International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Exploring the Integration of Artificial Intelligence in Delphi Studies: A Comparative Analysis of Human and AI Expert Panels

Phillip L. Davidson

Ph.D, Senior Research Methodologist, Grand Canyon University, Phoenix, Arizona, USA

Abstract

This study compares the outcomes of two Delphi technique implementations investigating cybersecurity threats to online education: a traditional human expert panel from a 2014 study and a virtual panel generated using ChatGPT-4. The research evaluated whether artificial intelligence (AI) can produce results comparable to human experts in Delphi studies. Through a three-round process, both panels identified and prioritized key cybersecurity concerns. Results revealed significant overlap in core concerns, with both panels emphasizing training, data security, and system infrastructure as critical priorities. The AI panel introduced novel perspectives, such as collaboration and continuous improvement, while maintaining alignment with the human panel's recommendations. These findings suggest that AI can expedite-Delphi studies and produce meaningful insights, albeit with limitations in contextual understanding and practical nuance. This research contributes to methodological advancements in Delphi studies, offering implications for incorporating AI into expert-driven research.

Keywords: Delphi technique, Artificial Intelligence, ChatGPT, cybersecurity, online education, expert panels, qualitative research

1. Introduction

The-Delphi Technique is a research design originally developed in the 1950s by researchers at the RAND Corporation to forecast solutions to poorly understood problems. Named after the ancient Greek oracle of Delphi, the method was designed to improve the prediction of trends extending as far as fifty years into the future (Gordon & Helmer, 1964). Recognizing that long-term predictions often rely on intuitive judgment, the-Delphi Technique structured this intuition by systematically gathering input from panels of experts. The quality of these expert panels has consistently been viewed as critical to the method's validity and reliability (Goodman, 1987; Hill & Fowles, 1975).

The primary role of expert panels in Delphi Studies is to generate informed predictions, explore alternative scenarios, and achieve consensus on complex issues characterized by uncertainty. However, assembling human expert panels often involves logistical challenges, including scheduling conflicts and lengthy timelines. This study explores how artificial intelligence (AI) might address these challenges by comparing an AI-driven expert panel to a traditional Delphi study with human experts.

Since its inception in the 1950s, Artificial Intelligence (AI) has increasingly been integrated into research methodologies (Haenlein & Kaplan, 2019). AI offers the ability to process vast amounts of data efficiently and cost-effectively, though concerns about its accuracy remain. Recent studies have highlighted AI's

potential in fields such as healthcare (Johnson et al., 2021), economics (Djama, 2024), and politics (Ulnicane & Erkkila, 2023). As AI technologies evolve, their ability to mimic expert processes and synthesize large datasets presents intriguing opportunities for enhancing traditional methodologies like the-Delphi Technique.

This study examines the implications of integrating AI into the-Delphi process, focusing on whether AI can replace or supplement human experts without compromising the credibility and reliability of results. By addressing these questions, the research contributes to methodological innovation and provides practical guidelines for researchers considering AI-informed approaches. The findings hold significance not only for academia but also for industries where expert consensus is critical, offering insights into the evolving role of AI in reshaping traditional research techniques.

This study addresses three primary research questions:

1. To what extent can AI-generated expert panels produce comparable results to traditional human expert panels in Delphi studies?
2. What are the key differences and similarities between AI and human expert panel responses regarding cybersecurity threats in online education?
3. What are the potential advantages and limitations of using AI in Delphi technique research?

The experts in this current study are virtual experts, generated by a generative artificial intelligence (AI) chatbot. This paper replicates a previous Delphi study focused on cybersecurity threats to online education (Davidson & Hasledalen, 2014). A comparison of the final data between the original study and the current AI study follows.

Overview of the-Delphi Technique

The-Delphi Technique, developed by the RAND Corporation in the 1950s, emerged as an innovative methodological tool designed to systematically elicit expert consensus on complex topics. Conceived initially to forecast technological advancements and strategic military decisions, the technique has since been adapted across diverse fields, including healthcare, education, public policy, and technology assessment.

The core of the-Delphi process involves a series of rounds in which a panel of selected experts responds to questionnaires. Between each round, the responses are aggregated and shared among the participants, allowing for refined and convergent opinions. This iterative process ensures that the gathered consensus is informed, balanced, and reflective of a spectrum of expert perspectives.

Over time, the-Delphi Technique has become valued for its ability to manage varied opinions and reduce the influence of dominant voices often present in face-to-face group settings. By transforming qualitative judgments into quantitative data, the method provides a structured means to address multifaceted questions that benefit from expert insight but lack definitive solutions.

Despite its widespread use, critiques of the-Delphi Technique note potential limitations, such as the subjective nature of expert selection, the potential for bias in questionnaire design, and the need for careful moderation to maintain engagement across rounds. Nonetheless, its adaptability and focus on expert-driven data interpretation continue to make it a relevant and powerful tool in research today.

2. Methodology

This study compares an original study that used an expert panel with six experts (Davidson & Hasledalen, 2014). The design was a classical Delphi technique but conducted via email (e-Delphi). Selection of an expert panel is a critical part of any Delphi study, and the panel members in the original study were all

involved with both cyber security and higher education at some level. In addition, all were active in national and international discussions on the topic of cyber threats to educational systems.

The e-Delphi approach used the traditional three rounds of questions and responses. A series of seven topics emerged from the second round, including vulnerability of data, the need for improved use authentication, outdated hardware and software, encryption, leader concerns, and training for staff and students. The third round asked the expert panel to expand on the most critical issues, which included vulnerability of data, user authentication, and outdated hardware and software. The panel was then asked three additional questions about each of the three most critical issues and multiple subthemes developed. The responses to the third round from both panels are listed. In addition, content analysis was conducted on the responses to develop codes, categories, and ultimately theme. The process designed by Saldana (2016) was followed and the resulting themes are also reported.

The use of content analysis of panel responses is an additional part of these studies not typically included with Delphi studies. However, it was believed that digging deeper, qualitatively, into the responses in the final round could potentially provide detailed insights that could not be extracted from the short responses to the original questions. This same approach was followed with the original study and the study with the virtual experts.

Using the previously published Delphi study on cyber security (Davidson & Hasledalen, 2014), the same-Delphi process was followed as precisely as possible. There were three separate rounds. All three rounds in the original study were conducted via email. The identity of the panel members was never revealed, as anonymity of the expert panel is considered one of the top priorities of a Delphi study. Using Chat-GPT4, the bot was asked to create six virtual panel members as similar as possible to the original six, and not match any existing individuals.

AI Implementation Parameters

The ChatGPT-4 model was prompted to generate responses as six distinct virtual experts, each with backgrounds closely matching the original study's expert qualifications. To maintain consistency, the same three-round structure was followed, with each virtual expert providing independent responses. The AI was instructed to consider current cybersecurity threats and best practices while maintaining the temporal context of online education security challenges.

Key parameters for the AI implementation included:

- Generation of responses from six distinct expert perspectives
- Maintenance of response independence between virtual experts
- Consideration of both technical and organizational factors
- Integration of current cybersecurity knowledge while maintaining relevance to educational contexts

3. Results: The Original Delphi Study with a Human Expert Panel

Round One Initial Request

The following instructions were emailed to the original participants individually.

“Assuming that online educational systems are vulnerable to cyberattacks and that there are issues of cyber security, please list at least three of the most critical issues that, in your opinion, institutions of higher learning must address now and especially in the future. Please label your comment with two or three words and then follow with a one-paragraph explanation. These initial responses are intended to be brief. Your responses will be combined into a list for the second round, which will be emailed to you as soon as all the responses from round one have been received.”

Table 1: The 17 Answers Given as a Response to the Initial Question

1) Continuous vulnerability translates to being a soft target	2) Lack of security training for online learners
3) Data security	4) Low leadership priority status translates to continuous vulnerability.
5) Higher ed institutions do not have a clear understanding of the threat	6) Not enough trained and motivated staff.
7) Identify and access management.	8) Outdated hardware
9) Educating the user on how to protect their privacy	10) Outdated software
11) Integrity of data	12) Staff lacks appropriate training in cyber security issues
13) Lack of Encryption	14) Uploading/downloading of harmful files
15) Lack of Multifactor to access cloud-based assets 16) Lack of Multifactor to access devices.	17) User Authentication

Round Two

For the second round, similar issues were merged (e.g., Multifactor access as "user authentication"), and the seven most commonly selected vulnerabilities were presented to the expert panel. The panel was asked to rate the seven items from 1 to 7, with one being the most important. The list was presented to the panel in alphabetical order. Table 2 shows how the list was presented via email to each participant.

Table 2: Seven Top Priorities/Vulnerabilities from Round One (Presented in Alphabetical Order)

Encryption
Learner training
Low understanding or priority focus by leadership
Outdated hardware and software
Staff training
User authentication
Vulnerability of data (data integrity)

When the participants replied, their priorities were averaged to determine the top three vulnerabilities. The lower the average, the higher the level of importance in the expert panel's opinion. Table 3 indicates the averaged responses to the panel prioritization from round 2.

Table 3: Priorities of Top Seven Priorities/Vulnerabilities

Human Expert Panel	Average
Vulnerability of data (data integrity)	2.6
User authentication	3.4
Outdated hardware and software	3.8

Encryption	4.2
Low understanding or priority focus by leadership	4.4
Staff training	4.4
Learner training	5.2

Round 3

The top three issues noted in Table 3 were then emailed to the expert panel for round three. An open-ended question accompanied each issue.

1. If you were setting the cyber security policy for an online learning program, what would you do, specifically, to reduce the vulnerability of online data and protect data integrity?
2. What tools, processes, etc., would you implement to enhance user authentication? What would user authentication cost, and what would be the impact on faculty and students?
3. When dealing with the issues of outdated hardware and software, what hardware and software should an online learning system have in place? Please be as specific as you can. Can the additional costs of new hardware and software be justified? How?

Responses from the Human Expert Panel to the Three questions

Question #1: If you were setting the cyber security policy for an online learning program, what would you do, specifically, to reduce the vulnerability of online data and protect data integrity?

The textual responses from the expert panel were submitted to content analysis following the method of Saldaña (2016).

Six different themes developed from this question and are presented below. The listed themes are presented from the most frequent theme to the least frequent, but each appeared at least three separate times. Some comments from panel members are in quotation marks.

1. Strong authentication and verification of all personnel, including students, faculty, and administration is critical. This includes multi factor and multi-layer authentication. This also includes software biometrics.
2. It is important that hardware and software be up to date and reviewed on a regular schedule (at least every 2 to 3 years). This includes firewalls and routers.
3. Audits are essential. Audits of the system should be performed on a regular basis. "Internal and external data security/integrity audits [to] ensure proper controls are in place (and audited) with regards to data access." There should be regular audits of user identification, and an audit trail created. The audit trail would also capture user "behaviors" and suspicious activity noted.
4. Encryption of devices and passwords
5. Restriction of access, including account management policies. Data access audited and restricted.
6. Training on security fundamentals

Question #2: What tools, process, etc. would you put into place to enhance user authentication? What would be the costs and/or impact of user authentication on faculty and students?

This question was more focused, and five themes developed. The focus was on authentication. Authentication in this question has four subthemes.

1. Standardized protocols such as the InCommon protocol for hardwired connections and EDUROAM for wireless.
2. Security costs will increase by failure will be costlier.

3. Multi factor authentication software authentication harder login process
4. different passwords for different applications or levels two factor authentication on password changes
5. Training of users with good communication Independent third-party testing.

Question 3: When dealing with the issues of outdated hardware and software, what hardware and software should an online learning system have in place? Please be as specific as you can. Can the additional costs of new hardware and software be justified? How?

Five themes developed in responses from the expert panel in relation to the third question. This was the first time internal threats were specifically mentioned. When dealing with costs, the issue of public relations fallout was also mentioned for the first time.

1. Internal threats are as dangerous as external threats; they last longer, and are most costly to overcome.
2. The Learning Management System (LMS) must be up to date and flexible enough to include current security software and updates.
3. Strong authentication software and encryption is essential
4. Up to date software including authentication software, data encryption software, and access management software.
5. Increased costs are justifiable, especially when you consider the downside costs and bad public relations.

The-Delphi Study with a Virtual the Expert Panel

This research aimed to compare the results detailed above from an original Delphi study on cybersecurity for online education (Davidson & Hasledalen, 2014) to responses from an AI bot. However, the chatbot was not given information from the original study. The AI Bot used was ChatGPT. ChatGPT is a chatbot developed by OpenAI (OpenAI.com) and offered free to the public in November 2022. It is a simple and intuitive process where questions are asked, and the bot responds very quickly, pulling its responses from a super database.

Round One Initial Request: AI Response

The following first-round request was submitted to the virtual expert panel.

Assuming that online educational systems are vulnerable to cyberattacks and that there are issues of cyber security, please list three of the most critical issues that, in your opinion, institutions of higher learning must address now and especially in the future. Please label your comment with two or three words and then follow with a one-paragraph explanation.

The instruction above is the same sent to the expert panel in the original study.

Table 5: Responses from the AI Bot to Question #1

Collaboration and Information Sharing
Continuous Improvement
Crisis Communication and Public Relations
Cyber Threat Awareness and Training
Data Privacy
Data Privacy and Compliance
Emerging Technologies and Trends

Incident Response Planning
Network Infrastructure
Regular Security Audits and Assessments
Resource Allocation and Investment
Secure Online Learning Platforms
User Awareness

Round Two

The list was reduced to 10 items for the second round as they were very similar. Ten vulnerabilities were submitted to the AI chatbot with the request to prioritize the ten as to the level of importance, with one being the most important. Table 5 is the list of the priorities submitted to the AI expert panel in priority order. The lower the average, the higher the level of importance in the expert panel's opinion.

Table 6: List of Ten Priorities Ranked for "Least Important to Most Important."

Virtual Expert Panel	Average
Secure Online Learning Platforms	1.8
Data Privacy and Compliance	3.5
Regular Security Audits and Assessments	4.0
Cyber Threat Awareness and Training	4.3
Network Infrastructure	4.3
Resource Allocation and Investment	4.5
Emerging Technologies and Trends	7.2
Incident Response Planning	8.2
User Awareness	8.2
Collaboration and Information Sharing	9.5

Following the same process as in the original study, the virtual expert panel was asked to do the following. Using the top three issues noted in Table 6, the expert panel was asked the following three open-ended questions.

1. If you were responsible for the cybersecurity policy of an online learning program, what specific measures would you implement to ensure the security of the online learning platforms? How would these measures enhance the overall security of the system and protect against potential cyber threats?
2. What specific tools, processes, or policies would you recommend to enhance data privacy and ensure compliance with relevant regulations in an online learning environment? What would be the cost implications of these measures, and how would they impact the faculty, students, and the overall learning experience?
3. What specific hardware, software, or processes should an online learning system have in place? Please be as specific as you can. Can the additional costs of these audits and assessments be justified? How would they contribute to the overall security of the online learning environment?

Responses from the Virtual Expert Panel to the Three questions

Question #1: If you were responsible for the cybersecurity policy of an online learning program, what specific measures would you implement to ensure the security of the online learning platforms? How would these measures enhance the overall security of the system and protect against potential cyber threats?

Six different themes evolved from the question and are presented below.

1. There is a need to ensure the security of online learning platforms. The implementation of Multi-layered security approach is needed.
2. Data needs to be encrypted in transit and at rest.
3. There would be a need to include intrusion detection systems to monitor and alert any suspicious activity.
4. There is a need to conduct regular vulnerability assessments.
5. Penetration testing should be conducted to identify potential vulnerabilities
6. AI and machine learning algorithms should be developed and installed to detect and respond to threats in real-time.

Question #2: What specific tools, processes, or policies would you recommend to enhance data privacy and ensure compliance with relevant regulations in an online learning environment? What would be the cost implications of these measures, and how would they impact the faculty, students, and the overall learning experience?

Five different themes emerged from questions put to the virtual expert panel.

1. The implementation of a comprehensive data governance framework is recommended, with strict access controls.
2. Data encryption to protect data.
3. Regular audits
4. Privacy-enhancing technologies such as anonymization and pseudonymization to protect individual identities.
5. Advocate a culture of data privacy with regular training to cover topics such as phishing, and the use of strong passwords.

Question #3: What specific hardware, software, or processes should an online learning system have in place? Please be as specific as you can. Can the additional costs of these audits and assessments be justified? How would they contribute to the overall security of the online learning environment?

Six themes were developed from the textual analysis of the virtual panel responses to question #3.

1. An online learning system should have a robust security information and event management (SIEM) system in place.
2. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for suspicious activities and take action to prevent potential attacks.
3. Regular internal audits to ensure system security.
4. Regular third-party audits to ensure compliance with security policies and regulations.
5. Continuous security assessment with real-time monitoring and analysis of system activity.
6. Use of AI and machine learning techniques to identify unusual patterns.

4. Analysis

The purpose of this research study was to compare the outcomes of a traditional Delphi Technique study

using an expert panel to the outcomes of the same questions asked of an AI chatbot. The AI chatbot used was ChatGPT.

Comparison of Round 1 Responses

The human expert panel and the virtual expert panel were each asked the following question.

Assuming that online educational systems are vulnerable to cyberattacks and that there are issues of cyber security, please list three of the most critical issues that, in your opinion, institutions of higher learning must address now and especially in the future.

Table 6: Comparison of Question # 1 Expert Panel Priorities versus ChatGPT Priorities

Original Expert Panel	ChatGPT 4
Continuous vulnerability translates to being a soft target	Collaboration and Information Sharing
Data security	Continuous Improvement
Higher ed institutions do not have a clear understanding of the threat	Crisis Communication and Public Relations
Identify and access management	Cyber Threat Awareness and Training
Educating the user on how to protect their privacy	Data Privacy
Integrity of data	Data Privacy and Compliance
Lack of Encryption	Emerging Technologies and Trends
Lack of Multifactor to access cloud-based assets	Incident Response Planning
Lack of Multifactor to access devices.	Network Infrastructure
Lack of security training for online learners	Regular Security Audits and Assessments
Low leadership priority status translates to continuous vulnerability.	Resource Allocation and Investment
Not enough trained and motivated staff.	Secure Online Learning Platforms
Outdated hardware	User Awareness
Outdated software	
Staff lacks appropriate training in cyber security issues.	
Uploading/downloading of harmful files	
User Authentication	

Comments on Round 1: Looking at the two sets of issues to address, many were similar and overlapped. However, the comments from the original expert panel are almost all stated in negative terms, whereas the chatbot responses are in a simple list of priorities. This underscores the importance of the wording of the initial question or questionnaire. It would appear that the human panel resonated with the term "vulnerable," whereas the AI bot did precisely what was asked, and without emotional context..

The question is whether the two lists are comparable. When examining responses to the first question, the AI ChatGPT responses appear to have three priorities not listed by the expert panel.

1. Collaboration and Information Sharing
2. Continuous Improvement
3. Incident Response Planning

However, the remaining ten items relate closely to the responses from the expert panel.

- Crisis Communication and Public Relations could relate to Low leadership priority status relates to continuous vulnerability.
- Cyberthreat awareness and training could relate to staff lacks appropriate training in cyber security issues.
- The Data Privacy and Data Privacy and Compliance priorities in the ChatGPT column could be combined and relate to Integrity of Data and Lack of Encryption. This could also relate to the two comments about a lack of multifactor authentication for devices and cloud-based assets.
- The Emerging Technologies and Trends priority could also relate to the comments about multifactor authentication (MFA). The original study was conducted in 2014 when MFA was less widespread and "emerging."
- Network Infrastructure would include Outdated hardware and software.
- Regular Security Audits and Assessments would tie in with the comment of Continuous vulnerability translates to being a soft target.
- Resource Allocation and Investment relate to the Low Leadership priority from the expert panel.
- Secure Online Learning Platform relates to some expert panel priorities, including the lack of encryption, MFA, and training priorities.
- The User Awareness priority relates to the comments that staff lack appropriate training, insufficient trained and motivated staff, lack security training for online learners, and educating the user on how to protect their privacy.

Comparison of Question #2

For question #2, the expert panel and the chatbot AI were asked to prioritize their respective lists of priorities.

Table 7: Comparison of Top Priorities between the Expert Panel and the ChatGPT Bot

Expert Panel	ChatGPT AI bot
Vulnerability of data (data integrity)	Secure Online Learning Platforms
User authentication	Data Privacy and Compliance
Outdated hardware and software	Regular Security Audits and Assessments

As both the panel and the AI bot prioritized different lists, the expectation was that there would be minimal overlap. However, the expert panel's priority of vulnerability of data and data integrity does align with Data Privacy and Compliance as well as with the secure online learning platforms.

Comparison of Question #3

In any Delphi Technique study, the last iteration is ultimately the most important. Comments and responses in the final round of questions are the end product of the research. The question is whether the expert panel and the chatbot AI shared common perspectives.

The final five themes from the human expert panel were as follows:

1. Internal threats are as dangerous as external threats; they last longer and are most costly to overcome.
2. The Learning Management System (LMS) must be up to date and flexible enough to include current security software and updates.
3. Strong authentication software and encryption is essential

4. Up to date software including authentication software, data encryption software, and access management software.
5. Increased costs are justifiable, especially when you consider the downside costs and bad public relations.

The final six themes from the virtual expert panel were as follows:

1. An online learning system should have a robust security information and event management (SIEM) system in place.
2. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for suspicious activities and take action to prevent potential attacks.
3. Regular internal audits to ensure system security.
4. Regular third-party audits to ensure compliance with security policies and regulations.
5. Continuous security assessment with real-time monitoring and analysis of system activity.
6. Use of AI and machine learning techniques to identify unusual patterns.

The outcomes are similar. The concern of internal threats and threat detection is a common issue. Both focus on security of the learning management system.

It would appear that Group 1 is more focused on pinpoint issues that can be addressed directly through technical solutions, whereas Group 2 adopted a holistic approach, suggesting that education, platform-level solutions, and adherence to data protection standards are equally crucial.

5. Discussion

This was an interesting exercise that provided opportunities to learn more about the use of AI bots in research. In the beginning, multiple AI bots were used. Because each has a slightly different training, they give potentially different viewpoints, but it was decided to use ChatGPT4 for the final results for this study.

One noticeable difference between the human expert panel and the virtual expert panel is that the latter is very "politically correct." The chatbots are never negative. They might make suggestions for improvement, but the common focus by the human expert panel on "lack" was not found with the chatbots.

Another difference with the chatbot was that it tends to try and cover all areas equally. For example, when the virtual panel was originally created, each member of the panel was from a different country and there was an even split between the genders. I had to ask the chatbot to change the gender mix to align with the original panel more closely and also indicated that all the participants were from the United States, as in the original study.

Having made those changes, I still used the original virtual panel as suggested by the AI to test and see if there were any differences based on the changes I have made. The responses from the all U.S. all male panel did not make any substantive difference compared to the original panel as suggested by the chatbot.

This framework reveals that while both panels produced valuable insights, each demonstrated distinct advantages. The human panel provided more contextual and experience-based responses, while the AI panel offered more systematic and comprehensive coverage of security domains.

For those researchers who are familiar working with AI chatbots, it is noticed that most chatbots tend to respond in a similar manner. Experienced AI users can typically spot AI written material quickly because of the way the text is written. AI chatbots do not get emotional and tend to focus on exactly what is asked.

One concern with using chatbots for research is that they do not discriminate as to the material they use to support their statements. For example, in most scholarly research, the goal is to use peer-reviewed journal

articles as much as possible. Chatbots that have access to the internet will take data from blogs and websites without discriminating as to the quality of the data input.

One other issue that is frequently mentioned when using chatbots is the tendency to make errors. For example, when the virtual expert panel was asked to prioritize the top ten list for round two, the chatbot returned 11 priorities. One was a duplicate. When this was pointed out to the AI bot and the question was asked again, the response was, "I apologize for the duplication in my previous response. That was an oversight on my part. Here is the corrected ranking of the ten items from least to most important."

6. Conclusions

This comparative study of human and AI expert panels in Delphi research yields several significant findings. First, the AI-generated responses showed good alignment with human expert priorities in cybersecurity for online education, particularly in identifying critical areas like training, data security, and infrastructure needs. Second, the AI panel demonstrated the ability to provide comprehensive, structured responses while maintaining consistency across multiple rounds. However, the study also revealed limitations in AI implementation. The AI responses, while technically sound, sometimes lacked the nuanced understanding of institutional constraints and practical implementation challenges that characterized the human expert panel's responses. Additionally, the AI's tendency toward more formalized, systematic responses may not fully capture the experiential insights that human experts bring to Delphi studies.

These findings suggest that while AI could potentially augment or expedite certain aspects of Delphi studies, it may be most effective when used in combination with human expertise rather than as a complete replacement. Future research should explore hybrid approaches that leverage the strengths of both human and AI participants in Delphi studies.

Delimitation: The use of a paper published in 2014 might be questionable. The decision was made because the author of this paper was also the primary author of the original paper. To avoid any hint that this paper was criticizing the work of someone else, it was decided to use the author's own work. In addition, the world of cybersecurity has evolved rapidly over the last 10 years, the primary issues addressed with the both the previous and current studies are much the same.

References

1. Back, S., & Guerette, R. T. (2021). Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. Journal of Contemporary Criminal Justice, 37(2), 427-451. https://doi.org/10.1177/10439862211001628
2. Davidson, P. L., & Hasledalen, K. (2014). Cyber threats to online education: A Delphi Study. 2nd International Conference on Management, Leadership, and Governance, Boston, MA.
3. Djama, R. M.. (2024). The impact of Artificial Intelligence on the global economy: Opportunities and challenges. International Journal of Multidisciplinary Research, 6(6), 1-7. https://doi.org/10.36948/ijfmr.2024.v06i03.22385
4. Goodman, C. M. (1987, November). The Delphi technique: A critique. Journal of Advanced Nursing, 12(6), 729-734. doi:10.1111/j.1365-2648.1987.tb01376.x
5. Gordon, T. J., & Helmer, O. (1964). Report on a long-range forecasting study. Santa Monica, CA: Rand Corporation.

6. Haenlein, M., & Kaplan, A. (2019). A brief history of Artificial Intelligence: On the past, present, and future of Artificial Intelligence. California Management Review, 61(4), 5-14. https://doi.org/10.1177/0008125619864925
7. Hijji, M., & Alam, G. (2022). Cybersecurity awareness and training (CAT): Framework for remote working employees. Sensors, 22(22), 8663. https://doi.org/10.3390/s22228663
8. Hill, K. Q., & Fowles, J. (1975). The methodological worth of the Delphi forecasting technique. Technological Forecasting & Social Change, 7(2), 179-192. doi:10.1016/0040-1625(75)90057-8
9. Johnson, K. B., Wei-Qi, W., Weeranatne, D., Frisse, M. E., Misulis, K., Rhee, K., Zhao, J., & Snowdon, J. L. (2021). Precision Medicine, AI, and the future of personalized health care. Clinical and Translational Science, 14, 85-93. https://doi.org/10.1111/cts.12884
10. Saldaña, J. M. (2016). The coding manual for qualitative researchers. Sage Publications.
11. Ulnicane, I. & Erkkila, T. (2023). Politics and policy of Artificial Intelligence. *Review of Policy Research, 40*.(5), 612-625. https://doi.org/10.1111/ropr.12574