Online at www.e-iph.co.uk
Indexed in Clarivate Analytics WoS,

E-B
Environment - Behaviour Proceedings Journal

CSSR 2023
https://cssr.uitm.edu.my/2023/

e-IPH
e-International Publishing House Ltd., United Kingdom

10th International Conference on Science & Social Research
Virtual Conference
6 - 7 Nov 2023
Organised by: Research Nexus UiTM (ReNeU), Universiti Teknologi MARA

Enhancing Cyber Security Employees Ethical Competence with (AI) and Emotional Intelligence (EI) Elements: A survey of literature

Zan Azma Nasruddin[1], Marina Yusoff[1,2], Irwan Mazlin[1], *Aida Wati Zainan Abidin[1], Nor Hapiza Mohd Ariffin[3], Nurul Fadly Habidin[4]
**Corresponding Author*

[1] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia
[2] Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Kompleks Al-Khawarizmi, Universiti Teknologi MARA, Shah Alam 40450, Selangor, Malaysia
[3] College of Business, Sohar University, Oman
[4] Faculty of Management and Economics, Universiti Pendidikan Sultan Idris (UPSI), 35900 Tanjung Malim, Perak, Malaysia

zan649@uitm.edu.my, marina998@uitm.edu.my, irwanmazlin@gmail.com, aida018@uitm.edu.my, drnorhapiza@gmail.com, ,Fadly@fpe.upsi.edu.my
Tel: +60192509799

Abstract
Ethical competence is considered a fundamental requirement for the daily practice of cybersecurity professionals. As of now, there is a lack of comprehensive research on ethical competence in cybersecurity organisations. The acquisition of ethical competence skills is imperative for effectively addressing the ethical intricacies and obstacles arising from the advent of advanced technologies and digital transformation in the context of the Fourth Industrial Revolution (IR 4.0). This paper aims to conduct an in-depth survey of the literature on artificial Intelligence and emotional intelligence skills necessary to address both current and future technological demands effectively.

Keywords: Artificial Intelligence, Emotional Intelligence, Competence skill, Cybersecurity

DOI: https://doi.org/10.21834/e-bpj.v10iSI40.7713

1.0 Introduction

Cybersecurity is now a top priority in politics and diplomacy due to the increasing threats to communities' essential operations. It also presents opportunities for economic growth in areas like hardware and software development, cybersecurity insurance, education, and research. To address the evolving technology landscape and the multifaceted challenges, a comprehensive approach is needed to enhance professionals' skills in both industry and government, going beyond traditional education and basic training. In recent years, cyberattacks have affected various industries, with notable incidents such as NotPetya in Ukraine costing businesses an estimated $1.2 billion. This highlights the global significance of cybercrime as a serious concern for all businesses. The IT sector has been heavily targeted by web application cyberattacks in 2017. These ongoing threats emphasise the need for proactive measures to prevent data breaches. An initiative-taking cybersecurity strategy to protect private information and confidentiality still needs initiatives to prevent recurring dangerous attacks. Cybersecurity specialists should acquire ethical competence and demonstrate the ability to manage

eISSN: 2398-4287 © 2025. The Authors. Published for AMER by e-International Publishing House, Ltd., UK. This is an open access article under the CC BY-NC-ND license (http://c5eativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers
DOI: https://doi.org/10.21834/e-bpj.v10iSI40.7713

valuable information to support efficient decision-making, as ethical competence is a fundamental qualification for daily practice. It is a key distinction between simply having skills and having a true sense of professionalism. It goes beyond technical competence; ethical competence must also be considered to support employees' competencies. To date, the concept of ethical competence has still been insufficiently researched in cybersecurity organisations. There is a need to define what it means to be ethically competent in the era of IR4.0. The previous competence models still fail to consider both Artificial Intelligence (AI) and Emotional Intelligence (EI). AI brings new opportunities for cybersecurity organisations that focus on AI skills related to cognitive Intelligence or Intelligent Quotient (IQ). EI, which refers to Emotional Quotient (EQ), is a good predictor of ethical competence, as it enables precise perception and expression of emotions, facilitating thought to understand and manage them.

2.0 Literature Review

Researchers have identified links between Emotional Intelligence (EI) and various positive outcomes, including improved performance, organisational commitment, mental well-being, study habits, communication skills, and relationship quality (Cobb & Mayer, 2000). The concept of Emotional Intelligence (EI) was introduced by Cobb and Mayer (2000). Goleman (n.d) contributed to and refined the idea of EI in the workplace, particularly in 1998. Building on Gardner's premise from 1983 that multiple types of Intelligence exist, including interpersonal Intelligence, Goleman popularised the concept of EI in his 1995 book titled "Emotional Intelligence." Goleman defined EI as "the capacity to recognise our own emotions and those of others, to motivate ourselves, and to manage emotions effectively in ourselves and in our relationships." This definition gained attention from both the public and the academic community, leading to further research and discussion.

Ethics is all about understanding morals, ethical principles, and how to make good decisions. It concerns beliefs and ideas about being a good person (Godse et al., 2017). Some researchers have investigated how ethics relates to Emotional Intelligence (EI). For instance, Sivanathan (2002) compared EI with Transformational Leadership and studied how moral reasoning affects both. They wondered if people who score high in EI might be better at figuring out what is right in tricky situations. Their study supported this idea, suggesting that future researchers should explore how EI and moral reasoning connect in different situations.

The new methods of ethics are based on the outdated idea of ethics, which is the study of individual behaviour, with an emphasis on the distinction between correct and incorrect. Their purpose in contemporary economic manufacturing society has been warped and tangled in the quest for a new, more noble principle of convenience by grabbing for benefit rather than for what is correct (Butts & Rich, 2019). Thus, the ethical regulations of the past gain modern, demanding prominence in the current era, particularly in the era of IR4.0.

3.0 Methodology

The protocol for the SLR comprises three sequential processes, namely planning the Review, performing the Review, and presenting the Review.

3.1 Planning the Review

To ensure the comprehensiveness of the literature search, the complete texts of potentially relevant research were meticulously reviewed to determine eligibility. The literature will examine existing research on enhancing ethical competence among cybersecurity employees through the integration of AI and EI. The objective of this paper is to identify the key components and frameworks associated with ethical competence development in the context of cybersecurity. The inclusion and exclusion criteria for selecting the literature sources are summarised in Table 1.

Table 1: Criteria Selection.

Criteria	Inclusion	Exclusion
Article Type	Journal articles and conference proceedings	Non-research article
Language	English	Non-English
Year of Publication	2000 until 2022	<2000
Database	Web of Science, Scopus, IEEE Xplore, SpringerLink	None
Country	Any countries	None

3.2 Performing the Review

The search keywords used for the literature search were "ethical competence", AI in cybersecurity", "EI in cybersecurity", "cybersecurity professional" and "cybersecurity ethics". After reviewing the titles and abstracts, 24 studies were selected for final Review. For quality assessment, the Mixed Methods Appraisal Tool (MMAT), Version 2018, was employed.

3.2 Presenting the Review

The SLR examines the landscape of studies on artificial Intelligence and emotional intelligence competencies within the cybersecurity ethical framework. Analysing 24 studies, the following key themes were identified. The details of the themes were discussed in the results section.

a) Emotional Intelligence (EI) in cybersecurity: The significance of Emotional Intelligence (EI) in the context of cybersecurity cannot be overstated, as it has a significant impact on various aspects of this dynamic, high-pressure occupation. There are multiple justifications for the significance of emotional intelligence (EI) in cybersecurity.
b) Ethical principles in cybersecurity: Ethical principles play an essential role in cybersecurity, serving as the basic standards and guidelines that govern the actions and behaviours of individuals, organisations, and institutions responsible for safeguarding and monitoring information systems and digital assets. Compliance with these principles is of utmost importance to preserve trust, safeguard data privacy, and uphold the integrity of digital ecosystems.
c) Ethical Competence Frameworks: Ethical competency frameworks are systematic constructs or guidelines designed to help individuals and organisations foster and sustain ethical competence across diverse domains and professions. These frameworks offer a methodical way to tackle ethical dilemmas, formulate ethical judgements, and maintain ethical principles. In the IT field, frameworks enable professionals to navigate the complex landscape of cybersecurity ethics, data protection, and responsible technology development effectively.

4.0 Results and Discussion

4.1 Emotional Intelligence in cybersecurity

Cherniss (n.d) delved into the history of EI to provide a more detailed explanation of the concept. He defined EI as "the ability to perceive and express emotions in thought, understand and reason with emotions, and regulate emotions in oneself and others." Some may view EI as contradictory, as traditional Western thinking tends to favour rationality while regarding emotions as chaotic and undesirable interruptions to thought (Cobb & Mayer, 2000). Yocum (2007) pointed out that there are conflicting views on EI today. One perspective, known as the capability model, equates EI with a general ability akin to the concept of general Intelligence (or "g"). Another group of models, called mixed models of EI, includes approaches such as Goleman's (n.d.), which emphasises behavioural traits, and Bar-On's (2006), which focuses mainly on character traits. Researchers in the field have aligned with one of these views, while others have sought to bridge the gap between the two conceptual schools by clarifying the concept of EI and the terminology used to describe it. Cherniss (n.d) outlines four main models of EI that currently dominate the research field: Bar-On's (2006) mixed model, Mayer, Salovey, and Caruso's mixed model, Goleman and Boyatzis' model, and the trait model. This last model can be considered a second-generation approach. The lack of consensus regarding definitions and models in EI research has been a subject of debate within the field.

Another point of contention in the field of EI is measurement, as various methods have been used, sparking academic debate. Cherniss suggests that resolving the debate over different models could involve making a critical distinction between EI and emotional or social competence (ESC) as two distinct concepts. This differentiation could lead to new research directions, facilitate correlations between EI and ESC competencies, enhance predictive capabilities, and offer practical implications for the field. Emotional Intelligence (EI) skills involve recognising, generating, and understanding emotions to help us grow emotionally and intellectually (Mayer & Salovey, 1997). It means being competent at recognising and expressing emotions accurately, which allows us to understand and control our emotions (Brackett et al., 2004). According to Goleman (n.d.), five key elements of EI include self-awareness, self-regulation, motivation, empathy, and social skills.

4.2 Ethical principles in cybersecurity

Ethics is all about understanding morals, ethical principles, and how to make good decisions. It concerns beliefs and ideas about being a good person (Godse et al., 2017). Some researchers have investigated how ethics relates to Emotional Intelligence (EI). For instance, Sivanathan (2002) compared EI with Transformational Leadership and studied how moral reasoning affects both. They wondered if people who score high in EI might be better at figuring out what is right in tricky situations. Their study supported this idea, suggesting that future researchers should explore how EI and moral reasoning connect in different situations. EI also plays a role in making ethical decisions, especially in personal choices and understanding what others think is right. It helps us see the difference between our own ethical choices and others' beliefs about what is right (Jessica et al., 2010). Researchers have found that EI can predict how people behave across settings, such as in their studies, at work, and in everyday life. This means that EI might also be able to predict when people might act unethically (Jessica et al., 2010).

When it comes to making ethical decisions, our understanding of what is right and wrong can be influenced by what we see others doing. People with high EI are good at understanding their emotions and the emotions of others. This skill helps them think and act in a more controlled way, especially when it comes to dealing with their own and others' actions (Cobb & Mayer, 2000). In other words, people with high EI are better at handling their emotions and reacting calmly to what others do. This suggests that those with high EI might be better at understanding ethical and unethical behaviour. They are more likely to see why others act the way they do and are less likely to assume bad intentions. This ability makes it easier for them to act ethically and make ethical decisions (Jessica et al., 2010). EI has a connection to ethics. It helps us understand what is right and wrong, both in our own decisions and in how we perceive the choices of others. People with high EI tend to make better ethical choices and understand the ethics of others. This suggests that EI may also be linked to ethical behaviour in the workplace. When we talk about business ethics, we are talking about a broad field that deals with moral issues in the world of business and organisations. It is also about how people in this world deal with ethical and moral questions and concerns.

4.3 Ethical Competence Framework

Furthermore, Goleman specified emotional competence as "a learned capability based on EI that results in outstanding performance at work." Even though difficult to calculate, Goleman advised that EI is detectable as the value that differentiates successful performance outside training and knowledge and high cognitive Intelligence as evaluated by IQ tests. An Ethical Competence Framework is developed on the idea of the Emotional Competence Framework described by Goleman in Working with EI. The Ethical Competence Framework includes three aspects of competence, starting with the personal and going beyond community competence to worldwide competence. Each aspect of the Ethical Competence Framework is further allocated into descriptive elements that produce a total of thirty things that are categorised into the Ethical Competence Scale. By allocating values from 1 to 10 for each of the 30 items, a result can be achieved, which, stated as a ratio, becomes the Ethical Quotient (EQ), following the practice of stating cognitive Intelligence as the Intelligence Quotient or IQ. Nevertheless, no assertion is made that the Ethical Quotient is a precise or differentiating measure between persons or companies on their stage of ethical competence. Different Ethical Competence Frameworks from earlier studies did not consider AI elements in their framework (Maesschalck & Schrijver, 2018).

Therefore, an ethical competence for cybersecurity employees or potential employees using a new model that considers AI elements is necessary. We proposed the Cyber Artemotional Model as a tool for measuring employee ethical competence in a cybersecurity organisation. This model blends two elements, which are AI skills and EI skills. This proposed model gives an innovative approach to measuring ethical competence as it focuses on individual dimensions of humanity that are constructed through EI skills. Earlier, no model for ethical competence in cybersecurity raised concerns about EI skills as part of employee skills that must be present in an organisation. Therefore, this Cyber Artemotional model improves the combined value of the lack of employee ethical competence measurement.

4.4 Common Methodologies

The existing advanced quantitative methodology in education and social sciences research depends on well-established bivariate and multivariate statistical analysis techniques to solve research objectives and hypotheses (Bailey, 2013). Quantitative methods use a highly objective, systematic approach and work with numerical data. On the contrary, qualitative methods apply descriptions and words to analyse individual experiences and realities from the subject's perspective. It is regularly an iterative method whereby the theory or hypotheses appear from the data as it is gathered, making the researcher key in the data collection and analysis processes. The legality of qualitative methods can be better by utilising a blend of data collection techniques that known as triangulation and by analysis of the data by more than one person (Wang, 2015), SPSS (Bala,2016) (Li & Wong, 2014), Rasch procedures (Davier, 2014), (Abd-El-Fattah, 2015), (Boone & Staver, 2020), Correlation coefficient is the measure to quantify such degree of relationship of the variables (Senthilnathan, 2019), (Akiyoshi et al., 2023), NVivo Software (Zamawe, 2015) and JMP Software.

5.0 Conclusions

As a conclusion, it is vital to combine the strengths of AI and EI in the realm of cybersecurity to address the ever-evolving challenges posed by cyber threats effectively. AI competence in cybersecurity revolves around identifying and mitigating potential threats. AI-driven tools excel at sifting through vast data sets, identifying patterns indicative of cyber threats, and empowering cybersecurity experts to detect and preempt attacks swiftly. For example, AI algorithms can spot irregular patterns in system and network operations, signalling potential cyber intrusions.

However, practically, most cybersecurity organisations focus on AI skills and disregard EI skills' roles or vice versa. Despite the existing body of knowledge on this topic, there has been limited exploration of the links between ethics and EI. Rather than delving further into the existing literature on ethics and EI, this discussion suggests considering the integration of ethics in business practices. Professionals specialising in cybersecurity, particularly those well-versed in artificial Intelligence, possess the skills to effectively interpret and respond to these notifications, ensuring swift action. AI-driven automation streamlines routine security tasks such as patch management and log analysis, allowing cybersecurity experts to allocate their efforts to more strategic threat mitigation approaches. AI also enhances incident response capabilities by facilitating real-time analysis and decision-making support, enabling rapid and intelligent response to security incidents.

Professionals with high emotional Intelligence can convey complex technical concepts to non-technical personnel and managerial staff, fostering effective collaboration. Interdisciplinary teamwork is commonplace in cybersecurity, where individuals with strong EI skills can efficiently collaborate with colleagues from diverse backgrounds, facilitating information sharing and effective problem-solving. Given the high-pressure nature of cybersecurity, EI skills are instrumental in stress management and resilience building.

By integrating AI and EI competencies, cybersecurity can effectively detect complex cyber threats, including social engineering tactics. This synergy capitalises on AI's prowess in data analysis and EI's insights into human behaviour, thereby enhancing security protocols. EI ensures that security measures consider users' needs and emotions, while AI excels at swiftly detecting and identifying potential threats. Furthermore, AI and EI competencies empower cybersecurity teams to communicate effectively during emergencies, manage stress, and make well-informed decisions within tight timeframes. Professionals can leverage advanced technology while upholding a human-centred and emotionally intelligent approach to cybersecurity, thereby enhancing both technical and ethical dimensions of security practices.

Acknowledgment

We want to express our most profound appreciation for the financial support for the research and publications from the RMC Grant: FRGS/1/2021/SS02/UITM/02/20 and the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Selangor, Malaysia.

References

Abd-El-Fattah, S. M. (2015). Rasch Rating Scale Analysis of the Arabic Version of the Physical Activity Self-Efficacy Scale for Adolescents: A Social Cognitive Perspective. *Psychology*, *06*(16), 2161–2180.

Akiyoshi, L. E., Suzuki, S., Bitencourt, D., Eloy, J. ·, Pauletto, A., Strieder, G., Tetteh, J., Aboagye, D., Yamba, E. I., Daniel -Buor, ·, Massini, D. A., Almeida, T. A. F., Macedo, A. G., & Muller, D. (2023). *Compressibility of a Cambisol Submitted to Periods of Rotational Grazing and Strategies to Avoid Additional Soil Compaction*.

Bailey, D. A. (2013). Les Cheaux de Landiras et de Montferrand and Their Seigneurial Families—Part One: Setting, Medieval History, and Genealogy. *Advances in Historical Studies*, *02*(02), 81–93.

Bala, J. (2016). Contribution of SPSS in Social Sciences Research. In *International Journal of Advanced Research in Computer Science* (Vol. 7, Issue 6).

Bar-On, R. (2006). *The Bar-On Model of Emotional-Social Intelligence. The Bar-On Multifactor Model of Performance and Well-Being. View project. Bar-On Multifactor Measure of Performance (MMP) Development, Validation and Application. View project*.

Boone, W. J., & Staver, J. R. (2020). Advances in Rasch Analyses in the Human Sciences. In *Advances in Rasch Analyses in the Human Sciences*. Springer International Publishing.

Boone, W. J., Yale, M. S., & Staver, J. R. (2014). Rasch analysis in the human sciences. In *Rasch Analysis in the Human Sciences*. Springer Netherlands.

Brackett, M. A., Mayer, J. D., & Warner, R. M. (2004). Emotional Intelligence and its relation to everyday behaviour. *Personality and Individual Differences*, *36*(6), 1387–1402.

Cherniss, C. (n.d.). *Consortium for Research on Emotional Intelligence in Organizations Emotional Intelligence 1 Emotional Intelligence: What it is and Why it Matters*.
Cobb, C. D., & Mayer, J. D. (2000). Emotional Intelligence. *Educational Leadership*, *58*(3), 14–18.

Davier, M. (2014). Rasch Analysis. In *Encyclopedia of Quality of Life and Well-Being Research* (pp. 5393–5396). Springer Netherlands.

Godse, V. W., Rindhe, S. S., Kotai, L., Kendrekar, P. S., & Pawa, R. P. (2017). L-Pyrrolidine-2-Carboxylic Acid Sulfate (LPCAS): A New Ionic Liquid for the Synthesis of 14-Aryl-14H-Dibenzo[a,j] Xanthenes under Solvent-Free Conditions. *International Journal of Organic Chemistry*, *07*(02), 99–105.

Goleman, D. (n.d.). *EMOTIONAL INTELLIGENCE: WHY IT CAN MATTER MORE THAN IQ*.

Jessica, M.-M., Chockalingam, V., Satish P., D., & Jacob, J. (2010). Emotional Intelligence, Individual Ethicality, and Perceptions. *Revista de Psicología Del Trabajo y de Las Organizaciones*, *26*(1), 35–45.

Li, H.-B., & Wong, M.-L. (2014). Knowledge Discovering in Corporate Securities Fraud by Using Grammar Based Genetic Programming. *Journal of Computer and Communications*, *02*(04), 148–156.

Maesschalck, J., & Schrijver, A. De. (2018). Researching and Improving The Effectiveness of Ethics Training. In *Ethics in Public Policy and Management* (pp. 197–211). Routledge.

Mayer, J. D., Caruso, D. R., & Salovey, P. (2000). *Emotional Intelligence Meets Traditional Standards for an Intelligence*.

Senthilnathan, S. (2019). Usefulness of Correlation Analysis. *SSRN Electronic Journal*.

Sivanathan. (2002). *Emotional intelligence, moral reasoning, and transformational leadership _ Emerald Insight*.

Wang, M. (2015). Impulsive Synchronisation of Hyperchaotic Lü Systems with Two Methods. *International Journal of Modern Nonlinear Theory and Application*, *04*(01), 1–9.

Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, *27*(1), 13–15.