BMIJ
ISSN: 2148-2586

bmij (2024) 12 (3):610-628
doi: https://doi.org/10.15295/bmij.v12i3.2396
Research Article

Integrating AI with aviation cybersecurity: The strategic role of human resources

Yapay zekâ ile havacılık siber güvenliğinin entegrasyonu: İnsan kaynaklarının stratejik rolü

Filiz Mızrak[1]

[1] Assist. Prof. Dr., Beykoz University, Istanbul, Türkiye, flzmizrak@gmail.com

ORCID: 0000-0002-3472-394X

Abstract

The escalating complexity of cyber threats in aviation highlights the crucial need to integrate advanced technologies and strategic human resource management. This study delved into incorporating artificial intelligence (AI) in aviation cybersecurity, explicitly focusing on the strategic role of human resources (HR) in supporting these endeavours. Semi-structured interviews with eight industry experts from Turkey were analysed using NVivo to identify critical themes such as HR's involvement in cybersecurity, challenges in AI implementation, and the significance of cultural integration and interdepartmental collaboration. Sentiment analysis with Python's TextBlob indicated high positivity towards AI and strategic HR involvement. The findings underscored the necessity for continuous education, strategic recruitment, and resilient cybersecurity frameworks, emphasising AI's transformative impact on real-time threat detection and predictive analytics. The research offered valuable insights and recommendations for enhancing aviation cybersecurity, highlighting the essential role of HR and the advantages of AI integration.

Keywords: Human Resource Management, Aviation Management, Cybersecurity, Artificial Intelligence

Jel Codes: M50, L93, L86, O33

Öz

Havacılıkta siber tehditlerin artan karmaşıklığı, gelişmiş teknolojilerin ve stratejik insan kaynakları yönetiminin entegrasyonunun önemini vurgulamaktadır. Bu çalışma, yapay zekanın (YZ) havacılık siber güvenliğine entegrasyonunu, insan kaynaklarının (İK) bu girişimleri desteklemedeki stratejik rolünü incelemektedir. Türkiye'den sekiz sektör uzmanıyla yapılan yarı yapılandırılmış görüşmeler, NVivo kullanılarak analiz edilmiştir. Bu analiz sonucunda, İK'nın siber güvenlikteki rolü, YZ uygulamasındaki zorluklar, kültürel entegrasyon ve departmanlar arası iş birliğinin önemi gibi ana temalar belirlenmiştir. Python'ın TextBlob kütüphanesi ile yapılan duygu analizi, YZ ve stratejik İK katılımına yönelik yüksek düzeyde pozitiflik olduğunu göstermiştir. Bulgular, sürekli eğitim, stratejik işe alım ve dayanıklı siber güvenlik çerçevelerinin gerekliliğini vurgulamaktadır. Ayrıca, YZ'nin gerçek zamanlı tehdit tespiti ve tahmine dayalı analizler üzerindeki dönüştürücü etkisine de dikkat çekmektedir. Araştırma, havacılık siber güvenliğini geliştirmek için değerli bilgiler ve öneriler sunarak, İK'nın temel rolünü ve YZ entegrasyonunun avantajlarını öne çıkarmaktadır.

Anahtar Kelimeler: İnsan Kaynakları Yönetimi, Havacılık Yönetimi, Siber Güvenlik, Yapay Zeka

Jel Kodları: M50, L93, L86, O33

Submitted: 20/05/2024

1th Revised: 27/06/2024

2nd Revised: 30/06/2024

Accepted: 4/07/2024

Online Published: 25/09/2024

Citation: Mızrak, F., Integrating AI with aviation cybersecurity: The strategic role of human resources, bmij (2024) 12 (3): 610-628 doi: https://doi.org/10.15295/bmij.v12i3.2396

Introduction

In a world where new cyber threats evolve faster than traditional defences, aviation stands at the forefront of cybersecurity, which is crucial for safeguarding its operations and sensitive passenger data. This highlights the growing importance of integrating Artificial Intelligence (AI) into cybersecurity measures. This shift is not merely technical but represents a comprehensive organisational transformation, particularly within Human Resources (HR). HR plays a pivotal role in bridging the data-human divide, managing the workforce that operates these technical tools and ensuring the effective oversight of human supervisors who control these systems (Mizrak, 2023).

This study focuses on the link between AI-driven automation and HR Cyber Security in the Aviation Sector. It aims to examine the adopted strategies and the obstacles faced, notably in HR policy, in light of technological improvements and developments. This study is novel in its importance, as cyber threats against the aviation sector are becoming more sophisticated, and security incidents could have catastrophic consequences. This environment calls for a new role for HR: from a traditional focus on compliance and damage limitation to one in which continual preparedness and awareness are created through strategic training and development.

Situated within various Human Resource Management (HRM) theories, this study is grounded in the Resource-Based View (RBV), Human Capital Theory, Contingency Theory, Systems Theory, Organizational Learning Theory and Strategic Human Resource Management (SHRM). These theories present a solid theoretical basis to explain how HR practices can help build cybersecurity mechanisms in the aviation industry. Prior research has tended to study AI and HR due to certain aspects or has emphasised the importance of regular up-skilling/training, tactful hiring, and collective action between departments. Nonetheless, there is a gap in the literature on treating this multimorbidity with a comprehensive and integrated approach.

In order to address this gap, this study proposes the following research questions:

Research Questions:

- How can HR integration improve cybersecurity measures in the aviation industry through AI-driven automation?
- What are the specific strategies employed by HR to enhance cybersecurity?
- What challenges do organisations face in aligning HR policies with technological advancements in cybersecurity?
- How can a cybersecurity awareness and readiness culture be fostered within the aviation sector?

The research uses an empirical qualitative design with semi-structured interviews with eight aviation and cybersecurity experts/HR professionals in Turkey. The results of these interviews will be coded in NVivo to perform a thematic analysis and will also be analysed using the TextBlob library in Python for sentiment analysis. This approach ensures a holistic view of expert perspectives and contributes to identifying the major themes and sentiments regarding integrating AI with cybersecurity, HR, and cybersecurity.

This research addresses a critical research gap by conceptualising the interplay among AI technologies, HR strategies, and cybersecurity practices in aviation. The undertaking synthesises theoretical knowledge with applied examples and expert opinions and will offer constructive suggestions to strengthen aviation's cybersecurity.

Literature review

The literature on AI integration in aviation cybersecurity and the strategic role of HR provides a comprehensive understanding of the current state of knowledge and identifies significant gaps that this study aims to address. Whitworth et al. (2023) studied the utilisation of AI in 5G aviation networks that focused on detecting Distributed Denial of Service (DDoS) attacks. Their study reports the development of a fault-tolerant structure from an AI algorithm to identify scenarios of a DDoS attack from flight networks, an essential step for real-time detection and mitigation of DDoS events. They concluded that further research is necessary to operationalise AI with the latest technology, such as 5G, to enhance the aviation sector's security. Kumar (2022) studied the essentials of artificial intelligence for optimisation in the air market and emerging possibilities produced by AI for the overall betterment of aviation operations, such as cybersecurity.

A few studies have also focused on the importance of cybersecurity training and awareness in the aviation industry. Sabillon et al. (2023) stated that security awareness training helps detect cyber threats and security flaws for exploitation. The study establishes that training programs significantly enhance cybersecurity in aviation establishments. To address this issue, the authors proposed increased efforts to educate and raise awareness about better digital hygiene measures in the industry as a long-term solution.

Llorens (2017) investigated the role of HRM in cybersecurity, particularly in the public sector. The study examined how HR policies and practices can support cybersecurity initiatives by improving employee knowledge and compliance. The results suggest that HRM is the cornerstone for the pro-integration of cybersecurity in the organisation. Furthermore, Manoharan (2024) discussed cybersecurity steps in HR systems, this time plotted to secure the data of employees in the era of AI. This study, published under the General Data Protection Regulation (GDPR), emphasised the necessity of safeguarding HR data against cyber threats and highlighted HR professionals' role in establishing these protections.

Beyond this, studies have investigated current or future challenges in aviation regarding cyber security and the best strategies to address challenges. These emerging cybersecurity challenges were the topic of a seminar on applied cybersecurity strategy for managers by Duchamp et al. (2016). They identified some of the most pressing dangers and suggested recommendations on how these risks should be dealt with, with solid cybersecurity frameworks being pivotal.

Scott's (2019) study extensively examined the European Union's approach to regulating aviation cybersecurity. That philosophical underpinning emerged in his book Aviation Cybersecurity, which examined current regulations and suggested improvements to counter the changing threat surface. The study identified deficiencies in the existing regulatory environment and recommended better cybersecurity governance in aviation.

Further inquiry has focused on integrating human-centric and multidisciplinary perspectives for cybersecurity problems. According to the Roadmap (2020), a human-centric approach to applying AI in Air Traffic Management (ATM) is recommended, emphasising the importance of considering human factors in designing and implementing AI systems. This report, published by the European Aviation Safety Agency, emphasised the need to align AI applications with human capabilities and limitations to ensure safe and effective operations.

Although these studies have helped advance the aggression research field, several limitations still pervade the literature. A significant gap in the literature is the necessary empirical work to assess the long-term effects of AI integration into aviation cybersecurity practices. Much research has been conducted on the benefits offered by AI, but fewer longitudinal studies to inform us of the continued effectiveness of AI. HR departments should probably question how they can better foster cybersecurity-conscience and how they can do the research with these specific strategies. More research is needed to investigate holistic frameworks that merge AI technologies and strategic HR practices to improve cybersecurity in aviation. Finally, the significant advancements discussed in this paper regarding the integration of AI, HR, and cybersecurity in aviation stress the necessity for more comprehensive research to analyse the industry's multifaceted challenges.

Past airline cyberattacks

Over the years, the aviation industry has faced attacks, on several occasions, from cyber threats, further accentuating the growing importance of cybersecurity to combat new threats, protect these critical systems, and secure vital data. The most significant DDoS attack in the UK affected Heathrow Airport in July 2015, when the servers became overloaded with traffic and online services collapsed. ACI World (2023) emphasised the need to implement DDoS protection solutions, keep essential services redundant, and carry out stress tests to defend power services from such attacks.

In May 2015, Polish airline LOT experienced a significant flight disruption due to a breach of its ground operations system. This incident proved an urgent need for more sophisticated intrusion detection systems to prevent such security breaches. All necessary isolation of the critical element’s networks on regular security audits of the Air Traffic Control ATC breach (Atlantic Council, 2017) suggested similar actions to thwart such incidents. During another supply chain attack in September 2018, a third-party service compromise disrupted Bristol Airport's flight information display systems and impacted the airport's operations. This demonstrates the importance of a robust vendor assessment process, supply chain cybersecurity measures, and third-party access monitoring (Bitsight, 2020).

San Francisco International Airport's web servers were compromised in a ransomware attack in April 2020. If nothing else, this attack demonstrated the necessity of backup solid solutions, consistent patching, and companywide phishing education to try to limit the amount of ransomware damage that is done by events like this (Kazim, 2023). In October 2020, several European airports were lured into clicking on phishing emails that attempted to compromise their systems. The incident again flagged the necessity of forging email filters, providing two-factor (or multi-factor) authentication (MFA), and running periodic phishing simulations to help staff (Atlantic Council, 2020).

The Dark Web has exposed sensitive information about the top 100 airports, with a massive data breach in Nov 2020. This breach stressed the importance of encrypting sensitive data, utilising data loss prevention tools, and conducting vulnerability and misconfiguration assessments to prevent unauthorised data access (Bitsight, 2020). The analyst cited an insider threat at a major European airport in January 2023 when an employee leaked access credentials, posing security risks. This made apparent to all how significant the role of background checks, role-based accesses, and robust insider threat programs (Kazim, 2023).

In March 2023, airport networks were accessible by taking advantage of weak security in Internet of Things (IoT) devices like smart cameras. The attack demonstrates the need for strong authentication, regular firmware updates, and secure network segmentation for IoT devices, often targeted for vulnerabilities (Atlantic Council, 2020). German airports, including Lufthansa, were hit in May 2023 by IT failure and flight disruptions due to DDoS attacks. The attack demonstrated the importance of deploying DDoS protection, maintaining redundant services, and subjecting systems to thorough stress testing (CM Alliance, 2023).

The following October, the Russia-residing group KillNet was responsible for DDoS attacks that took down the websites of US airports, such as Los Angeles International Airport (LAX) and Chicago O'Hare. The attack reinforced the need to ensure web application firewalls were in place, improve monitoring, and develop incident response strategies for service disruption (InformationWeek, 2023). ALTOUFAN TEAM launched DDoS attacks on Gulf Air and Bahrain International Airport in November 2023, exposing customer data with Gulf Air. These incidents reinforced the importance of beefing up network security, DDoS mitigation plans, incident response preparedness, data encryption, and access management (Resecurity, 2023).

In December 2023, Qatar Airways was hacked by the R00TK1T ISC Cyber Team, putting its flight and operational data at risk. This breach proved the importance of encrypting sensitive data, strengthening access controls, and conducting regular security audits to prevent such incidents. (Resecurity, 2023).

Significant historical cyberattacks in the aviation industry illustrate this diversity and development of cyber threats. These cases emphasise the need for businesses to adopt a full suite of cyber security tools and practices, including technical defences, routine audits, employee training and superior incident response, to mitigate these ongoing risks.

Theoretical framework: Aligning HRM theories with aviation cybersecurity and AI integration

HRM theories provide a framework for understanding how AI can be integrated into aviation cybersecurity and HR's strategic posture. These theories offer insights into how HR practices can be utilised to support and enhance cybersecurity measures within the aviation industry.

According to the RBV, organisations that effectively manage their valuable, rare, inimitable, and non-substitutable resources can gain a competitive advantage (Harvey & Turnbull, 2020). This applies to the HRM domain, where strategic talent promotion in cybersecurity is crucial. This confirms the importance of treating HR practices as critical elements in gaining competitive advantages, which involves continuous training and strategic recruitment in cybersecurity.

The Human Capital Theory suggests that employee education and training investments lead to more skilled and knowledgeable employees, thus improving organisational performance (Gillam, 2019). The study emphasises the significance of continuous training and development programs to ensure employees are well-versed in the cybersecurity skills needed to effectively integrate AI and strong cybersecurity measures in the aviation industry.

Contingency Theory highlights that there is no universal best way to organise or manage and that organisational structures should be appropriate in terms of their impact on organisational performance and cost of implementation based on the specific situation (Kankaew & Pongsapak 2020). The study emphasises the importance of customising HR practices to address challenges in integrating AI into cybersecurity. For instance, balancing automation with human oversight and addressing specific training needs are context-specific actions aligned with Contingency Theory. This theory suggests that HR strategies in the aviation industry should be adaptable and resilient to be effective.

Organisations can be considered complex systems with interrelated and interdependent parts (Henning, 2015). The study's emphasis on collaboration between IT, HR, and cybersecurity teams aligns with the principles of Systems Theory. Comprehensive cybersecurity requires organisations to take a comprehensive approach that accounts for the interdependencies in an organisation. Aviation companies can also unite the workforce by creating an environment that promotes partnerships across departments, yielding a more robust cybersecurity approach.

The organisational learning theory concerns how organisations learn and adapt over time (Jung & Takeuchi, 2010). This study reflects the Organizational Learning Theory, which states that continuous information security education and regular security audits are necessary to update current cyber security practices repeatedly. There is no one-size-fits-all solution for any company in aviation; all must learn from experience and evolve cyber approaches. This theory enforces the need for an organisational culture of learning and continuous improvement.

The underlying focus of SHRM is to coordinate HR practices with the organisation's strategic objectives and goals to enhance performance (Harvey & Turnbull, 2020). The integration of HR strategies with cybersecurity goals at the heart of the study reflects SHRM principles as a norm. The HR practices such as strategic recruitment, continuous training, and fostering a cybersecurity culture support the organisation's strategic objectives to improve cybersecurity. This focus area is crucial as it ensures that HR practices have a direct bearing on the abilities of the organisation to address and reduce cybersecurity risks.

Together, these HRM theories present a solid basis for explaining how HR practices can facilitate and help in cybersecurity activities in aviation. By incorporating these theories into their HR strategies, businesses can mitigate the hurdles faced in AI-enabled integration with Cybersecurity and empower a robust, proactive Cybersecurity workforce. While serving as a valuable basis to offer an integrated perspective on HRM-cybersecurity mediating mechanism, the research also forms the basis of critical recommendations that could strengthen cybersecurity practices for aviation companies adopting strategic HRM.

Methodology

Data collection

For this investigation, data were collected through semi-structured interviews with eight experts in Turkey specialising in various fields such as aviation, cybersecurity, and human resources. These experts were chosen based on their extensive experience and knowledge in their respective sectors to provide a comprehensive view of the integration of AI in aviation cybersecurity and a strategic perspective on HR. The interviews were conducted between January 2024 and March 2024, each lasting roughly 60 minutes. Table 1 details the eight experts interviewed, including their years of experience and positions. This table highlights the diverse and extensive expertise of the participants, which is crucial for providing a comprehensive view of the research topics. The researcher obtained ethical committee approval for this study from Beykoz University, dating 06.06.2024, ensuring compliance with ethical standards throughout the research process.

Table 1: Information about the Participants

Expert	Experience (Years)	Position
Expert 1	15	Chief Information Security Officer (CISO)
Expert 2	12	Head of Cybersecurity
Expert 3	18	Senior HR Manager
Expert 4	20	Director of IT Operations
Expert 5	10	Cybersecurity Consultant
Expert 6	14	Aviation Safety and Security Specialist
Expert 7	17	AI and Machine Learning Engineer
Expert 8	13	HR Business Partner

The interview questions were formulated to capture comprehensive insights into the integration of AI in aviation cybersecurity and the strategic role of HR. Several critical objectives guided this formulation process. Firstly, understanding the experts' roles and responsibilities was crucial, as it established the context and relevance of their experiences. Questions like "Can you describe your current role and responsibilities in cybersecurity and HR management within the aviation sector?" were inspired by studies like those by Llorens (2017).

Exploring the experts' perspectives on AI integration was another critical objective. This included understanding the benefits and challenges of AI-driven automation in cybersecurity. Questions like "How has your experience shaped your views on the integration of AI in aviation cybersecurity?" and "How do you see AI-driven automation impacting the cybersecurity landscape in aviation?" were influenced by research conducted by Garcia et al. (2021).

Identifying the prevalent cybersecurity threats facing the aviation industry today was essential for understanding the current landscape. Questions designed to uncover these threats were based on findings from studies such as those by Kumar (2022). Similarly, assessing the strategic involvement of HR in supporting cybersecurity initiatives was guided by insights from Sabillon and Bermejo (2023), leading to questions like "What role does HR play in supporting cybersecurity initiatives within your organisation?" and "Can you provide examples of how HR has successfully contributed to mitigating cybersecurity risks?"

Another critical area of focus was understanding the practical challenges of integrating AI-driven tools into cybersecurity measures. This was inspired by the work of Duchamp et al. (2016), resulting in questions like "What are the main challenges you face when integrating AI-driven tools in cybersecurity measures?" and "How does HR address these challenges, particularly in training and development?" The exploration of effective strategies for aligning HR policies with AI-driven cybersecurity enhancements also drew from similar studies.

To gain insights into future directions and trends at the intersection of HR, AI, and cybersecurity, questions such as "What future trends do you anticipate in the intersection of HR, AI, and cybersecurity within the aviation sector?" were asked, considering the evolving landscape highlighted by Whitworth et al. (2023). Finally, questions designed to elicit actionable insights and recommendations for HR professionals were inspired by practical approaches discussed in the literature.

Appendix 1 contains the specific interview questions. Table 3 in the appendix explains the reasons for asking each question and references the studies that guided their formulation. This comprehensive approach ensured that the interviews were well-structured and aimed at gathering in-depth and relevant expert information.

Data analysis

After the interviews, the data were systematically analysed using NVivo to identify primary themes and sub-themes. These themes included the role of HR in cybersecurity, challenges in AI integration, and the impact of AI on cybersecurity. The data were coded to provide an exhaustive and descriptive categorisation and frequency count of each theme.

The coding method involved categorising the data into themes and sub-themes, identifying patterns, and gaining a deep understanding of the most prominent issues discussed by the experts. This coding process was facilitated by NVivo's powerful query tools, which enabled an exhaustive and descriptive categorisation of each theme.

Next, the coded data were exported from NVivo and visualised using Matplotlib, a Python library, to perform frequency analysis. This process involved creating a bar chart to illustrate the frequency of mentions for each theme and sub-theme. The count axis on the bar chart represents the number of times each theme was mentioned, providing a clear comparison of the prevalence of each theme.

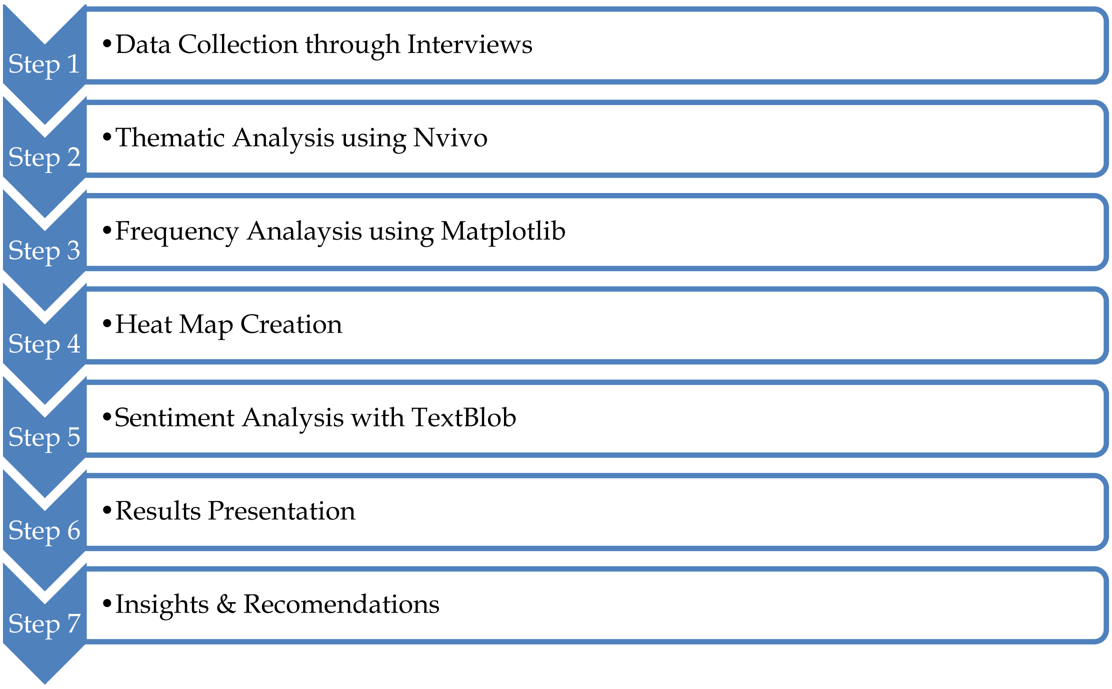
Step 1
•Data Collection through Interviews
Step 2
•Thematic Analysis using Nvivo
Step 3
•Frequency Analaysis using Matplotlib
Step 4
•Heat Map Creation
Step 5
•Sentiment Analysis with TextBlob
Step 6
•Results Presentation
Step 7
•Insights & Recomendations

Figure 1: Workflow of the Analysis

Figure 1 illustrates the workflow of the analysis process, from data collection through semi-structured interviews to the thematic analysis using NVivo and the visualisation of frequency analysis using Matplotlib.

During the thematic analysis, each segment of the interview transcripts relevant to the research objectives was assigned to a code representing a theme or sub-theme. This coding process in NVivo allowed for the systematic categorisation of the data. NVivo's query tools counted the times each theme and sub-theme appeared across all interview transcripts. This provided a frequency count for each code, indicating how often the participants mentioned a particular theme. The frequency data were then exported from NVivo, resulting in a dataset that contained the number of mentions for each theme and sub-theme. Using Matplotlib, a Python library, the exported frequency data were visualised. A bar chart was created where the count axis represents the number of times each theme was mentioned.

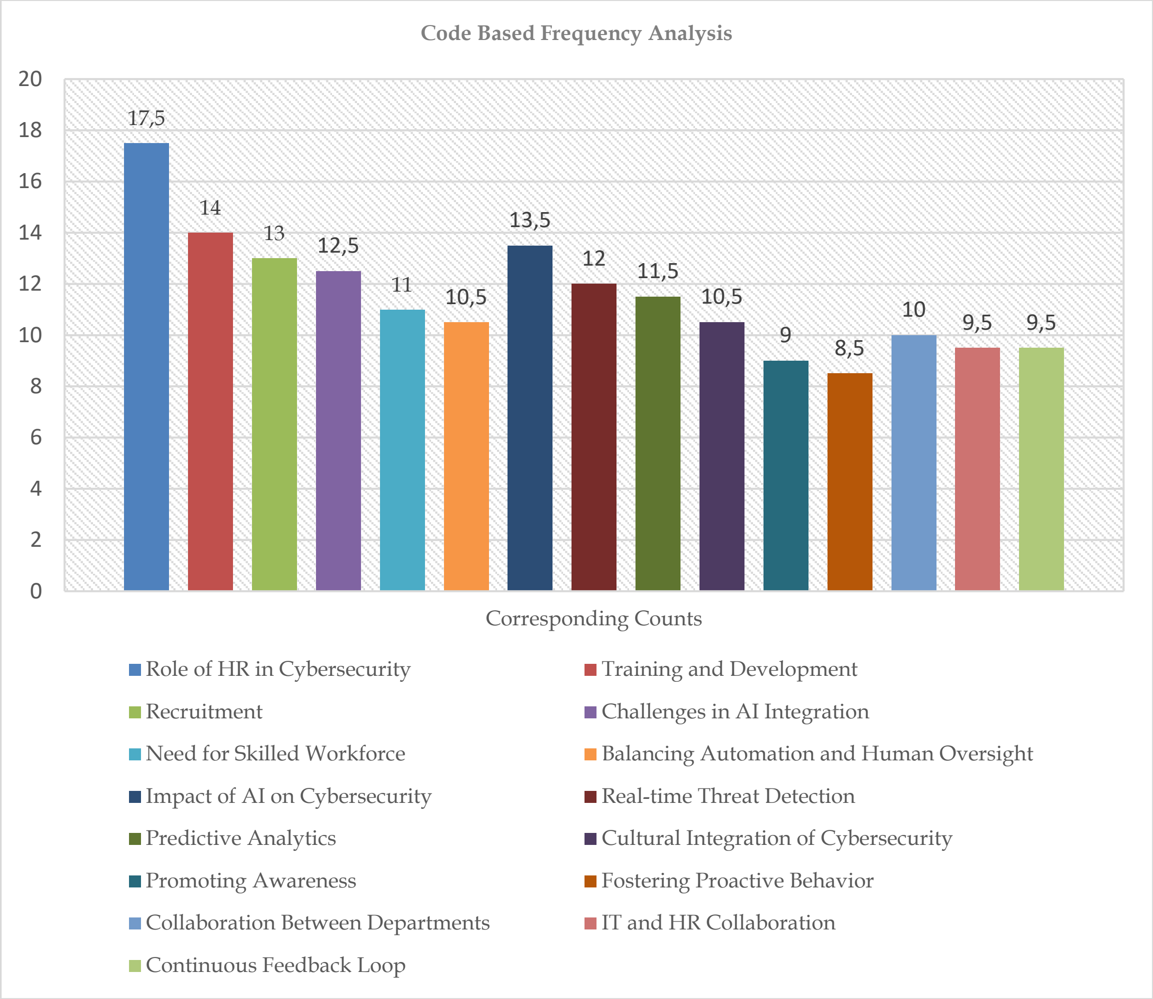

Figure 2: Code-Based Frequency Analysis

After the code-based frequency analysis, a heat map was created to visualise the relationships between various themes and sub-themes identified in the study. The process of creating the heat map involved several steps. Each interview transcript was carefully coded to identify themes and sub-themes. This coding process allowed for the systematic categorisation of data into meaningful segments. NVivo's query tools were used to count the times each theme and sub-theme appeared and to analyse the frequency of co-occurrence between different codes. This means identifying how often two themes or sub-themes were mentioned in the same context. Co-occurrence data were then exported from NVivo, resulting in a dataset that contained the frequency of co-occurrences between different themes and sub-themes. Using Matplotlib, the co-occurrence data were visualised as a heat map. In the heat map, each cell represents the frequency of co-occurrence between two codes, with the colour intensity indicating the strength of their relationship. More intense colours correspond to higher co-occurrence frequencies, while lighter colours indicate lower frequencies, allowing for a clear visual distinction between stronger and weaker code relationships.

As shown in Figure 3, the heat map visually represents the relationships between various themes and sub-themes. For instance, the theme "Challenges in AI Integration" is strongly associated with "Need for Skilled Workforce" (frequency of 9) and "Balancing Automation and Human Oversight" (frequency of 7). Similarly, the theme "Role of HR in Cybersecurity" shows significant relationships with sub-themes such as "Training and Development" (frequency of 10) and "Recruitment" (frequency of 8). The theme "Impact of AI on Cybersecurity" is notably linked with "Real-time Threat Detection" (frequency of 11) and "Predictive Analytics" (frequency of 8).

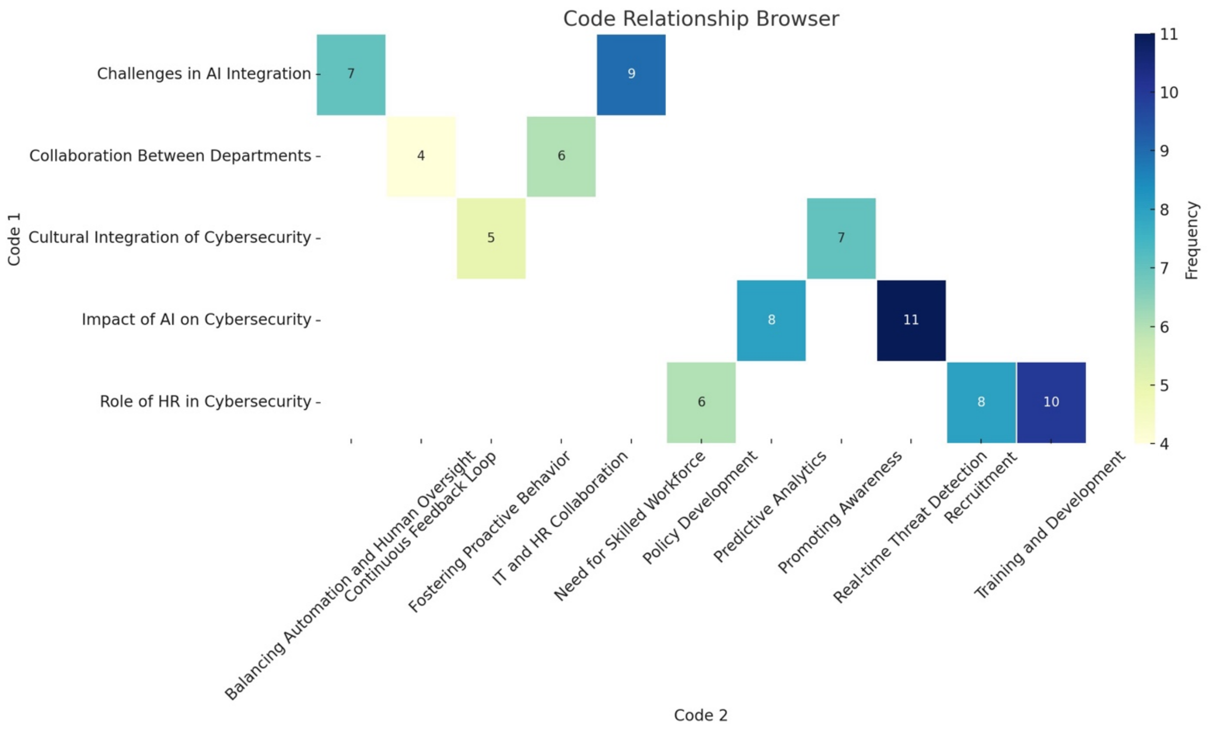

Figure 3: Code Relationship Browser

After analysing the heat map, sentiment analysis was performed on interview answers related to two key issues: the integration of AI in aviation cybersecurity and the contribution of HR in this study. Sentiment analysis measures the sentiment expressed in a data set and generates an emotional tone in the text. Each response was assigned a sentiment polarity (positive, negative, neutral) using sentiment analysis techniques recommended by TextBlob, a Python library that employs natural language processing functions to distil sentiment from text (Loria, 2018). The process began by creating a dataset of interview responses and then performing sentiment analysis on each to generate sentiment scores using the TextBlob sentiment analysis function. These sentiment scores were then classified, and the distribution of sentiments was visualised using Seaborn and Matplotlib. This approach enables a rigorous and quantitative comprehension of participant sentiment toward AI introduction and HR's ability to guide the integration of improved cybersecurity measures (Bird, Klein, & Loper, 2009).

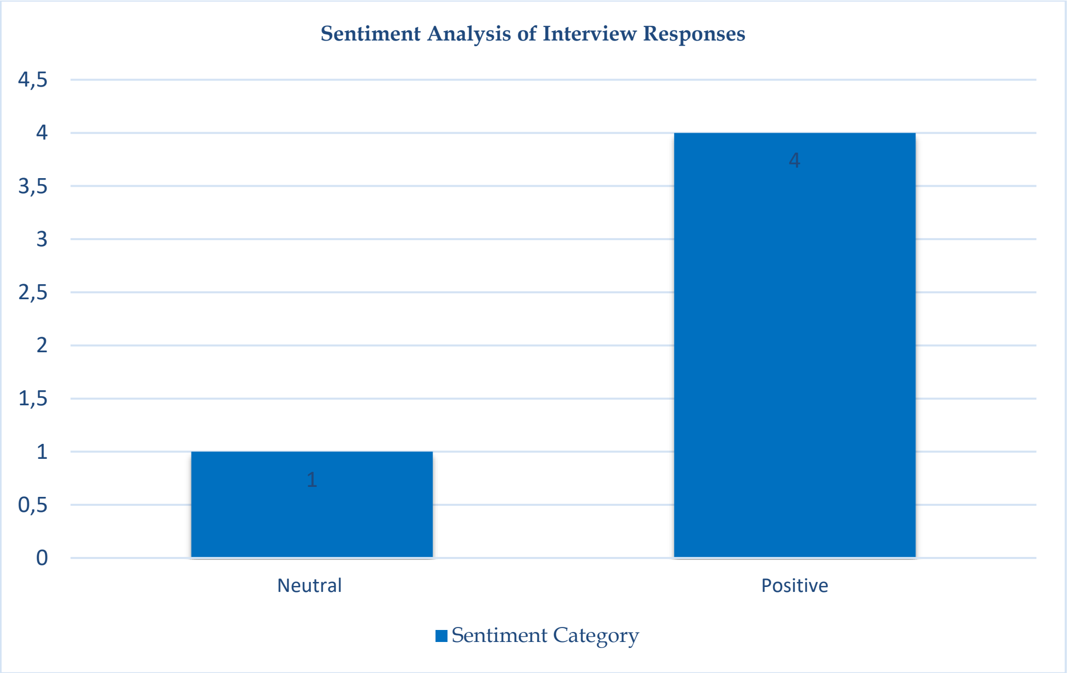

Figure 4: Sentiment Analysis Results

The data analysis in this study underscores the critical role of HR in enhancing cybersecurity within the aviation industry through the strategic integration of AI. The thematic analysis revealed vital themes such as the essential involvement of HR in training, development, and recruitment to bolster cybersecurity measures. It also highlighted the challenges of integrating AI, particularly the need for a skilled workforce and the balance between automation and human oversight. The sentiment analysis indicated a generally positive outlook on AI integration and HR's strategic roles, reflecting optimism about the potential benefits and acknowledging the challenges. The detailed findings of the analysis will be presented in the following part of the study.

Results

This section presents the findings from semi-structured interviews with eight experts in Turkey specialising in aviation, cybersecurity, and human resources. The analysis aimed to uncover critical themes related to the integration of AI in aviation cybersecurity and the strategic role of HR. Data collected from these interviews were analysed using NVivo to identify primary themes and sub-themes, which were then quantified through frequency analysis. The insights obtained provide an understanding of the experts' perspectives on AI integration, the challenges encountered, and the strategic involvement of HR in cybersecurity initiatives.

Thematic analysis

The thematic analysis identified several key themes related to the role of HR in cybersecurity, challenges in AI integration, and the impact of AI on cybersecurity. Each theme was further divided into sub-themes to provide a comprehensive understanding of the issues discussed by the experts. Table 2 summarises the participants' primary themes, sub-themes, and representative quotes.

Table 2: Thematic Analysis Results

Theme	Sub-theme	Participant	Quote
Role of HR in Cybersecurity	Training and Development	Participant 8	"HR plays a crucial role in supporting cybersecurity initiatives by ensuring that our workforce is equipped with the necessary skills and knowledge to protect our systems."
		Participant 8	"HR is responsible for developing and implementing comprehensive training programs that enhance our employees' understanding of cybersecurity principles and best practices."
		Participant 3	"Our HR team conducts regular training sessions on cybersecurity awareness to keep everyone up-to-date with the latest threats and best practices."
	Recruitment	Participant 8	"HR prioritises candidates with strong cybersecurity backgrounds and relevant experience during recruitment."
		Participant 5	"We have updated our recruitment criteria to specifically look for candidates with experience in cybersecurity and AI technologies."
	Policy Development	Participant 8	"HR collaborates closely with our IT and cybersecurity teams to develop policies and procedures that support our overall cybersecurity strategy."
		Participant 6	"By aligning our HR policies with cybersecurity goals, we ensure that all employees understand their role in protecting our systems."
Challenges in AI Integration	Need for Skilled Workforce	Participant 8	"Effective use of AI requires a skilled workforce that can interpret AI outputs and make informed decisions based on those insights."
		Participant 3	"We must continuously train our staff to understand and utilise AI tools effectively."
		Participant 6	"Finding talent with the right combination of AI and cybersecurity skills is a significant challenge."
	Balancing Automation and Human	Participant 8	"While AI can handle many tasks autonomously, human oversight is still essential to interpret AI outputs and address more complex threats."
	Oversight	Participant 4	"AI helps streamline our processes, but we still need skilled professionals to manage and oversee these systems."
		Participant 5	"Maintaining the balance between AI capabilities and human intervention is critical to our cybersecurity strategy."
Impact of AI on Cybersecurity	Real-time Threat Detection	Participant 8	"AI-driven tools can analyse vast amounts of data in real-time, identify patterns and anomalies, and predict potential threats with a high degree of accuracy."
		Participant 3	"Real-time monitoring with AI has significantly reduced our response time to cyber threats."
		Participant 6	"AI's real-time capabilities are a game-changer for our cybersecurity operations."
	Predictive Analytics	Participant 8	"AI-driven tools can provide predictive analytics, helping us anticipate and prepare for potential threats before they materialise."
		Participant 4	"Predictive analytics allow us to foresee and address potential issues proactively."
		Participant 7	"Using AI for predictive analytics helps us stay ahead of emerging threats."
Cultural Integration of Cybersecurity	Promoting Awareness	Participant 1	"We have significantly reduced the risk of successful phishing attacks and other common threats by ensuring that all employees understand the basics of cybersecurity and are vigilant in recognising potential threats."
		Participant 3	"Creating a culture of cybersecurity awareness is essential for the safety of our digital environment."
	Fostering Proactive Behavior	Participant 1	"This decentralised approach has been highly effective in fostering a culture of vigilance and proactive behaviour, as employees are more likely to adhere to cybersecurity protocols when they see their peers leading by example."

		Participant 4	"Encouraging proactive behaviour among employees is crucial for our cybersecurity efforts."
		Participant 7	"A proactive approach to cybersecurity, supported by continuous learning, is vital to our success."
Collaboration Between Departments	IT and HR Collaboration	Participant 2	"By including HR in these discussions, we ensure that our policies and procedures are aligned with our overall cybersecurity goals from the outset."
		Participant 5	"Collaborative efforts between IT and HR have strengthened our cybersecurity policies and practices."
	Continuous Feedback Loop	Participant 2	"Implementing a continuous feedback loop between HR and our cybersecurity team allows us to quickly address any issues or gaps in training and development and ensure that our programs remain relevant and up-to-date."
		Participant 7	"Regular feedback and collaboration between departments are key to maintaining effective cybersecurity measures."

Participants emphasised the importance of HR in providing comprehensive training programs, prioritising candidates with strong cybersecurity backgrounds, and collaborating with IT and cybersecurity teams to develop supportive policies. The need for a skilled workforce and balancing automation with human oversight were key obstacles in AI integration. Additionally, the impact of AI on cybersecurity was discussed, particularly its capabilities in real-time threat detection and predictive analytics. Cultural integration of cybersecurity, promoting awareness, and fostering proactive behaviour were highlighted as essential for building a resilient security posture. Effective collaboration between IT and HR and a continuous feedback loop were crucial for maintaining robust cybersecurity measures.

Frequency analysis

The frequency analysis, visualised in Figure 2, illustrates the number of mentions for each theme and sub-theme. The role of HR in cybersecurity emerged as the most frequent theme, underscoring its critical involvement in training, development, and recruitment to enhance cybersecurity measures. Challenges in AI integration also featured prominently, highlighting the need for a skilled workforce and balancing automation with human oversight. The impact of AI on cybersecurity was noted for its transformative capabilities in real-time threat detection and predictive analytics.

Heat map analysis

The heat map, shown in Figure 3, visualises the relationships between various themes and sub-themes identified in the study. It highlights strong associations, such as the link between "Challenges in AI Integration" and "Need for Skilled Workforce," as well as between "Role of HR in Cybersecurity" and "Training and Development." These relationships indicate that specific themes are frequently discussed together, providing insights into the interconnected nature of these issues.

These conclusions can be drawn as a result of interpreting the heat map:

- The role of HR in cybersecurity is strongly associated with sub-themes such as training and development and recruitment, indicating that these areas are frequently discussed together.

- Challenges in AI Integration show a notable relationship with the Need for Skilled Workforce and Balancing Automation and Human Oversight, highlighting the critical challenges perceived by the participants.

- The impact of AI on cybersecurity is closely linked to real-time threat detection and predictive analytics, which showcase the importance of AI's capabilities in enhancing cybersecurity measures.

- Cultural Integration of Cybersecurity is associated with Promoting Awareness and Fostering Proactive Behavior, emphasising the need for continuous education and proactive engagement.

- Collaboration Between Departments is connected to IT and HR Collaboration and Continuous Feedback Loop, underscoring the significance of interdepartmental cooperation and ongoing communication in maintaining effective cybersecurity measures.

Based on the participants' responses, this diagram helps us understand how AI integration and cybersecurity are interlinked and identifies the areas that must be focused on for efficacious deployment and management.

Sentiment analysis

The sentiment analysis of the interview responses regarding AI integration in aviation cybersecurity and HR roles reveals the following insights:

Positive sentiments:

- "Integrating AI into our processes presents significant challenges." (Sentiment Score: 0.375)
- "Real-time threat detection with AI has greatly improved our security measures." (Sentiment Score: 0.800)
- "Balancing automation and human oversight is essential for effective AI integration." (Sentiment Score: 0.200)
- "Promoting cybersecurity awareness across departments is vital for our success." (Sentiment Score: 0.200)

Neutral Sentiments:

- "HR's involvement in cybersecurity training is crucial for protecting our systems." (Sentiment Score: 0.000)

These results show that cybersecurity professionals are generally optimistic about AI integration and that HR in information security is doing well to support this integration regarding training and awareness initiatives. The results indicate an overall positive perception of potential AI applications to strengthen cybersecurity in aviation.

The findings underscore the critical role of HR in enhancing cybersecurity within the aviation industry through the strategic integration of AI. Key themes included HR's involvement in training, development, and recruitment, challenges in AI integration, and the transformative impact of AI on real-time threat detection and predictive analytics. Promoting cybersecurity awareness, fostering proactive behaviour, and effective collaboration between IT and HR were essential for building a resilient security posture. The sentiment analysis revealed a positive outlook on AI integration and HR's strategic roles. In the discussion part of the study, these findings will be compared with the literature review to provide a comprehensive understanding of how the current research aligns with or diverges from existing knowledge on AI integration and HR's role in aviation cybersecurity.

Discussion

The examination of previous cyberattacks in the aviation field and insights gleaned from interviews provide valuable information on the impact of different countermeasures and the significant role of HR in addressing these challenges. The literature highlights the need to use advanced technologies, notably AI and machine learning, to strengthen cybersecurity. The power of AI to enhance the speed of threat detection and response, which Garcia et al. (2021) discussed, was a recurrent theme in many of our interviews. Participants often referred to AI as revolutionising real-time threat detection. For example, one participant stated, "AI-driven real-time threat detection has helped us in improving our security a lot," reinforcing the strengths of AI found in the literature.

Several studies show that the integration of AI brings both opportunities and challenges. Baron Garcia (2022) explained how machine learning can help process vast security data and recognise patterns and anomalies. One interviewee expressed this idea straightforwardly: "To fully derive the value of AI in diagnostic decision-making, good AI outputs have to be interpretable and placed into the human decision-making process." This is consistent with the findings of Garcia et al. (2021) and Whitworth et al. (2023), who also highlighted the requirement for ongoing training and state-of-the-art intrusion detection systems.

Another critical topic involves the role of HR in building a cybersecurity culture, which appears both in the literature and the interviews. Sabillon and Bermejo (2023) elaborated on the added value of cybersecurity awareness training, specifically in enacting timely detection of threats. As one participant noted, "HR should be part of the training on cybersecurity because they are the gatekeepers to our systems." This view is supported by both the literature and practical insights. They also emphasised the role of HR policies in creating a culture of cybersecurity awareness (Llorens, 2017), aligning with the widely shared view that "Creating a culture of cybersecurity awareness is fundamental to ensuring our digital spaces are safe."

By comparing the challenges identified in the literature with those pinpointed during the interviews, a comprehensive selection of challenges related to AI-based cybersecurity solutions can be identified.

According to Duchamp et al. (2016), strategic policies, such as air-gapping critical systems and conducting routine cybersecurity audits, are necessary to address the problem. Interview insights echoed this sentiment, underscoring the importance of balancing automated processes with time and cost-saving measures. One interviewee said, "Striking the right balance between automation and human oversight is paramount to effective AI implementation." This aligns with Scott's (2019) assertion that strict cybersecurity frameworks are essential and should be complemented by timely feedback mechanisms.

This analysis also underscores the need for cross-departmental collaboration, as supported by the literature and the interviews. Roadmap (2020) took a human-centric point of view, focusing on AI aligned with human capacities. Respondents emphasised that IT and HR need to partner closely. A key message from one participant was, "Tighter IT-HR collaboration contributes to stronger security policies and controls," which speaks to the value of having cross-functional teams closely aligned.

Furthermore, the literature indicates that the best approaches to cybersecurity threats include robust backup solutions and regular security assessments to prevent ransomware and data leaks (Kazim, 2023; Bitsight, 2020). Interview responses underlined the importance of solid data protection practices and ongoing cybersecurity awareness training to combat phishing and other threats.

In summary, the comparison between the literature and interview findings reveals a strong alignment in the importance of AI and HR within the cybersecurity environment of the aviation industry. Both sources stress the importance of consistent training, new technology solutions, and an all-hands approach to address changing cyber threats. Integrating insights from the literature and practical experience in aviation enables a comprehensive understanding of cybersecurity challenges and opportunities, informing effective and sustainable security practices. This research contributes to the existing body of knowledge by providing a synthesised model that integrates AI technologies with HR strategies and cybersecurity practices, offering a holistic approach to addressing cybersecurity in the aviation industry.

Future research should expand the findings of this study by incorporating larger sample sizes and quantitative methods to validate and generalise results, conducting longitudinal studies to assess the long-term impact of AI integration on cybersecurity, and performing cross-industry comparisons to identify unique challenges and best practices. Detailed case studies of successful AI and HR integration in cybersecurity, exploring specific HR interventions that foster a cybersecurity-aware culture, and addressing ethical and legal considerations are also crucial. Additionally, ongoing research should focus on the latest technological advancements in AI and their implications for enhancing cybersecurity practices.

Implications

A thematic analysis of the interview data, combined with a literature review, revealed critical insights into the strategic role of HR in AI integration within aviation cybersecurity. While specifics may vary, several recurring themes highlight vital areas needing attention. Notably, the role of HR in cybersecurity emerges as central, particularly in training, development, and recruitment. This underscores the importance of HR's involvement in cybersecurity initiatives, ensuring that employees are well-trained on emerging threats and equipped with the skills to protect themselves effectively. Continuous training programs will help employees tackle cyber threats with more tremendous success. Additionally, the availability of AI-focused cybersecurity expertise is crucial. Recruitment efforts must go beyond simply refining strategies; they must actively seek talent capable of managing increasingly sophisticated AI-driven cybersecurity systems.

Innovative HR practices

- Gamified Training Programs

The practical training programs in cybersecurity could be gamified, which will maintain interest/engagement and enhance learning outcomes. They would be based on the principles of point scoring, leaderboards, and rewards, offering a more game-like training experience. These employees could participate in realistic and controlled simulations of cyberattack scenarios, rehearsing how to respond to a security threat before it happens.

- Cybersecurity Boot Camps

One possible approach could be intensive cybersecurity boot camps targeted at new hires and existing employees. Military-style boot camps would provide immersive, hands-on training in the latest cybersecurity tools, techniques, and AI applications needed to secure information and computers in the most critical industries and settings. Skills-based boot camps could be structured into various tiers based on an employee's ability level, providing everyone from beginners to advanced practitioners with the necessary training.

- AI-Powered Recruitment Platforms

Monster or other AI-driven recruitment platforms could be used to find and recruit the best cybersecurity professionals. These platforms use predictive analytics to analyse profiles of people who are candidates, then match them to hopefully best-suited roles based on existing skills and experience. This could be achieved by using AI technology to streamline the recruitment process and help the candidates better match their requirements for the job.

- Cybersecurity Talent Pipeline-related Programs

Developing cybersecurity talent pipeline programs in partnership with universities and technical institutes could include scholarships leading to cyber and AI co-op positions for students and opportunities for internships and hands-on experience. These programs would create a pipeline of cybersecurity-proficient talent for the future so that suitable candidates would continue to be available for consideration.

- Continuous Learning Platforms

In the future, continuous learning platforms based on AI could offer suggestions for training that match staff member's current skills and career goals. These platforms would keep a check on their growth, recommend ideal courses, and provide micro-learning modules to lower employees who lack knowledge of the changing dynamics of the cybersecurity arena.

AI integration challenges Security: one of the ever-present challenges of using AI in cybersecurity is the constant need to have a highly skilled workforce across the board and not allow automation to overshadow human cognition. In fixtures, participants must know the skills and knowledge that employers will fill through strategic training programs. Another critical aspect is the balance between making AI systems automated and having them controlled by humans to ensure that their functionality does not result in new vulnerabilities coming in. New generation tools should be more like frameworks of expert knowledge and technology to assist AI rather than trying to duplicate expert decision making. Instead, they expose relevant information interfaces between expert AI and AI decision support.

- Cultivating Cybersecurity Together

Users are an excellent first line of defence when setting up a cybersecurity-aware culture at an organisation. Human Resources have one of the most critical roles in driving increased cyber awareness and proactive behaviour among employees. With repetitive behaviours aimed at prevention, defences, and safety, companies would start embracing vigilance and realisation. Cybersecurity must be a part of the business culture, and the onus of incorporating cybersecurity principles in the company's service offerings lies at the doorstep of each level of authority.

- Cybersecurity Ambassadors Program

One possibility might be establishing a cybersecurity ambassadors' program that consists of a team of employees with higher-level awareness training and serving as cybersecurity role models within their departments. These ambassadors would set the standard, offer the best practices, and act as peers to one other, helping to strengthen a culture of cyber-awareness at the organisation.

- Monthly Challenge – Cyber Security

An engaging way to teach employees is to introduce monthly cybersecurity challenges where employees can test their knowledge - and understand basic things like never downloading files from unfamiliar sources. The challenges involved subjects from spotting phishing emails to securing personal devices to data privacy regulations. Workers could receive recognition and rewards for participating and succeeding in the challenge.

Interdepartmental collaboration

The best practice is to work together with IT, HR and cybersecurity. Regular, often daily, communications and standard processes among these teams are instrumental in ensuring that policies and practices are in sync and up to date. Once these capabilities are realised, the institutions should operate with constant feedback loops on training and development to detect and correct gaps quickly and keep their cybersecurity programs on course and practical. This would eventually shape the landscape into a more robust cyber environment based on a familiar, department-to-department, collaborative spirit pursuing shared cybersecurity objectives.

Task forces of IT, HR, and cybersecurity teams could be developed with cross-functional groups that come together to address specific challenges or initiatives. For example, CIFAR will convene new task forces to funnel more detailed expertise from each department into specific goals, which would be identified by the proposed Working Group, and meeting at regular intervals to share intel, harmonise tactics, and then develop cross-departmental approaches, which would build on the strengths of each.

Periodic interdepartmental workshops on critical topics of cyber security can be arranged. Workshops fostering collaboration and sharing best practices and knowledge can be organised. Integration of the different views leads to more comprehensive and robust cybersecurity strategies.

Conclusion

One of the critical gaps in the existing literature is understanding how AI is being integrated with aviation cybersecurity and how HR is strategically important in cybersecurity in aviation. This study fills this gap by identifying several key themes, including HR's role in cybersecurity, challenges in AI integration, the influence of AI on cybersecurity, and the importance of interdepartmental collaboration for cultural integration. Sentiment analysis results show an overall positive outlook on AI integration and HR's current strategic roles, with a mix of optimism about potential benefits and recognition of the challenges involved.

The findings support the necessity for ongoing education, targeted hiring, and resilient cybersecurity infrastructure. HR departments play a crucial role in the success of cybersecurity efforts by facilitating practices that equip employees with the necessary skills and knowledge to protect organisational servers and systems. Although the development of predictive analytics is still progressing, the study demonstrates how AI can be transformative in real-time threat detection, significantly enhancing cybersecurity. Additionally, HR needs to foster a culture of security mindfulness, promoting proactive behaviour and emphasising security resilience. This collaboration between IT and HR is essential, particularly in developing continuous feedback loops, to ensure effective and adaptive cybersecurity measures.

The study's findings support several hypotheses. Firstly, the hypothesis that HR integration significantly enhances the effectiveness of AI-driven cybersecurity measures in the aviation industry is supported. The findings indicate that HR practices, such as strategic training and recruitment, are crucial for successfully integrating AI into cybersecurity. Secondly, the hypothesis that strategic HR practices, including targeted training and development, are crucial for improving cybersecurity readiness and resilience is also supported. The study shows that ongoing education and targeted hiring significantly contribute to cybersecurity readiness and resilience. Thirdly, the hypothesis that organisations face significant challenges in aligning HR policies with the rapid pace of technological advancements in cybersecurity is validated. The results highlight the difficulties in aligning HR policies with technological advancements, particularly in maintaining a skilled workforce and balancing automation with human oversight. Lastly, the hypothesis is supported by the fact that comprehensive HR-led initiatives can foster a culture of cybersecurity awareness and readiness within the aviation sector. The study highlights that HR-led initiatives, including ongoing training and encouraging proactive behaviour, are crucial for cultivating a culture of cybersecurity awareness and preparedness.

The study's results are consistent with several HRM. According to RBV, HR practices like training and strategic recruitment are vital resources that can provide a competitive advantage (Harvey & Turnbull, 2020). Gillam (2019) concluded that Human Capital Theory emphasises investing in employee education and training to enhance organisational performance. Contingency Theory suggests tailoring HR practices to specific problems, resonating with the need to balance automation and human oversight. Systems Theory underscores the importance of interdependent departmental collaboration, supporting the study's emphasis on IT and HR collaboration (Henning, 2015). Organisational Learning Theory highlights the need for ongoing training and routine security assessments to keep pace with evolving threats (Jung & Takeuchi, 2010). SHRM principles align HR practices with organisational objectives, creating a culture that effectively supports cybersecurity (Harvey & Turnbull, 2020).

This research marks an essential step towards addressing the existing gaps in the literature by combining AI technologies with HR strategies and cybersecurity practices in the aviation industry. While past studies have focused on individual factors, this paper consolidates these elements, presenting a comprehensive model delineating their interconnected nature and a conceptual reference architecture for cybersecurity in aviation.

However, the study has some limitations. The small sample size may limit the generalizability of the results, and the reliance on qualitative data could be strengthened by incorporating more quantitative analyses. Additionally, the focus on the aviation sector means findings may not be widely generalisable without further contextual analysis. Future research should expand the sample size and include quantitative methods to support qualitative findings. Longitudinal studies should evaluate the long-term effects of AI integration on cybersecurity efforts. Further research is needed to investigate HR interventions that promote a cybersecurity-aware culture across various organisations. Exploring integrated frameworks of AI/HR strategic practices across industries could yield broader perspectives and increase the generalizability of the research.

Peer-review:

Externally peer-reviewed

Conflict of interests:

The author has no conflict of interest to declare.

Grant Support:

The author declared that this study has received no financial support.

Ethics Committee Approval:

Ethics committee approval was received for this study from Beykoz University, Ethics Committee on 06/06/2024 and E-45152895-299-2400008121 document number.

References

ACI World. (2023). Ways to reduce DDoS attacks on airports. ACI World Insights. Retrieved from https://blog.aci.aero/cybersecurity/ways-to-reduce-ddos-attacks-on-airports/

Atlantic Council. (2020). Aviation cybersecurity: Scoping the challenge. Retrieved from Atlantic Council https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-scoping-the-challenge-report/.

Baron Garcia, A. (2022). Machine Learning and Artificial Intelligence Methods for Cybersecurity Data within the Aviation Ecosystem.

Bird, S., Klein, E., & Loper, E. (2009). Natural language processing with Python: analysing text with the natural language toolkit. " O'Reilly Media, Inc.".

Bitsight. (2020). New Study Reveals Cybersecurity Risks in the World's Largest Airports. Retrieved from https://www.bitsight.com/blog/new-study-reveals-cybersecurity-risks-in-the-worlds-largest-airports.

CM Alliance. (2023). Recent Cyber Attacks 2023: 5 major data breaches & ransomware attacks. Retrieved from https://www.cm-alliance.com/cybersecurity-blog/may-2023-recent-cyber-attacks-data-breaches-ransomware-attacks

Duchamp, H., Bayram, I., & Korhani, R. (2016, June). Cyber-Security, a new challenge for the aviation and automotive industries. In Seminar in information systems: applied cybersecurity strategy for managers (pp. 1-4).

Garcia, A. B., Babiceanu, R. F., & Seker, R. (2021, April). Artificial intelligence and machine learning approaches for aviation cybersecurity: An overview. In 2021 Integrated Communications Navigation and Surveillance Conference (ICNS) (pp. 1-8). IEEE.

Gillam, A. R. (2019). Cyber security and human resource development implications for the enterprise. Cyber Security: A Peer-Reviewed Journal, 3(1), 73-92.

Harvey, G., & Turnbull, P. (2020). Ricardo flies Ryanair: Strategic human resource management and competitive advantage in a Single European Aviation Market. Human Resource Management Journal, 30(4), 553-565.

Henning, S. (2015). The wellness of airline cabin attendants: A systems theory perspective. African Journal of Hospitality, Tourism and Leisure, 4(1), 419-430.

InformationWeek. (2023). Understanding DDoS Attacks on US Airport Websites and Escalating Threats. Retrieved from InformationWeek

Jung, Y., & Takeuchi, N. (2010). Performance implications for the relationships among top management leadership, organisational culture, and appraisal practice: Testing two theory-based models of organisational learning theory in Japan. The International Journal of Human Resource Management, 21(11), 1931-1950.

Kankaew, K., & Pongsapak, T. (2020, October). Contingency theory: the analysis in air transportation before, during, and after the pandemic in Thailand. In IOP Conference Series: Materials Science and Engineering (Vol. 918, p. 012047). IOP Publishing.

Kazim, J. (2023). Aviation Cybersecurity: Risks and Mitigations. National Business Aviation Association. Retrieved from https://nbaa.org/news/business-aviation-insider/2023-07/aviation-cybersecurity-risks-and-mitigations/

Kumar, M. (2022). Optimised application of artificial intelligence (AI) in aviation market. International Journal of Recent Research Aspects, 9(4).

Llorens, J. J. (2017). The Role of Human Resource Management in Cybersecurity. In Public Personnel Management (pp. 192-199). Routledge.

Manoharan, P. (2024). A Review on Cybersecurity in HR Systems: Protecting Employee Data in the Age of AI. Regulation (GDPR), 4(5).

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Research Journal of Business and Management, 10(3), 98-108.

Resecurity. (2023). The Aviation and Aerospace Sectors Face Skyrocketing Cyber Threats. Retrieved from Resecurity. https://www.resecurity.com/blog/article/the-aviation-and-aerospace-sectors-face-skyrocketing-cyber-threats

Roadmap, A. I. (2020). A human-centric approach to AI in aviation. European Aviation Safety Agency, 1.

Sabillon, R., & Bermejo Higuera, J. R. (2023, July). The importance of cybersecurity awareness training in the aviation industry for early detection of Cyberthreats and vulnerabilities. In International Conference on Human-Computer Interaction (pp. 461-479). Cham: Springer Nature Switzerland.

Scott, B. I. (2019). Aviation Cybersecurity: Regulatory Approach in the European Union. Aviation Cybersecurity, 1-266.

Whitworth, H., Al-Rubaye, S., Tsourdos, A., & Jiggins, J. (2023). 5G Aviation Networks Using Novel AI Approach for DDoS Detection. IEEE Access.

Appendix

Appendix 1: Interview Questions Table

Interview Question	Reason for Asking	References
Can you describe your current role and responsibilities in relation to cybersecurity and HR management within the aviation sector?	To establish the context and relevance of each expert's experience.	Llorens (2017)
How has your experience shaped your views on the integration of AI in aviation cybersecurity?	To explore the experts' perspectives on AI integration, including benefits and challenges.	Garcia et al. (2021)
In your opinion, what are the critical cybersecurity threats facing the aviation industry today?	To identify prevalent threats and vulnerabilities in the aviation sector.	Kumar (2022)
How do you see AI-driven automation impacting the cybersecurity landscape in aviation?	To understand the impact of AI-driven automation on the cybersecurity landscape.	Garcia et al. (2021)
What role does HR play in supporting cybersecurity initiatives within your organisation?	To assess the strategic involvement of HR in cybersecurity.	Sabillon and Bermejo (2023)
Can you provide examples of how HR has successfully contributed to mitigating cybersecurity risks?	To gather specific examples of HR's contributions to cybersecurity risk mitigation.	Sabillon and Bermejo (2023)
What are the main challenges you face when integrating AI-driven tools in cybersecurity measures?	To understand the practical challenges of integrating AI-driven tools in cybersecurity.	Duchamp et al. (2016)
How does HR address these challenges, particularly in training and development?	To explore HR's role in addressing challenges related to AI integration, focusing on training and development.	Gillam (2019)
What strategies have proven effective in aligning HR policies with AI-driven cybersecurity enhancements?	To identify effective strategies for aligning HR policies with AI-driven cybersecurity enhancements.	Duchamp et al. (2016)
What future trends do you anticipate in the intersection of HR, AI, and cybersecurity within the aviation sector?	To gain insights into future directions and trends at the intersection of HR, AI, and cybersecurity.	Whitworth et al. (2023)
How should HR professionals prepare to meet the evolving demands of cybersecurity in the coming years?	To provide recommendations for HR professionals on how to prepare for evolving cybersecurity demands.	Whitworth et al. (2023)
Based on your experience, what advice would you give to HR professionals looking to enhance their organisation's cybersecurity through AI?	To elicit actionable insights and recommendations for HR professionals.	Practical approaches discussed in the literature
Are there any best practices or lessons learned that you can share regarding the integration of AI in cybersecurity efforts?	To gather best practices and lessons learned from the experts regarding AI integration in cybersecurity.	Practical approaches discussed in the literature