Forging the Future: Pioneering Approaches in Business, Management and Economics Engineering to Overcome Emerging Global Challenges - 2024

https://doi.org/10.24867/FUTURE-BME-2024-109 Original scientific paper

CYBER RISKS OF CYBERLOAFING - HRM PERSPECTIVES OF ORGANIZATIONAL SECURITY

Maja Križanec Cvitković[1] [0009-0007-7910-3764], Ana Globočnik Žunac[2] [0000-0002-4008-6027], Marko Antić[3] [0009-0001-5510-6713]

Abstract

Cyberloafing is becoming an increasing challenge for organizations. This practice presents a significant security risk to organizational systems. Security breaches can lead to serious consequences, including financial losses, compromised confidential information, and damage to the organization's reputation. Additionally, cyberloafing can negatively impact communication, disrupting work processes and reducing the effectiveness of team collaboration. The aim of this paper is to explore cyber risks related to cyberloafing and organizational security, focusing on analysing existing studies to identify the main risk factors and propose guidelines for their effective management. Using the systematic literature review (SLR) methodology, the Scopus and Web of Science databases were examined. The search identified relevant literature related to cyberloafing and cybersecurity. This document answers questions about the most common cyber risks associated with cyberloafing in organizations, how it affects the security of organizational data and networks. It explores the effects of cyberloafing on organizational communication and team collaboration effectiveness and provides guidelines and strategies for managing cyberloafing risks within organizations. These findings can contribute to security in organizations to better understand the security threats associated with cyberloafing, which can be valuable for academia and organizations especially in today's digitalized work environments.

Key words: *cyberloafing, cyber risks, organizational security, organizational communication, systematic literature review.*

[1] University North, Department of Media and Communication, Croatia, mkcvitkovic@unin.hr
[2] University North, Department of Business Economics, Croatia, ana.globocnik.zunac@unin.hr
[3] University North, Department of Media and Communication, Croatia, marantic@unin.hr

1. Introduction

Surfing the Internet by employees during work hours for personal reasons is called Cyberloafing or “non-work related computing” (Khansa et al., 2017, p. 142). Cyberloafing has become increasingly common and creates concern among business owners about organizational security. The rise of virtual work teams, flexible work arrangements, and the widespread use of electronic devices are some of the reasons that allow employees to engage in non-work-related activities during working hours. It may seem harmless, but it represents a significant challenge in the work environment. While cyberloafing can sometimes have a positive effect on employees by providing them with short mental breaks from work tasks, it also represents a significant challenge for organizations, primarily due to reduced productivity and increased security risks (Kirk et al., 2023). Some studies have identified cyberloafing as a deviant behavior in the workplace, specifically classified as "productivity deviance" because of its negative impact on employee productivity and financial losses for companies (Lim, 2002; Lim & Teo, 2005). Additionally, cyberloafing can increase an organization's vulnerability to security threats and cause network traffic disruptions due to excessive network usage (Liberman et al., 2011; Pee et al., 2008). More serious forms of cyberloafing, such as illegally downloading material or viewing inappropriate content, can expose companies to legal and ethical responsibilities (Vitak et al., 2011). So according to Statista data (2023), the manufacturing sector in the United States recorded 259 cases of data compromise and 638 ransomware attacks globally. Such figures point to the need for improved cyber security, considering that the number of attacks on the US supply chain will double between 2022 and 2023. In order to increase the security of the organizations and reduce the risks, the management of the online activities of employees becomes a key factor in strengthening the cyber security of the organizations if we take into account the fact that many companies face high costs of data breaches, on average 4.73 million dollars per incident in industrial organizations. Liberman et al. (2011, pp. 2192–2199) consider that Internet browsing carries risks for network security because employees may inadvertently download viruses that threaten organizational systems. For example, if employees engage in activities such as online gambling or viewing inappropriate content using organizational IT resources, the company could face serious damage to the organization's reputation and may face legal consequences.

1.1 Research objectives

The aim of this paper is to investigate the cyber risks associated with cyberloafing and organizational security through the analysis of existing studies, to determine the main risk factors and propose guidelines for their effective management. To achieve the goal of this work, the following research questions are asked:

Q1. What cyber risks are most often associated with cyberloafing in organizations?

Q2. How can cyberloafing compromise the security of organizational data and networks?
Q3. How can cyberloafing affect communication within organizations and the effectiveness of team collaboration?
Q4. What guidelines and strategies are outlined for managing cyberloafing risks in the organization?

1.2 Research approach

In this research, a systematic literature review (SLR) methodological approach was used (Snyder, 2019; Kraus et al., 2022). This approach ensures objectivity, systematicity and reliability in the collection of information and research results, contributing to existing knowledge about the risks of cyberloafing for organizational security. Scopus and Web of Science (WoS) databases were searched, with the key terms "cyberloafing", "risks" and " security".

2. Results

Using the Scopus database with the search term (TITLE-ABSTRACT-KEY ("cyberloafing" AND "risk" AND "security")), 5 scientific papers were found, while the keywords (TITLE-ABSTRACT-KEY ("cyberloafing" AND " risk")) resulted in a total of 10 scientific papers from 2017 to 2024, with searches conducted across all fields of the database. In the Web of Science (WoS) database, searches with the keywords: "cyberloafing" AND "risk" AND "security" yielded 5 scientific papers. "cyberloafing" AND "risk" resulted in 11 scientific papers from 2017 to 2024 across all fields (Figure 2). The total number of documents in the Scopus and WoS databases with the keywords "cyberloafing," "risk," and "security" amounts to 21 documents from 2017 to 2024 (Figure 1).

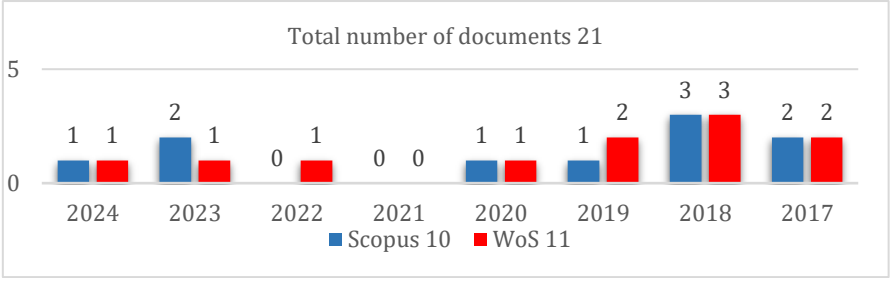

Figure 1. Documents by year investigating Cyberloafing, Risk, Security in Scopus and Wos database (2017- October 2024). Source: Authors' work: 2024

The area of the research topic/categories presents the period of 2017 to October 2024 and include various subject area. In both databases, the highest number of documents is found in the field of computer science and related disciplines, as well as in social sciences (Figure 2).

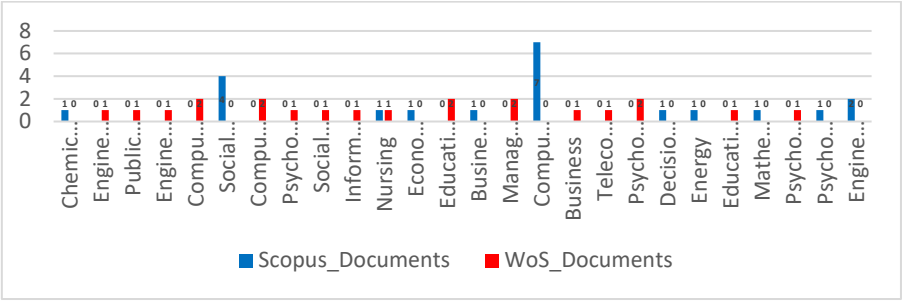

Figure 2. Documents by subject area investigating Cyberloafing, Risk, Security in Scopus and Wos database (2017- October 2024). Source: Authors' work: 2024

A systematic literature review found a total of 21 documents, of which 10 are in the Scopus database, and 11 in the WoS database. Overlaps were found in 8 documents and 2 documents found only in Scopus and 3 in WoS. A total of 13 documents. All 13 documents were reviewed, 7 of which are relevant to the research topic. Access is not possible for one document. During the review process, 4 relevant documents (from 2012 to 2023) were found outside the Scopus and Wos databases, bringing the total number of relevant documents to 11, which will be further analyzed in this work. The table shows the titles of scientific papers found by the specified search. It includes the database, the title of the work, the year of publication, the purpose (goal) of the work and the risks of cybelofing for the security of organizations from the perspective of human resource management (HRM) (Table 1).

Tabel 1. Risks of cybelofing to the security of organizations from a human resource management (HRM) perspective.

ID	**Author name, year** **The name of the work**	**The purpose(goal) of the work** **Risks of cybelofing to the security of organizations from a HRM perspective**
1	Khansa, L., Kuem, J., Siponen, M., & Kim, S. S. (2017) To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls	Examines how announcing formal controls affects employees' cyberloafing. - downloading malicious software or allowing unauthorized access to the organization's network, disrupting operations by overloading network resources, engaging in illegal activities (downloading pirated content, accessing inappropriate websites) exposes the company to legal and ethical responsibilities
2	Hadlington, L., & Parsons, K. (2017)	Explores (from UK) how cyberloafing and internet addiction endanger organizational information security.

ID	Author name, year The name of the work	The purpose(goal) of the work Risks of cybelofing to the security of organizations from a HRM perspective
	Can cyberloafing and internet addiction affect organisational information security?	-employees with a lower awareness of information security increases vulnerability to cyber threats, visiting unsafe websites (gambling sites, adult content, checking personal e-mail) increases the risk of malware infections and cyber-attacks, leads to network congestion through excessive use of network
3	Ross, J. (2018)	Highlights the growing trend of cyberloafing among healthcare professionals, who engage in non-work during work hours.
	Cyberloafing' in health care: A real risk to patient safety	- jeopardizing patient safety and information security in healthcare institutions, risk of infection with malicious software and data breaches, proposed solution "zone without interruption"
4	Vernon-Bido, D., Grigoryan, G., Kavak, H., & Padilla, J. (2018)	Explores how employee cyberloafing affects organizational cyber risk by reducing productivity and increasing malware and security breach risks.
	Assessing the impact of cyberloafing on cyber risk	-introduction of malicious software through unsafe websites (pornography, gambling), employees with a lower level of information security awareness (online shopping, checking personal e-mail and social media)
5	Jiang, H., Tsohou, A., Siponen, M., & Li, Y. (2020)	Discusses how Internet monitoring, intended to reduce cyberloafing and improve security, can negatively affect employees.
	Examining the side effects of organizational Internet monitoring on employees	-Internet surveillance can reduce employee trust and commitment, which weakens compliance with security policies and reduced awareness of security practices
6	Kolog, E. A., Mensah, I., & Egala, S. B. (2024).	Examines the impact of cyberloafing on productivity and cybersecurity risks in Ghana's public sector, focusing on factors such as security, surveillance and security risks that deter cyberloafing.
	Cyberloafing deterrence in the public sector of Ghana	-strain network resources (slowing down or interrupting critical operations), personal use of organizational systems can reduce system performance, introduction of malicious software (visiting unprotected websites - viruses, trojans), access to unprotected websites (spyware infections), leads to unauthorized access to confidential information, data leakage (use of personal e-mail or other unprotected communication channels), frequent use of the Internet reduces the security vigilance of employees (identity theft, manipulative tactics)
7	Schroeder, A. N., & Whitaker, J. H. (2018)	Explores technology-enabled employee deviance, like cyberbullying and cyberloafing, through Robinson and Bennett's workplace deviance model.

ID	Author name, year The name of the work	The purpose(goal) of the work Risks of cybelofing to the security of organizations from a HRM perspective
	An examination of workplace cyberdeviance	-visiting unsafe websites (downloading viruses or malware), risk of leaking sensitive information (Using unprotected platforms or unencrypted channels), Downloading unverified applications from unauthorized sources, exposure to phishing attacks (checking personal email and social media), reduced awareness about security protocols, network overload (excessive data usage, reduces bandwidth and system performance)
8	Kim, K., del Carmen Triana, M., Chung, K. & Oh, N. (2016)	Examines cyberloafing, focusing on how personality traits such as conscientiousness and emotional stability influence its frequency.
	When do employees cyberloaf? An interactionist perspective examining personality, justice, and empowerment	-Organizations in areas with high data security requirements should consider conscientiousness and emotional stability when hiring (screening candidates for traits such as conscientiousness), negative emotional states (consider interventions that reduce negative impacts on employee emotions)
9	Koay, K. Y., Soh, P. C. H., & Chew, K. W. (2017)	Examines the relationship between employees' private demands, job stress, and cyberloafing.
	Do employees' private demands lead to cyberloafing?	- high levels of stress reduce employee attention to security protocols (unauthorized access or malware infection), reduced attention to safe use of information systems
10	Lim, V. K. G., & Teo, T. S. H. (2022)	Reviews existing research on cyberloafing and offers guidelines for future studies.
	Cyberloafing: A review and research agenda	- exposing the system to unsafe websites (downloading malicious software and compromising network security), excessive personal use of the Internet (overloading network resources, slowing down business applications)
11	Fei, Z (2023)	Examines various aspects of cyberloafing, including its predictors and consequences, and how it affects the work environment.
	The impact of cyberloafing: A literature review and future prospects	-depletes the working resources of employees (reduced work efficiency), browsing the Internet and downloading programs (introduce viruses), exposure of the organization to significant legal and reputational problems (online gambling or watching inappropriate content)

The reviewed papers represent theoretical frameworks or empirical research on the topic. Findings from the literature review indicate that cyberloafing represents a significant security risk for organizations. The findings reveal that cyberloafing can cause a slowdown or interruption of critical operations. Employees who are often involved in cyberloafing generally have a lower level of awareness of security threats, thereby increasing the organization's vulnerability to cyber-attacks such as identity theft and manipulative tactics. Cyberloafing can reduce productivity

and strain network resources, increasing the risk of malware infection from visiting unsafe websites, such as gambling sites or adult content. Such activities can result in data leakage as employees use unsecured channels to communicate or view personal e-mail. From the example in the health sector, there are possible serious implications for patient safety, given that the use of personal devices and access to insecure websites can compromise information security, which can lead to disruptions in key health services. Cyberloafing can result in reduced employee awareness of security protocols, which increases the possibility of overlooking threats such as phishing attacks. Monitoring the online behavior of employees can have certain psychological consequences because it reduces trust, which can weaken compliance with security policies, which further increases the vulnerability of the organization. Organizations in sectors with high data security requirements should consider traits such as conscientiousness and emotional stability when hiring. High levels of stress at work can also result in an increased frequency of cyberloafing, further compromising information security within an organization.

3. Discussion

The systematic review of the literature carried out in this paper presents an overview of cyber risks related to cyberloafing from the perspective of human resource management in the context of organizational security. In the Scopus and Web of Science databases, many works related to cyberloafing can be found, but the results show an insufficient number of works that deal with the researched topic.

3.1 The most often cyber risks associated with cyberloafing in organizations

The most common risks cited are the reduction of information security due to unknowingly downloading a malicious file or visiting unsafe sites, which can lead to malware infections and unauthorized network access. Excessive use of network resources for personal needs can overload the network, slow down the system and reduce the efficiency of business applications. Activities such as illegally downloading content or visiting inappropriate sites can cause legal and ethical consequences and threaten the reputation of the organization. Frequent cyberloafing reduces employee awareness of security protocols and increases the risk of security threats such as phishing attacks. The use of personal e-mail or insecure communication channels can compromise data confidentiality and lead to information leakage.

3.2 Cyberloafing can compromise the security of organizational data and networks

Cyberloafing can significantly compromise the security of organizational data and networks because employees often visit insecure websites or use unsecured communication channels, increasing the risk of downloading malware, such as viruses and spyware. Security aspects of the network can be compromised due to

excessive use of network resources leading to congestion, network slowdowns and business disruptions. Visiting unsafe sites increases the possibility of infections and cyberattacks. Access to confidential information is provided due to personal use of e-mail or unsecured communication channels. Reduced awareness of security threats due to employees' reduced attention to security protocols, making it easier for attackers to exploit system weaknesses, such as phishing attacks and identity theft.

3.3 The impact of cyberloafing on organizational communication and team collaboration efficiency

Cyberloafing can positively and negatively affect organizational communication and team collaboration. By distracting employees and disrupting work processes, which reduces their attention and responsibility towards colleagues, which affects the efficiency of communication and can lead to delays in completing tasks. For example, if they are burdened with personal problems and their concentration is divided, they may inadvertently compromise organizational security by clicking on the Internet or communicating without sufficient attention to sensitive information, which can prevent the flow of essential information and reduce the effectiveness of teamwork. Reduced engagement in collaborative activities weakens team cohesion, making it difficult to achieve goals that rely on effective team collaboration. Occasional cyberloafing allows employees to take a mental break from work tasks, and in this way can help reduce stress and increase productivity through short breaks to increase efficiency after returning to work tasks.

3.4 The guidelines and strategies for managing cyberloafing risks in organization

To reduce the cyber risks caused by cyberloafing to increase the security of organizations, a combination of formal rules on internet use, strategic supervision and employee education is recommended. Through clear guidelines on acceptable behavior on the Internet during working hours, with sanctions for violations if necessary, and through employee training on security protocols and raising awareness of security threats, the likelihood of risky behavior can be reduced. Establishing "no-disturbance zones" for key tasks and limiting the use of personal devices, when necessary, is recommended. Organizations can use monitoring systems that notify administrators when employees are visiting unsafe websites or spending too much time on non-work activities. A balanced approach is recommended to avoid negative effects on employee motivation and confidence. Encourage responsible use of the Internet and actively involve employees in the development of security policies. Setting a proportionate share of time for personal Internet use and limiting access to non-business websites. Regular training on cyber security further increases employees' awareness of potential threats, creating a secure work environment.

4. Conclusions

Cyberloafing represents a security risk, potentially endangering data, communication and security within organizations. By identifying key risks and vulnerable security aspects and proposing strategies for managing these risks, an important scientific contribution is made to understanding and mitigating cyber risks associated with cyberloafing in organizations. The necessary digitization of work environments highlights the need for constant research into the role of human resources in managing this problem to maintain the security of organizations. These findings and guidelines are valuable for the academic community, the public sector, private organizations and companies because they can contribute to the development of new approaches to reducing security threats and be a starting point for new research in digitized work environments.

REFERENCES

[1] Adawiyah, R., Azizan, A., Sahar, A., & Herawati, I. (2023). Relationship between smartphone addiction, personality traits and cyberloafing behaviour among Malaysian youths. *Asian Journal of University Education, 19*(2), 395–402. https://doi.org/10.24191/ajue.v19i2.22228

[2] Banerjee, S., & Thakur, S. (2018). Understanding intrafactor relationships in cyberloafing using predictive apriori algorithm. In D. K. Mishra, M. K. Nayak, & A. Joshi (Eds.), *Information and communication technology for sustainable development* (pp. 223–230). Springer. https://doi.org/10.1007/978-981-10-3932-4_23

[3] Fei, Z. (2023). The impact of cyberloafing: A literature review and future prospects. *Journal of Education, Humanities and Social Sciences, 24*, 904–911. https://doi.org/10.54097/ez4hda76

[4] Gökçearslan, Ş., Durak, H. Y., & Esiyok, E. (2023). Emotion regulation, e-learning readiness, technology usage status, in-class smartphone cyberloafing, and smartphone addiction in the time of COVID-19 pandemic. *Journal of Computer Assisted Learning, 39*(5), 1450–1464. https://doi.org/10.1111/jcal.12785

[5] Hadlington, L., & Parsons, K. (2017). Can cyberloafing and internet addiction affect organisational information security? *Cyberpsychology, Behavior, and Social Networking, 20*(9), 567–571. https://doi.org/10.1089/cyber.2017.0239

[6] Jiang, H., Tsohou, A., Siponen, M., & Li, Y. (2020). Examining the side effects of organizational Internet monitoring on employees. *Internet Research, 30*(6), 1613–1630. https://doi.org/10.1108/INTR-08-2019-0360

[7] Khansa, L., Kuem, J., Siponen, M., & Kim, S. S. (2017). To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls. *Journal of Management Information Systems, 34*(1), 141–176. https://doi.org/10.1080/07421222.2017.1297173

[8] Kirk, A., Parker, S. K., & Zacher, H. (2023). Cyberloafing: Investigating the importance and implications of new and known predictors. *Collabra: Psychology, 9*(1), 57391. https://doi.org/10.1525/collabra.57391
[9] Koay, K. Y., Soh, P. C. H., & Chew, K. W. (2017). Do employees' private demands lead to cyberloafing? The mediating role of job stress. *Internet Research, 27*(5), 1062–1081. http://doi.org/10.1108/MRR-11-2016-0252
[10] Kolog, E. A., Mensah, I., & Egala, S. B. (2024). Cyberloafing deterrence in the public sector of Ghana. *Information Systems Development, 23*(1), 1–23. https://doi.org/10.1002/isd2.12316
[11] Kraus, S., Breier, M., Lim, W. M., Dabić, M., Kumar, S., Kanbach, D., & Ferreira, J. J. (2022). Literature reviews as independent studies: Guidelines for academic practice. *Review of Managerial Science, 16*(8), 2577–2595. http://doi.org/10.1007/s11846-022-00588-8
[12] Li, Q., Xia, B., Zhang, H., Wang, W., & Wang, X. (2022). College students' cyberloafing and the sense of meaning of life: The mediating role of state anxiety and the moderating role of psychological flexibility. *Frontiers in Public Health, 10*, 905699. https://doi.org/10.3389/fpubh.2022.905699
[13] Liberman, B., Seidman, G., McKenna, K. Y. A., & Buffardi, L. E. (2011). Employee job attitudes and organizational characteristics as predictors of cyberloafing. *Computers in Human Behavior, 27*(6), 2192–2199. https://doi.org/10.1016/j.chb.2011.06.015
[14] Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing, and organizational justice. *Journal of Organizational Behavior, 23*(5), 675–694. https://doi.org/10.1002/job.161
[15] Kim, K., del Carmen Triana, M., Chung, K. and Oh, N. (2016), When Do Employees Cyberloaf? An Interactionist Perspective Examining Personality, Justice, and Empowerment. *Hum Resour Manage*, *55*, 1041-1058. https://doi.org/10.1002/hrm.21699Lim, V. K. G., & Teo, T. S. H. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. *Information & Management, 42*(8), 1081–1093. https://doi.org/10.1016/j.im.2004.12.002
[16] Lim, V. K. G., & Teo, T. S. (2024). Cyberloafing: A review and research agenda. *Applied Psychology, 73*(1), 441–484. http://doi.org/10.1111/apps.12452
[17] Ross, J. (2018). 'Cyberloafing' in health care: A real risk to patient safety. *Journal of Peri Anesthesia Nursing, 33*(4), 560–562. https://doi.org/10.1016/j.jopan.2018.05.003
[18] Schroeder, A. N., & Whitaker, J. H. (2018). An examination of workplace cyberdeviance. *The Brave New World of eHRM 2.0*, 279–312.
[19] Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
[20] Statista. (2023). *Annual number of data compromises in manufacturing and utilities in the U.S*. https://www.statista.com/statistics/1367262/us-annual-number-of-data-compromises-in-manufacturing/

[21] Statista. (2023). *Industries targeted by ransomware attacks*. Retrieved October 4, 2024. https://www.statista.com/statistics/1368824/industries-targeted-industrial-ransomware-attacks-by-number-of-attacks/
[22] Statista. (2023). *Most targeted industries by ransomware attacks in the U.S*. Retrieved October 4, 2024. https://www.statista.com/statistics/1323599/us-most-targeted-industries-by-ransomware-attacks/
[23] Vernon-Bido, D., Grigoryan, G., Kavak, H., & Padilla, J. (2018). Assessing the impact of cyberloafing on cyber risk. *Proceedings of the 2018 Spring Simulation Conference* (SpringSim). https://doi.org/10.22360/SpringSim.2018.ANSS.020
[24] Vitak, J., Crouse, J., & LaRose, R. (2011). Personal internet use at work: Understanding cyberslacking. *Computers in Human Behavior, 27*(5), 1751–1759. https://doi.org/10.1016/j.chb.2011.03.002
[25] Wagner, D. T., Barnes, C. M., Lim, V. K. G., & Ferris, D. L. (2012). Lost sleep and cyberloafing: Evidence from the laboratory and a daylight- saving time quasi-experiment. *Journal of Applied Psychology, 97*(5), 1068–1076. https://doi.org/10.1037/a0027557