HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 3. szám 101–112.
DOI: 10.32567/hm.2025.3.6

Pál Károly Laska[1]

Empirical Analysis of the Impact of Personality Traits on Cybersecurity Awareness

A Scientometric and Network-Based Approach

Abstract

This study investigates the relationship between personality traits and cybersecurity awareness through a bibliometric and network analysis of scientific publications indexed in Scopus between 2000 and 2023. Using VOSviewer software, the research identifies keyword co-occurrence patterns, thematic clusters and temporal research trends in this interdisciplinary domain. The scientometric approach is complemented with theoretical insights from psychology – particularly the Big Five personality model – and cybersecurity behaviour research. Results indicate that personality traits significantly shape security awareness, influencing susceptibility to social engineering, phishing and compliance behaviour. Network analysis highlights the increasing integration of psychological constructs into cybersecurity education and policy. The study argues for the adoption of personality-based adaptive training programmes, particularly in the public sector, where tailored interventions can enhance resilience against human-factor-related security breaches.

Keywords: cybersecurity awareness, personality traits, Big Five model, scientometric analysis, network analysis, social engineering, adaptive training

[1] Doctoral candidate, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: Laska.Pal.Karoly@uni-nke.hu

Introduction

Cybersecurity has evolved from a purely technical discipline into a complex, multidisciplinary field that increasingly recognises the human factor as a critical component of security resilience. While technological solutions such as encryption, firewalls and intrusion detection systems remain essential, empirical evidence suggests that human behaviour often constitutes the weakest link in the security chain.[2] Among the various human factors influencing security outcomes, personality traits have emerged as a significant determinant of cybersecurity awareness, decision-making and policy compliance.[3]

The Big Five personality model – openness, conscientiousness, extraversion, agreeableness, and neuroticism – has been widely studied in psychology as a predictor of behaviour across diverse domains, including workplace performance, health behaviour and risk-taking.[4] In the cybersecurity context, these traits influence not only the likelihood of engaging in risky online behaviour but also the capacity to detect and resist social engineering attacks.[5] For example, high conscientiousness has been associated with greater adherence to security protocols, whereas high openness may correlate with exploratory behaviour that increases exposure to threats.[6]

Despite these insights, the integration of psychological constructs into cybersecurity strategy remains limited. Existing research is fragmented, with studies dispersed across information systems, psychology, criminology and behavioural sciences.[7] This fragmentation complicates the development of unified, evidence-based interventions that could enhance security awareness through personality-tailored training programmes.

To address this gap, the present study applies a scientometric and network analysis approach to systematically map the literature on personality traits and cybersecurity awareness. By analysing keyword co-occurrence patterns, thematic clusters and temporal evolution in the research landscape, we aim to:

1. Identify the central concepts and dominant research themes in this interdisciplinary field.
2. Examine the degree to which psychological frameworks have been incorporated into cybersecurity studies over time.
3. Highlight potential directions for future empirical research and policy development.

Ultimately, the study seeks to contribute to the emerging paradigm of psychologically informed cybersecurity, advocating for adaptive awareness programmes that align

[2] Pont–Mata 2016; Amankwa et al. 2020.
[3] Barabási–Albert 1999; Blasco–Quaglia 2018.
[4] Boban 2014.
[5] Wang et al. 2021.
[6] McCormac et al. 2017; Padayachee 2022.
[7] Doucek et al. 2019; Uffen et al. 2012.

with individual differences in personality.[8] This approach aligns with recent calls for moving beyond "one-size-fits-all" training and towards personalised, data-driven interventions.[9] Moreover, latest developments in cybersecurity education emphasise the implementation of adaptive learning frameworks that dynamically respond to individual learner profiles. For instance, the Adaptive Cybersecurity Training Framework for Social Media Risks (ACSTF-SMR) demonstrated significant improvements in employee engagement and learning outcomes by customising training modules to individual preferences and proficiency levels.[10] This evidence underscores the feasibility and effectiveness of personalised, psychology-informed interventions, which align precisely with the evolving paradigm of human-centred cybersecurity.

Research objective

The overarching objective of this research is to conduct a comprehensive scientometric and network-based investigation into the relationship between personality traits and cybersecurity awareness, with the aim of advancing both the theoretical understanding and the practical application of psychologically informed cybersecurity strategies. While isolated studies have examined the influence of specific psychological variables on security-related behaviour, there is a notable lack of integrative, cross-disciplinary mapping of the field. This study addresses this gap by systematically analysing the global body of research indexed in the Scopus database over the period 2000–2023, thereby identifying conceptual patterns, thematic clusters and temporal dynamics.

The research is guided by three interrelated objectives:

1. *Conceptual Mapping of the Field:* To identify and categorise the dominant themes, frameworks and methodological approaches in the literature on personality traits and cybersecurity awareness. This includes examining the prevalence of psychological constructs – particularly the Big Five personality model[11] – and their integration into cybersecurity-focused research. Mapping the conceptual terrain provides a clearer picture of the intellectual structure of the field and reveals underexplored intersections between disciplines such as psychology, information systems and criminology.[12]
2. *Network Structure and Interdisciplinary Linkages:* To perform a co-occurrence network analysis using *VOSviewer* in order to visualise the relationships among keywords, authors and thematic clusters. The analysis seeks to determine the degree of interdisciplinarity, the centrality of key concepts and the presence of network properties such as *small-world* and *scale-free* characteristics.[13] These structural properties can reveal how knowledge flows within the research

[8] This is also supported by Weems et al. in their study, when they state that insecure cyber behaviours were associated with lower levels of conscientiousness, higher levels of psychological symptoms such as somatic and depressive symptoms (Weems et al. 2018).
[9] Uffen–Breitner 2015; Wang et al. 2023.
[10] Ben Salamah et al. 2023.
[11] Boban 2014.
[12] McCormac et al. 2017; Uffen et al. 2012.
[13] Barabási–Albert 1999; Watts–Strogatz 1998.

community and whether certain clusters function as bridges between otherwise disconnected domains.[14]

3. *Implications for Adaptive Cybersecurity Interventions:* To derive actionable insights for policymakers, educators and organisational leaders on how personality assessment can be systematically incorporated into cybersecurity awareness programmes. The study argues that tailoring training content to personality profiles – rather than relying on uniform, generic approaches – can enhance engagement, retention and ultimately behavioural change.[15] This is particularly relevant for high-risk sectors such as government agencies, healthcare providers and critical infrastructure operators, where human error can have severe consequences.[16]

From a scientific contribution perspective, this research offers several advancements. First, it synthesises a fragmented literature base, bridging the gap between psychological theory and cybersecurity practice. Second, it applies bibliometric techniques to quantify and visualise the structural evolution of the field, enabling a more objective understanding of how research trends have shifted towards greater psychological integration over the past two decades. Third, it proposes a conceptual framework for the incorporation of personality-based tailoring into cybersecurity awareness interventions, grounded in empirical evidence from the analysed literature.

In sum, the research objective is not merely to describe the existing literature, but to generate a strategic, evidence-based roadmap for advancing psychologically informed cybersecurity. By integrating scientometric mapping with behavioural theory, this study seeks to facilitate a paradigm shift from reactive, technology-centred security measures to proactive, human-centred resilience strategies.

Methodology

This study adopts a mixed-method scientometric approach combining *bibliometric analysis* and *network analysis* to systematically explore the relationship between personality traits and cybersecurity awareness in academic literature. The methodological design follows three core principles: transparency, reproducibility and integration of quantitative mapping with qualitative interpretation.

Data source and search strategy

The primary data source was the Scopus database, selected for its comprehensive coverage of peer-reviewed journals, conference proceedings and book chapters

[14] Doucek et al. 2019.
[15] McCormac et al. 2017; Padayachee 2022; Uffen–Breitner 2015.
[16] Wang et al. 2023; Yeng et al. 2021.

across disciplines. The search strategy was defined to maximise precision (minimising irrelevant results) and recall (capturing the broadest relevant set of publications).[17]

This search string ensures inclusion of studies explicitly addressing both cybersecurity and personality-related variables, in line with the research objective. The publication period 2000–2023 was chosen to encompass the emergence of human-centric security research in the early 2000s and the recent acceleration of psychological integration in security studies.[18]

Inclusion and exclusion criteria

From the initial 1,082 records, a two-stage screening process was applied:

1. Title and abstract screening – Excluded papers not focusing on the human aspect of cybersecurity or personality-related constructs.
2. Full-text screening – Excluded works that:
   – focused solely on technical aspects without behavioural analysis
   – addressed personality traits but in non-cybersecurity contexts
   – were duplicates or non-peer-reviewed sources

The final dataset comprised 50 publications, representing the most relevant and methodologically rigorous contributions to the field.

Data extraction and pre-processing

For each selected publication, the following metadata were extracted:

- authors and affiliations
- year of publication
- source type (journal, conference, book chapter)
- keywords (author keywords and indexed keywords)
- abstract and full-text content (when accessible)
- citation counts
- DOI and Scopus identifiers

To ensure consistency, keyword harmonisation was performed, merging synonyms (e.g. *cyber security* to *cybersecurity*) and unifying American/British spelling variations (*behaviour* vs. *behavior*).

[17] Scopus 2023.
[18] McCormac et al. 2017; Padayachee 2022; Uffen–Breitner 2015.

Network analysis procedure

Bibliometric mapping was conducted using VOSviewer 1.6.19 to visualise keyword co-occurrence networks. Network parameters were configured as follows:

- counting method: full counting
- minimum keyword occurrence threshold: 3
- layout algorithm: VOS mapping with normalisation
- clustering resolution: 1.0 (default)
- attraction and repulsion parameters: default (2 and –1)

The resulting network graphs allowed the identification of clusters, each representing a thematic concentration in the literature. The size of nodes reflects the frequency of occurrence, while the proximity and link strength between nodes indicate conceptual relatedness.

To deepen the structural analysis, network metrics were calculated:

- degree centrality: measures the number of direct connections a keyword has
- betweenness centrality: indicates keywords acting as bridges between clusters
- closeness centrality: reflects the average shortest path length to all other keywords
- clustering coefficient: measures the extent to which nodes tend to cluster together

These metrics provided a quantitative basis for interpreting the role of central concepts such as *personality traits, security awareness* and *human behaviour*.

Validation and reliability measures

To ensure methodological robustness:

- search results were cross-validated with a secondary search in Web of Science
- two independent reviewers conducted screening to minimise selection bias
- network visualisations were replicated with alternative clustering resolutions to check stability
- all data processing steps were documented for reproducibility

Results

The bibliometric and network analysis revealed several distinct thematic clusters in the literature on personality traits and cybersecurity awareness. These clusters reflect the evolving interdisciplinary integration between *psychology, information security* and *human behaviour research*.

Cluster analysis

The co-occurrence network generated from the dataset identified four major clusters:

1. Cluster 1 – Human Factors in Cybersecurity Awareness
   - Core keywords: *cybersecurity, security awareness, information security, training, human error*
   - This cluster represents research focusing on awareness programmes, training effectiveness and behavioural interventions. Personality traits are examined in the context of susceptibility to phishing, password management habits and compliance with security policies.
2. Cluster 2 – Psychological Models and Personality Frameworks
   - Core keywords: *personality traits, Big Five, individual differences, risk perception*
   - This cluster links psychometric models to security behaviours, often testing how openness, conscientiousness, extraversion, agreeableness and neuroticism affect security decision-making.
   - Several studies within this cluster explore risk-taking behaviour and impulsivity as predictors of vulnerability to cyber threats.
3. Cluster 3 – Social Engineering and Insider Threats
   - Core keywords: *social engineering, phishing, insider threats, trust*
   - Here, personality traits are related to social manipulation susceptibility, with emphasis on trust propensity and agreeableness as double-edged factors – facilitating collaboration but also increasing vulnerability.
4. Cluster 4 – Network Security and Behavioural Modelling
   - Core keywords: *network analysis, behavioural modelling, resilience, incident response*
   - This cluster focuses on modelling human-in-the-loop security systems, often combining graph theory with behavioural parameters to predict system resilience.

Cross-cluster interactions

Analysis of inter-cluster links showed strong conceptual ties between:

- Psychological Models (Cluster 2) and Social Engineering (Cluster 3), indicating the increasing role of personality profiling in phishing defence strategies.
- Human Factors (Cluster 1) and Network Modelling (Cluster 4), suggesting that behavioural metrics are now integrated into system resilience simulations.

These connections indicate a paradigm shift from purely technical safeguards towards human-centric, behaviourally adaptive security systems.

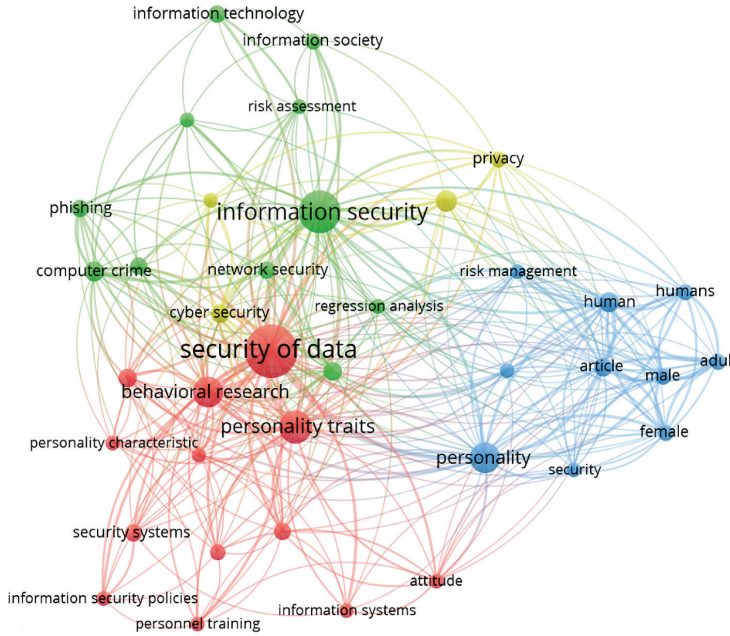

Figure 1: Keyword co-occurrence network – colour-coded clusters
Source: compiled by the author

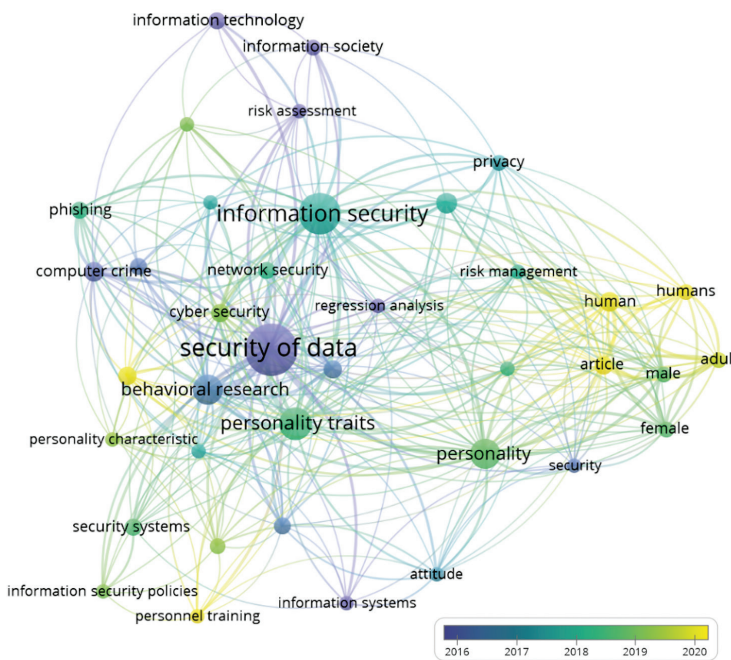

Figure 2: Inter-cluster connection map
Source: compiled by the author

Discussion

The results of this study confirm that personality traits exert a measurable and significant influence on cybersecurity awareness and related behaviours. This aligns with prior empirical findings,[19] which have repeatedly demonstrated that *individual differences* – particularly in the domains of conscientiousness, openness to experience and neuroticism – affect the degree to which users comply with security policies, detect phishing attempts and adhere to safe digital practices.

From a network analysis perspective, the high degree and betweenness centrality scores of *personality traits* and *security awareness* highlight their bridging role between the psychological and technical domains of cybersecurity. This suggests that the interdisciplinary integration of these domains is not only theoretical but is also reflected in the structure of the scientific literature itself.

Notably, the cross-cluster connections between *psychological models* and *social engineering* studies underline the critical role of personality profiling in countering phishing and manipulation attacks. For example, individuals with high agreeableness may be more prone to trust unsolicited communications, while those with high openness may be more likely to engage with unfamiliar digital content – both traits that can be leveraged in targeted attacks if not addressed in training.

The implications for policy and practice are clear:

- Cybersecurity awareness programmes should integrate personality-based risk assessments to optimise content delivery and engagement.
- Public sector organisations and critical infrastructure operators, which face heightened risks from targeted social engineering, could significantly improve resilience by embedding psychological screening and tailored training into security protocols.
- Network-based monitoring of research trends can help policymakers and educators anticipate emerging vulnerabilities, ensuring that awareness initiatives remain current and evidence-based.

At the same time, the study's reliance on secondary data and bibliometric analysis presents limitations. While network analysis reveals structural relationships within the literature, it does not capture causal mechanisms between personality traits and security behaviours. Thus, the next stage of research should combine scientometric insights with *primary* empirical data – for instance, controlled experiments or large-scale surveys – to validate and expand upon the observed patterns.

Furthermore, advanced network metrics such as modularity scores, eigenvector centrality and temporal clustering coefficients could be incorporated in future analyses to deepen the understanding of how research themes evolve and interconnect. These metrics, when combined with content analysis, could identify not only *what* is being studied but also *how* the conceptual framing of personality in cybersecurity shifts over time.

[19] McCormac et al. 2017; Padayachee 2022; Uffen–Breitner 2015.

Ultimately, the evidence points towards an emerging research paradigm in which human factors, particularly personality traits, are not peripheral considerations but central determinants of cybersecurity strategy effectiveness. Recognising and operationalising this fact in both academic research and practical training design will be critical to strengthening digital resilience in an era of increasingly sophisticated cyber threats.

Conclusion

This study has demonstrated that personality traits play a decisive role in shaping cybersecurity awareness, influencing not only users' adherence to security protocols but also their susceptibility to social engineering and other human-targeted attacks. Through bibliometric and network analysis of literature indexed in the Scopus database between 2000 and 2023, the research has mapped the intellectual structure of this interdisciplinary field, revealing that the connection between psychological science and cybersecurity practice has become increasingly prominent over time.

The scientometric mapping confirms that the domain is characterised by a "small-world" and partially "scale-free" network structure, indicating the existence of highly connected research nodes that facilitate cross-disciplinary knowledge exchange. This network configuration also suggests that targeted integration of concepts from psychology – such as the Big Five personality dimensions – into cybersecurity strategies could have an outsized impact on both academic discourse and applied training methodologies.

From a practical perspective, the findings point towards a paradigm shift:

1. Moving from uniform, technical training modules towards adaptive, psychologically-informed security awareness programmes.
2. Incorporating personality-based profiling into both public and private sector security policies to tailor interventions more precisely to user risk profiles.
3. Leveraging network monitoring of research trends to maintain up-to-date, evidence-based awareness initiatives that anticipate emerging threats.

However, the present study is not without limitations. As the analysis relied exclusively on secondary data, causal inferences regarding the influence of personality traits on cybersecurity behaviours cannot be drawn. Future research should therefore complement bibliometric analysis with primary empirical methods – including experimental designs, longitudinal surveys and sector-specific case studies – to validate and extend the observed relationships.

In addition, the methodological framework could be enhanced by incorporating advanced network indicators (e.g. betweenness and closeness centrality, modularity optimisation) and by integrating quantitative content analysis of the most influential works in the field. This would provide not only a structural but also a substantive understanding of how key concepts are operationalised across disciplines.

In conclusion, recognising and systematically integrating personality traits into cybersecurity awareness frameworks represents both a scientific opportunity and

a practical necessity. The resilience of individuals and organisations against cyber threats will increasingly depend on the ability to merge human factors research with technical security measures – creating holistic, adaptive and psychologically grounded defence strategies that are responsive to the evolving threat landscape.

References

Amankwa, Eric – Loock, Marianne – Kritzinger, Elmarie (2020): A Composite Framework to Promote Information Security Policy Compliance in Organizations. In Serrhini, Mohammed –Silva, Carla – Aljahdali, Sultan (eds.): *Innovation in Information Systems and Technologies to Support Learning Research.* Cham: Springer, 458–468. Online: https://doi.org/10.1007/978-3-030-36778-7_51

Barabási, Albert-László – Albert, Réka (1999): Emergence of Scaling in Random Networks. *Science,* 286(5439), 509–512. Online: https://doi.org/10.1126/science.286.5439.509

Ben Salamah, Fai – Palomino, Marco A. – Craven, Matthew J. – Papadaki, Maria – Furnell, Steven (2023): An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work. *Applied Sciences,* 13(17). Online: https://doi.org/10.3390/app13179595

Blasco, Jorge – Quaglia, Elizabeth A. (2018): *InfoSec Cinema: Using Films for Information Security Teaching.* ASE 2018 – USENIX Workshop on Advances in Security Education, Co-Located with USENIX Security 2018. Conference Paper. Online: www.usenix.org/system/files/conference/ase18/ase18-paper_blasco.pdf

Boban, Marija (2014): *Information Security and the Right to Privacy in Digital Economy – The Case of the Republic of Croatia.* 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 26–30 May 2014, Opatija, Croatia. Online: https://doi.org/10.1109/MIPRO.2014.6859804

Doucek, Petr – Basl, Josef – Pavlicek, Antonin M. – Tjoa, A. Min – Detter, Katrin – Raffai, Maria eds. (2019): *Research and Practical Issues of Enterprise Information Systems.* Cham: Springer. Online: https://doi.org/10.1007/978-3-030-37632-1

McCormac, Agata – Zwaans, Tara – Parsons, Kathryn – Calic, Dragana – Butavicius, Marcus – Pattinson, Malcolm (2017): Individual Differences and Information Security Awareness. *Computers in Human Behavior,* 69, 151–156. Online: https://doi.org/10.1016/j.chb.2016.11.065

Padayachee, Keshnee (2022): Understanding the Effects of Situational Crime Prevention and Personality Factors on Insider Compliance. *Journal of Information Security and Applications,* 70. Online: https://doi.org/10.1016/j.jisa.2022.103338

Pont, Ana – Mata, Francisco J. eds. (2016): *ICT for Promoting Human Development and Protecting the Environment.* Cham: Springer. Online: https://doi.org/10.1007/978-3-319-44447-5

Scopus (2023): *Content Coverage Guide.* Online: https://assets.ctfassets.net/o78em1y1w4i4/EX1iy8VxBeQKf8aN2XzOp/c36f79db25484cb38a5972ad9a5472ec/Scopus_ContentCoverage_Guide_WEB.pdf

Uffen, Jörg – Guhr, Nadine – Breitner, Michael H. (2012): *Personality Traits and Information Security Management: An Empirical Study of Information Security Executives.* International Conference on Information Systems, ICIS 2012. Conference Paper. Online: https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/5

Uffen, Jörg – Breitner, Michael H. (2015): Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions. In *Standards and Standardization: Concepts, Methodologies, Tools, and Applications.* Hershey: IGI Global, 836–853. Online: https://doi.org/10.4018/978-1-4666-8111-8.ch039

Wang, Dawei (David) – Durcikova, Alexandra – Dennis, Alan R. (2023): Security Is Local: The Influence of the Immediate Workgroup on Information Security. *Journal of the Association for Information Systems,* 24(4), 1052–1101. Online: https://doi.org/10.17705/1jais.00812

Wang, Zuoguang – Zhu, Hongsong – Sun, Limin (2021): Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access,* 9, 11895–11910. Online: https://doi.org/10.1109/ACCESS.2021.3051633

Watts, Duncan J. – Strogatz, Steven H. (1998): Collective Dynamics of "Small-World" Networks. *Nature,* 393(6684), 440–442. Online: https://doi.org/10.1038/30918

Weems, Carl F. – Ahmed, Irfan – Richard, Golden G. III – Russell, Justin D. – Neill, Erin L. (2018): Susceptibility and Resilience to Cyber Threat: Findings from a Scenario Decision Program to Measure Secure and Insecure Computing Behavior. *PLoS One,* 13(12). Online: https://doi.org/10.1371/journal.pone.0207408

Yeng, Prosper K. – Fauzi, Muhammad A. – Yang, Bian (2021): Assessing the Effect of Human Factors in Healthcare Cybersecurity Practice: An Empirical Study. In Vassilakopoulos, Michael Gr. – Karanikolas, Nikitas N. (eds.): *PCI 2021: Proceedings of the 25th Pan–Hellenic Conference on Informatics.* New York: Association for Computing Machinery, 472–476. Online: https://doi.org/10.1145/3503823.3503909