


Human-Centric Approach to Cyber Threat Identification: The Role of Cognition, Experience, and Education in Decision-Making

Ricardo Gregorio Lugo

 <https://orcid.org/0000-0003-2012-5700>

Østfold University College, Norway & Estonian Maritime Academy, Estonia

Ausrius Juozapavicius

 <https://orcid.org/0000-0002-8852-8605>

General Jonas Žemaitis Military Academy of Lithuania, Lithuania

Kristina Lapin

Vilnius University, Lithuania

Torvald F. Ask

Østfold University College, Norway & Norwegian University of Science and Technology, Norway

Benjamin J. Knox

Institute for Welfare, Leadership, and Organisation, Norway

Stefan Sütterlin

Albstadt-Sigmaringen University, Germany & Østfold University College, Norway

ABSTRACT

This study explores the impact of human factors on cybersecurity, emphasizing how cognitive biases and the blend of knowledge, experience, and education affect cyber threat detection. It reveals that specialized education and experience enhance the ability to identify complex threats. The research, using a gamified questionnaire, assesses decision-making in simulated cyber attacks, highlighting the value of domain expertise in critical tasks like threat identification and response. It suggests further research into confidence and self-efficacy's roles in cybersecurity and underscores the need for focused training to improve detection skills and incident reporting, aiming to bolster cybersecurity defences.

Keywords Cybersecurity, Human Factors, Decision-Making, Threat Identification, Cybersecurity Behaviors, Experience, Education, Cognition

INTRODUCTION

Human factors play a critical role in decision-making in the ever-changing field of cybersecurity, especially in the context of identifying cyber threats. Research on human factors has identified several aspects that inform decision-making processes, such as cognitive biases, perceptions, and competencies. These aspects are also relevant in the realm of cyber threat detection, where judgments to determine whether a perceived abnormality is harmless or malicious are critical (Ask et al., 2021; Rajivan & Gonzalez, 2018). The process of identifying cyber threats involves various complex components related to human decision-making, including cognitive, psychological, and behavioral elements (Gutzwiller et al., 2015).

DOI: 10.4018/JCIT.368220

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

The importance of human factors in the identification of cyber threats is emphasized by the role played by cognitive processes, situational awareness, and experience in the decision-making process (Ask et al., 2021). These elements are crucial in differentiating between normal and malicious actions inside network settings. The process of decision-making is complex, since it entails the examination of accessible information, the appraisal of several choices, and the ultimate choosing of a particular course of action. The cognitive process is subject to the influence of an individual's knowledge, experience, and educational background. The prioritization of human cognition, behavior, and interactions with cybersecurity systems is a fundamental aspect of the human-centric approach to cyber threat identification (Gutzwiler et al., 2015). In the context of a human-centric framework, the factors of experience and specialized education play a crucial role in determining the effectiveness of decision-making for cyber threat identification. The acquisition of knowledge and skills in cybersecurity through long-term involvement and exposure enhances an individual's capacity for cyber situational awareness (Barford et al., 2010). Enhanced capacity for perception of critical events or information facilitates a more comprehensive understanding of the current situation and ability to predict or produce multiple possible outcomes. This involves using both intuitive and analytical skills that are crucial for recognizing subtle and otherwise ambiguous information and making sense of possible cyberattacks (Rid & Buchanan, 2015). Therefore, specialized education, combined with practical experience, offers the fundamental knowledge and theoretical frameworks necessary for understanding, analyzing, and mitigating diverse and intricate cyber threats. Here too, the development of analytical, ethical, and technical skills are crucial for understanding the complexities of cyber settings (Barford et al., 2010; Franke & Brynielsson., 2014; Knox et al., 2019).

Cyber Education and Performance

The education of cybersecurity involves knowledge of social and technical domains. Specific cyber security workplaces encompass the relevant combination of social and technical competencies. Therefore, training must be adapted to the specific cybersecurity workplace requirements. The National Initiative for Cybersecurity Education (NICE) workforce framework for cybersecurity (Newhouse et al., 2017) relates knowledge, skills, abilities, and tasks with specific cybersecurity workplaces. The cybersecurity competency model (Keeton et al., 2019) complements the NICE framework with the competencies for specified cybersecurity roles (U.S. Office of Personnel Management, 2018). The subject-specific and human-specific competencies affect students' accomplishments and performance (Impagliazzo & Pears, 2018; Wetzel, 2021). The guidelines for cybersecurity education and training developed by the European Union Agency for Network and Information Security (ENISA) incorporate social sciences into cybersecurity education to mitigate risky cybersecurity behaviors and to reduce slips and errors (Drogkaris & Bourka, 2019). Introducing the social aspect to education is important in explaining the causes of cybersecurity incidents within organizations. Focusing solely on the technical cause might result in a technical fix, whereas addressing cultural issues, which might be to blame for the same incident, could subsequently lead to the improvement of the security culture (Ebert et al., 2023).

Expertise and Reporting of Cyber Threat Incidences

Ask et al. (2021) examined human-to-human communication dynamics in cybersecurity threat scenarios to have a better understanding of cybersecurity communication. They found a lack of research within cybersecurity communication and determined that effective communication is necessary for task progress and for reducing risks of under-communication and task redundancies (Ask et al., 2021).

Perseverance

Basyurt et al. (2022) highlight the importance of tailored communication in cyber threat scenarios, emphasizing its necessity across various levels of education and expertise. They argue that decision-makers require specific, crucial information to base their decisions on evidence and potential

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/human-centric-approach-to-cyber-threat-identification/368220

Related Content

A Credit-Based System for Traffic Routing in Support of Vehicular Networks

Ammar Kamel, Maysaa Husam, Zaid Shafeeq Bakrand Ziad M. Abood (2021).

Journal of Cases on Information Technology (pp. 1-11).

www.irma-international.org/article/a-credit-based-system-for-traffic-routing-in-support-of-vehicular-networks/281212

Building and Management of Trust in Information Systems

István Mezgar (2005). *Encyclopedia of Information Science and Technology, First Edition* (pp. 298-306).

www.irma-international.org/chapter/building-management-trust-information-systems/14253

Building a Machine Learning Algorithm-Based Model to Suggest Tourist Attractions in Response to Travelers' "Slow Life" Requirements

Xiuxia Li (2025). *Journal of Cases on Information Technology* (pp. 1-16).

www.irma-international.org/article/building-a-machine-learning-algorithm-based-model-to-suggest-tourist-attractions-in-response-to-travelers-slow-life-requirements/371409

ERP Systems and the Strategic Management Processes that Lead to Competitive Advantage

Thomas Kalling (2003). *Information Resources Management Journal* (pp. 46-67).

www.irma-international.org/article/erp-systems-strategic-management-processes/1244

An Overarching Guide to Data Governance

Kritika (2024). *Creating and Sustaining an Information Governance Program* (pp. 283-307).

www.irma-international.org/chapter/an-overarching-guide-to-data-governance/345430