified in prior empirical research. Stanton and colleagues showed that users experiencing security fatigue could develop resignation, decision avoidance, and diminished perceived control, while Chen, Liu, and Lyu demonstrated that information-security fatigue can transmit the effects of security-related stress into weaker policy-compliance intentions. These findings imply that security governance becomes vulnerable when organizations continually increase employee obligations without examining the psychological and operational cost of compliance.

This interpretation is particularly important in remote work. Protective behavior often competes with tasks that employees perceive as more immediately connected with performance, customers, deadlines, or managerial expectations. Posey and Shoss found that competing security demands predicted increases in security violations among employees working from home, while Trang and Nastjuk experimentally linked time-pressure stress with non-compliance behavior. The problem is therefore not necessarily that employees undervalue cybersecurity. A worker may simultaneously believe security is important and bypass a procedure when the immediate cost of compliance becomes too high. Cybersecurity-fatigue management consequently requires attention to workflow design, not merely attempts to increase employee concern about threats.

6.2 From Repetitive Awareness to Usable and Adaptive Security

The results also question the assumption that the preferred response to every employee-related cyber risk is additional training. Reeves and colleagues found that employees can disengage from cybersecurity training when it is perceived as boring, generic, confusing, or poorly implemented; subsequent research on advice-related fatigue demonstrated that cybersecurity messaging itself can become a source of fatigue. Organizations should therefore distinguish between necessary learning and unnecessary repetition. Mandatory annual modules that present identical material to experienced employees may produce completion without meaningful behavioral learning.

A stronger approach would combine short contextual interventions, role-specific scenarios, phishing-resistant technical controls, just-in-time guidance, meaningful feedback, and employee-friendly reporting mechanisms. Bitrián and colleagues' gamification research provides evidence that interactive training can enhance security self-efficacy and improve behavioral outcomes. This does not imply that every security program should become a game. Rather, it demonstrates that employee engagement, confidence, relevance, and learning design matter. Training should help employees successfully perform protective behavior rather than repeatedly remind them that cyber threats exist.

Security controls themselves should also be evaluated for usability. If employees must repeatedly authenticate unnecessarily, interpret poorly designed warnings, remember numerous credentials, switch between incompatible security tools, or complete procedures that substantially interrupt productive work, the security system may create conditions favorable to avoidance. Human-centered cybersecurity therefore requires organizations to remove preventable friction while maintaining necessary assurance. The objective should be to make the safest action the easiest legitimate action whenever possible.

6.3 Organizational Responsibility and Sustainable Protective Behavior

The findings further support a shift away from narratives that characterize employees primarily as the weakest link in cybersecurity. Such narratives can encourage organizations to attribute incidents to individual carelessness while overlooking system design, workload, managerial pressure, confusing policy, inadequate technical controls, and poorly designed training. The behavioral typology developed by Baltuttis, Teubner, and Adam illustrates that employees differ substantially in their cybersecurity patterns, reinforcing the limitations of uniform interventions.

A sustainable security culture should distribute responsibility between employees and the organization. Employees remain responsible for reasonable protective actions, but organizations are responsible for making those actions understandable, achievable, proportionate, and compatible with legitimate work. Leaders can support this goal by monitoring the volume of security prompts, measuring security-related workload, simplifying access architecture, reducing duplicative policies, improving technical automation, and ensuring that incident reporting is psychologically safe.

The appropriate governance question is therefore not merely whether employees comply. Organizations should also ask whether their security environment is designed in a way that allows ordinary employees to comply consistently during real working conditions. Cybersecurity programs that appear effective in training rooms but collapse under deadline pressure, remote interruptions, or authentication overload are behaviorally fragile. Addressing cybersecurity fatigue can strengthen resilience by recognizing that human attention is an organizational resource that must be managed carefully rather than treated as unlimited.

7. Conclusion

Cybersecurity fatigue represents an increasingly important dimension of organizational security because modern employees are required to make frequent security decisions while performing digitally intensive primary work. Remote employment amplifies this issue by distributing security responsibility across home networks, cloud services, digital communication systems, multiple devices, and less standardized work environments. Existing research shows that security fatigue can involve resignation, frustration, loss of control, and decision avoidance, while occupational stress, competing security demands, and poorly designed training can undermine secure behavior.

The simulation developed in this study demonstrates the analytical implications of this relationship. Across 240 synthetic observations, cybersecurity fatigue and protective behavior exhibited a strong negative correlation of approximately −0.76. The simulated low-fatigue group displayed an average protective-behavior score of approximately 4.10 compared with approximately 2.50 among high-fatigue cases. These values are intentionally illustrative and must not be interpreted as observed employee statistics. Their purpose is to demonstrate a transparent quantitative framework that can subsequently be tested with genuine remote-worker data.

The organizational implication is that effective cybersecurity cannot depend indefinitely on adding more rules, warnings, training modules, authentication steps, and employee obligations. Security governance should actively reduce avoidable cognitive burden. Simplified workflows, phishing-resistant authentication, role-sensitive controls, contextual learning, supportive incident reporting, improved self-efficacy, and careful management of security notifications can help organizations maintain protection

without exhausting the workforce. Security effectiveness should therefore be evaluated partly through the ease with which employees can perform protective behavior under genuine operational pressure.

Future research should empirically test the proposed relationship using validated multi-item measures, diverse occupational populations, longitudinal or experience-sampling methods, and objective security-behavior indicators where ethically feasible. Important moderators may include security self-efficacy, workload, organizational support, policy usability, job autonomy, cybersecurity awareness, digital interruptions, and organizational security culture. Such research would allow investigators to determine when legitimate security demands become excessive and to identify the point at which additional cybersecurity requirements cease to improve protection and begin to undermine it. Sustainable cybersecurity ultimately requires not only secure technology and informed employees, but security systems designed around realistic human cognitive capacities.

References

1. Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal, 31*(4), 521–549. First published online in 2020.
2. Hsu, J. S.-C., Hung, Y. W., Hsieh, P.-J., & Chiu, C.-M. — Note: this study is 2024, so it should not be included if your cutoff is strictly before 2021.
3. Olt, C. M., & Mesbah, N. (2019). Weary of watching out? Cause and effect of security fatigue. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*.
4. 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. *Information & Management, 56*(7), 103151.
5. Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13–24.
6. Stanton, B. C., Prettyman, S. S., Theofanos, M. F., & Furman, S. M. (2016). Security fatigue. *IEEE Software*.
7. Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70–82.
8. Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security, 22*(4), 334–345.
9. Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79.
10. Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and Protection Motivation Theory. *Information & Management, 49*(3–4), 190–198.
11. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95.

12. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.
13. Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643.
14. Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64–71.
15. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125.
16. Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS)*.
17. Warkentin, M., & Johnston, A. C. (2009). An identity and social influence perspective on employee compliance with information security policies: Theoretical development and empirical test. *MIS Quarterly*.
18. D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98.
19. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.
20. Ertan, A., Crossland, G., Heath, C., Denny, D., & Jensen, R. (2020). Cyber security behaviour in organisations. *arXiv preprint arXiv:2004.11768*.