


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

outcomes, underscoring the need for relevant and concise communication in the field of cybersecurity. They also emphasize the need for standardized communications to aid in decision-making.

Previous research has shown the significance of expertise and practical knowledge in the context of cyber threat analysis, which involves the classification as either threats or non-threats (Ben-Asher & Gonzalez, 2015). They showed that while cybersecurity knowledge aids in identifying individual malicious events, specific network knowledge is crucial for accurate overall attack detection. No significant differences were found regarding the determination of whether the complete sequence constituted a cyberattack. Ben-Asher and Gonzalez (2015) concluded that knowledge in information and network security is more effective in identifying malicious activities than in detecting an overall cyberattack. This indicates that specialized security knowledge is key to recognizing specific harmful incidents. One possible reason for the enhanced ability of experts to identify malicious events is their extensive knowledge, which enables them to interpret a network event, comprehend the interrelationships among various attributes that constitute an event, and evaluate the event in the context of the particular network and its activities. This could explain their persistent behavior in pursuing the identification of possible threats. While there is a focus on identifying individual factors related to positive cybersecurity behaviors, findings on demographic factors such as age and gender are inconclusive and only focus on domain knowledge and expertise. Amador et al. (2020) identified factors linked to effectively handling expectations and seeking support in cybersecurity. However, there is a notable gap in research and frameworks concerning specific human factors critical for effective cybersecurity. This highlights the need for more focused studies in this area. Therefore, the purpose of this study is to identify the effects of domain-specific cybersecurity knowledge and expertise that can be identified as resilience factors in cyber threat situations, and how these factors contribute to communicating recognized cyber threats.

Hypotheses

- H_1 : The level of expertise or domain-specific knowledge is associated with persistent behaviors in cyber threat detection.
- H_0 : Expertise or domain specific knowledge is not associated with persistent behaviors in cyber threat detection.
- H_2 : Persistent behaviors (continuing and support) are associated with communication of recognized cyber threats.
- H_0 : Persistent behaviors (continuing and support) are not associated with communication of recognized cyber threats.

METHODS

Data Collection and Participants

The questionnaire, designed as gamified educational content, was presented to participants in the international red-blue cybersecurity exercises Amber Mist 2022, organized by the Lithuanian Armed Forces. A total of 49 valid responses were collected. The questionnaire had over 200 possible paths, with two possible endings: quitting or submitting an incident report to the chief information security officer (CISO). The reports, which were used to operationalize communication of recognized cyber threats, were manually evaluated in three domains (dependent variable): the attack objectives (0.5 points for reporting a database [DB] leak and an additional 0.5 points for mentioning ransomware), the exploited vulnerabilities (0.5 points for highlighting weak passwords and another 0.5 points for identifying DB vulnerabilities, such as an exposed port or excessive user rights), and the indicators of compromise (0.5 points for accurately reporting the attacker's IP address and 0.5 points for pinpointing

attack artifacts). Consequently, scores could range from zero to three. The length of the submitted reports was also measured in terms of word count. The number of steps (step count) taken through the questionnaire before quitting was quantified to indicate perseverance as a measure of resilience. The number of support calls initiated by the participants and the number of premature calls were quantified to indicate support seeking and quitting, respectively, as additional measures of resilience.

Expertise of the participants was measured using the National Institutes of Health proficiency scale. This is a tool designed to assess a person's capacity to show proficiency in the workplace. The scale, which ranges from “Fundamental Awareness” to “Expert,” encompasses a wide range of skill levels (National Institutes of Health, 2009).

Demographic information was also collected. Respondents reported their level of education: undergraduate, graduate, or other (no higher education), and the type of education (information technology [IT] non-security, IT security, or non-IT).

Procedure

To investigate the communication patterns of cybersecurity specialists during a cyberattack, we designed a scenario of a simulated attack. Despite the artificial nature, each element of the attack was realistic and plausible. The attack was executed on a test system, and we captured screenshots of error messages, relevant excerpts from server logs, file listings in pertinent folders, and the contents of selected files. These pictures were then employed to develop a Google form-based questionnaire with various potential outcomes. Respondents were asked to assume a role of one of two system administrators for a fictitious company with 50 employees and several servers on-site. In the scenario, this system administrator receives a call from an employee named Peter, who reports corrupted files on his Windows desktop and an inability to access the internal client resource management (CRM) web server. The respondents were informed that upon connecting to Peter's machine via the remote desktop protocol, the system administrator identified a malfunctioning shortcut file. After providing their demographic data, participants received incremental information describing the cyberattack as it progressed. At each stage, they could opt to discontinue, contact their CISO, reach out to the co-administrator, or delve further into the issue. If participants chose to contact their technical colleague, the questionnaire supplied a snippet of information but rerouted them back to the attack's logs and screenshots under the pretense that the colleague was on vacation. If participants attempted to contact the CISO, they were prompted to provide a brief report. The questionnaire concluded unless this interaction was deemed too premature—wherein not enough technical data had been disclosed yet. We labeled these premature interactions and redirected users back to the server logs.

Scenario

In the scenario's backstory, a system administrator (referred to as “the colleague”) inadvertently exposed an external DB port 5432 for a PostgreSQL server on a Linux machine. At 03:43 a.m., an assailant carried out a successful brute force (or password spraying) attack from a specific IP address, with the user “temp” gaining access to the CRM DB. This unauthorized user then listed the tables and siphoned off all the CRM data. Later, at 15:06, they connected from a different IP address, uploaded a precompiled PostgreSQL library, and added a user-defined function named “sys” that could run arbitrary commands on the server. This resulted in the establishment of a reverse shell to the attacker's machine.

Evidence, like the presence of “ncat” and “Responder” in the temporary folder on the DB server, suggests that the attacker managed to escalate privileges to root level on the server. Specifically, the “Responder” tool requires root rights, and its presence implies that the attacker was able to monitor the network and intercept a Windows new technology LAN manager password hash using it. This hash capture was facilitated by the attacker uploading a tailored shortcut file to a shared Windows folder on Peter's system. It is plausible that Peter's password for this machine was located within the compromised DB, unless the file share permitted uploads without needing a password. The shortcut

pointed back to the DB server where “Responder” was active. As such, when any user navigated the shortcut's directory on Peter's machine, Windows, attempting to follow the link, inadvertently transmitted the user's password hash.

During the preliminary investigation into Peter's grievance, the administrator (represented by the questionnaire respondent) accessed Peter's system via the remote desktop protocol and explored the shared folder. Consequently, the attacker intercepted this administrator's password hash at that point. After decrypting the password, the attacker used it to breach other company systems and deploy ransomware—this included a system where backups were housed. From the questionnaire's displayed data, it was uncertain whether multiple machines were encrypted by that time. Only the backup server unmistakably displayed a ransomware note. However, given the access durations and the timestamp of the “Responder” files, the attack seemed to be ongoing. The complete narrative could be inferred from the questionnaire's screenshots. Still, participants had to be able to interpret the provided outputs, such as DB logs, web server logs, port status logs, and file directory listings. Moreover, if they decided to submit their concluding report to the CISO prematurely, they might have missed out on viewing all available data.

Data Analysis

Quantitative Data

The data were summarized and presented in tables using mean and standard deviations for continuous and numerical variables, and frequency (count) and percentage for ordinal variables. Alpha levels for hypothesis testing were set at the 0.05 level for all analyses. All data were analyzed using JASP version 0.17.3 (Jeffrey's Amazing Statistics Program Team, 2023). Standard text processing software was used for thematic analysis.

Qualitative Data

Exploratory Thematic Analysis. Participants' final reports were analyzed using thematic analysis (Braun & Clark, 2012). This entails systematically examining responses in a data set to identify recurring patterns that fit higher order themes. Reflexivity is characterized by the active engagement of the researcher. In this research, one author is an expert in the field of cybersecurity, designed the exercise, and can interpret the responses of the participants in relation to the applied exercise. The steps defined by Braun and Clark (2012) allow for flexible approaches enabling rich data interpretation and are as follows:

- Familiarization with the data.
- Generate initial codes to organize data into meaningful categories.
- Identify themes.
- Check themes against the data set for verification.

Ethics

This study was conducted under the Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations project (Norwegian Research Council #302495). The present study conformed to institutional guidelines and was eligible for automatic approval by the Norwegian Social Science Data Services' ethical guidelines for experimental studies. Participation was voluntary and all participants were informed about the aims of the study; the methods applied; that they could withdraw from participation at any time and without any consequences; and that, if they did so, all the data that was gathered from them would be deleted. The questionnaire was completely anonymous.

RESULTS

Participant demographics and descriptive statistics can be found in Figures 1 and 2 and Table 1, respectively.

Figure 1.

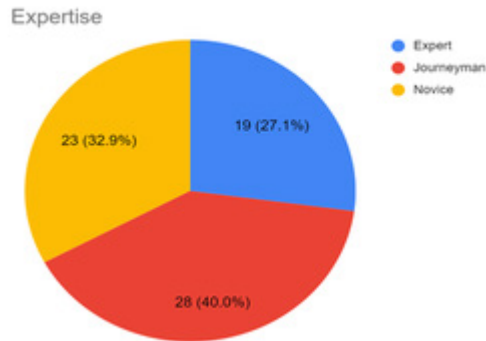


Figure 2.

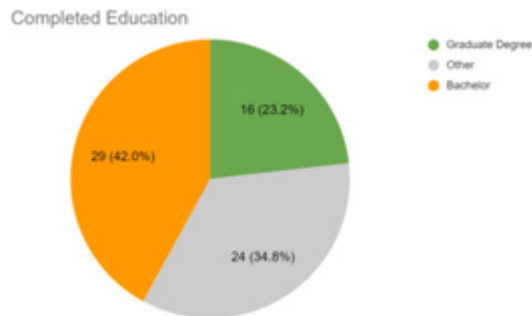


Table 1. Descriptive statistics and Pearson correlations of measured variables

	Mean	SD	Min	Max	1	2	3	4
1. Grade	0.68	0.76	0	3	—			
2. Report Length	216.29	244.51	0	915	.731**	—		
3. Step Count	5.59	2.42	1	10	.510**	.474**	—	
4. Calls Count	1.59	1.19	0	4	.370**	.620**	.654**	—

Note. N = 49; SD = standard deviation.

*p < .05; **p < .01.

There were no difference in how expertise was distributed among participants and their educational level ($\chi^2 = 4.19, p = .381, df = 4, V = .207$).

To test H_1 : The level of expertise or domain specific knowledge was associated with resilient behaviors in cyber threat detection, analysis of variance on education levels (vocational, undergraduate, graduate) and on final grade on the exercise was conducted.

There was a significant amount of premature calls (32.7%, $p < .01$) where we expected 28.6 (novices) but this was not significant between expertise levels ($\chi^2 = 4.39$, $df = 2$, $p = .111$, $V = .299$).

While grades were not significantly different between educational levels (Figure 3; $F = .90$, $p = .413$, $\eta^2 = .038$), expertise was significant (Figure 4; $F = 3.24$, $p = .048$, $\eta^2 = .123$). Post hoc Tukey's tests showed that there were differences between the novices and experts ($M_{diff} = -.679$, $t = 2.49$, $p = .043$, Cohen's $d = .94$) but not between novices and technicians ($M_{diff} = -.226$, $t = .91$, $p = .638$, Cohen's $d = .31$) or technicians and experts ($M_{diff} = -.452$, $t = 1.82$, $p = .176$, Cohen's $d = .63$), partially supporting H_1 .

Figure 3.

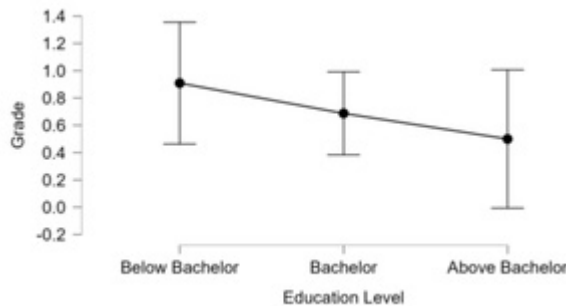
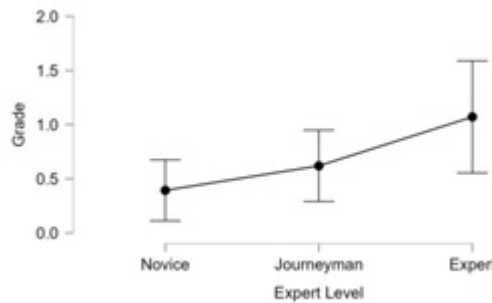


Figure 4.



To test H_2 , persistent behaviors (continuing and support) were associated with communication of recognized cyber threats, and a regression analysis was performed where resilience (step count), supports (calls count), and report length were regressed on the final grade. Both step count ($\beta = .298$, $t = 2.53$, $p = .015$) and report length ($\beta = .494$, $t = 4.18$, $p < .01$) were significant predictors of the final grade (Figure 3; $R^2 = .466$, $p < .01$, $F = 13.11$), while calls for support ($\beta = -.270$, $t = 1.72$, $p = .092$) were not, partially supporting the hypothesis.

Experts wrote longer reports ($F = 6.82$, $p = .003$, $\eta^2 = .229$). They differed from technicians ($M_{diff} = 194.19$, $t = 2.57$, $p = .036$, Cohen's $d = .885$) and novices ($M_{diff} = 300.71$, $t = 3.63$, $p = .002$,

Cohen's $d = 1.37$) but there was no significant difference between technicians and novices ($M_{diff} = 1.654$, $t = 1.41$, $p = .346$, Cohen's $d = .486$).

We explored other factors for possible explanations of the results. When asked to identify the stage of the kill chain in the attack, only 30% reported correctly (action on objectives) but the result was not significant in relation to the expert level ($\chi^2 = 12.42$, $df = 12$, $p = .413$). Similarly, confidence of the participants in their report accuracy was not a factor ($R^2 = .045$, $F = .81$, $p = .455$) in predicting the grade.

Qualitative Findings of Reports

Following the steps for thematic analysis defined by Braun and Clark (2012), and using the incident reports submitted by the participants, three distinct themes arose from the data:

- Ransomware. Examples of this are:
 - “Backups are encrypted by ransomware; DB files are missing.”
 - “It seems we fell for ransomware, which crippled our DB.”
- Data breach
 - “The DB was hacked; we need to reinstall server and restore data from backup.”
 - “Something's wrong in the DB, and strange structured query language calls are in logs.”
- A need for a further investigation
 - “There are several breach signs; we need to investigate the damage.”
 - “Someone is changing the DB. We need to investigate.”

The themes were well inline with the scenario, as a data breach eventually led to the ransomware attack in the story. Those reports that called for a further investigation belonged to the respondents who failed to correctly identify the attack. They decided to report prematurely, without obtaining enough information from system logs.

DISCUSSION

The objective of this study was to examine the relationship between domain-specific cybersecurity knowledge and competence on the adoption of persistent behaviors in the context of cyber threat detection, as well as the role of these behaviors in the communication of identified cyber risks. The hypotheses were subjected to empirical testing, and the obtained results yielded valuable insights into the interplay between expertise, resilience, and communication within the cybersecurity domain.

Quantitative Findings

Expertise and Resilience in the Context of Cyber Threat Detection

The results of the investigation provided support for H_1 , which posited that there exists a relationship between the degree of expertise or domain-specific knowledge and the manifestation of resilient behaviors in the context of cyber threat detection. The findings of the study indicate that individuals with expertise in the domain of cybersecurity had greater resilience in their behaviors as compared to those with less experience, as proven by their superior performance in the exercise, as reflected in their higher final grades. While our findings indicate that performance degrades with higher education, this partially supports Barford et al. (2010), where individuals who possess specialized education and practical experience in the field of cybersecurity are equipped with the necessary information and theoretical frameworks to comprehend, evaluate, and address intricate cyber risks. The combination of knowledge and experience allows individuals to properly identify crucial events and information, hence promoting a thorough comprehension of the current situation as also described in Rajivan and Gonzalez (2018). Furthermore, it augments their capacity to anticipate

and develop a wide range of potential results, necessitating a combination of intuitive and analytical capacities. These abilities are essential for understanding possible cyberattacks and identifying complex and possibly ambiguous information, also found in Gutzwiller et al. (2015). Numerous studies have demonstrated the importance of developing analytical, ethical, and technological abilities in order to successfully navigate the complex environment of cybersecurity situations (Barford et al., 2010; Franke & Brynielsson, 2014; Knox et al., 2019).

This finding indicates that the possession of expertise and domain-specific information has a substantial impact on individuals' reactions to cyber risks. Professionals who possess superior skills to navigate the exercise make well-informed decisions and proficiently identify network events. In this study, higher levels of expertise enabled participants to better analyze network events, gain a better understanding of the ambiguous and complex, and assess events within the network's framework, hence enhancing their ability to identify potential risks. This supports the Ben-Asher and Gonzalez (2015) findings where they identified that the process of conducting cyber threat assessments necessitates the possession of levels of expertise and practical knowledge in order to effectively identify potential threats. Their findings showed that professionals with higher expertise had a higher proficiency in identifying hazardous network event sequences compared to novices, similar to the results of this study. Experts may have acquired the ability to evaluate network event descriptions, identify relationships among attributes, and assess network operations with a high level of competence. Their level of experience with threat detection and resilience enhances their ability to mitigate such compromises. Nonetheless, this study did not reveal any statistically significant disparities in resilience behaviors between individuals at the novice and technician levels. This suggests that it may require higher expertise levels rather than experience to exert a more influential role in determining resilience outcomes. This underscores the need of acquiring specific education and expertise in the field of cybersecurity as specified in the NICE (Newhouse et al., 2017), ENISA (Drogkaris & Bourka, 2019) and the cybersecurity competency model (Keeton et al., 2019).

The study's findings provided limited support for H_2 , which suggested that there is an association between resilient behaviors and the communication of recognized cyber threats. The findings of the analysis indicate that there is a statistically significant relationship between the final grade and the number of steps taken throughout the exercise and the length of the incident report. Participants who showed higher levels of resilience, as indicated by their increased step count, and those who submitted more comprehensive incident reports tended to exhibit superior performance in the identification and communication of cyber risks. Nevertheless, the quantity of support calls made did not have a substantial impact on the ultimate grade. These findings indicate that engaging in proactive measures and generating comprehensive incident reports are associated with improved performance. However, it is not necessarily the case that requesting support via phone conversations enhances an individual's capacity to identify and convey cyber threats, contrary to the Amador et al. (2020) findings. There is a potential for individuals who relied on support calls to exhibit greater caution or a lack of trust in their own abilities, which may have resulted in less effectiveness in detecting threats.

Additional variables and qualitative observations were examined in the study, including the specific stage of the kill chain involved in the attack and the level of trust exhibited by participants regarding the veracity of their reports. It is noteworthy that the performance of participants was not significantly affected by either the stage of the kill chain or their level of confidence. This finding implies that the participants' capacity to identify and convey cyber risks was primarily shaped by their level of competence, resilience, and adherence to the exercise's procedural guidelines, rather than their familiarity with the particular phase of the attack or their self-perceived confidence.

Qualitative Findings

The qualitative analysis of the event reports revealed three unique themes pertaining to acknowledged cyber threats: ransomware, data breach, and the necessity for additional inquiry. The aforementioned themes were congruent with the scenario shown in the exercise, wherein a data leak

ultimately resulted in a ransomware assault. This supports H_1 . The level of expertise or domain-specific knowledge is associated with resilient behaviors in cyber threat detection. Specific knowledge of data breach and ransomware can explain the attack, whereas participants who lacked such insights needed additional inquiries. These reports also support Barford et al.'s (2010) and Gutzwiller et al.'s (2015) findings that expertise gives better situational awareness of a recognized cyberattack.

Participants who asked their supervisor for additional inquiry generally demonstrated an inability to accurately identify the assault and provided premature reports lacking adequate information derived from system logs, which contradicted H_2 ; persistent behaviors (continuing and support) are associated with communication of recognized cyber threats, but supported the findings in the quantitative data, where the number of calls was not associated with better performance. These results are also contradictory to previous findings where supervisor support and communication were identified as facilitators of performance (Amador et al., 2020).

Limitations

The study's methodology, involving a simulated cyberattack scenario, presents several limitations. Firstly, the artificial nature of the simulated attack, despite its realistic elements, may not fully capture the complexity and unpredictability of real-world cyber threats. Participants' responses might differ in an actual attack situation due to heightened stress and unpredictability. Secondly, the use of a Google form-based questionnaire with predefined outcomes limits the range of possible responses and may not accurately reflect the decision-making process in a dynamic cyberattack environment. The reliance on a single scenario also restricts the generalizability of the findings. Different types of attacks or variations in attack complexity could yield different results. Additionally, the method of capturing screenshots and logs for the questionnaire may not encompass all nuances of a real-time cyberattack, potentially overlooking certain aspects of threat detection and response. Another important limitation of our study is the operationalization of perseverance by the number of steps and calls taken. This operationalization needs to be validated through scientific rigor.

The study's participant pool, drawn from the Amber Mist 2022 exercise, may not be representative of the broader cybersecurity community. The responses and expertise of participants from this specific event may not translate to other professionals with different backgrounds or experience levels. Furthermore, the scoring system for incident reports, while comprehensive, may not fully account for the complexity of real cyberattack analysis and response. Furthermore, the number of participants was limited ($N = 49$). When creating group for the analysis of variance, group sizes were small ($n = 11$, $n = 14$, $n = 24$) and variation of report length was quite large for the expert group, even though there were significant differences.

The research findings might not be universally applicable, as variations in human cognition, experiences, and educational backgrounds may differ across the population. This may impact the effectiveness of cyber threat identification strategies for this experiment. For example, individuals with different levels of technical expertise may interpret security warnings differently, and cultural differences can influence how people perceive and respond to cyber threats. Additionally, varying educational backgrounds may affect the ability to understand and implement security measures, but this does highlight the need for including human factors in future research.

Finally, the use of the National Institutes of Health proficiency scale to measure expertise, while standardized, may not perfectly align with the specific skills and knowledge required in cyber threat detection and response. The demographic information collected, though informative, may not sufficiently account for other factors influencing participants' performance, such as their practical experience in handling cyberattacks.

CONCLUSION AND IMPLICATIONS

This study emphasizes the importance of specialized knowledge and expertise in promoting resilience and effective communication in the realm of cybersecurity. It demonstrates that while foundational knowledge is essential, advanced expertise greatly improves the capability to recognize and address cyber threats. The research suggests areas for future exploration, including determining the level of expertise required to influence resilience in cyber threat detection, examining the kinds of support that could improve risk communication, and understanding how confidence and self-efficacy affect the detection and response to cyber threats. This research emphasizes the significant importance of possessing domain-specific knowledge and experience in the field of cybersecurity, particularly when it comes to the identification of cyber threats. Results showed that experts had more persistent behaviors and enhanced abilities in identifying and effectively conveying cyber threats. The study found that proactively taking steps and producing full incident reports was positively correlated with improved performance in the detection of cyber threats while support seeking behaviors did not influence performance.

These findings can be significant in the context of cybersecurity education and training. The prioritization of specialized education and the acquisition of domain-specific knowledge are factors in adequately equipping individuals to proficiently identify and address cyber risks, but as the results of this study show, education should also focus on fostering resilient behaviors such as perseverance to ensure that a complete cyber picture is established. Furthermore, the promotion of persistent behaviors, such as conducting comprehensive investigations and reporting incidents, has the potential to improve the overall cybersecurity stance of businesses. Further studies should incorporate human factors, such as persistence and support, and how these behaviors can persistently inform the intricate dynamics among expertise levels, competence development, and the ability to effectively detect threats.

COMPETING INTERESTS

The authors of this publication declare there are no competing interests.

FUNDING

No funding was received for this work.

AUTHOR NOTE

The datasets generated for this study are available on request to the corresponding author. Further inquiries can be directed to the corresponding author/s. Some or all data, models, or code generated or used during the study are proprietary or confidential in nature and may only be provided with restrictions.

PROCESS DATES

January 17, 2025

Received: March 27, 2024, Revision: June 25, 2024, Accepted: July 24, 2024

CORRESPONDING AUTHOR

Correspondence should be addressed to Ricardo Lugo (Norway, Ricardo.G.Lugo@hiof.no)

REFERENCES

- Amador, T., Mancuso, R., Moore, E., Fulton, S., & Likarish, D. (2020). Enhancing cyber defense preparation through interdisciplinary collaboration, training, and incident response. *Journal of the Colloquium for Information Systems Security Education*, 8(1), 6.
- Ask, T. F., Lugo, R. G., Knox, B. J., & Sütterlin, S. (2021). Human-human communication in cyber threat situations: A systematic review. In Stephanidis, C., Harris, D., Li, W.-C., Schmorow, D. D., Fidopiastis, C. M., Antona, M., Gao, Q., Zhou, J., Zaphiris, P., Ioannou, A., Sottolare, R. A., Schwarz, J., & Rauterberg, M. (Eds.), *HCI International 2021 - Late breaking papers: Cognition, inclusion, learning, and culture* (pp. 21–43). Springer. DOI: 10.1007/978-3-030-90328-2_2
- Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., & Ou, X. (2010). Cyber SA: Situational awareness for cyber defense. In S. Jajodia, P. Liu, V. Swarup, C. Wang (Eds.), *Cyber situational awareness: issues and research* (pp. 3-13). Springer.
- Basyurt, A. S., Fromm, J., Kuehn, P., Kaufhold, M. A., & Mirbabaie, M. (2022). Help wanted - Challenges in data collection, analysis and communication of cyber threats in security operation centers. *Wirtschaftsinformatik 2022 Proceedings*. https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/20
- Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51–61. DOI: 10.1016/j.chb.2015.01.039
- Braun, V., & Clarke, V. (2012). *Thematic analysis*. American Psychological Association. DOI: 10.1037/13620-004
- Drogkaris, P., & Bourka, A. (2019). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. European Union Agency for Network and Information Security. ENISA.
- Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security*, 134, 103435. DOI: 10.1016/j.cose.2023.103435
- Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security*, 46, 18–31. DOI: 10.1016/j.cose.2014.06.008
- Gutzwiller, R. S., Fugate, S., Sawyer, B. D., & Hancock, P. A. (2015). The human factors of cyber network defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 59(1), 322–326. DOI: 10.1177/1541931215591067
- Impagliazzo, J., & Pears, A. N. (2018). The CC2020 project — Computing curricula guidelines for the 2020s. *2018 IEEE Global Engineering Education Conference (EDUCON)*, 2021-2024. DOI: 10.1109/EDUCON.2018.8363484
- Jeffrey's Amazing Statistics Program Team. (2023). JASP (Version 0.17.3) [Computer software]. <https://jasp-stats.org/>
- Keeton, J., Brown, H. N., Miller, C., & Campbell, S. (2019). *Mississippi cybersecurity labor market analysis*. The University of Southern Mississippi.
- Knox, B. J., Lugo, R. G., & Sütterlin, S. (2019). Cognisance as a human factor in military cyber defence education. *IFAC-PapersOnLine*, 52(19), 163–168. DOI: 10.1016/j.ifacol.2019.12.168
- National Institutes of Health. (2009). *Competencies proficiency scale*. Office of Human Resources. <https://hr.od.nih.gov/workingatnih/competencies/proficiencyscale.htm>
- Rajivan, P., & Gonzalez, C. (2018). Human factors in cyber security defense. In Saman, S. (Ed.), *Human factors and ergonomics for the gulf cooperation council* (pp. 85–104). CRC Press. DOI: 10.1201/b21145-5
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *The Journal of Strategic Studies*, 38(1-2), 4–37. DOI: 10.1080/01402390.2014.977382
- U.S. Office of Personnel Management. (2018). *Interpretive guidance for cybersecurity positions attracting, hiring and retaining a federal cybersecurity workforce*. <https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf>

Wetzel, K. (2021). NICE framework competencies: Assessing learners for cybersecurity work (Report No. NIST IR 8355 [Initial Public Draft]). *National Institute of Standards and Technology*. <https://csrc.nist.gov/Pubs/ir/8355/IPD>

Dr. Ricardo Gregorio Lugo specializes in the behavioral dynamics of cyber defense, focusing on both individual and team aspects. His expertise lies in human factors and cognitive engineering, particularly within cyber defense exercises. His research integrates microcognitive elements like self-efficacy and metacognition with macrocognitive environments, exploring how factors like time-pressure and intuitive decision-making influence performance. Collaborating with national institutions and sports clubs, Dr. Lugo applies his insights across elite sports, education, and health sectors, bridging theoretical research with practical application in both team and individual sports contexts.

Aušrius Juozapavičius holds a PhD in physics from Kungliga Tekniska Högskolan Royal Institute of Technology, Sweden. Currently he is a professor responsible for the cybersecurity specialization of study programs at General Jonas Žemaitis Military Academy of Lithuania. His recent research focuses on cybersecurity, with a particular interest in cyber hygiene, education of specialists, and penetration-testing.

Kristina Lapin received a doctoral degree in informatics in 2001 from Vilnius University. She is an associate professor at Vilnius University, Faculty of Mathematics and Informatics, Department of Computer Science. She is chair of the Board of the Faculty of Mathematics and Informatics and the Software Engineering Bachelor Study Program Committee. Her research interests focus on the intersection of security and usability within interactive system design, cognitive aspects of decision support, and educational design.

Torvald Ask is a neuroscientist researching neurological and cognitive factors related to human performance in cyber operations, neurophysiological and cognitive antecedents to cellular stress and age-related disease, cognitive control and emotions in adults, neurodevelopment, and cognitive warfare.

Benjamin J. Knox holds a PhD in cyber and information security from the Norwegian University of Science and Technology (NTNU). He is a full-time researcher at the Norwegian Armed Forces Cyber Defense. In addition, he has associate professor positions at the Faculty of Health, Welfare and Organization at Østfold University College, Norway, and at the Center for Cyber and Information Security, Norwegian University of Science and Technology, Gjøvik. His research interests lie in the fields of human factors in cyberspace operations, cognitive warfare, and applied cognitive performance.

Stefan Sütterlin is a professor of cyberpsychology at Albstadt-Sigmaringen University's Faculty of Computer Science. His research interests include the human factor in IT security as well as other security-related or safety-sensitive questions around human cognition and behavior.