THE NATURE OF THE RISK: PERCEPTIONS ACROSS G7 COUNTRIES REGARDING RISKS FROM INFORMATION TECHNOLOGY VERSUS THOSE ARISING FROM CLIMATE CHANGE, 2022-2025

David C. Wyld

Department of Management, Southeastern Louisiana University, Hammond, LA, USA

ABSTRACT

Today, the world is facing a world of risks. No matter the country, the riskiest elements are perceived to emanate from the realms of information technology and climate change. In this article, we look at how the nature of today's risks are perceived across the G7 Nations - Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States – and how this can – and is – impacting strategic management decision-making. We begin with a look at how we individually and collectively process risk, and specifically, risks that are spurred both by information technology, specifically from cyberattacks and artificial intelligence, and by climate change in general and specifically, as it relates to extreme weather and forest fires and the destruction of natural habitats. Then, using a database constructed from the four years of existence of the Munich Security Index, we examine how the perception of both IT-related and climate-driven risks has elevated between 2022-2025 in the G7 countries, but with important intercountry differences and discrepancies between IT-related risks and those coming from "Mother Nature." The results of this analysis and then discussed, along with directions for future research in this area and the implications of all of this for strategic management. .

TBD - This article gives complete guidelines for authors submitting articles for the AIRCC Journals. 150 word limit on Abstract.

KEYWORDS

Strategic Management, Business Strategy, Information Technology, Climate Change, Value Chain Management, Supply Chain Management, Risk, Change

1. INTRODUCTION

Risk. It is something that is just part of life. And yes, life today has *plenty* of risks. Today, two of the most "loud" threats are the risks emanating from information technology and climate change. The contemporary focus on these two specific risk areas stems from an intricate interplay of psychological, sociological, and communicative factors. As society confronts the issues posed by rapid technological advancements and the impending effects of climate change, public engagement and awareness become crucial dimensions that shape how risks are understood and addressed, and ultimately, how these risk perceptions play into the decisions we make as individuals – and collectively, in corporate management.

Starting with climate change, the urgency of this issue has galvanized attention due to perceived existential threats posed to future generations. The framing of climate change as a moral and

ethical dilemma elevates the salience of this risk in public discourse, driving a fear of disenfranchising the future [1]. Studies indicate that when citizens engage with information about climate risks, they often encounter an array of narratives that can lead to divergent perceptions. Some may underestimate risks due to a lack of comprehensible communication, while others may experience overestimation, influenced by sensationalized media portrayals [2]. The challenge of effectively communicating risks requires an understanding of how these perceptions are formed and evolve, attributing significant importance to the influential roles of trust in researchers and the context of information dissemination [3] [4].

Regarding information technology, the rapid advancement of digital platforms and artificial intelligence has generated significant public discourse around associated risks, such as privacy concerns, cybersecurity threats, and threatsarising from the rapid and stunning growth of artificial intelligence (AI). The advent of technologies like ChatGPT unveils complex cognitive responses where individuals often evaluate risks based on personal relevance and previous experiences [5]. Furthermore, the management of information technology risks within organizations underscores an ongoing struggle to mitigate potential hazards that could endanger companies and societal integrity [6]. The public often amalgamates perceptions of risks from varied technology sources, including social media, which can lead to heightened anxieties based solely on the prevalent narratives propagated therein [7].

Public perception plays a pivotal role in both domains. Effective risk governance necessitates the inclusion of public sentiment and apprehension regarding both climate and technological risks, as these perceptions influence not only individual behaviors but also community and governmental responses. For instance, insights demonstrate that when individuals possess a higher level of trust in the mechanisms that govern these technologies or policies, there is a resultant decrease in perceived vulnerability, thereby enabling more engaged societal participation [3]. This interplay indicates a reciprocal relationship between risk perception and communal trust where increased transparency and effective communications can alleviate fears at scale.

Moreover, the phenomenon of amplification in risk communication suggests that perceptions can be disseminated remarkably quickly through network effects, influencing broader societal sentiments [4]. Thus, addressing these perceived risks requires deliberate and calibrated communication strategies that reduce misinformation and promote informed discussions.

In brief, the heightened focus on risks from information technology and climate change is driven by a complex web of public perceptions, influenced by ethical considerations, communication failures, and trust in governing bodies. By understanding these dynamics, there exists potential for more effective engagement strategies that not only address the risks but also align public concerns with actionable solutions.

1.1. Threats from Information Technology-Related Sources

As the digitization of societal functions deepens, concerns surrounding threats from information technology, particularly in the form of cyberattacks and the influence of artificial intelligence, have escalated significantly. Cybersecurity has emerged as a paramount concern across various sectors, including healthcare, finance, and supply chains. Both cyberattacks and AI pose unique challenges that necessitate robust countermeasures, heightened awareness, and strategic innovation.

1.1.1. Cyber Threats

Cyberattacks are increasingly sophisticated, evolving from mere nuisances to major threats that can compromise organizational integrity and even national security. Indeed, there are multifaceted roles within cybersecurity frameworks that underscore the need for a comprehensive approach to counteracting these threats, emphasizing roles like security provision, operation and maintenance, and analysis [8]. The increasing prevalence and complexity of these attacks have engendered a toxic mix of technical vulnerabilities and human factors that contribute to security breaches. For instance, attacks can stem from a variety of actors, including individual hackers and state-sponsored groups, each with diverse motives, ranging from financial gain to espionage [9].
The proliferation of artificial intelligence in cybersecurity presents both immense opportunities and challenges. AI systems have been integrated into various aspects of threat detection and response strategies, which greatly enhances the ability to recognize and neutralize threats before they can cause substantial harm [10]. Moreover, advancements in machine learning (ML) are facilitating real-time threat detection, allowing organizations to pivot quickly in response to evolving cyber challenges [11]. Nonetheless, the same technologies that enhance security can also be exploited by malicious actors to conduct sophisticated cyberattacks [12].

1.1.2. The Double-Edged Sword of Artificial Intelligence

AI serves as a critical tool for enhancing cybersecurity measures, but its capabilities can also be misused for malicious purposes. For example, AI technologies can analyze vast datasets to identify patterns indicative of potential cyber threats that might remain hidden from human analysts [13]. A comprehensive understanding of the implications of AI in cybersecurity is necessary for organizations to harness its benefits while mitigating the associated risks. One must always bear in mind the dual-use nature of AI; while it improves defense mechanisms and incident response, it also requires robust governance strategies to prevent misuse [9].

Integrating AI with established cybersecurity frameworks enhances overall resilience against cyber threats. Research has shown that the convergence of these technologies, powered by AI, leads to transformative improvements in threat management and incident response [13]. This synergistic approach ensures that organizations can adapt to the dynamic nature of modern cyber threats, highlighting the necessity for innovative and forward-thinking cybersecurity strategies.

1.1.3. Resilience in the Cyber Landscape

In addressing cybersecurity, a focus on resilience has become increasingly critical. Resilience not only involves the capacity to protect information systems against attacks but also the ability to recover swiftly from incidents. The evolving landscape of cybersecurity today necessitates a shift from reactive to proactive strategies [11]. Organizations must embrace continuous learning and adaptive approaches that allow them to anticipate potential threats before they materialize.
Particularly within supply chains, the integration of digital technologies expands vulnerabilities to cyber threats that can significantly disrupt operational integrity. As supply chains today increasingly converge with digital platforms, the risks from cyber threats escalate, thus underlining the need for strategic cybersecurity measures [14]. Prior researchin this area has highlighted the importance of constant vigilance and adaptability, ensuring that organizations not only defend against current threats but also anticipate future challenges and adapt accordingly [15].

1.1.4. The Role of Governance and Human Factors

Implementing robust cybersecurity practices requires not only technological advancements but also sound governance structures and a culture of security awareness. Organizations must cultivate a security-conscious workforce, as human errors continue to be a leading cause of data breaches. The importance of cybersecurity training is also underscored as an essential best practice today, as organizations with enhanced awareness programs have consistently shown significant improvements on the cybersecurity front [16]. Additionally, governance structures must be built on recognized standards to ensure alignment between IT capabilities and organizational objectives to provide the best possible cyberdefense for organizations [17].

1.1.5. Summary on Cybersecurity Threats

As cybersecurity challenges continue to evolve, the interplay of AI and increasing cyber threats presents both opportunities and challenges for all. Organizations must adopt holistic strategies that encompass advanced technologies, effective governance, and a culture of security to enhance their protective measures. By understanding the complex dynamics of cybersecurity and adapting to emerging threats, entities can fortify their defenses in an increasingly digital world.

1.2. Threats from Natural Sources (Relating to Climate Change)

As climate change continues to escalate, it poses significant threats that affect ecosystems, human health, and economic stability globally. These threats manifest primarily through the increasing severity and frequency of natural disasters, impacts on biodiversity, and alterations in agricultural productivity. The intensity of these changes calls for urgent recognition and action across multiple sectors.

1.2.1. Climate Change as a Driver of the Threat Environment

The amplified frequency of extreme weather events is one of the most concerning consequences of climate change, profoundly affecting both the natural environment and human societies. Climate change acts as a macro-driver behind various threats by exerting pressure on institutional capacities and diminishing the availability of essential natural resources [18]. This pressure intensifies the probability of disasters such as floods, droughts, and hurricanes, which have been linked with climate variability and change, and the intensification of climate change renders communities vulnerable to natural disasters, ultimately leading to societal upheaval [19].

1.2.2. The Impact of Climate-Driven Threats

Human health is deeply intertwined with the effects of climate change, particularly through the exacerbation of pre-existing conditions and the emergence of new health threats. Extreme weather events, changes in infectious disease patterns, and food security issues have been consistently shown to have severe repercussions for population health [20]. The health risks associated with climate change are often compounded by socio-economic factors, whereby vulnerable populations face disproportionately higher risks due to limited resources for adaptation [21]. Furthermore, increasing awareness regarding the adverse impacts of climate change on health is essential for promoting urgent public health interventions [22].

The implications of climate change extend beyond environmental and health concerns to encompass broader socio-economic stability and security. Today, there can be no doubt that climate change contributes to instability and may exacerbate conflicts over dwindling resources such as water and arable land [18]. Water scarcity, in particular, is a critical concern as changing

precipitation patterns threaten access to clean water, necessary for both human consumption and agricultural activities [23]. Understanding these cascading effects is crucial for developing effective climate adaptation and mitigation strategies.

As communities assess the perceived risks of climate change, it becomes evident that both individual and collective actions are necessary to combat its effects. Psychological distance plays a role in shaping responses, as local experiences often motivate action more than distant effects [24]. By fostering awareness and encouraging community-centric adaptive strategies, initiatives can better incorporate localized knowledge into addressing climate challenges related to natural disasters, agricultural shifts, and biodiversity protection [25].

Furthermore, the role of insurance and risk management in adapting to these threats must be emphasized. Indeed, many have recognized that climate change necessitates a reevaluation of risk frameworks and insurance models due to the increasing unpredictability of natural disasters [26]. Building resilience within communities and empowering local governance structures becomes essential in mitigating the socio-economic fallout of climate change.

1.2.3. Summary on Climate-Driven Threats

In brief, the threats posed by climate change today present multifaceted challenges that necessitate concentrated efforts across various sectors. From enhancing agricultural resilience to protecting biodiversity and promoting public health, it is vital to acknowledge climate change as a profound security threat that underscores the interconnectedness of environmental, economic, and social systems. Activating adaptive strategies and fostering resilience at local levels while addressing broader systemic issues will be crucial in constructing pathways toward sustainability amid these pervasive threats.

1.3. Overview of This Study

The present research examines the interplay between individual risk perceptions, specifically those relating to the risks associated with threats emanating from information technology and climate change, and strategic management. The study is unique in that it looks transnationally across the G7 countries - Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, making use of a database constructed from the results of surveys conducted for the Munich Security Conference to produce the Munich Security Index (MSI) over the most recent four-year period (2022-2025). The study begins with an extensive review of the related literature, examining the impact of risk perceptions on both personal and corporate decision-making, along with a look specifically at the areas of risks associated with IT risks (specifically those risks emanating from cyberattacks and AI) and climate change (climate change generally, and more specifically, extreme weather and forest fires, along with the destruction of natural habitats, coming as a result of climate change). Examining these five specific areas of IT and climate change risks, both within and between the G7 nations, enables us to gain insights into how risks from information technology-related sources and those arising as an outgrowth of climate change predominate much of our thinking today in the Western World. The article concludes with a discussion of the implications of all of this for strategic management and directions for future research.

2. REVIEW OF THE LITERATURE

In looking at how risk regarding threats from various sources is processed, we will begin with an overview of how we process risks in our minds. Then, we will look at how we look at risks from

the two areas under specific focus in the present research – risks emanating from information technology and from natural sources, specifically those relating to climate change. Finally, we bring this review full circle, examining how our personal perceptions of risk impactupon decision-making in the corporate realm and ultimately, company strategy and performance.

2.1. Personal Perceptions of Risk

The nature of personal perceptions of risk is a complex and multifaceted construct influenced by a variety of psychological, cultural, and situational factors. At its core, risk perception refers to individuals' subjective judgments about the likelihood and severity of negative events arising from specific actions or situations. This subjective evaluation significantly shapes individual and collective behaviors, particularly in contexts such as health, entrepreneurship, and environmental concerns.

Research has shown that personal risk perception is often closely intertwined with psychological factors such as anxiety, emotional response, and cognitive biases. For instance, we all lived through seeing how the heightened fear during the COVID-19 pandemic affected individuals' risk perceptions, contributing to increased emotional distress[27]. Similarly, prior research has shown that risk perceptions can mobilize protective behaviors, indicating that anxiety and perceived vulnerability can lead to proactive measures, such as increased adherence to health recommendations [28]. Thus, emotional and cognitive components play pivotal roles in how risks are assessed and acted upon.

Cultural dimensions further complicate the landscape of risk perception. Research by has demonstrated that cultural attitudes, such as collectivism and uncertainty avoidance, shape how various populations perceive environmental risks, with older individuals often displaying heightened concern for health-related risks compared to younger counterparts[29]. The role of media and cultural narratives also cannot be understated, as they contribute to shaping public perception and societal norms regarding risk, especially in health crises like HIV/AIDS [30]. These cultural factors influence not only individual risk perception but also community responses to risks, necessitating effective risk communication strategies tailored to cultural contexts [31].
Moreover, personal risk perception varies significantly across different domains, as evidenced in studies related to health (e.g., stroke risk) [32], entrepreneurship [33] [AA], and technology (e.g., cell phone radiation) [34]. The understanding of risks in these domains is not solely based on objective assessments but is affected by socio-economic status, previous experiences, and psychological factors, reinforcing the notion that risk perception is a subjective construct [35] [36].

Finally, emerging evidence indicates that risk perception can evolve over time and is susceptible to change through social interventions and education [37]. For instance, discussions about perceived risks can enhance knowledge, thereby improving individuals' ability to make informed decisions concerning their health and safety. This dynamic nature of risk perception underscores the importance of continuous research and tailored strategies in public health and risk management initiatives.

In brief, personal perceptions of risk are fundamentally shaped by a combination of emotional, cognitive, cultural, and situational factors. Understanding this complex interplay is crucial for developing effective interventions and communication strategies aimed at enhancing public awareness and safety in the face of various risks.

2.2. Perceptions of Risks from Information Technology

Perceptions of risks associated with information technology (IT) are shaped by various factors, including individual experiences, cognitive biases, emotional responses, and the information disseminated through multiple channels. Understanding how individuals perceive these risks is crucial for stakeholders in technology development and implementation, as perception significantly influences acceptance, usage, and behavior concerning specific technologies.

One crucial element affecting risk perception in IT is the emotional response to technology. For instance, research indicates that feelings associated with using or interacting with technology can influence perceptions of potential risks and benefits. For example, individuals with more experience using self-driving cars tend to express lower risk perceptions and higher trust in the technology, suggesting that familiarity and emotional engagement significantly shape risk attitudes [38]. This finding aligns with the broader literature, where emotional responses have been shown to mediate how individuals assess risks, especially in contexts involving emerging technologies [39].

Another important aspect is the influence of information sources and communication channels on risk perception. The proliferation of information through social media and other online platforms significantly impacts how risks are perceived during public health emergencies. Prior research has confirmed that exposure to varied information affects users' health risk perceptions, particularly during crises such as the COVID-19 pandemic [40]. Additionally, research on avian influenza indicated that repeated messaging through mass media amplified public awareness and heightened risk perceptions [41]. This highlights the role of media in framing risk narratives and shaping public understanding.

Cognitive biases and individual differences also play a substantial role in risk perception within IT contexts. Studies have shown that women generally perceive greater risks from technology than men [42]. Furthermore, perceptions of risks may vary based on individual attributes, such as previous experiences with technology, levels of expertise, and personal information-seeking behaviorsPersonal methodological differences in individuals' risk assessment can impact perceptions, emphasizing that various factors, including individual beliefs and organizational contexts, affect perceptions of IT-related risks [43].

Moreover, the interplay between trust in technology and risk perception is critical. Trust acts as a mediating variable that can mitigate perceived risks associated with technology use and adoption. For instance, individuals exhibiting higher levels of trust in the accuracy and utility of technological messages are more likely to adopt those technologies despite potential risks, as evidenced in the context of autonomous vehicles [44]. This illustrates how trust can modify often-negative perceptions surrounding emerging technologies.
In brief, perceptions of risks associated with information technology are shaped by emotional responses, the information environment, cognitive biases, demographic factors, and levels of trust. Understanding these dynamics is essential for developing effective communication strategies and designing technologies that align with user perceptions and concerns.

2.3. Perceptions of Risks from Climate Change and Related Natural Forces

Perceptions of risks associated with climate change and related natural forces are complex constructs influenced by various factors, including individual experiences, educational background, cultural context, and trust in information sources. Understanding these perceptions is essential for developing effective communication strategies and policy frameworks aimed at mitigating climate impacts.

One key construct in understanding climate change risk perception is the significance of education and knowledge. Research has shown that individuals with higher educational attainment tend to have a greater awareness of climate change risks [45]. Moreover, studies have shown that knowledge significantly influences risk perception, as those with more information about climate phenomena are generally more likely to recognize and respond to potential dangers [46] [NN] (Aksit et al., 2017).For instance, prior research has found that educated farmers in Ghana were more aware of climate risks, attributing this to their access to relevant information about climate impacts [47]. Such insights underline the necessity of educational interventions aimed at enhancing public understanding of climate change to foster proactive behavior in risk mitigation.

Moreover, psychological and emotional factors play a pivotal role in shaping climate risk perceptions. Prior research has shown that evolving emotional responses, including eco-anxiety, significantly influence individuals' intentions to engage in behaviors that mitigate climate change effects [48]. Similarly, research has also demonstrated how personal stakes, familiarity with the issue, and perceived fairness can enhance or mitigate climate change risk perception, particularly when moderated by political orientations [49]. These findings imply that emotional and affective aspects must be carefully considered in climate communication to foster constructive public engagement.

Political orientation further complicates the landscape of climate risk perception. For instance, in the United States, which has markedly differing views on climate issues among its populace, political affiliation has been determined to affect how individuals perceive flooding risks associated with climate change, revealing significant disparities in perceptions based on whether individuals identify as Republicans or Democrats [50]. This divergence reflects broader sociopolitical narratives that can either exacerbate or alleviate public concern over climate risks. Additionally, the framing of scientific consensus on climate change plays a critical role in shaping perceptions, with studies indicating that awareness of scientific agreement can lead to increased public support for climate policies [51].

Social context and collective experiences, such as exposure to extreme weather events, can also influence perceptions of climate-related risks. Personal experiences with extreme climatic phenomena are strongly linked to heightened risk perception among individuals [52]. Indeed, skeptical individuals often perceive climate change as a distant threat, dampening their engagement with climate mitigation efforts [53]. As such, personal and collective experiences must be integrated into public discourse to enhance the urgency surrounding climate action.

In brief, perceptions of risks from climate change are shaped by an interplay of educational, emotional, political, and experiential factors. An effective response to climate change requires not only enhancing public knowledge but also understanding the underlying emotional and sociopolitical contexts that influence these perceptions. By addressing these dimensions, policymakers and communicators can better engage the public and promote collective actions toward climate resilience.

2.4. How Personal Perceptions of Risk Impact Corporate Decision Making

Personal perceptions of risk are crucial in shaping corporate management decisions and influencing strategies across multiple dimensions, such as innovation, financial performance, and compliance. Key decision-makers, including CEOs and top management teams, frame their corporate strategies based on their risk perceptions, which can stem from individual experiences, psychological traits, and organizational cultures.

One significant aspect is how risk perceptions dictate managerial decision-making styles. Research has demonstrated that decision-makers exhibit varying levels of risk aversion and risk-seeking tendencies based on their personal backgrounds and experiences. For instance, decision-makers who perceive high personal risk are more likely to adopt conservative strategies aimed at safeguarding their wealth and corporate reputation [54][55]. These tendencies reflect a broader behavioral finance perspective where cognitive biases influence managerial behavior, indicating that not all corporate decisions are made under conditions of rational expectation [55]. Consequently, CEOs and top executives who experience prior financial failures may become risk-averse, prioritizing stability over aggressive growth [54].

Moreover, the organizational environment and culture significantly influence how personal perceptions of risk are integrated into corporate decision-making. The establishment of a risk-aware corporate culture can help mitigate individual biases in risk assessment. By fostering open discussions regarding risk, companies can better align their risk appetite with strategic objectives, leading to more informed and collective decision-making [57]. Findings indicate that firms actively engaging in comprehensive risk management practices, which consider both internal and external threats, tend to perform better in the long run [56]. This holistic approach encourages transparency and accountability, essential for effective governance and performance [57].

The role of innovation is another critical area where personal perceptions of risk manifest in corporate management decisions. Innovation often requires significant investment in uncertain outcomes, and understanding these inherent risks is vital. Studies suggest that a decentralized decision-making style can enhance innovation by empowering employees to pursue novel and risk-laden projects. When leaders perceive the potential for substantial rewards from innovations, they might foster a risk-taking climate that allows for creative solutions and competitive advantages [58].

Climate risk, especially in contemporary discussions about sustainability, is another crucial dimension of risk perception affecting decision-making. Corporate management's awareness of climate-related risks has transformed strategic planning processes, prompting organizations to integrate sustainability into their core business strategies [59]. Managers often respond to perceived climate risks by adopting proactive measures, which can include shifting organizational resources towards sustainable practices, thereby aligning long-term corporate goals with societal expectations [58][59].

In brief, personal perceptions of risk are fundamentally intertwined with corporate management's decision-making processes. These perceptions shape managerial behaviors, influence the adoption of innovative strategies, and determine how organizations respond to external risks, including climate change. Understanding the psychological underpinnings of these perceptions can lead to more effective risk management frameworks, ultimately contributing to resilient corporate governance and enhanced organizational performance.

3. RESEARCH METHODS

3.1. Background on the Munich Security Index

The present research is based on the Munich Security Index (MSI). The MSI Index is part of an annual report issued since 2022 by the Munich Security Conference (MSC), The MSC produces this report in conjunction with Kekst CNC, a leading global strategic communications consultancy.

To generate the MSI Index, an annual survey is done across 11 countries, all 7 G7 nations (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States) and the "BICS" countries (the nations commonly referred to as "BRICS," Brazil, India, China, and South Africa, excluding Russia since its invasion of Ukraine in 2022). Each national sample is made up of 1,000 individuals, carefully selected to represent the respective country's demographics in terms of gender, age, residency, formal education, and income in order to ensure representativeness. Taken together, the 11 national surveys combine to produce an annual survey size of 11,000 for the MSI Index. The annual surveys that form the basis for each year's Munich Security Indexes [60, 61, 62, 63] and larger, more comprehensive Munich Security Conference Reports[64, 65, 66, 67] are conducted late in the preceding year (hence, the surveys for the 2025 MSI Index were actually taken in the field in November 2024.

The Munich Security Index is comprised of a series of composite scores drawn from five questions that elicit input from survey participants in each of the 11 countries about 27 of today's major global risks. These risks, which will be examined in the analysis section of this article, span the gamut of risk factors facing us as a society, from economic to political to technological to natural forces.

Each survey participant was asked to respond to 5 questions regarding each of the 33 risk areas (the 27 risk factors and the 6 countries). In the words of the researchers in the most recent (2025) MSC Index Report, "The Munich Security Index combines the crucial components that make a risk more serious. Public perceptions of trajectory are combined with imminence and severity alongside a measure to give equal weight to perceptions of preparedness" [63] To that end, the 5 questions asked of all participants across the 11 surveyed countries were:

- Question 1 – How great is the overall risk to your country? (*assessing overall risk perception*);
- Question 2 – Will the risk increase or decrease over the next twelve months? (*assessing perception of the trajectory of the risk - i.e. will it increase, decrease, or stay the same) over the next 12 months*);
- Question 3 – How severe would the damage be if it happened? (*assessing perception of risk severity - i.e. how severe the damage would be to your country if this risk actually did occur*);
- Question 4 – How imminent is the risk? (*assessing perception of the imminense of the risk - i.e. is it likely to happen in the short-term, the long-term, or never*); and
- Question 5 – How prepared is your country? (*assessing perception of the how prepared - or unprepared - the country may be for the specific risk*).

To calculate the Munich Security Index score for each risk factor for each country, participant responses to these 5 questions - overall risk, trajectory, severity, imminence, and preparedness - are totaled and then rescaled to range from 0 to 100. The final MSI index score is an absolute figure (with 100 indicating the highest perception of risk and 0 being the lowest possible risk indicator). With this standardized risk assessment methodology, the MSI index allows for comparisons of risk perceptions in nations to be made between countries and over time, something that is being done for the first time in the present study. Further, the Munich Security Indexis unique among risk analysis tools in its connection between subjective perceptions of a wide variety and types of risk factors today andobjective criteria (including risk imminence, severity, and preparedness).

3.2. Data Analysis Using the Munich Security Index

In the present research, the author analyzed the four annual Munich Security Conference Reports that, to date, have included the Munich Security Index. The author extracted the data from these reports [60, 61, 62, 63] and created a data set that spans the MSC Reports from 2022 to 2025 (the present year). The construction and analysis of this new, large data set formed the foundation for the present study, which examines both inter and intra-country trends found in the MSI Index. The present research is novel in that it is the first longitudinal study to be conducted on the annual data collected for the MSI Index, and as such, it establishes a new way of gaining insights into cross-national perspectives on a variety of pressing technological, social, political, and economic issues facing business leaders - and the general public - in the nations included in the research that underlies both the Munich Security Conference Reports [64, 65, 66, 67]and the MSI Indexes [60, 61, 62, 63] created to date.

4. DATA ANALYSIS

The results of the analysis of this data set, constructed from combining the results of the four years of the MSI Indexproduced to date (2022-2025) are presented in this section, with a discussion provided for the reader as to each specific area of the analysis. First, the researcher looked at overall risk perception across the seven G7 countries regarding the twenty-seven distinct risks investigated for the Munich Security Conference Reports. Then, the analysis turns to perceptions regarding two specific areas of information-technology-related risks - cyberattacks and artificial intelligence – and then three specific areas of threats springing from "Mother Nature" – namely climate change (generally), extreme weather and forest fires, and finally, destruction of natural habitats. The culminating area of analysis in the present research examines overall risk perceptions across the G7 countries concerning the aggregate IT and climate change-related risks addressed within the MSI Index framework. As highlighted in the analysis and discussion regarding the findings, across the G7 nations, despite all the "hype" associated with risks arising out of information technology, today, risks stemming from natural causes – specifically climate change – raise a higher alarm levelamong the general populace of these countries.

4.1. Overall Risk Perception in the G7 Countries

As you can see in Table 1 (*Ranking of Risk Perceptions in the G7 Countries and in the United States, 2025*), the analysis of risk perceptions across the G7 indicates that cyberattacks emerge as the most critical risk factor, receiving a high index score of 69, ranking first in both the G7 overall and the United States individually (for reference, the average rating of all 27 distinct threat areas across the G7 nations stood at 55.43 for 2025). The consensus regarding the severity of cyber threats underscores a comprehensive understanding within the G7 of the evolving nature of digital security, where knowledge and preparedness are pivotal in shaping national security strategies [68] [69].

Table 1. Ranking of Risk Perceptions in the G7 Countries and in the United States, 2025.

Risk Factor	2025 Index Score – G7 Overall	2025 G7 Index Rank	2025 USA Index Rank
Cyberattacks on your country	69	1	1
Extreme weather and forest fires	68	2	3
Destruction of natural habitats	67	3	5
Climate change generally	66	4	10
Mass migration	64	5	16
Economic or financial crisis in your country	63	6	6
Disinformation campaigns from enemies	62	7	2
Rising inequality	61	8	23
Radical Islamic terrorism	60	9	17
International organized crime	60	10	20
Divisions amongst major global powers	59	11	7
Use of nuclear weapons by an aggressor	58	12	11
Political polarization	57	13	4
Racism and other discrimination	56	14	21
Use of biological weapons by an aggressor	55	15	13
Divisions among Western powers and institutions	55	16	15
Trade wars	55	17	12
Use of chemical weapons and poisons by an aggressor	55	18	18
Artificial intelligence	54	19	8
Civil war or political violence	51	20	14
Energy supply disruption	50	21	19
Food shortages	49	22	25
Rapid change to my country's culture	47	23	22
Breakdown of democracy in my country	47	24	9
Right-wing terrorism	46	25	26
Coronavirus pandemic	31	26	27
Future Pandemic	31	27	24

Source Data: Munich Security Index Reports, 2022-2025

After the concurrence on the risk of cyberattacks as the number one risk today, the MSI Index data shows that the perceived threat level from climate change and related risksis high among the G7 countries. Following cyber threats, the perception of extreme weather and forest fires ranks second overall among the G7 nations. The heightened awareness reflects a growing recognition of the impacts of climate change, particularly in vulnerable regions. As climate-related adversities become increasingly prevalent, G7 countries are expected to prioritize environmental resiliency within their security agendas to mitigate these risks effectively [68]

[70].The ranking continues with the destruction of natural habitats and climate change generally, scoring 67 and 66, respectively across the G7 countries. These concerns are indicative of a global trend toward recognizing the interconnections between ecological health and socioeconomic stability, where threats to biodiversity and climate are perceived as critical risk factors. The implications of environmental degradation on human migrationcannot be underestimated, as much of this emigration is driven by the impact of armed conflicts, economics, and yes, climate change (ranked fifth in risk perception with an index score of 64), further illustrating how interconnected these factors are in the G7's risk landscape [69][71].

Economic and financial crises are also highly ranked, reflecting the intrinsic vulnerabilities of modern economies. With a rank of sixth, the concern for economic stability aligns with the understanding that financial turmoil can exacerbate social tensions and lead to increased susceptibility to other risks, such as disinformation campaigns and rising inequality, which rank seventh and eighth, respectively [72][73]. These perceptions highlight the multifaceted nature of risk, where social and economic elements are inextricably linked, forming a complex web of vulnerabilities that demand comprehensive management strategies.

In contrast, some risks, such as political polarization (ranked 13th) and breakdown of democracy (ranked 24th) across the G7 nations, indicate varying perceptions of the urgency of domestic issues compared to external threats, which may shape the political discourse and policy-making processes differently across the G7 nations. Such divergence could stem from differing national contexts, influencing the prioritization of responses to perceived internal vs. external threats [69][74].

The diversity of concerns also highlights the different levels of preparedness and focus areas within G7 nations. For instance, the United States ranks disinformation campaigns significantly higher (ranked 2) compared to its G7 counterparts, suggesting a more acute awareness of the strategic threat posed to democracy and social cohesion [75] [76]. Overall, as can be clearly seen inTable 1, climate-related risks, while still perceived as being high in threat potential, were assessed much lower in the U.S. than these same risks were in the remainder of the G7 countries. In assessing these risk perceptions, it is essential to consider the various underlying factors, including geopolitical scenarios, economic stability, and the evolving landscape of technological threats, which collectively inform the G7's strategic orientations toward risk management [77][78].

In brief, the ranking of risks for G7 countries illustrates a comprehensive and interconnected understanding of the myriad threats anticipated in 2025. The prioritization of cyber threats, environmental challenges, and socio-economic issues points toward a collective approach to addressing security that incorporates both immediate and long-term perspectives. These insights can serve as a foundation for further research and intervention strategies to enhance resilience within these nations.

4.2. Risk Perception of IT-Related Threats

The Munich Security Conference research encompassed two IT-related threats in the MSI Index, specifically the perceived threats arising from cyber attacks and artificial intelligence. In this section of the research, we will explore and analyze how these threats were viewed across the G7 countries over the most recent four-year period, 2022-2025.

4.2.1. Risk Perception of Cyberattacks

As you can see in Table 2*(Perceptions of Risk from Cyberattacks in the G7 Countries from the Munich Security Index, 2022-2025),*the analysis of cyberattack risk perceptions in G7 countries reflects significant trends in public sentiment amidst evolving cybersecurity landscapes. Overall, there is a noticeable rise in perceived risk across most G7 nations, highlighting an increased awareness of cyber threats. The average perception of risk has increased from 63.71 to 69 between 2022 and 2025, with notable variation among the countries analyzed.

Table 2. Perceptions of Risk from Cyberattacks in the G7 Countries from the Munich Security Index, 2022-2025.

Country/Year	2022	2023	2024	2025
Canada	62	61	63	67
France	60	62	65	69
Germany	68	74	70	76
Italy	65	65	64	67
Japan	68	67	72	69
United Kingdom	57	61	61	69
United States	66	64	65	66
Average	*63.71*	*64.86*	*65.71*	*69.00*
Average w/o USA	*63.60*	*65.80*	*66.40*	*70.00*

Source Data: Munich Security Index Reports, 2022-2025

Overall, the statistics from the Munich Security Index indicate a collective increase in risk perception regarding cyberattacks across the G7 nations and underlines the urgent need for cohesive cyber policies and interconnected strategies. The differing initial perceptions of risk could stem from varying levels of media coverage of cybersecurity threats and the effectiveness of governmental awareness campaigns[79] [80]. Indeed, the heightened fear of cyberattacks seen across the G7 nations may be influenced by recent high-profile cyber incidents and governmental responses to enhance national cybersecurity measures [81] [82]. These findings align with literature suggesting that the severity of past cyberattacks substantially shapes public perceptions of risk and vulnerability. Indeed, research has shown that countries that have experienced a higher number of cyberattacks tend to exhibit a greater awareness of their severity and the consequent need for protective measures [81] [82]. This correlation is critical for understanding how past events influence future perceptions and strategies toward cybersecurity in G7 nations.These statistics underscore how cultural and historical contexts shape each country's approach to cybersecurity, evidenced by diverging educational initiatives and government policies [83] [84]. For example, the emphasis on cybersecurity education varies significantly across not just the G7 countries, but globally as well. affecting the perceived competence in handling cybersecurity issues [84][85].

In brief, the Munich Security Index data on cyberattack risk perceptions illustrates a growing awareness of cyberattack risks among G7 countries, which appears to be driven by past experiences with cyber threats, governmental responses, and public discourse around cybersecurity. This trend suggests that policymakers must consider these perceptions when formulating future cybersecurity strategies to effectively mitigate risks.

4.2.2. Risk Perception of Artificial Intelligence

As you can see in Table 3*(Perceptions of Risk from Artificial Intelligence in the G7 Countries from the Munich Security Index, 2022-2025)*, the analysis of the perceptions of risk stemming from artificial intelligence in the G7 countriesreveals significant trends and variations across different nations. This period witnessed an evolution in public sentiment concerning AI, reflective of growing global discourse on its implications for society and individual lives.

Table 3. Perceptions of Risk from Artificial Intelligence in the G7 Countries from the Munich Security Index, 2022-2025.

Country/Year	2022	2023	2024	2025
Canada	39	42	55	55
France	40	42	49	52
Germany	44	45	55	59
Italy	39	40	49	52
Japan	48	48	51	53
United Kingdom	35	38	53	54
United States	41	41	52	52
Average	*40.86*	*42.29*	*52.00*	*53.86*
Average w/o USA	*41.20*	*42.60*	*51.40*	*54.00*

Source Data: Munich Security Index Reports, 2022-2025

From 2022 to 2025, the average perception of AI risk among G7 countries rose from 41 to 54, suggesting a growing concern about AI's role and its potential impacts on various sectors, including employment, privacy, and security. This aligns with findings in the literature regarding public anxiety about transformative technologies.

The significant rise in the perceived risks posed by AI taking place across all G7 nations can be ascribed to several factors. First, this trend possibly reflects increased media coverage and governmental policy discussions on AI [86][87]. This jump mirrors a trend where nations with more engaged public discourse around technological impacts demonstrate higher awareness and concern [88].This substantial jump may also suggest heightened public awareness and sensitivity in light of current political and societal debates surrounding technology and privacy, especially post-COVID-19 [87][89]. Japan saw the lowest real percentage increase in perceived risks from AI, rising from 48 and rising to 53 over the four years. Japan's cultural dynamics toward technology acceptance likely contribute to this steadiness, emphasizing trust in technology while being cautious of its risks [88].The overall slowing growth in AI risk perception seen over the past two years (2024-25)suggests that while individual countries are increasing their awareness of AI risks, they're facing similar challenges regarding public education and trust in AI technologies [86] [87].

In brief, the findings from the Munich Security Index regarding the perceived risks posed by artificial intelligence emphasize a collective movement towards heightened awareness of AI risks across G7 countries. This sentiment shift calls for policymakers to address public concerns through transparent regulations and robust frameworks that prioritize ethical considerations and societal implications of AI deployment. The data suggests that fostering trust and understanding in AI technologies will be paramount in navigating the future landscape of artificial intelligence,

especially as public perceptions become increasingly pivotal in shaping technological acceptance [87] [89].

4.3. Risk Perception of Threats from "Mother Nature"

The Munich Security Conference research encompassed three specific areas of threats springing from "Mother Nature" in the MSI Index, namely climate change (generally), extreme weather and forest fires, and finally, destruction of natural habitats.In this section of the research, we will explore and analyze how these threats were viewed across the G7 countries over the most recent four-year period, 2022-2025.

4.3.1. Risk Perception of Climate Change

As you can see in Table 4(*Perceptions of Risk from Climate Change in the G7 Countries from the Munich Security Index, 2022-2025)*, the perceptions of risk associated with climate change – in general - among G7 countries exhibit notable. When analyzing these perceptions, it becomes evident that each country reacts differently to climate change risks, influenced by a multitude of socioeconomic factors and existing policies.

Table 4. Perceptions of Risk from Climate Change in the G7 Countries from the Munich Security Index, 2022-2025.

Country/Year	2022	2023	2024	2025
Canada	69	65	62	63
France	71	68	69	74
Germany	74	70	63	64
Italy	78	82	75	78
Japan	70	66	70	73
United Kingdom	62	65	61	58
United States	53	52	50	52
Average	*68.14*	*66.86*	*64.29*	*66.00*
Average w/o USA	*71.00*	*70.20*	*67.60*	*69.40*

Source Data: Munich Security Index Reports, 2022-2025

Italy emerged with the highest risk perception scores among the G7 over the 2022-2025 time frame, while the United States consistently scored the lowest. Italy's elevated perception could be linked to its vulnerabilities to extreme weather events, as prior research has demonstrated that countries with higher exposure to climate-related issues often exhibit increased concern regarding their long-term impacts on energy security and economic stability [90]. On the other hand, the U.S.'s much lower risk perception, which slightly decreased by 2023 and later fluctuated, may be attributed to prevailing skepticism among segments of the population regarding the severity of climate change effects [91] [92]. Notably, public attitudes toward climate change often diverge, comprising complex layers influenced by political, economic, and social contexts, which indicates that countries with robust environmental policies tend to develop greater public concern for climate-related risks [90] [93].

The average risk perception across the G7 countries without the U.S. remains higher (71) than the overall average (68.14) through the years analyzed, suggesting that when excluding the least

concerned nation, a more significant awareness prevails [91] This trend emphasizes the need for global cooperation and aligned strategies targeting climate change, reinforcing prior research as to how green policies and sustainability efforts in G7 nations collectively bolster national and global resilience against climate change [94].Research has also shown how nations that consistently face climate change repercussions align their public policies with evidence-based environmental strategies, which directly impact risk perception[95].Such trends could correlate with prior research suggesting that effective communication about climate tipping points significantly enhances public concern in nations actively engaging in climate discourse [91] [93]. In brief, the perceptions of climate change risk among G7 countries reflect the complex interplay of national policies, public sentiment, and socio-environmental dynamics. Key factors contributing to these perceptions include existing ecological policies, public awareness efforts, and vulnerability to climate-related phenomena. These dynamics ultimately shape the nations' responses and adaptations toward climate change, influencing both individual and collective actions for future resilience.

4.3.2. Risk Perception of Extreme Weather and Forest Fires

As you can see in Table 5 (*Perceptions of Risk from Extreme Weather and Forest Fires in the G7 Countries from the Munich Security Index, 2022-2025)*, the analysis of the perceptions of risk in the MSI Index from extreme weather and forest fires among G7 countriesreveals notable trends in public sentiment regarding these pressing environmental issues. Over this period, a consistent concern regarding extreme weather patterns and forest fire risks has emerged, reflecting both immediate experiences and longer-term trends associated with climate change.The data from the Munich Security Index indicates a perception of risk from extreme weather and forest fires across G7 countries, which fluctuated only slightly from 68.57 in 2022 to an average of 68.29 in 2025. This slight decline suggests a generally stable but cautious attitude toward the risks posed by these environmental phenomena[96].

Table 5. Perceptions of Risk from Extreme Weather and Forest Fires in the G7 Countries from the Munich Security Index, 2022-2025.

Country/Year	2022	2023	2024	2025
Canada	71	68	68	69
France	70	69	69	74
Germany	75	73	66	68
Italy	81	82	78	82
Japan	68	63	68	70
United Kingdom	57	61	60	56
United States	58	59	57	59
Average	*68.57*	*67.86*	*66.57*	*68.29*
Average w/o USA	*70.20*	*69.60*	*68.20*	*70.00*

Source Data: Munich Security Index Reports, 2022-2025

In brief, the findings indicate that risk perceptions regarding extreme weather and forest fires among G7 nations remain a complex interplay of experience, preparedness, and public awareness. Over the analyzed period, nations with high exposure and historical experiences—such as Canada and Italy—exhibit higher risk perceptions, while those with a comparatively milder history of extreme weather, like the United Kingdom, maintain lower perceptions.And yet,

in the United States, where hurricanes and wildfires have presented extreme danger across almost the entirety of the nation over the past few years (witness the January 2025 urban wildfire that destroyed parts of Los Angeles [97] [98], the risk perception from such climate change-fueled weather phenomena has remained relatively steady, even in the face of demonstrably rising dangers [99].

In brief, as countries confront these environmental challenges, the data underscores the necessity for proactive communication strategies that educate the public about risks and foster adaptive behaviors. Continued investment in disaster preparedness and response strategies will be crucial for bridging the perception-reality gap and enhancing resilience to extreme weather events, and forest fire incidences in the face of climate change threats.

4.3.3. Risk Perception of Destruction of Natural Habitats

As you can see in Table 6(*Perceptions of Risk from Destruction of Natural Habitats in the G7 Countries from the Munich Security Index, 2022-2025*), the MSI Index results present a nuanced view of how countries perceive the risk associated with the destruction of natural habitats. The data indicates varying levels of concern across G7 nations, with three key themes emerging from this analysis: stability of perceptions over time, implied socio-political influences, and implications for biodiversity conservation strategies.

Table 6. Perceptions of Risk from Destruction of Natural Habitats in the G7 Countries from the Munich Security Index, 2022-2025.

Country/Year	2022	2023	2024	2025
Canada	69	68	66	67
France	68	66	65	70
Germany	75	73	68	70
Italy	79	78	73	76
Japan	69	63	68	69
United Kingdom	60	65	62	60
United States	57	59	56	58
Average	*68.14*	*67.43*	*65.43*	*67.14*
Average w/o USA	*70.20*	*69.00*	*67.20*	*69.00*

Source Data: Munich Security Index Reports, 2022-2025

Starting with the stability of perceptions, it is significant to note that Italy consistently ranks the highest in perceived risk from the destruction of natural habitats in the MSI Index throughout the period assessed from 2022 to 2025, peaking at a high-risk level of 79 in 2022 before slightly declining to 76 in 2025. This suggests a robust concern for habitat destruction that might reflect broader socio-political commitments to environmental issues in Italy, as indicated by research that illustrates the intrinsic link between public perception and environmental advocacy [100][101]. Other countries like Germany and Canada exhibit moderately high levels of concern, albeit with a gradual decrease over the years. Such trends may reflect an increasing normalization of habitat destruction as an accepted risk but could also indicate a fatigue regarding environmental issues, often amplified in contemporary discourse [102].

Implied socio-political influences on these perceptions can provide further insight. The United States, which consistently ranks lowest in the perceived risk level of destruction of natural habitats, with values between 57 and 59, might suggest a diminished public prioritization of ecological concerns, possibly reflecting political and administrative narratives focusing on economic growth over environmental stewardship [102]. Conversely, countries like Japan and the United Kingdom, with risk perceptions showing greater fluctuation, may experience shifting political landscapes or socio-ecological strategies that influence public opinion on the importance of habitats [103].

Lastly, the implications for biodiversity conservation strategies are paramount. The average perception of risk regarding the destruction of natural habitats among the G7 countries shows a slight, marginal decline, decreasing from 68.14 in 2022 to 67.14 by 2025. This downward trend in collective risk perception does raise concern about the future prioritization of biodiversity conservation efforts, which face challenges due to habitat destruction — noted as one of the residing threats to biodiversity [104] [105]. These findings reiterate calls for global environmental efforts to address habitat destruction, affirming that a concerted focus on public awareness and political will is essential for fostering an effective response to ecological risks [106].

In brief, while there remains a general concern regarding habitat destruction among G7 countries, the observed fluctuations in perception signify underlying socio-political factors and pose questions about future biodiversity conservation efforts. Continued engagement with ecological education and proactive governmental policies will be crucial for reversing any complacency toward habitat destruction in the coming years.

4.4. Comparison of Risk Perceptions from IT-Related Threats and Natural Threats

The culmination of this analysis is to compare the relative threat levels that are perceived by the populace of the G7 countries regarding threats that emanate from the realm of information technology versus those found in the natural world. The analysis of the data presented in Tables 7 *(Perceptions of Risk from All IT-Related Threats Across the G7 Countries from the Munich Security Index, 2022-2025)*and 8 *(Perceptions of Risk from All Natural ThreatsAcross the G7 Countries from the Munich Security Index, 2022-2025)*on IT risks and natural risks highlights contrasting trends in public perception over the years 2022 to 2025. The data reflects an increasing concern over cyberattacks and AI-related risks, while simultaneously revealing a decline in the perception of natural risks associated with climate change.

Table 7. Perceptions of Risk from All IT-Related Threats Across the G7 Countries from the Munich Security Index, 2022-2025.

Risk Factor	2022	2023	2024	2025
Cyberattack Risk Perception: G7 Countries	63.71	64.86	65.71	69.00
AI Risk Perception: G7 Countries	40.86	42.29	52.00	53.86
Average	*52.29*	*53.57*	*58.86*	*61.43*

Source Data: Munich Security Conference Index, 2022-2025.

Table 8. Perceptions of Risk from Destruction of Natural Habitats Across the G7 Countries from the Munich Security Index, 2022-2025.

Risk Factor	2022	2023	2024	2025
Climate Change Risk Perception: G7 Countries	68.14	66.86	64.29	66.00
Extreme Weather and Forest Fires Risk Perception: G7 Countries	68.57	67.86	66.57	68.29
Destruction of Natural Habitats Risk Perception: G7 Countries	68.14	67.43	65.43	67.14
Average	*68.29*	*67.38*	*65.43*	*67.14*

Source Data: Munich Security Conference Index, 2022-2025.

In the realm of IT risks among G7 countries, there is a noticeable increase in the perception of cyberattack risks, which has risen from 63.71 in 2022 to 69.00 in 2025, representing a rise of 8.63%. Additionally, AI risk perception has surged significantly, from 40.86 to 53.86 during the same period, marking a remarkable 32.85% increase. These escalating concerns about IT risks illustrate a heightened awareness of cybersecurity threats and the implications of AI technology[107], possibly fueled by increasing media coverage of cyber incidents and public discourse on AI ethics and safety measures [108]. The substantial increase in AI risk perception aligns with research indicating that public sentiment can shift rapidly based on recent events and societal debates around technology [87].

Conversely, the aspects of natural risks displayed in the data indicate a decline in perceived threats, particularly regarding climate change and related phenomena. The perception of climate change risk fluctuated, showing a net decrease of 3.15% from 2022 to 2025, along with similar trends in perceptions about extreme weather events and the destruction of natural habitats [48] [109]. These decreasing trends might reflect a normalization of climate risk perception as communities become accustomed to the discourse surrounding climate change, a phenomenon noted in studies indicating that higher exposure can sometimes lead to reduced perceived risk. Furthermore, various research suggests that societal and institutional responses to climate change can alter individual risk perceptions, potentially leading to complacency about the urgency of climate action [110].

Furthermore, the comparison of average risk perception between IT and natural risks demonstrates that while IT risks show rising concerns, natural risks appear to be suffering from a decreasing urgency in terms of public perception internationally. The G7 composite average for IT risks climbed from 52.29 to 61.43 (an increase of 20.74% over the four years under review), whereas the composite average for natural risks marginally declined, from 68.29 to 67.14 (or -1.57%), between 2022 and 2025. This divergence suggests a shifting landscape where technological threats are becoming more prominent in public consciousness compared to natural disasters, despite the potentially far-reaching implications of climate change [111].

In brief, the contrast in findings sheds light on a significant shift in public risk perception over the years, with a clear escalation in fears surrounding IT-related risks juxtaposed against a backdrop of diminishing anxiety regarding natural climate-related threats. This analysis underscores the complexity of how societal influences, media narratives, and personal experiences converge to shape public perception, highlighting the need for continuous engagement and education around both technology and climate change issues to ensure a balanced understanding of risk.

5. CONCLUSIONS

Through an extensive exploration of risk perception relating to the dual threats posed by information technology and climate change, this article has highlighted the intricate interconnections between individual perceptions, corporate decision-making, and collective responses across diverse contexts, especially within the G7 nations. As examined throughout the article, the framing of these risks is colored by factual impacts and social, emotional, and communicative influences that shape how various stakeholders understand and react to these dangers.

Understanding the perceptions surrounding climate change reveals how moral and existential dimensions amplify risks as they are perceived by both individuals and societies. While awareness of impending environmental changes fosters a heightened sense of urgency to act, there exists a counterbalance in misinformation and apathy propagated by media portrayals and emotional distancing. Prior research confirms that the escalation of extreme weather events, driven by climate change, correlates with increased public awareness and concern, yet complexities arise in how different demographics digest and respond to such information [112]. Further, trust in governing bodies, educational background, and psychological attributes directly influence risk perceptions and subsequent behaviors [113]. Therefore, trust in risk management frameworks can alleviate such vulnerabilities, thereby fostering greater community engagement and proactive behaviors in response to climate-related threats.

Similarly, the landscape of risk associated with advancements in information technology, particularly concerning cybersecurity and artificial intelligence, unveils a complex interplay between perceived risks and personal experiences with technology. The emotional responses elicited by technological innovations often dictate acceptance and use, establishing a direct connection between user familiarity and perceived safety. Moreover, the landscape of emotions tied to technology extends beyond mere acceptance; individuals' perceptions are inherently shaped by their social circles, media consumption, and prior experiences, fostering environments rich in both anxiety and trust [114]. The dual-edged nature of AI presents both enhanced security capabilities and heightened risks of exploitation, requiring a calibrated approach to governance and communication [115] [116].

The findings converge on the critical role of education and effective communication in shaping public perceptions, as evidenced by the correlation between knowledge levels and risk recognition across varied contexts. Educational initiatives that provide clear, accurate information on the risks associated with climate change and advancements in technology can significantly enhance public understanding and engagement. As reported in various studies, individuals with more extensive knowledge of climate phenomena demonstrate greater awareness and willingness to engage in adaptive behaviors. This suggests that concerted efforts to disseminate accurate information can bridge the gap between risk awareness and practical action, ultimately leading to more resilient communities.

Moreover, the implications of these findings stretch into the corporate realm, where perceptions of risk inform strategic decisions markedly. As individuals at the top of organizations process their own risk perceptions, these insights directly influence innovation, sustainability efforts, and governance. Firms operate under increasing societal and environmental scrutiny, and leaders who integrate an understanding of climate risks into their business strategy benefit from enhanced financial performance and stability. Research indicates that effective corporate governance linked to sustainability initiatives can mitigate perceived risks attached to climate change effects, and, in turn, affect creditworthiness and financial terms granted by lenders engaged in sustainability practices [114][117].

Aligning strategic management with heightened risk perceptions regarding both climate-related and technological threats is therefore not merely advantageous, but imperative. The societal expectation for corporations to adopt ethical practices around sustainability and risk management reflects a shifting paradigm whereby firms must not only comply with regulatory frameworks but also actively engage in transparent risk communication and responsibility [31] [118]. By fostering a culture of accountability and proactive risk management within organizations, decision-makers can navigate the litany of risks while enhancing their firm's reputation and market performance.

From a policy perspective, the intertwined dynamics of personal risk perceptions and organizational responses necessitate a multi-faceted approach. Investments in educational frameworks that promote understanding of both climate change and emerging technological risks can encourage community participation and informed decision-making. Furthermore, developing communication strategies that resonate with public sentiment and foster trust will be pivotal in promoting cooperative efforts at both local and global scales. As societies globally navigate the uncertainties ushered in by climate change and rapid technological advances, a collective, informed, and trust-driven approach will be paramount in addressing perceived risks effectively.

In conclusion, this research underscores the significance of perceiving risks from both climate change and technological sources as interconnected phenomena that demand nuanced understanding and multi-level responses. The evolving landscape of risks calls for strategic management approaches that consider psychological, social, and emotional dimensions influencing public engagement and organizational behavior, ultimately shaping a safer, more sustainable future for all stakeholders involved. Future research should delve deeper into the longitudinal impacts of trust-building measures and educational interventions, focusing on their effectiveness in changing behaviors and perceptions surrounding these critical issues.

6. IMPLICATIONS FOR STRATEGIC MANAGEMENT

As the present research demonstrates, the Munich Security Index (MSI) provides a comprehensive framework for understanding global risk perceptions, focusing on differences – and similarities - across countries. This article synthesized insights derived from the MSI surveys conducted between 2022 and 2025, emphasizing their relevance for strategic management across diverse sectors, focusing on the differing perceptions of perceived threats originating from information technology and those based on changes in the climate. The present research allows for a nuanced understanding of how citizens across various demographics perceive security risks, thus aiding policymakers and business leaders in making informed strategic decisions going forward [119]. It also sets the stage for future longitudinal research making use of the MSI Index involving a whole host of cutting-edge issues today, beyond the realm of IT and climate change.

One of the key insights from this analysis of MSI data is the prominence assigned to cyber threats, particularly cyberattacks, which consistently rank as the most significant risk across G7 nations. This increase underscores a growing acknowledgment of digital vulnerabilities, significantly influencing strategic management practices within businesses and governments that rely increasingly on digital platforms [120]. The recognition of cyber threats can drive organizations to prioritize cybersecurity, necessitating investments in technology, training, and policy formation that align with evolving risks [121].

Another salient aspect revealed through this analysis of the MSI data is the escalating concerns regarding climate-related threats. Perceptions of extreme weather, habitat destruction, and

general climate change risk have developed significantly, particularly among nations with high exposure to environmental changes. The G7 countries exhibit varying risk perceptions; for instance, Italy ranks the highest in concern around climate risks, which correlates with regional vulnerabilities to extreme weather events. Strategic management in these contexts must reflect an acute understanding of these risks. For instance, companies engaging in sectors sensitive to climate fluctuations may prioritize adaptive strategies that enhance resilience against environmental impacts [122].

Furthermore, the radical shift in perceptions toward artificial intelligence also raises strategic management considerations, reflecting widespread public anxieties surrounding the technology's potential implications for employment, privacy, and security [121]. This rising concern compels organizations to consider ethical guidelines and regulatory frameworks in their strategic planning processes, emphasizing responsible AI development and deployment [123]. Effective management strategies would include transparent decision-making protocols, aiming to bolster public trust and regulatory compliance amidst technological advancements [124].

Risk perception analysis within this analysis of the MSI Index data also emphasizes the interdependence of economic stability and security. For instance, concerns around financial crises rank highly, indicating that economic uncertainties can exacerbate other risks, such as social unrest, cyber threats, and political polarization. This interconnectedness suggests that organizations must adopt holistic strategic management approaches that accommodate economic health as a core component of national and organizational security [125] [126].

Additionally, the divergence in risk perceptions highlighted across the G7 points to varying levels of preparedness and overall response strategies. The United States, for example, demonstrates a distinct emphasis on disinformation and political polarization, ranking these risks higher relative to its G7 counterparts. This variance suggests a need for tailored strategic responses that account for national contexts and the unique challenges each country faces [127]. In this regard, strategic managerial frameworks must incorporate comprehensive risk assessments reflective of both domestic and international landscapes, ensuring that organizations adapt their strategies accordingly to manage perceived threats effectively.

The present research, based on an extensive analysisof the MSI data, thus aids strategic management by providing critical insights that inform resource allocation and risk prioritization through detailed cross-national comparisons. By interpreting these data metrics, organizations can better navigate the complexities posed by both immediate and emerging threats while fostering resilience. The insights derived from the MSI Index convey essential lessons regarding proactive risk management, urging leaders to prioritize educational and communicative initiatives that raise awareness of the security landscape [128].

Finally, the intersection of technology and climate change risk compels strategic management actors to integrate environmental considerations into their operational strategies. The increasing acknowledgment of climate-related risks necessitates organizations to adopt sustainable practices that not only comply with regulatory directives but also enhance their competitive advantage by addressing rising public expectations for corporate responsibility in environmental stewardship [129] [130].

In conclusion, the implications of the Munich Security Index for strategic management resonate profoundly amid contemporary uncertainties. By identifying shifting public perceptions of risks—from cybersecurity and AI to economic stability and climate change—organizations and governments can ensure their strategies are reflective of real-world challenges. By embedding an understanding of risk perception into their strategic agendas, enterprises can enhance

resilience, foster stakeholder trust, and better navigate the complexities of an interconnected – and increasingly volatile - global landscape.

REFERENCES

[1] Hanson-Easey, S., Williams, S., Hansen, A., Fogarty, K., & Bi, P. (2015). Speaking of climate change. *Science Communication*, 37(2), 217-239. https://doi.org/10.1177/1075547014568418.

[2] Jagiello, R. & Hills, T. (2018). Bad news has wings: Dread risk mediates social amplification in risk communication. *Risk Analysis*, 38(10), 2193-2207. https://doi.org/10.1111/risa.13117.

[3] Kamarulzaman, N., Lee, K., Siow, K., & Mokhtar, M. (2019). Psychological and sociological perspectives for good governance of sustainable nanotechnology development in Malaysia. *Journal of Nanoparticle Research*, 21(7), 164. https://doi.org/10.1007/s11051-019-4583-5.

[4] Moussaïd, M., Brighton, H., &Gaissmaier, W. (2015). The amplification of risk in experimental diffusion chains. *Proceedings of the National Academy of Sciences*, 112(18), 5631-5636. https://doi.org/10.1073/pnas.1421883112.

[5] Lee, S., Chung, M., Kim, N., & Jang, S. (2024). Public perceptions of ChatGPT: Exploring how nonexperts evaluate its risks and benefits. *Technology Mind and Behavior*, 5(4). https://doi.org/10.1037/tmb0000140.

[6] Handayani, R., Utami, E., &Luthfi, E. (2023). Systematic literature review on auditing information technology risk management using the COBIT framework. *Prisma Sains JurnalPengkajianIlmu Dan PembelajaranMatematika Dan IpaIkipMataram*, 11(4), 1028. https://doi.org/10.33394/j-ps.v11i4.8871.

[7] Jones, B., Sherman, J., Rojas, N., Hosek, A., Vannette, D., Rocha, R., … & García-Amador, J. (2019). Trump-induced anxiety among Latina/OS. *Group Processes & Intergroup Relations*, 24(1), 68-87. https://doi.org/10.1177/1368430219889132.

[8] Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., … & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: a systematic review. *Sensors*, 21(15), 5119. https://doi.org/10.3390/s21155119.

[9] Chimezie, O., Akagha, O., Dawodu, S., Anyanwu, A., Onwusinkwue, S., & Ahmad, I. (2024). Comprehensive review on cybersecurity: modern threats and advanced defense strategies. *Computer Science & IT Research Journal*, 5(2), 293-310. https://doi.org/10.51594/csitrj.v5i2.758.

[10] Camacho, N. (2024). The role of AI in cybersecurity: Addressing threats in the digital age. *JAIGS*, 3(1), 143-154. https://doi.org/10.60087/jaigs.v3i1.75.

[11] Nazir , I. &Tiwari , S. (2023). Impact of machine learning in cybersecurity augmentation. *QTanalytics Publication* (Book), 147–154. https://doi.org/10.48001/978-81-966500-9-4_12.

[12] Gudimetla, S. &Kotha, N. (2024). Enhancing threat detection and response strategies. *International Research Journal of Modernization in Engineering Technology and Science*, 6(5), 1374-1376. https://doi.org/10.56726/irjmets55883.

[13] Ramakrishnan, S. &Chittibala, D. (2024). Enhancing cyber resilience: convergence of SIEM, SOAR and AI in 2024. *International Journal of Computing and Engineering*, 5(2), 36-44. https://doi.org/10.47941/ijce.1754.

[14] Ibiyemi, M. &Olutimehin, D. (2024). Cybersecurity in supply chains: addressing emerging threats with strategic measures. *International Journal of Management & Entrepreneurship Research*, 6(6), 2024-2047. https://doi.org/10.51594/ijmer.v6i6.1241.

[15] Abrahams, T., Ewuga, S., Dawodu, S., Adegbite, A., & Hassan, A. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. *Computer Science & IT Research Journal*, 5(1), 1-25. https://doi.org/10.51594/csitrj.v5i1.699.

[16] Alharbi, F., Alsulami, M., Al-Solami, A., Alotaibi, Y., Al-Osimi, M., Al-Qanor, F., … & Alotaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: the perspective of small enterprises in Saudi Arabia. *Sensors*, 21(20), 6901. https://doi.org/10.3390/s21206901.

[17] Darmi, Y., Fernandez, S., Fathoni, M., &Wijayanto, S. (2024). Evaluation of governance in information systems security to minimize information technology risks. *IntensifJurnalIlmiahPenelitian Dan PenerapanTeknologiSistemInformasi*, 8(1), 40-51. https://doi.org/10.29407/intensif.v8i1.21221.

[18]   Kalliojärvi, S. (2020). Age of Changes: Threat of Climate Change and Its Meaning for Security. In: Heininen, L., Exner-Pirot, H. (eds) *Climate Change and Arctic Security*. Palgrave Pivot, London. 9-32. https://doi.org/10.1007/978-3-030-20230-9_2.

[19]   Fetzer, T. (2012). Internationalization and the paradox of cross-border trade union cooperation, in *Paradoxes of internationalization: British and German trade unions at Ford and General Motors 1967-2000* (Manchester, 2012; online edn, Manchester Scholarship Online, 23 Jan. 2014), 160-187. https://doi.org/10.7228/manchester/9780719080975.003.0006.

[20]   Bradley, B., Blumenthal, D., Early, R., Grosholz, E., Lawler, J., Miller, L., … & Olden, J. (2011). Global change, global trade, and the next wave of plant invasions. *Frontiers in Ecology and the Environment*, 10(1), 20-28. https://doi.org/10.1890/110145.

[21]   McMichael, A. (2012). Insights from past millennia into climatic impacts on human health and survival. *Proceedings of the National Academy of Sciences*, 109(13), 4730-4737. https://doi.org/10.1073/pnas.1120177109.

[22]   Paulson, J., Ahdoot, S., Baum, C., Bole, A., Brumberg, H., Campbell, C., … &Trasande, L. (2015). Global climate change and children's health. *Pediatrics*, 136(5), e1468-e1484. https://doi.org/10.1542/peds.2015-3233.

[23]   Kiplimo, T. &Makame, M. (2020). Assessing socio-economic factors influencing household vulnerability to climate change in Kaskazini (A) district, Zanzibar, Tanzania. *International Journal of Innovative Research and Development,* 10(9), 54-66. https://doi.org/10.24940/ijird/2021/v10/i11/166928-404473-3-sm.

[24]   Abdallah, S., Akayim, A., Amedor, E., &Afetsu, J. (2023). Climate change, who is responsible?.*Open Journal of Applied Sciences*, 13(12), 2431-2446. https://doi.org/10.4236/ojapps.2023.1312190.

[25]   Spence, A., Poortinga, W., & Pidgeon, N. (2011). The psychological distance of climate change. *Risk Analysis*, 32(6), 957-972. https://doi.org/10.1111/j.1539-6924.2011.01695.x.

[26]   Tenbrink, T. & Willcock, S. (2023). Place attachment and perception of climate change as a threat in rural and urban areas. *Plos One*, 18(9), e0290354. https://doi.org/10.1371/journal.pone.0290354.

[27]   Han, M., Mahendran, R., & Yu, J. (2021). Associations between fear of COVID-19, affective symptoms and risk perception among community-dwelling older adults during a COVID-19 lockdown. *Frontiers in Psychology*, 12 (Article 638831). https://doi.org/10.3389/fpsyg.2021.638831.

[28]   He, S., Chen, S., Kong, L., & Liu, W. (2020). Analysis of risk perceptions and related factors concerning COVID-19 epidemic in Chongqing, China. *Journal of Community Health*, 46(2), 278-285. https://doi.org/10.1007/s10900-020-00870-4.

[29]   Matanggaran, V. &Gutteling, J. (2021). Explaining risk perception of climate change in Indonesia through cultural dimension of uncertainty avoidance, collectivistic, and long-term orientation. *International Journal of Research and Innovation in Social Science*, 05(05), 336-345. https://doi.org/10.47772/ijriss.2021.5519.

[30]   Tsasis, P. (2008). Vulnerability and risk perception in the management of HIV/AIDS: Public priorities in a global pandemic. *Risk Management and Healthcare Policy*, 2008(1), 7-14. https://doi.org/10.2147/rmhp.s4245.

[31]   Aung, K., Razak, R., &Nazry, N. (2023). Preparedness for the future pandemic: Understanding the impacts of risk perception in public health emergencies. *The Malaysian Journal of Nursing*, 14(4), 192-196. https://doi.org/10.31674/mjn.2023.v14i04.020.

[32]   Aycock, D., Clark, P., & Araya, S. (2017). Measurement and outcomes of the perceived risk of stroke: a review. *Western Journal of Nursing Research*, 41(1), 134-154. https://doi.org/10.1177/0193945917747856.

[33]   Yin, L. & Wu, Y. (2023). Opportunities or threats?: The role of entrepreneurial risk perception in shaping the entrepreneurial motivation. *Journal of Risk and Financial Management*, 16(1), 48. https://doi.org/10.3390/jrfm16010048.

[34]   Seo, M., Choi, J., Kim, K., & Choi, H. (2020). The relationship between risk perception of cell phones and objective knowledge of EMF in Korea. *International Journal of Environmental Research and Public Health*, 17(19), 7207. https://doi.org/10.3390/ijerph17197207.

[35]   Gu, J., He, R., Wu, X., Tao, J., Ye, W., & Wu, C. (2022). Analyzing risk communication, trust, risk perception, negative emotions, and behavioral coping strategies during the COVID-19 pandemic in China using a structural equation model. *Frontiers in Public Health*, 10 (Article 843787). https://doi.org/10.3389/fpubh.2022.843787.

[36] Ackert, L., Church, B., & Qi, L. (2020). Cross-cultural differences in the perception of portfolio risk. *Review of Economics and Finance*, 18, 19-30. https://doi.org/10.55365/1923.x2020.18.03.

[37] Heydari, S., Zarei, L., Sadati, A., Moradi, N., Akbari, M., Mehralian, G., … &Lankarani, K. (2021). The effect of risk communication on preventive and protective behaviours during the covid-19 outbreak: Mediating role of risk perception. *BMC Public Health*, 21(1). https://doi.org/10.1186/s12889-020-10125-5.

[38] Raue, M., D'Ambrosio, L., Ward, C., Lee, C., Jacquillat, C., & Coughlin, J. (2019). The influence of feelings while driving regular cars on the perception and acceptance of self-driving cars. *Risk Analysis*, 39(2), 358-374. https://doi.org/10.1111/risa.13267.

[39] Loewenstein, G., Weber, E., Hsee, C., & Welch, N. (2001). Risk as feelings. *Psychological Bulletin*, 127(2), 267-286. https://doi.org/10.1037/0033-2909.127.2.267.

[40] Huang, S., Zhou, C., Yuan, Q., Chen, G., & Shen, H. (2023). How do online users perceive health risks during public health emergencies?: Empirical evidence from China. *Frontiers in Psychology*, 14. https://doi.org/10.3389/fpsyg.2023.1087229.

[41] Fang, D., Fang, C., Tsai, B., Lan, L., & Hsu, W. (2012). Relationships among trust in messages, risk perception, and risk reduction preferences based upon avian influenza in Taiwan. *International Journal of Environmental Research and Public Health*, 9(8), 2742-2757. https://doi.org/10.3390/ijerph9082742.

[42] Costa-Font, M. & Roig, J. (2011). Does expert trust and factual knowledge shape individual's perception of science? *International Journal of Consumer Studies*, 36(6), 668-677. https://doi.org/10.1111/j.1470-6431.2011.01044.x.

[43] Nikolic, B. &Ružic-Dimitrijevic, L. (2013). Comparative analysis of two risk assessment methods in information systems.*Proceedings of Informing Science & IT Education Conference (InSITE) 2013*, 173-182.https://doi.org/10.28945/1842.

[44] Brell, T., Philipsen, R., &Ziefle, M. (2018). Scary! Risk perceptions in autonomous driving: The influence of experience on perceived benefits and barriers. *Risk Analysis*, 39(2), 342-357. https://doi.org/10.1111/risa.13190.

[45] Sun, Y. & Han, Z. (2018). Climate change risk perception in Taiwan: correlation with individual and societal factors. *International Journal of Environmental Research and Public Health*, 15(1), 91. https://doi.org/10.3390/ijerph15010091.

[46] Aksit, O., McNeal, K., Gold, A., Libarkin, J., & Harris, S. (2017). The influence of instruction, prior knowledge, and values on climate change risk perception among undergraduates. *Journal of Research in Science Teaching*, 55(4), 550-572. https://doi.org/10.1002/tea.21430.

[47] Ndamani, F. & Watanabe, T. (2017). Determinants of farmers' climate risk perceptions in agriculture—a rural Ghana perspective. *Water*, 9(3), 210. https://doi.org/10.3390/w9030210.

[48] Arya, B. & Kumar, H. (2023). An investigation of climate change, eco-anxiety and risk perception in the context of theory of planned behaviour. *IOP Conference Series Earth and Environmental Science*, 1279(1), 012020. https://doi.org/10.1088/1755-1315/1279/1/012020.

[49] You, M. &Ju, Y. (2020). The outrage effect of personal stake, familiarity, effects on children, and fairness on climate change risk perception moderated by political orientation. *International Journal of Environmental Research and Public Health*, 17(18), 6722. https://doi.org/10.3390/ijerph17186722.

[50] Botzen, W., Michel-Kerjan, E., Kunreuther, H., Moel, H., & Aerts, J. (2016). Political affiliation affects adaptation to climate risks: Evidence from New York City. *Climatic Change*, 138(1-2), 353-360. https://doi.org/10.1007/s10584-016-1735-9.

[51] Linden, S., Leiserowitz, A., Feinberg, G., & Maibach, E. (2015). The scientific consensus on climate change as a gateway belief: Experimental evidence. *Plos One*, 10(2), e0118489. https://doi.org/10.1371/journal.pone.0118489.

[52] Fasolin, G., Spektor, M., Marques, R., & Camargo, J. (2023). Correlates of climate change risk perception: Evidence from Latin America (preprint). https://doi.org/10.21203/rs.3.rs-3328562/v1.

[53] Liu, T., Shryane, N., & Elliot, M. (2022). Attitudes to climate change risk: Classification of and transitions in the UK population between 2012 and 2020. *Humanities and Social Sciences Communications*, 9(1). https://doi.org/10.1057/s41599-022-01287-1.

[54] Larraza-Kintana, M., Wiseman, R., Gómez-Mejía, L., & Welbourne, T. (2007). Disentangling compensation and employment risks using the behavioral agency model. *Strategic Management Journal,* 28(10), 1001-1019. https://doi.org/10.1002/smj.624.

[55] Aabo, T. & Eriksen, N. (2018). Corporate risk and the humpback of CEO narcissism. *Review of Behavioral Finance,* 10(3), 252-273. https://doi.org/10.1108/rbf-07-2017-0070.

[56] Gacar, B. &Gacar, A. (2021). Determination of corporate risk management application level: a survey in Manisa province. *Dokuz Eylül ÜniversitesiSosyalBilimlerEnstitüsüDergisi*, 23(2), 605-626. https://doi.org/10.16953/deusosbil.854268.

[57] Kanu, M. (2020). Integrating enterprise risk management with strategic planning for improved firm performance. *European Journal of Business Management and Research*, 5(5), 1-11. https://doi.org/10.24018/ejbmr.2020.5.5.488.

[58] García-Granero, A., Llopis, Ó., Fernández-Mesa, A., & Alegre, J. (2015). Unraveling the link between managerial risk-taking and innovation: the mediating role of a risk-taking climate. *Journal of Business Research*, 68(5), 1094-1104. https://doi.org/10.1016/j.jbusres.2014.10.012.

[59] Sun, X., Ci, F., Cifuentes-Faura, J., & Liu, X. (2024). Firm-level climate risk and corporate violations: Perspective of corporate managers' pressure perception. *Managerial and Decision Economics*, 45(8), 5430-5448. https://doi.org/10.1002/mde.4323.

[60] Bunde, T., Eisentraut, S., Johnson, J., Knapp, N., Carr, R., Hammelehle, J., Kump, I., Miehe, L., & Mudie-Mantz, A. (2022).Munich Security Index 2022, Munich: Munich Security Conference, February 2022, https://securityconference.org/en/publications/munich-security-index-2022/.

[61] Bunde, T., Eisentraut, S., Johnson, J., Knapp, N., Lubbock, T., & Schütte, L. (2023).*Munich Security Index 2023*, Munich: Munich Security Conference, February 2023. https://securityconference.org/en/publications/munich-security-report-2023/munich-security-index-2023/.

[62] Bunde, T., Eisentraut, S., Johnson, J., Knapp, N., Lubbock, T., & Schütte, L. (2024).*Munich Security Index 2024*, Munich: Munich Security Conference, February 2024, https://securityconference.org/en/munich-security-report-2024/munich-security-index-2024/.

[63] Bunde, T., Eisentraut, S., & Schütte, L. (2025).Munich Security Index 2025, Munich: Munich Security Conference, February 2025, https://securityconference.org/en/publications/munich-security-report-2025/munich-security-index-2025/.

[64] Bunde, T., Eisentraut, S., Knapp, N., Carr, R., Hammelehle, J., Kump, I., Miehe, L., & Mudie-Mantz, A. (2022). *Munich Security Report 2022: Turning the Tide – Unlearning Helplessness*, Munich: Munich Security Conference, February 2022, https://doi.org/10.47342/QAWU4724.

[65] Bunde, T., Eisentraut, S., Johnson, J., Knapp, N., Lubbock, T., & Schütte, L. (2023).*Munich Security Report 2023: Re: Vision*, Munich: Munich Security Conference, February 2023. https://doi.org/10.47342/ZBJA9198.

[66] Bunde, T., Eisentraut, S., Johnson, J., Knapp, N., Lubbock, T., & Schütte, L. (2024). *Munich Security Conference Report 2024: Lose-Lose?*, Munich: Munich Security Conference, February 2024. https://doi.org/10.47342/BMQK9457.

[67] Bunde, T., Eisentraut, S., & Schütte, L. (2025). *Munich Security Report 2025: Multipolarization*, Munich: Munich Security Conference, February 2025, https://doi.org/10.47342/EZUC8623.

[68] Judijanto, L., Rahardian, R., Muthmainah, H., &Erkamim, M. (2023). Analysis of threat detection, prevention strategies, and cyber risk management for computer network security in government information systems in Indonesia. *West Science Information System and Technology*, 1(02), 90-98. https://doi.org/10.58812/wsist.v1i02.479.

[69] Challa, N. (2022). Unveiling the shadows: A comprehensive exploration of advanced persistent threats (APTS) and silent intrusions in cybersecurity. *Journal of Artificial Intelligence & Cloud Computing,* 1(4), 1-5. https://doi.org/10.47363/jaicc/2022(1)190.

[70] Ayers, J. (2020). Automated image analysis of Instagram posts: implications for risk perception and communication in public health using a case study of #HIV. *Plos One*, 15(5), e0231155. https://doi.org/10.1371/journal.pone.0231155.

[71] Alraddadi, A. (2023). Developing an abstraction framework for managing and controlling Saudi banks' cybersecurity threats based on the NIST cybersecurity framework and ISO/IEC27001. *Journal of Software Engineering and Applications*, 16(12), 695-713. https://doi.org/10.4236/jsea.2023.1612036.

[72] Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., … & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, 21(15), 5119. https://doi.org/10.3390/s21155119.

[73] Khalifa, N. (2020). Identification and prevention of expected cybersecurity threats during 2022 FIFA World Cup in Qatar. *Journal of Poverty Investment and Development*, 5(1), 49-84. https://doi.org/10.47604/jpid.1135.

[74] Silaule, C., Makhubele, L., & Mamorobela, S. (2022). A model to reduce insider cybersecurity threats in a South African telecommunications company. *South African Journal of Information Management*, 24(1), a1573. https://doi.org/10.4102/sajim.v24i1.1573.

[75] Peinado, S., Treiman, K., Uhrig, J., Taylor, J., & Stryker, J. (2020). Effectively communicating about HIV and other health disparities: Findings from a literature review and future directions. *Frontiers in Communication*, 5(1), 1-16. https://doi.org/10.3389/fcomm.2020.539174.

[76] Kim, S., Lee, J., & Oh, P. (2023). Questioning AI: How racial identity shapes the perceptions of algorithmic bias (preprint). https://doi.org/10.31234/osf.io/afcdn.

[77] Camacho, N. (2024). The role of AI in cybersecurity: Addressing threats in the digital age. *Journal of Artificial Intelligence General Science*, 3(1), 143-154. https://doi.org/10.60087/jaigs.v3i1.75.

[78] Nazir, I. & Tiwari, S. (2023). Impact of machine learning in cybersecurity augmentation.*QTanalytics Publication (Books)*, 147-154. https://doi.org/10.48001/978-81-966500-9-4_12.

[79] Mobin, M., Hassan, M., Khalid, A., & Abdul-Rahim, R. (2022). COVID-19 pandemic and risk dynamics of financial markets in G7 countries. *International Journal of Islamic and Middle Eastern Finance and Management,* 15(2), 461-478. https://doi.org/10.1108/imefm-09-2021-0358.

[80] Khojah, M., Ahmed, M., Khan, M., Haddad, H., Al-Ramahi, N., & Khan, M. (2023). Economic policy uncertainty and stock market in G7 countries: A panel threshold effect perspective. *Plos One*, 18(7), e0288883. https://doi.org/10.1371/journal.pone.0288883.

[81] Wulandari, N., Adnan, M., &Wicaksono, C. (2022). Are you a soft target for cyber attacks?:Drivers of susceptibility to social engineering-based cyber attack (SECA): A case study of mobile messaging application. *Human Behavior and Emerging Technologies*, 2022, 1-10. https://doi.org/10.1155/2022/5738969.

[82] Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. (2022). Digital healthcare - cyberattacks in Asian organizations: An analysis of vulnerabilities, risks, NIST perspectives, and recommendations. *IEEE Access*, 10, 12345-12364. https://doi.org/10.1109/access.2022.3145372.

[83] Sarker, S. and Khan, R. (2024). Cybersecurity considerations for smart Bangladesh: Challenges and solutions. *Asian Journal of Research in Computer Science*, 17(6), 145-156. https://doi.org/10.9734/ajrcos/2024/v17i6464.

[84] Perälä, P. & Lehto, M. (2024). Educating cybersecurity experts: Analysis of cybersecurity education in Finnish universities. *European Conference on Cyber Warfare and Security*, 23(1), 371-378. https://doi.org/10.34190/eccws.23.1.2256.

[85] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119, 102754. https://doi.org/10.1016/j.cose.2022.102754.

[86] Gabbiadini, A., Durante, F., Baldissarri, C., & Andrighetto, L. (2024). Artificial intelligence in the eyes of society: assessing social risk and social value perception in a novel classification. *Human Behavior and Emerging Technologies*, 2024, 1-11. https://doi.org/10.1155/2024/7008056.

[87] Kerstan, S., Bienefeld, N., & Grote, G. (2023). Choosing human over AIdoctors?: How comparative trust associations and knowledge relate to risk and benefit perceptions of ai in healthcare. *Risk Analysis*, 44(4), 939-957. https://doi.org/10.1111/risa.14216.

[88] Isaksen, A., Schaarup, J., Bjerg, L., &Hulmán, Á. (2025). Changes in public perception of AI in healthcare after exposure to ChatGPT (preprint). https://doi.org/10.1101/2025.01.23.25321048.

[89] Wen, C. & Chen, Y. (2024). Understanding public perceptions of revolutionary technology: The role of political ideology, knowledge, and news consumption. *Journal of Science Communication*, 23(5), A07. https://doi.org/10.22323/2.23050207.

[90] Alehile, K., Ebeh, J., Sani, I., &Opaluwa, H. (2024). Probing the interplay between climate change and global energy security: Insights from nonlinear analysis. *Energy Research Letters*, 5(4). https://doi.org/10.46557/001c.94675.

[91] Nadeau, C., Milkoreit, M., Eriksen, T., & Hessen, D. (2023). Missing the (tipping) point: The role of climate tipping points on public risk perceptions in Norway.*Earth Systems Dynamics*, 15(4), 969–985. https://doi.org/10.5194/esd-2023-23.

[92] Murfree, J. (2023). Exploring major league baseball fans' climate change risk perceptions and adaptation willingness. *Sustainability*, 15(10), 7980. https://doi.org/10.3390/su15107980.

[93]   Formanski, F., Pein, M., Loschelder, D., Engler, J., Husen, O., & Majer, J. (2022). Tipping points ahead?: How laypeople respond to linear versus nonlinear climate change predictions. *Climatic Change*, 175(1-2). https://doi.org/10.1007/s10584-022-03459-z.

[94]   Chen, Y., Zhou, Y., Raza, S., & Sarwar, S. (2023). What we learn from nexus between greener growth and energy-related emissions: Sustainability perspective evidence in context of financial globalization. *Geological Journal*, 59(2), 595-611. https://doi.org/10.1002/gj.4883.

[95]   Li, C. (2025). The evolution of food security in Japan - based on an indicator evaluation system including climate change indicators. *Plos One*, 20(2), e0317180. https://doi.org/10.1371/journal.pone.0317180.

[96]   Stolero, N., Elkady, S., Labaka, L., Tov, M., Peleg, K., & Adini, B. (2024). Do first responders and populations perceive risks similarly?: A comparative study of seven countries. *Frontiers in Psychology*, 14. https://doi.org/10.3389/fpsyg.2023.1219927.

[97]   Marthoenis, M. (2025). The January 2025 Southern California Wildfires: Public mental health impacts and a call to action. *Asian Journal of Public Health and Nursing*, 1(3). https://doi.org/10.62377/fdtqx765.

[98]   Gimello-Mesplomb, F. (2025). Decoding January 2025 Los Angeles Wildfires: How (and why) the emotional power of iconic fires revives ancestral fears and fuels misinformation (preprint). https://doi.org/10.33767/osf.io/p6cfn.

[99]   Arias, S. & Blair, C. (2024). In the eye of the storm: Hurricanes, climate migration, and climate attitudes. *American Political Science Review*, 118(4), 1593-1613. https://doi.org/10.1017/s0003055424000352.

[100]   Hogue, A. & Breon, K. (2022). The greatest threats to species. *Conservation Science and Practice*, 4(5), e12670. https://doi.org/10.1111/csp2.12670.

[101]   Dong, K., Liu, Z., Li, Y., Chen, Z., Hou, G., & Sun, J. (2022). Comparing the effectiveness of biodiversity conservation across different regions by considering human efforts. *Frontiers in Ecology and Evolution*, 10. https://doi.org/10.3389/fevo.2022.855453.

[102]   Zhang, A., Yang, H., Tian, Z., & Tong, S. (2022). Evolution model and simulation study of the public risk perception of COVID-19. *International Journal of Environmental Research and Public Health*, 19(18), 11581. https://doi.org/10.3390/ijerph191811581.

[103]   Wang, Y., Zhao, R., Li, Y., Yao, R., Wu, R., & Li, W. (2023). Spatial and temporal heterogeneity of rural habitat level evolution and its influencing factors—a case study of rural villages in nature a reserve of China. *Sustainability*, 15(7), 5775. https://doi.org/10.3390/su15075775.

[104]   Duan, H., Yu, X., Kai, S., Zhang, C., & Liu, H. (2022). Effects of habitat loss on migratory shorebird community structure at stopover sites: a case study in the Yellow River Delta, China. *Frontiers in Marine Science*, 9. https://doi.org/10.3389/fmars.2022.1049765.

[105]   Wang, J., Abulizi, A., Mamitimin, Y., Mamat, K., Yuan, L., Bai, S., … & Shen, F. (2024). Spatiotemporal evolution of habitat quality and scenario modeling prediction in the Tuha region. *Land*, 13(7), 1005. https://doi.org/10.3390/land13071005.

[106]   Liu, Y., Wang, Y., Lin, Y., Ma, X., Guo, S., Ouyang, Q., … & Sun, C. (2023). Habitat quality assessment and driving factors analysis of Guangdong Province, China. *Sustainability*, 15(15), 11615. https://doi.org/10.3390/su151511615.

[107]   Isaksen, A., Schaarup, J., Bjerg, L., &Hulmán, Á. (2025). Changes in public perception of AI in healthcare after exposure to ChatGPT (preprint). https://doi.org/10.1101/2025.01.23.25321048.

[108]   Araujo, T., Helberger, N., Kruikemeier, S., & Vreese, C. (2020). In AI we trust?: Perceptions about automated decision-making by artificial intelligence. *AI& Society*, 35(3), 611-623. https://doi.org/10.1007/s00146-019-00931-w.

[109]   Han, P., Tong, Z., Sun, Y., & Chen, X. (2022). Impact of climate change beliefs on youths' engagement in energy-conservation behavior: The mediating mechanism of environmental concerns. *International Journal of Environmental Research and Public Health*, 19(12), 7222. https://doi.org/10.3390/ijerph19127222.

[110]   Eitzinger, A., Binder, C., & Meyer, M. (2018). Risk perception and decision-making: Do farmers consider risks from climate change? *Climatic Change*, 151(3-4), 507-524. https://doi.org/10.1007/s10584-018-2320-1.

[111]   Poortinga, W., Whitmarsh, L., Steg, L., Böhm, G., & Fisher, S. (2019). Climate change perceptions and their individual-level determinants: A cross-European analysis. *Global Environmental Change*, 55, 25-35. https://doi.org/10.1016/j.gloenvcha.2019.01.007.

[112] Ruz, M., Rufin-Soler, C., Héquette, A., Révillon, R., Hellequin, A., Deboudt, P., … & Marin, D. (2020). Climate change and risk perceptions in two French coastal communities. *Journal of Coastal Research*, 95(sp1), 875-879. https://doi.org/10.2112/si95-170.1.

[113] Huang, H., Kerstein, J., Wang, C., & Wu, F. (2022). Firm climate risk, risk management, and bank loan financing. *Strategic Management Journal*, 43(13), 2849-2880. https://doi.org/10.1002/smj.3437.

[114] Ejelöv, E., Hansla, A., Bergquist, M., & Nilsson, A. (2018). Regulating emotional responses to climate change – A construal level perspective. *Frontiers in Psychology*, 9. https://doi.org/10.3389/fpsyg.2018.00629.

[115] Dawid, I. & Mohammed, F. (2022). Review on the link between technological change, climate finance, and market in mitigating climate change. International *Journal of Weather Climate Change and Conservation Research,* 8(1), 1-5. https://doi.org/10.37745/ijwcccr.15/vol8n1pp15.

[116] Reyes, R., Nguyen, V., Schott, S., Berseth, V., Hutchen, J., Taylor, J., … & Klenk, N. (2021). A research agenda for affective dimensions in climate change risk perception and risk communication. *Frontiers in Climate*, 3. https://doi.org/10.3389/fclim.2021.751310.

[117] Ginglinger, E. & Moreau, Q. (2023) Climate Risk and Capital Structure. *Management Science*, 69(12), 7492-7516.https://doi.org/10.1287/mnsc.2023.4952

[118] Landi, G., Iandolo, F., Renzi, A., & Rey, A. (2022). Embedding sustainability in risk management: The impact of environmental, social, and governance ratings on corporate financial risk. *Corporate Social Responsibility and Environmental Management*, 29(4), 1096-1107. https://doi.org/10.1002/csr.2256.

[119] Raji, E., Ijomah, T., &Eyieyien, O. (2024). Integrating technology, market strategies, and strategic management in agricultural economics for enhanced productivity. *International Journal of Management & Entrepreneurship Research*, 6(7), 2112-2124. https://doi.org/10.51594/ijmer.v6i7.1260.

[120] Abdelsadek, P. (2023). The role of strategic management accounting tools in developing accounting measurement and disclosure for the effects of climate changes. *International Journal of Accounting and Management Sciences*, 2(1), 1-29. https://doi.org/10.56830/eyof5574.

[121] Oriekhova, K., Golovko, O., & Gayda, P. (2022). Strategic provising of enterprise financial security in COVID-19 conditions. *Social Economics*, (64), 63-78. https://doi.org/10.26565/2524-2547-2022-64-07.

[122] Chmutova, I. &Hainalii, A. (2024). Transformations in the global risk landscape: Considerations for strategic risk management system development. *Modeling the Development of the Economic Systems*, (4), 328-337. https://doi.org/10.31891/mdes/2024-14-43.

[123] Ahmad, A. Y., Kumar, B., Sharma, J., Khan, K., Pramanik, S., Mohammad, F., & Prasad, K. K. (2025). Analyzing the impact of economic trends on hospitality security strategies. In A. Derbali (Ed.), *AI, Economic Perspectives, and Firm Business Management* (pp. 121-142). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-7357-6.ch007.

[124] Jiao, Z. &Kurbanbaeva, A. (2024). Innovative approaches in the system of anti-crisis management of agricultural enterprises. *IzdenisterNatigeler*, 2 (102), 593-600. https://doi.org/10.37884/2-2024/59.

[125] Phiri, F. (2024). Impact of climate change risk management strategies on child protection systems in Zambia: A case study on Mansa district of luapula province. *Texila International Journal of Management*. 10(2), 1-15. https://doi.org/10.21522/tijmg.2015.10.02.art001.

[126] Us, Y. &Lytovchenko, V. (2024). Implementation of the strategy for managing the energy security of enterprises in the context of growing instability: the organizational aspect. *Business Inform*, 9(560), 313-320. https://doi.org/10.32983/2222-4459-2024-9-313-320.

[127] Ye, W. & Li, M. (2022). Are we vulnerable?: Climate risk perception and vulnerability of small and medium size agricultural enterprises in China. *Asian Social Research: CMU Journal of Social Sciences and Humanities*, 9(2). https://doi.org/10.12982/cmujasr.2022.006.

[128] Tin, D., Granholm, F., Guirguis, M., Almulhim, M., &Ciottone, G. (2024). Integrating disaster and dignitary medicine principles into a medical framework for organizational travel health and security planning. *Prehospital and Disaster Medicine*, 39(3), 233-235. https://doi.org/10.1017/s1049023x2400044x.

[129] Liu, H. &Rahimzhanova, G. (2024). Strategic approaches to corporate governance: Prospects for ensuring economic security. *IzdenisterNatigeler*, (2 (102), 572-579. https://doi.org/10.37884/2-2024/56.

[130] Naab, J. & Amusa, O. (2024). Mitigating security risks in global supply chains: the role of strategic communication and criminological approaches in countering illicit trade and cyber threats. *Computer Science & IT Research Journal*, 5(9), 2197-2215. https://doi.org/10.51594/csitrj.v5i9.1579.

AUTHOR

David C. Wyld (dwyld@selu.edu) is the Merritt Professor of Strategic Management at Southeastern Louisiana University in Hammond, Louisiana. He is a management consultant, researcher/writer, publisher, executive educator, and experienced expert witness.