



Synchronized Coevolution: A Conceptual Framework for Sustaining a Human-Centered Security Culture in AI-Driven Environments

Spiros Katiforis

2024 Laurea





Laurea University of Applied Sciences

**Synchronized Coevolution: A Conceptual Framework for
Sustaining a Human-Centered Security Culture in AI-Driven
Environments**

Spiros Katiforis
M.B.A in Leading Transformational Change
Thesis
September 2024

Spiros Katiforis

Synchronized Coevolution: A Conceptual Framework for Sustaining a Human-Centered Security Culture in AI-Driven Environments

Year	2024	Number of pages	101
------	------	-----------------	-----

The present study explores how a human-centered security culture can be sustained within modern business environments progressively affected by artificial intelligence applications. The primary objective of this study is to develop a comprehensive framework that outlines the actions required to foster a human-centered security culture. The study is relevant for business organizations that need to adopt a human-centered philosophy in developing security culture programs.

This thesis is grounded in an extensive review of existing literature in the domains of security, culture, AI technologies, ethics, sustainability, and data privacy. Insights from these areas are combined with the author’s experience in the field to produce an innovative framework that embraces the complexity of today’s business landscapes.

To investigate this complex subject, a qualitative method involving in-depth interviews is employed. An extensive literature review complements this methodology to ensure a comprehensive exploration of the topic.

The outcome of this study is a conceptual framework that will contain essential components and key performance indicators designed to assess the efficacy of human-centered security culture practices within AI-driven environments. This framework can potentially support organizations in ensuring that a human-centered approach is adopted while leveraging the advantages of AI technologies in modern business environments.

Keywords: security, culture, AI, human-centered, framework

Contents

1	Introduction	7
1.1	Background.....	7
1.2	Purpose, Objective, and Research Questions	7
1.3	Research Methods	8
1.4	Scope and Limitations	9
2	Literature Review	10
2.1	Analysis of Security Culture and its value to organizations	11
2.2	The Importance of Corporate Responsibility and Sustainability.....	15
2.3	Exploration of AI technologies and their security applications and implications .	18
2.4	Reviewing existing literature on security culture in AI-driven environments	22
2.5	Chapter Summary	23
3	Research and Development Methodology	24
3.1	Research Setting, Process, and Implementation.....	25
3.2	Research Parameters	27
3.3	Framework Design.....	29
3.4	Interview Protocol and Questions.....	30
3.5	Methodological Limitations	31
4	Building the Framework	32
4.1	Framework Variables	32
4.2	Framework Visualization	35
4.3	Framework Narration	36
5	Interviews	39
5.1	Participant Interviews	40
5.2	Interviewing the AI	50
6	Findings	52
6.1	Summary and Examination of Collected Data	52
6.2	Refining the framework	55
6.3	Addressing the Research Questions.....	60
6.4	Recommendations.....	62
7	Discussion.....	63
	References	64
	Figures	101
	Tables.....	101
	Appendix	101

1 Introduction

1.1 Background

The emergence of artificial intelligence (AI) technologies signals the beginning of a revolution across various fields, transforming the way people perceive and interact with their environment. One of the domains that are intensely impacted by AI advancements is security culture. The increased sophistication and widespread adoption of AI systems has made their integration both an opportunity and a challenge for organizations that desire to achieve a balance between technology and human values, while sustaining a strong security culture.

1.2 Purpose, Objective, and Research Questions

This chapter establishes the groundwork for the present thesis, outlining its purpose, objective, and research questions. The motivation for conducting this study stems from the drive to attain an equilibrium between integrating advanced technology in business environments (and, in extension, society itself) and preserving human rights and well-being, fostering a balanced coexistence of technology and humanity.

This thesis aims to investigate how a human-centered security culture can be sustained in business environments where AI solutions are installed and used to monitor and influence human behavior.

The present thesis's main objective is to develop a framework that defines the required principles and sets the foundation required to sustain a strong security culture which protects the organization's assets while focusing on human rights and well-being.

To attain its objective, the study is structured around the following research questions:

Research Question 1: What are the key challenges and opportunities in integrating AI technologies into security culture methods while sustaining a human-centered approach?

Research Question 2: What strategies can business organizations implement to ensure that AI-driven technologies prioritize human rights and well-being?

Research Question 3: What measurable Key Performance Indicators (KPIs) can be developed to evaluate the balance between AI-driven security solutions and human-centered values while accomplishing the organization's business goals?

1.3 Research Methods

The primary research approach of the present study is qualitative. In-depth interviews will be conducted with Subject Matter Experts (SMEs) from the security culture, HR, and AI technology fields, and the transcriptions will be analyzed in order to formulate a practical framework using an inductive approach, starting from data collection and analysis before transferring from particular examples to general conclusions.

The literature review offers significant insights into the existing knowledge base around the research topic. It presents a thorough examination of the existing research and key findings, and plays a crucial role in identifying gaps, and emerging trends in the current literature, by combining and critically analyzing a wide range of publications.

Research Question 1 will be approached theoretically by conducting a literature review. This review, which will be limited to the scope of the present thesis, will examine existing research on security culture and AI technologies, their correlation, applications, and associated implications. Its aim is to pinpoint the main challenges and opportunities related to integrating AI-driven solutions into security culture methods in business environments while remaining focused on human-centered values.

Research Question 2 will be addressed through qualitative methods, with a particular emphasis on conducting in-depth interviews with experts in security culture, AI technologies, and human resources. The interview questions will be formulated to explore the feasibility of strategies that enable AI solutions to advance human rights. The data collected from the interviews will be cross-analyzed with the conceptual framework that will be developed and the final result will be a refined framework that organizations can incorporate in their strategies to ensure that AI-driven technologies prioritize human rights and well-being.

Research Question 3 will be addressed by developing Key Performance Indicators (KPIs) to assess the final framework's effectiveness. These KPIs will focus on quantifiable outcomes, such as the reduction in security incidents through the efficiency of AI-driven threat detection, leadership commitment and employee engagement as well as compliance with applicable regulations.

1.4 Scope and Limitations

This study aims to investigate the subject of sustaining a human-centered security culture within environments increasingly influenced and powered by artificial intelligence (AI) technologies.

The study is based on the hypothesis that the continued technological advancements may reach a stage where AI solutions could potentially threaten human liberties within business environments. This hypothesis has its foundation in prior research and will undergo testing within the context of this study.

The study explores how security culture and AI-driven systems can be connected, focusing on measures that protect human rights and well-being, involving a multidisciplinary approach, drawing from cybersecurity, ethics, technology, and organizational behavior.

The aimed outcome of this study will be the development of a framework that business organizations can use to ensure a human-centered security culture can be sustained despite the technological advancements in these environments.

While the present research is extensive in its coverage, certain limitations must be acknowledged. Firstly, the study may be constrained by the availability of experts and participants willing to engage in interviews. Second, the research primarily focuses on the perspectives and experiences of professionals, potentially limiting the exploration of end-user perspectives. Additionally, the study's findings may be influenced by the evolving nature of AI technologies and the rapid pace of change in this field. Furthermore, while efforts will be made to ensure a diverse participant pool, the research may be limited by the geographical and cultural backgrounds of the respondents. Lastly, the scope of this thesis may cover only some aspects of the broader topic of AI ethics and security, necessitating future research to address additional sides of this evolving field.

Finally, this study is not intended to serve as an exhaustive technical examination of AI technologies; instead, it aims to provide a holistic view of the ethical and human-centered considerations around the integration of AI in business environments. While technical aspects are being addressed to some extent, the primary focus is on AI adoption's ethical, social, and organizational implications.

2 Literature Review

To develop a sustainable human-centered security culture in Artificial Intelligence (AI)-driven environments, specific terms must first be defined before deep-diving into the existing literature, such as organizational and security culture, corporate sustainability, AI technologies, and ethics. I have defined the terms below based on the literature reviewed later.

By organizational culture, within a business organization environment, we usually refer to the values, norms, beliefs, practices, and behaviors that form an organization's identity. Organizational culture is critical, as it defines the way an organization operates. Cultural characteristics may vary among organizations and can influence how employees behave, and how business goals are approached.

Security culture is the values, behaviors, and practices that help protect and keep an organization viable. In the security terminology, the fundamental security elements are Confidentiality, Integrity, and Availability (CIA). Confidentiality entails the measures that protect sensitive data from unauthorized access, Integrity ensures that data remains unaltered throughout its lifecycle, and Availability safeguards the accessibility and usability of resources. For an organization to stay secure, it must ensure that all three security aspects are adequately addressed. Security entails mitigating risks and threats, resilience from incidents, compliance, and protecting assets such as employees, data, and equipment. By establishing a security culture, organizations foster a mindset of security and sustainability for employees.

Corporate responsibility and corporate social responsibility (CSR) represent an organization's commitment to conducting its business ethically and responsibly, considering its operations' social, environmental, and economic impact. CSR involves a company voluntarily going beyond compliance with minimum legal requirements and actively engaging in actions that benefit society, the environment, and its stakeholders.

Corporate sustainability refers to incorporating social, ethical, and environmental considerations into an organization's strategy to maintain its long-term feasibility. An extensive body of literature has already been dedicated to corporate sustainability and the complexity introduced by phenomena such as climate change and population growth.

One of the main focus areas of this thesis literature review is the investigation of existing literature and identification of possible gaps concerning AI technology's role in corporate sustainability by adopting a human-centered perspective.

Artificial Intelligence (AI) technologies refer to the capacity of computers to carry out activities that traditionally require human intelligence. These technologies aim to emulate human performance and, in many cases, mitigate human biases and surpass human capabilities.

Ethics is the science that examines the moral principles, values, and standards that guide human behavior and decision-making. It involves distinguishing between right and wrong, and offers a structure for individuals and groups to make ethical judgments and choices based on principles such as honesty, fairness, integrity, and respect for the well-being and rights of others. Ethics is a fundamental aspect of human society, influencing personal conduct, professional behavior, and societal norms.

This chapter attempts to conduct a comprehensive literature search in security culture, corporate responsibility, and sustainability, the applications and implications of AI technologies in the security field, and the existing documentation in human-centered security culture in AI-driven environments. Identifying inspiring ideas as well as possible gaps will contribute to shaping a novel framework for developing security culture programs in AI-driven business environments.

2.1 Analysis of Security Culture and its value to organizations

Securing an organization involves protecting its assets, data, and employees from any harm. Whitman and Mattord (2012) explain that an organization should apply several layers of security to be protected. These include Physical security (protection of premises, objects, and areas), Personnel security (protection of individuals), Operations security, Information security, and more. Organizations rely on policies, technical solutions, and employees to maintain a secure workplace and secure critical assets from threats such as unauthorized data access, data breaches, malware attacks, social engineering, and others.

Technical solutions such as sophisticated intrusion detection software, firewalls, antivirus software, physical security measures such as personalized badges and CCTV, and policies and guidelines focusing on securing the organizations are known as security controls. These controls have as their main purpose to detect and prevent malicious actions from outsiders and even insiders that can compromise the confidentiality, integrity, and availability of assets and undermine the organization's security.

Despite the technological advancements in the security field and the comprehensive security policies and guidelines developed by security experts, the increasingly evolving threats challenge organizations to maintain the security and safety of their assets and data.

Even though security professionals develop strong security policies that describe proper employee behavior regarding security, the company's users themselves (usually unconsciously) cause damage by not following the security rules (Carpenter, 2019). In his book "Transformational Security Awareness," Carpenter supports that "humans are the most important part of your cybersecurity program." Humans actively participate in every aspect of developing a security program. According to Carpenter, even if technology advances rapidly, a team of humans will decide which technology solution to acquire, how it will be configured, and where, when, and how it will be used.

That makes the human factor the most impactful to an organization's security program. Carpenter continues by indicating that most security incidents occur due to employees' lack of security awareness. Some examples of human errors that have repeatedly led to security breaches are loss of paperwork and devices, accidental data disclosure, poor choice of passwords, and failure to identify phishing attempts. Hadnagy and Fincher (2015) elaborate on the methods attackers use to manipulate and deceive individuals into providing sensitive information, known as phishing.

Roer (2015) claims no universally accepted definition of "security awareness" exists. Security awareness refers to understanding risks, threats, and best practices that help employees make informed decisions to protect themselves and the organization. For most organizations, security awareness programs are mandatory training that employees must undergo but are usually very generic and do not have great results, and this is because awareness is mainly related to a person's knowledge and understanding. However, it does not entail their actions and behaviors.

Security culture goes beyond awareness, relating to the beliefs, values, and behaviors that reflect an organization's commitment to security. An effective security culture must be built into everyone's daily actions, decisions, and attitudes. This fosters a sense of responsibility and accountability and requires everyone's participation. According to Roer, the elements that collaboratively compose security culture are technology, policies/rules, and people/competence. Policies are documented policies that employees must respect and follow and the unwritten rules that regulate their behaviors. Technology refers to all the tools that humans use to perform tasks and the models and frameworks they follow. People are the ones who are developing the policies and making use of the tools. Cultural influences shape how someone formulates their policies and applies technology, which means that different organizations may have different perspectives on maintaining a secure environment. Culture encompasses the people's competence in how to use technology and behave.

Roer supports that each of these elements directly affects the other two, and every change in one of them impacts the other two elements. Understanding the underlying reasons behind the development of an inadequate security culture is imperative. Zinatullin (2016) claims that bad behaviors are usually contagious. In other words, if employees watch their colleagues act in ways that increase security risk, there is a high possibility that they will adopt those bad habits. Initial minor offenses can evolve into serious security breaches, so understanding how security is perceived within an organization can help shape the appropriate culture. To assess the situation accurately, the lens of psychological science must be used to grasp the fundamental drivers behind unethical conduct. It has been observed that to accomplish a task, people usually follow the easiest route, and if that means that security needs to be circumvented, then that is what most will choose to do.

Even though most of the employees of an organization will never consider stealing expensive equipment from their workplace, they may need to realize that failing to lock their computer when briefly leaving their desk is also a breach of the security policy.

Zinatullin supports that the first step in successfully establishing a security culture is to illustrate to employees that security is there to simplify their lives and not to create more challenges. In their book “The Security Culture Playbook” (2022), Roer and Carpenter observe that since technology is developing rapidly and the security controls in place that provide defense against attacks are getting stronger and stronger, it is now challenging and costly for hackers and other malicious users to bypass an organization’s security. That is the reason why they focus on the weakest link, which is the human. It can be remarkably effortless and cost-effective to take advantage of human vulnerabilities. It only takes a single employee to fall for deception and provide sensitive data to the attacker, and the whole organization can be at risk. One of the common strategies hackers employ is spreading malicious software known as “Ransomware,” which, once activated on an employee’s machine, can encrypt all files and render them useless without the decryption key, for which the attacker demands a ransom payment in exchange. Roer and Carpenter support that security culture has seven interdependent dimensions: Attitudes, Behaviors, Cognition, Communication, Compliance, Norms, and Responsibilities. By measuring these dimensions within an organization, we can obtain a precise depiction of its security culture. The authors emphasize the steps required to develop a robust security culture. First, the culture must match and support the business strategy, as carefully considering business objectives is essential. Furthermore, a clear mapping of the current culture needs to be crafted to identify the strengths and gaps. Finally, developing the security culture needs to be treated as a business challenge rather than a personnel issue, as the established policies and processes usually drive unneeded behaviors.

Roer and Carpenter suggest the adoption of a security culture framework (SCF), which is divided into three main phases: Measure, Involve, and Engage. During the first phase, the organization must map its current security culture state, decide the desired state, and identify the gaps between them. The second phase includes involving the higher management, as well as all the relevant stakeholders, using storytelling to effectively communicate risks and the ideas of how to overcome these risks. The last phase includes the various initiatives, activities, and content being shared with the different groups of stakeholders. The security culture emerges through these activities and the iterative process of measuring, involving, and engaging (Roer and Carpenter, 2012).

Cerra (2019) proposes a new way of thinking called “W.I.S.D.O.M (What I'll Say (and Do) Differently On Monday),” which can be applied by the different teams within a business environment to promote behavioral and cultural change by evaluating and rectifying bad habits that lead to unwanted results. The author supports that this methodology is suitable across various business domains, enhancing the organizational culture.

Hayden (2016) affirms that to understand and transform culture, we need to be able to “hack” it, using the term in its original meaning of breaking it down and identifying its key components. Considering that the overwhelming majority of security incidents arise from human actions, Hayden explains why human-centered security has yet to catch on but also highlights the necessity of adopting new perspectives and inspiring security-driven behaviors. He additionally supports that security culture requires everyone's contribution to succeed, from security practitioners to executives and from software developers to HR employees. To map the cultural threats to security, Hayden introduces a model known as PEPL, which is an abbreviation for Political, Emotional, Psychological, and Logistical, and describes the different kinds of threats that could impact organizations and affect desired security outcomes. Furthermore, Hayden introduces the “Security FORCE Behavioral Model,” where FORCE is an abbreviation for Failure, Operations, Resilience, Complexity, and Expertise. It provides another view on how organizations could assess their security from a behavioral perspective. Despite being an unwanted outcome for everyone, failure provides valuable insights into why something fails. If appropriately used, failure can be constructive to avoid more significant disasters. Operations and understanding the actual situation of this critical part of an organization's function can help make informed decisions. Resilience entails having the ability to take the proper steps when there is a failure. As failures are inevitable, having a proper reaction plan to address them is significant. Modern business environments are highly complex due to advanced threats and risks. Oversimplification might lead to the wrong assumptions of the real situation and wrong decisions. When an organization is aware of its complex environment, it can be better prepared for failure. Finally, expertise is related to leveraging the knowledge of experts to formulate plans. There are several key value behaviors that the FORCE framework is measuring to assess an organization's security culture.

Learning from the mistakes that cause failures, keeping the eyes open on how operations function, practicing failing and recovering, and not oversimplifying and enabling the transfer of authority are only some of these behaviors. Hayden claims that "people are the most important system to secure" as an organization can remain without technological solutions but not without its people.

Beyond the context of security culture but in the broader context of influencing culture, Denning (2011) deep-dives into the benefits of storytelling in organizations and how selecting appropriate narratives and styles can help transmit knowledge and shape culture.

For Denning, an ethical community comprises three fundamental elements: trust, loyalty, and solidarity. He highlights the ineffectiveness of transmitting values and creating culture by providing strict instructions or engaging in conversations regarding penalties for improper actions. He also supports using parables and stories to enforce the message that an organization's leadership wants to convey.

2.2 The Importance of Corporate Responsibility and Sustainability

Corporate responsibility and sustainability have been the subjects of extensive debate and research in recent years, reflecting society's growing awareness of the need for businesses to address environmental, social, and ethical issues proactively. This discussion has led to various frameworks, standards, and best practices that guide organizations in incorporating responsible and sustainable practices into their main strategies.

Most organizations nowadays have developed CSR-related policies and are engaged in relevant initiatives. According to Crowther and Aras (2008), the three fundamental principles of CSR comprise sustainability, accountability, and transparency. Sustainability guarantees that today's actions and choices do not jeopardize the welfare and potential of future generations by responsibly managing resources, ecosystems, and societal needs. Accountability entails an organization recognizing that its actions affect the external environment and, as a result, assumes responsibility for the outcomes of those actions. Transparency entails that the external consequences of the organization's actions can be determined through its reporting, and information is not concealed or obscured within that reporting.

Demartini and Taticchi (2021) link corporate sustainability to the broader subject of sustainable development and how businesses contribute to society. According to Zink et al. (2008), the concept of sustainable development is linked to three fundamental ideas: sustainable development is anthropocentric and not mainly focused on environmental challenges, the idea of intra-generational equity, and the notion that three pillars of economic, environmental, and social objectives are all equal.

The authors support that corporate sustainability is a conveyance of the overarching concept of sustainable development to the business landscape.

In recent years, a growing connection has been between corporate sustainability and responsibility and their alignment with the social, environmental, and economic dimensions. However, this was not always the case. Friedman (1970) claimed that the main responsibility of a business is to advance its financial performance. He argued that unless the organization is a charity, school, or hospital, investments aimed at furthering social objectives should be avoided, as they would conflict with the interests of the shareholders, indicating that any actions associated with social responsibility should be undertaken by individuals at their own cost.

Kuhndt and Tunçer (2007) highlight that the businesses, especially in the financial sector, are gradually broadening their view of corporate risks to encompass a holistic performance evaluation that includes social, environmental, and economic factors, going beyond sole reliance on financial performance indicators. They emphasize the importance of a stakeholder-oriented approach and introduce two pillars of responsible corporate governance.

The first pillar encompasses encouraging corporate responsibility, which includes stakeholder-empowered corporate governance, management and performance evaluation systems, transparency enhancement, and stakeholder verification. The second pillar aims to develop an institutional framework to coordinate interaction channels to foster corporate responsibility.

Within the "Corporate Sustainability in Practice" pages, Demartini and Taticchi observe that specific environmental and social disbalances must be mitigated. These disbalances include but are not limited to the growing population, climate change, and wealth disparity. Intending to address as many of these imbalances as possible, the international community decided to confront the 17 key challenges that society faces. These key challenges are known as Sustainable Development Goals (SDGs) or Global Goals and were adopted by the United Nations in 2015. They include tackling issues such as Clean Water and Sanitation, Reduced Inequalities, Affordable and Clean Energy, Climate Action, and Decent Work and Economic Growth. Each of these challenges requires a significant change in the social framework to maintain long-term sustainable development.

Soyka (2012) claims that sustainability is the concept that organizations need to contribute to the enhancement of society and that companies must harmonize their needs and interests with the greater welfare of society. Human potential is central, and only organizations prioritizing human well-being are likely viable and enduring.

In his work titled "Social Responsibilities of the Businessman," Bowen (2013) introduces eleven economic goals that should be aligned with a business's responsibilities towards society. These include Economic Progress, Personal Security, Justice, Freedom, Development of the Individual Person, and Community Improvement, among others.

Bowen, making mention of the "laissez-faire" theory, explores the relationship between self-interest and social welfare, observing that they are not always inconsistent. Furthermore, he refers to the key principles of the "laissez-faire" system, which include the freedom of choice for individuals, emphasizing the duty of businessmen to respect their employees on a human level. Nonetheless, the author underscores that, in reality, numerous conflicts have arisen between individual and societal interests. This is often due to employers' shortcomings in protecting employee safety and acknowledging their rights.

Furthermore, Bowen notes that the contemporary situation in Western nations often termed a "mixed economy," incorporates substantial elements of both laissez-faire and socialism alongside certain characteristics of syndicalism that preserve a significant degree of individual liberties. He characterizes this evolving model as "present-day capitalism." This development signifies an attempt to balance the businessmen's and employees' freedoms.

In the same publication, Bowen suggests adopting several proposals that promote enhanced social responsibility within organizations. One of these proposals is the introduction of a "social audit," which refers to a periodic examination of the businesses' social responsibility performance. The non-affiliated external specialists would assess human interactions, employment stability, and other factors during this audit. They would then present their evaluation and suggestions to the board of directors. This assessment could benefit the business, such as having an independent outsider's view on the company's activities and providing a pragmatic outlook of the situation combined with actionable recommendations to the management team.

Contrary to Friedman's stance in 1970 regarding the social responsibilities of businesses, Gollan (2000) argues that prioritizing the needs, potential, and ambitions of individuals in the workplace is essential. Otherwise, talented personnel will likely seek opportunities elsewhere, which could impact the organization's sustainability. Gollan presents a model aiming to enhance organizational value by focusing on the human element through training, active participation, and engagement. He proposes implementing consultation and employee involvement during corporate changes to instill confidence in employees to manage their workplace. Furthermore, he emphasizes career advancement and the financial gains that businesses can realize through investing in the development of their human resources instead of resorting to downsizing.

Gollan underscores that if businesses fail to put their rhetoric into action regarding people development, the likely consequence is that numerous talented individuals will depart from these organizations.

Read (2000) emphasizes that despite the allure of advanced technology, which both captivates and simplifies the lives of employees and consumers, the essence and caliber of human relationships will remain of utmost importance.

He points out that technology should be the enabler of the organization and not the driver. How people are managed within businesses mirrors the values and beliefs held about people, notably the extent of trust placed in them.

2.3 Exploration of AI technologies and their security applications and implications

Artificial Intelligence has unquestionably become an integral aspect of our daily lives. As Elliot (2019) points out in his publication "The Culture of AI," "AI has become, in a word, mainstream." He supports that AI transcends mere technological advancement; it signifies a complete metamorphosis of the entire technological landscape. Deep learning algorithms, sophisticated automation, and Internet-connected "smart" devices collectively introduce a completely new domain.

The corporate world has initiated the integration of various AI applications to automate operations and eradicate errors. Numerous business domains, such as Finance, HR, Marketing, Energy, Transportation, and others, are capitalizing on significant advancements in AI.

As Alpaydin (2016) notices, the strength of computers lies in their capacity to represent all forms of information in digital format. Computers can efficiently store, transmit, and exchange data at high speeds, free from geographical constraints. It is increasingly evident that the world relies on this data-driven paradigm, emphasizing the importance of harnessing and utilizing this wealth of information. Machine learning constitutes a subset of AI and refers to learning techniques that can provide the ability to analyze data, recognize patterns, and adapt by identifying and leveraging underlying structures and trends in the information provided. These techniques allow machines to make data-driven decisions, predictions, or recommendations without being explicitly programmed for each specific task. This adaptability is a fundamental strength of machine learning, enabling it to excel in diverse fields such as natural language processing, computer vision, financial modeling, healthcare diagnostics, and more. Additionally, as machine learning algorithms continuously learn from new data, they can improve their performance over time, making them valuable tools for solving complex problems and automating tasks in the modern world.

Russel and Novig (2022) claim that in order to say that a computer program performs the act of thinking as a human does, we first need to understand what the process of human thinking entails. The authors support that understanding human thought can be approached from three distinct angles: Introspection, Psychological experiments, and brain imaging. Introspection involves examining and reflecting on one's own thoughts. Psychological experiments refer to research conducted by psychology scientists to study human behavior.

Finally, brain imaging refers to the use of specialized medical equipment that can capture and analyze human brain images. By employing these three approaches, we can assess how the computer program's abilities compare to those of humans. If these abilities align, it serves as evidence that certain program mechanisms mimic human behavior.

AI finds numerous applications within the realm of security as well. SIEM (Security Information and Event Management) are AI-driven solutions that combine log analysis, network traffic analysis, and various other security detection methods. Organizations use SIEM tools to improve their cybersecurity by monitoring for security incidents, finding vulnerabilities, and ensuring compliance with rules and regulations. AI is also applied in security to enhance biometric authentication systems, improving the accuracy of solutions like iris and palmprint analysis through advanced AI processing. This leads to more precise authentication outcomes.

Furthermore, as highlighted by Yavuzkiliç et al. (2021), within the realm of social media, which has significantly altered our perception of reality, a multitude of malicious users exploit AI technologies to create "deep-fake" images and videos. In these manipulated media, faces are seamlessly swapped with those of other individuals. While many of these applications are benign in nature, they can also be used for nefarious purposes such as video impersonation for fraudulent activities and other malicious intents. Consequently, AI-driven deep-fake detection systems have been developed to detect and differentiate genuine content from fabricated ones effectively. Yet another way AI is employed within the security domain involves "anomaly detection" as Sharghivand and Derakhshan (2021) highlight. Anomaly detection refers to identifying patterns within data that deviate from expected behavior, commonly called anomalies. AI solutions are adept at inspecting vast volumes of data to identify anomalies within networks or computer files precisely. This capability enables the early detection and prevention of attacks, safeguarding the integrity of systems.

Weber (2021) supports that the dynamics in Cybersecurity will change due to the influence of AI. AI tools will conduct the vast majority of monitoring and reactive actions. Additionally, integrating built-in machine learning capabilities will enhance security tools, including firewalls, antivirus programs, and intrusion detection systems.

Weber sees a great prospect for AI in cybersecurity analytics and metrics, as several factors reinforce the need for this field's growth. Many checks require automation to secure an organization. For example, multiple devices need frequent configuration updates, users must be checked for access rights, and cyber incidents must be reported accurately. These security capabilities provide organizations with a proactive advantage over potential attackers.

A substantial body of literature studies the ethical and legal ramifications of integrating AI into business. Custers and Fosch-Villaronga (2022), while recognizing the benefits of AI applications in several realms, pinpoint that there might be unwanted side effects and unforeseen disadvantages. The capability of self-learning that AI currently possesses can develop rapidly and uncontrollably, similar to how children develop, having different personalities and behaviors from their parents. This requires adjusting the legal system accordingly to ensure the preservation of human interests.

A growing ethical concern emerging with the rise of AI technologies in the broader security domain is autonomous weaponry, as Liao (2020) observes. Intelligent weapon systems that no longer require human intervention while reducing the risk for military personnel, raise the question of whether humans should allow machines to decide when and where to use deadly force. Similarly, AI has the potential to detect potential malicious users and criminals within the law-abiding population. However, when there is an insufficient dataset to make informed decisions, it can lead to biased outcomes. Another ethical issue that might arise because of the advancement of AI technologies is the misuse of facial recognition technology.

While very useful in detecting criminals quickly, this technology also carries the potential for human surveillance, profiling, and discrimination. Liao additionally highlights that many people are concerned about the possibility of AI and automation displacing a substantial portion of existing human jobs in the foreseeable future, raising questions about job security for workers worldwide. Job security refers to the feeling of confidence that individuals have in the continuity of their employment. Some individuals believe that automation will render specific jobs obsolete, leaving some workers unable to find new employment opportunities.

While ethical concerns are being raised increasingly, and the unquestionable need for legal system adjustments to accommodate AI's rapid progress to ensure fairness and stability is evident, the outlook for AI in the security domain appears highly promising. Revett (2008) comprehensively explores behavioral biometrics, which involves recognizing individuals based on their unique behavioral traits, such as keystroke dynamics, mouse movement, and voice recognition. Revett supports that the possibilities are endless if we move from a software-only approach to a software-plus-hardware approach. This means that if specialized hardware is used to collect biometric data, the accuracy and reliability of the behavioral biometric systems will improve dramatically.

One illustration of this approach involves utilizing specialized noise-canceling microphones designed to eliminate background noise while capturing voice with exceptional precision. Sharghivand and Derakhshan (2021) study the applications of AI technologies in the data security and privacy realm and highlight the necessity of a framework that can secure data abstraction in any computing environment.

Efficient authentication and identification mechanisms are required to avoid data leakages, and AI technology has the potential to provide solutions to these data privacy matters. On the other hand, the application of AI in data analysis can raise concerns about individual privacy. Hence, relevant safeguards must be established to protect people's privacy and freedoms.

A novel risk connected to the rapid advancement of AI has emerged in recent literature, and it is tied to what is known as "technological singularity", a term introduced by Vernor Vinge in 1993. Vinge argued that humanity is on the verge of change since technology approaches a threshold that could surpass human capabilities.

When a higher intelligence than the human one is developed and takes the lead in driving progress, then the pace of advancement will significantly accelerate. It will be then that, according to Vinge, humanity will need to discard the old rules, and new models will emerge. He claims that the "post-human" era could potentially have adverse outcomes for humanity, going as far as the physical extinction of the human species. In the same publication, Vinge supports that there are alternative directions that humanity can choose to follow.

"Intelligence Amplification" (IA) occurs every time our capacity to retrieve information and convey it to others is enhanced, and it could potentially be a more straightforward route to accomplish "superhumanity" than just AI. He suggests we experiment with addressing problems commonly considered to be solvable by computers and design solutions that combine human intuition and computer hardware capabilities.

Kurzweil (2005) supports that by the end of the 2020s, machine intelligence will reach a point where it is virtually indistinguishable from biological human intelligence, placing the technological singularity timeframe in approximately 2045. He argues that by this point, humans will have moved beyond biology but will continue to exist within a human civilization, preserving their essential humanity.

Chrisley (2020) attempts another approach to AI ethics, supporting that a greater ethical risk arises from perceiving humans and robots as ethically equivalent rather than viewing them as fundamentally different in ethics. This human-centered approach prioritizes human welfare and responsibility.

It does not concentrate on whether AI systems can experience pain as humans do and if they should have the right to be property owners, but it focuses on human moral obligations. Chrisley raises concerns such as to what degree causing harm to an AI system should be considered more detrimental to a person than mere property loss and how the allocation of responsibility should be distributed across the various individuals for damage caused by an AI. The conclusion Chrisley is reaching is that people should not focus on the pursuit of creating ethical autonomous systems but on developing these systems in an ethical manner.

2.4 Reviewing existing literature on security culture in AI-driven environments

Although there is fragmented literature on the subject of security culture in AI-driven environments, there are diverse viewpoints currently available that have the potential to influence the advancement of human-centered security culture in AI-driven environments. When considering security in a corporate setting, the primary focus is on safeguarding assets, data, and operations, emphasizing the most critical components: the people.

From a political perspective, addressing the potential challenges that human society might confront in the digital era, Elliot (2019) notes that the proliferation of data could lead the way for the automation of political and public processes. This shift might contribute to a realm where citizen rights are subject to automation and programming, raising concerns about the viability of democracy under the influence of AI. Elliot observes that governments across the globe are already utilizing AI to nudge citizens toward specific social policies, which could potentially jeopardize people's freedoms. A possible gap in the existing policies and frameworks and, to an extent, in the body of literature that has been published is that even though there are several Sustainable Development Goals (SDGs) that could potentially be connected to the impact AI can have on society, currently there is no SDG that is mentioning AI by name or referring to potential ramifications to society because of AI misuse.

Zeide (2020) observes that since the Industrial Revolution, many proposals have suggested that "teaching machines" could automate aspects of the instruction process. These learning systems have become a reality, and they can emulate human teaching by gathering data from student interactions, monitoring their advancements, and offering feedback. Zeide underlines the possible advantages of these systems, including the decreased time teachers must allocate to grading and the swift integration of the most recent findings in learning science and research. She also highlights some potential drawbacks of AI learning systems, such as the potential for biased assessments resulting from insufficient data and the possible reduction in teachers' autonomy. Zeide seeks to draw a comparison between AI learning systems and human teaching capabilities. She argues that despite the numerous functionalities that AI systems possess, such as data analysis, ongoing evaluation, and decision-making, they rely on formal assessment.

Teachers additionally have the ability to informally personalize learning by taking into account various contextual factors, such as a student's body language and classroom engagement.

Tegmark (2017) underscores that AI technology possesses the capacity to shift society to a “perfect police state” very easily, making even the worst totalitarian scenarios true since machines do not have any feeling of doubt or hesitation when it comes to enforcing any directive. Tegmark stresses that humans maintain control over AI in these scenarios, but there is always the potential for these systems to transition into a self-controlling mode.

Zhu et al. (2022) support that to produce responsible AI systems, particular attention should be given to distinguishing between trust and trustworthiness and emphasize that performance capabilities that are related to trustworthiness could differ from the behavior that stakeholders expect and which is linked to trust. Several factors influence people's trust in AI systems, including existing societal regulations, potential job implications due to AI, and overall familiarity with AI, while trustworthiness plays a relatively minor role in establishing trust.

2.5 Chapter Summary

In this literature review, we established the definitions of key terms that are employed throughout the entire thesis. Furthermore, I conducted a limited review on the existing bibliography related to the topic of human-centered security culture in AI-driven environments following a modular approach, where every concept that the aforementioned topic entails was examined separately.

During this literature review, the focus was not limited to the technical aspects of AI; instead, it included the exploration of broader societal applications and implications of AI technology.

The review examined the concept of corporate responsibility and sustainability and its connection to the welfare of society, considering the role of people in it and their relationship with the advancement of technology.

Additionally, the research was conducted from an anthropocentric perspective, taking into account the ethical consequences of AI technology adoption and the numerous potential trajectories it might take.

The potential gaps in this literature review serve as essential areas for further investigation, as the integration of AI technologies in the security culture-shaping process of organizations offers countless possibilities.

3 Research and Development Methodology

To reiterate the study's primary goal, it attempts to construct a framework outlining the principles and approaches necessary for cultivating a robust security culture in AI-driven environments, which sustains a human-centered approach.

I chose to develop a framework rather than offer standalone recommendations because a framework provides a more holistic, comprehensive, and structured approach. Moreover, a framework highlights the relationships between different variables, helping organizations better understand how these elements are interconnected. This allows for easier customization and scalability based on specific needs.

The decision to develop a conceptual framework for this study is based on the need for a customized structure that addresses the study's research questions. While valuable, existing frameworks identified during the literature review do not fully encompass the complexities and dynamics of today's business environments.

To accomplish this, our approach will consist of the following three steps:

- 1) Framework Creation: We're going to construct our framework, drawing from the findings of our literature review.
- 2) Interviews:
 - a. People: We will be conducting interviews with the selected participants.
 - b. AI: We will include an AI language model interview as a component of our research.
- 3) Recommendations: Using the insights gained, we will formulate and present our recommendations.

To restate the research questions that this study will attempt to answer, these are:

Research Question 1: What are the key challenges and opportunities in integrating AI technologies into security culture methods while sustaining a human-centered approach?

Research Question 2: What strategies can business organizations implement to ensure that AI-driven technologies prioritize human rights and well-being?

Research Question 3: What measurable Key Performance Indicators (KPIs) can be developed to evaluate the balance between AI-driven security solutions and human-centered values while accomplishing the organization's business goals?

3.1 Research Setting, Process, and Implementation

Drawing from my expertise in Information Security—I have been a Security professional for around two decades—I decided to undertake a research topic based on existing literature while also supplementing this approach with qualitative research methods, specifically through interviews of established security culture professionals, to delve deeper into various aspects of the research topic.

I aim to develop a conceptual framework that will be able to serve as a blueprint for organizations of various industries and sizes to implement a security culture program that can adapt and evolve alongside AI integrations.

The qualitative data that will be used to adjust the conceptual framework will be gathered through interviews. Utilizing my professional network and LinkedIn connections, I have carefully selected interviewees to ensure a diverse representation of security and AI professionals, aiming for a comprehensive sample.

For experimental purposes, I will also be 'interviewing' a large AI language model. Although the data collected from this interaction will not be included in the formal framework of the current thesis, it is expected to provide useful insights and enhance the understanding of the potential and limitations of AI in research contexts. For these purposes, I will experiment with GPT-4, the most recent version available when this thesis was written.

Details on the process of the interviews will be provided later in this chapter (time horizon, approach, interview structure, tone, participant selection, etc.)

Once the in-depth interviews have been conducted, the transcripts generated will undergo an iterative inductive coding process, where valuable codes, categories, and themes, will emerge. The coding process will play a crucial role in analyzing the collected data, providing common themes, and interpreting participants' feedback. Bryman (2012) provides a comprehensive method for coding which will be used as a guide for my research.

Here is an example of the coding process, using as data the first interviewee's response on the first question from the interview:

"Spiros Katiforis

The first question I have for you is if the organizations that you have worked for have established a security culture.

Interviewee 1

Yes, I would say so. The one thing for me personally is I **don't use that terminology**, so I often don't think of it in that way, because if **you take the term security culture**, it can seem like it's separate as an entity from other forms of culture.

And so, I tend to think about it more as the security part of the day-to-day activity, whether it's the X company I am working at currently, or, where I've worked previously.

And yeah, **people think about it. People ask about it. They're intrigued about it.** We can ask questions and they react to posts or they will personally reach out, and there's just a level of low-level interest in the topic which promotes a lot of activity and people learning basically. **It's the same wherever I would work, I would never call it security culture specifically because I don't really enjoy the term.** But do we have an idea of it? Yes, yes, absolutely.”

Firstly, we highlight in bold letters the segments of data that capture important ideas. Then we assign a code (a word or a short phrase) to these segments. For these first highlighted segments we are going to assign the codes: *terminology rejection*, and *daily engagement*. Then, reading through the transcript we combine similar codes into broader categories. As a next step, through an iterative process, we continuously refine the categories and themes. Lastly, we ensure the validity of the emerging themes through rigorous review.

At the end of each interview, a table will be provided with the emerging codes, categories, and themes that will give us a better understanding of the interviewee's perspective on the research topic.

The selected approach allows the researcher to develop a strong understanding of the underlying patterns, gaining insights into the connections and commonalities arising and the contradictions inherent in the study subject.

The results obtained through the data analysis of the interview transcripts will be analyzed in the context of the existing knowledge derived from the literature review. Additionally, the interview results will be compared with the data gathered during the interview conducted with the AI language model to identify correspondences, divergences, and potential synergies between the human and the artificial entities. The findings will provide further insight into whether and how a balanced coexistence of technology and humanity can be achieved.

Finally, I will adjust the conceptual framework based on the qualitative research results and make my recommendations.

The present study embraces the philosophy of Interpretivism wherein the interpretation of reality is subjective and individualized to the researcher. I chose this research philosophy for the present study because I am exploring personal perceptions and experiences, and interpretivism prioritizes understanding subjective perspectives over objective facts. The analysis is conducted based on the cultural beliefs, norms, and values of the society and group of individuals in which the research is conducted.

Interpretivism is a qualitative method specifically employed to analyze data related to human actions in sociology. This approach suggests that individuals form their realities through subjective interpretations of their experiences, rather than adhering to objective truths (Bryman, 2012).

The study adopts the Inductive type of research, following a bottom-up approach. When adopting this research type, the researcher starts with specific observations and experiences, gradually developing broader theories or generalizations. The inductive research process is usually divided into three phases: observation, pattern recognition, and theory development. In contrast to deductive reasoning, where the researcher begins with a theory and tests it across specific hypotheses, inductive research involves exploring data, identifying patterns, and forming ideas based on observed patterns. This research type is particularly suitable for exploring unexplored areas, facilitating the generation of unique insights and hypotheses. Inductive research is popular in qualitative studies, ethnography, and grounded theory approaches (Bryman, 2012).

3.2 Research Parameters

In order to offer a grounded perspective on this research and its anticipated outcomes, certain parameters need to be defined.

The time horizon defines the time frame in which the research takes place. As the present thesis involves data collection at one specific point in time, the study adopts a cross-sectional horizon. The purpose of this choice is efficiency, as valuable data can be collected within a short period of time. Additionally, cross-sectional research can provide a valuable snapshot of the current situation and help identify trends in the subject of the study. The time horizon for the research is set for the Spring of 2024.

The participant selection strategy refers to the process of identifying the subjects of the research, and more specifically the individuals that will participate in the research. For the purposes of the present study, a non-probability, and more precisely a purposive participant selection strategy is chosen. This involves the selection of professionals from the fields of security culture, AI technologies, and human resources based on assumptions on their expertise and interests. The selection of the population that will participate in the research relies on this study's author's own judgment.

In addition to the individuals participating in the research, this study attempts the innovative approach of including an AI language model software in the list of the participants, to gather insights and perspectives from a source intimately linked to the subject matter of the research.

This software specializes in generating human-like text based on the input it receives, and it responds with contextually relevant and coherent text, based on diverse patterns of data that have been collected by its creators.

To ensure the confidentiality and privacy of the participants in this study, all individuals will be anonymized. Any personal identifiers, such as names or affiliations with specific companies, will be replaced with generic descriptors, such as work titles. This precautionary measure ensures that the results presented in the study cannot be traced back to any specific participant. All participants have given their consent to publish the interview transcripts following anonymization.

Indicative work titles of individuals participating in the research are as follows:

- Head of Cyber Culture
- Security Culture Manager
- Security Culture and Awareness Lead
- HR Director
- People and Culture Lead
- Head of Security Culture

The data collection method selected for this study is in-depth interviews with subject matter experts (SMEs) from the fields of security culture and AI technology, as well as an AI language model.

This type of qualitative research allows a deeper exploration of the subject as they can capture non-verbal data such as body language, facial expressions, and tone of voice, providing additional insights. Additionally, interviews can help capture the participant's view more efficiently, as they provide the flexibility of conducting them virtually, face-to-face, or through phone calls.

It is important to note that analyzing expert interviews is fairly different from working with sociological interviews. When talking to experts, we're looking to gather specialized knowledge and insights from people who have great experience in their field. This makes the analysis more focused and technical, often following structured questions designed to dig deep into specific topics. On the other hand, sociological interviews are about understanding people's social behaviors, experiences, and perspectives within their cultural or community settings. These conversations tend to be more open-ended, revealing more diverse social insights. The context between these two types of interviews is different—expert interviews focus on professional and technical settings, while sociological interviews pay close attention to the social and cultural backgrounds of the people involved. For the present research we will be focusing on expert interviews.

Not all of the above interview attributes apply to the AI language model, as it does not have facial expressions, nor can the interviews be conducted through video or phone calls. The purpose of including the AI software in the interview process is experimental.

3.3 Framework Design

Utilizing insights from the literature review, a framework will be formulated. The resulting framework will attempt to help modern business environments sustain a human-centered culture while answering the study's research questions. It can be adopted by companies of varying sizes and across diverse industries, whether they are currently incorporating AI solutions into their operations or considering doing so in the future.

Organizations have the flexibility to tailor the present framework to align with their specific requirements, enabling them to gain a competitive advantage in the field of the study.

The framework design describes the design decisions and provides insights into the approach and structure employed to develop the framework.

Frameworks are structured models that offer a systematic approach to understanding and resolving complex problems within various domains.

There are many different types of frameworks, such as theoretical frameworks that provide a theoretical foundation by integrating existing concepts, analytical frameworks that offer a structured approach for analyzing data, and policy frameworks that provide a structure for policy development, among others.

For the present study, the development of a conceptual framework has been deemed suitable. Conceptual frameworks offer a visual representation of the expected relationships between various variables. The use of variables in conceptual networks or frameworks, particularly in the social sciences, is a collective development built upon the foundational work of statisticians, experimental psychologists, and sociologists. While theoretical frameworks strongly rely on existing research and literature review, conceptual frameworks are grounded on the researcher's own thinking process, as well as their assumptions, expectations, and beliefs (Kivunja, 2018). A conceptual framework outlines, either through visuals or descriptive text, the primary elements to be studied, including key factors, constructs, or variables, and the assumed relationships between them (Miles & Huberman, 1994). Conceptual frameworks focus on establishing a deep understanding of the research topic as they outline the key elements relevant to the study and depict how these elements are connected to each other, providing coherent conclusions. Conceptual frameworks can connect different concepts and theories within the topic of research.

Our framework will be designed based on the approach described by Swaen and George (2022) and the suggestions made by Roer and Carpenter (2022) for initiating a security culture framework, which is structured around three phases: measure, involve, and engage.

3.4 Interview Protocol and Questions

The interview protocol for the present study consists of a series of open-ended questions aiming to explore participant's perspectives on the research topic. The questions are flexible, meaning there might be ad-hoc modifications/additions depending on the themes or ideas emerging from the discussions.

Through this approach, these interviews aim to capture the participants' viewpoints and experiences concerning the study topic. The literature review has led to the following questions.

1. Has your organization/business environment already established a security culture?
2. How would you define security culture within your organization and how is it measured? Would you define it as human-centered?
3. Has your organization integrated AI technologies into its security practices?
4. Do you personally identify any conflicts or other ethical considerations in the deployment of AI-driven security systems in business environments?
5. Do you anticipate AI posing a threat to human liberties and security within business environments? Do you foresee it affecting human job security?
6. What measures do you believe are necessary to ensure transparency and accountability in AI-driven environments regarding security?
7. How can organizations foster collaboration and coevolution between AI and human personnel?
8. What are the key components of a human-centered security culture?
9. How do you see the future coexistence of AI and humans in business environments?
10. How can humans safeguard their freedoms in the event of Technological Singularity?

While the above interview questions are applicable to the human participants, they are not all suitable for the experimental querying/interview with the AI language model software. For that purpose, the following version of the questions will be used:

1. How do you define your role within the security culture realm? What would be your responsibilities in a business environment?
2. How would you define security culture and how is it measured?
3. Do you identify any conflicts or other ethical considerations in the deployment of AI-driven security systems in business environments?

4. What measures do you believe are necessary to ensure transparency and accountability in AI-driven environments regarding security?
5. Do you anticipate AI posing a threat to human liberties and security within business environments? Do you foresee AI affecting human job security?
6. How can organizations foster collaboration and coevolution between AI and human personnel?
7. What are the key components of a human-centered security culture?
8. How do you see the future coexistence of AI and humans in business environments?
9. What safeguards do you have in place to secure sensitive data and adhere to privacy regulations?
10. How can humans safeguard their freedoms in the event of the Technological Singularity?

3.5 Methodological Limitations

Transparency regarding the shortcomings and limitations is crucial to provide a better context for interpreting the findings and to encourage future researchers to build upon the existing research. The methodological limitations of this study are approached from a critical perspective.

Despite its limitations, the present study aims to add value to the existing body of knowledge, offering valuable insights on the topic of sustaining a human-centered security culture in AI-driven environments.

The lack of infinite time to conduct the research is a limitation, as it limits the time frame for the collection and analysis of data. Additionally, cross-sectional studies similar to the present one cannot provide insights into changes over time.

Budget constraints limit the possibility of conducting in-depth interviews in person, which would add value to the research through the addition of non-verbal data, such as the interviewees' facial expressions, body language, etc.

Regarding the sampling strategy, various biases are related to non-probability sampling, such as the selection bias, as strong assumptions are made during the sampling process by the researcher about the participant's expertise and interests. Additionally, due to the study's limitations, other individuals who could add different perspectives to the research are not included in the sample.

From the perspective of the AI language model as a participant in the research, several limitations could impact the quality of the results, as these models lack a proper understanding of the natural world, base their knowledge strictly on existing data patterns, and do not have a human comprehension of reality.

Additionally, the information gathered by the AI software cannot be verified for its accuracy. Since AI software does not possess consciousness, there is a possibility of providing ambiguous responses due to the fact that it can misinterpret the input provided by the researcher.

4 Building the Framework

In this chapter, I am developing the conceptual framework based on the researcher's thinking process but also by drawing on the existing knowledge from the literature review.

I chose to use the framework variables model instead of others, such as first-order concepts/second-order concepts, because framework variables enhance clarity while also prioritizing replicability, which is important when it comes to solutions that can potentially be adopted by diverse business environments.

I provide a visual representation as well as a narrative explanation of the framework.

4.1 Framework Variables

The research variables of the conceptual framework are the key components that are being studied throughout the research study. There are several types of variables involved in a conceptual framework.

Independent Variables: These are variables that are controlled by the organization and are hypothesized to influence the dependent variables.

Dependent Variables: These are outcomes that are observed or measured as a result of changes in the independent variables.

Moderating Variables: These variables modify the impact of an independent variable on a dependent variable.

Mediating Variables: These are variables that connect the independent and dependent variables, assisting in explaining the relationship between them.

Control Variables: These are factors that are held constant or consistent to prevent influencing the relationship between independent and dependent variables.

For the framework of this study, I have selected the below variables:

Independent Variables:

- Security/Privacy Incidents related to AI integration: Any security/privacy incident or policy violation related to AI integration can potentially undermine the human-centered security culture within an organization.
- Leadership Commitment: The commitment of organizational leadership towards promoting a human-centered security culture.
- Regulatory Compliance: The compliance requirements that ensure a robust human-centered security culture.
- Employee Engagement: The commitment of employees towards promoting a human-centered security culture.

Dependent Variables:

- Human-Centered Security Culture: The values, behaviors, and practices within the organization towards security, focusing on human-centered values.
- Employee Well-being and Satisfaction: The satisfaction and well-being of the employees influenced by the security culture and the human-centered approach.
- Job Security: The degree of confidence that employees feel regarding the continuity of their employment within the organization.
- Organizational Resilience: The organization's capacity to mitigate security threats, maintaining business continuity.

Moderating Variables:

- Organizational Culture: The existing organizational culture may moderate the organization's ability to sustain a human-centered security culture when integrating AI solutions.
- Industry Landscape: The industry landscape concerns the broader environment in which the organization operates, and it can moderate the relationship between AI solutions and human-centered security culture.

Mediating Variables:

- **Security Awareness:** Security Awareness programs can help employees and organizations avoid or prevent security incidents and policy violations, maintaining a secure business environment.
- **Employee Trust:** The level of trust employees have in leadership, and their decisions regarding AI technology integration can mediate the relationship between AI technologies and the organization's human-centered security culture.

Control Variables:

- **Organizational Size:** The size of the organization (number of employees, revenue) can affect the human-centered security culture during the integration of AI technologies, as fewer resources or multiple integrations may result in reduced focus on security and increased security incidents. It is not part of this framework to address the implications that the organizational size might have on security culture in AI-driven environments.
- **Geographic Location:** The organization's geographic location can influence security culture and AI integration, necessitating a tailored approach. This variable's impact will not be taken into account for this framework.

4.2 Framework Visualization

The diagram that visualizes the conceptual framework can be seen below:

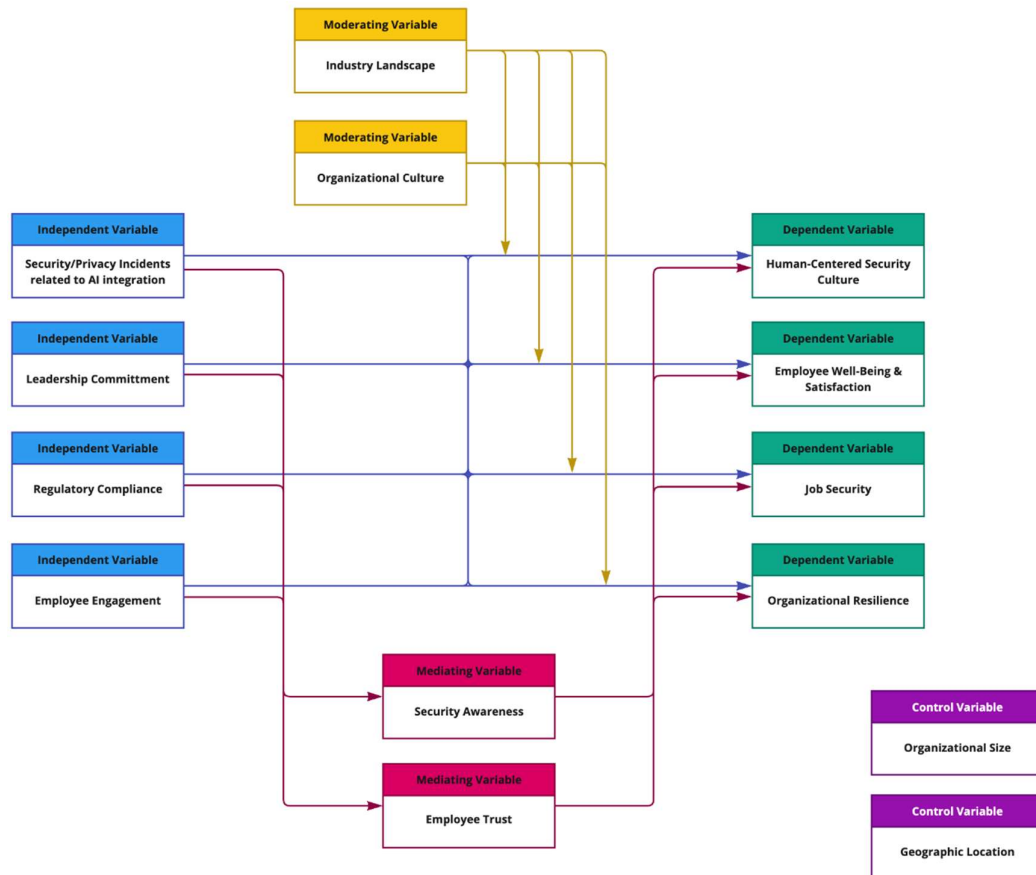


Figure 1.

Conceptual Framework for Sustaining a Human-Centered Security Culture in AI-Driven Environments

4.3 Framework Narration

In the diagram shown in Figure 1, it is evident that all dependent variables are influenced by the independent variables. Security or Privacy Incidents related to AI integration within organizations may positively or negatively impact the organization's human-centered security culture, the employees' well-being and feeling of job security, and overall organizational resilience, as such incidents test the organization's ability to respond, recover, and adapt to disruptions. Leadership commitment can drastically affect all dependent variables, as lack of commitment can result in low morale and disengagement among employees, which directly affects the security culture. On the other hand, strong leadership commitment ensures a clear strategic vision and proper resource allocation that safeguards the organization when a crisis occurs. Regulatory compliance fosters a culture of integrity and accountability which enhances an organization's security culture while impacts positively the employees' morale and well-being. Compliance with regulations also plays a crucial role in business continuity and resilience. Finally, employee engagement has a significant impact on the security culture of an organization, as engaged employees are more vigilant and more likely to respond properly to a security incident which also influences organizational resilience. Disengagement can lead to job dissatisfaction and reduced motivation which affects overall well-being. Engaged employees are also more likely to help prevent critical incidents that might affect organizational resilience.

The moderating variables shape the extent of the impact that independent variables have on dependent variables. The visual representation of the framework shows that if the existing organizational culture is robust, it can reinforce security values and the human-centered aspect of culture. On the contrary, if an organization does not have an established security culture, the resistance to changing behaviors and practices hinders its effort to establish a security culture that focuses on the human aspect. Additionally, employee well-being and morale can be moderated by the established security culture when a security/privacy incident occurs, as the incident can serve as an opportunity for learning when the organizational culture promotes openness. The same goes for job security, as employees do not feel threatened if incidents are openly discussed, and the established practices ensure their quick and effective resolution, which also positively impacts organizational resilience. A similar effect can be observed in leadership commitment. If the organizational culture aligns with the values and priorities of leadership, the commitment to a human-centered security culture in AI-driven environments is more likely to be effective. In the same way, employee well-being is bolstered when there is open communication and support from leadership. On the other hand, when the leadership does not invest in human resources and technology, the employees cannot have the same sense of job security as well as critical infrastructure is not maintained properly which leads to weaker organizational resilience.

The prevailing security culture also plays a significant role in regulatory compliance and how it affects the human-centered aspect of security culture. Employees and management who are well-versed in security practices will uphold their commitment to adhere to the required rules and regulations. Additionally, in an environment of transparency and support, employees feel secure when they understand that rules are in place to protect them and their organization, ensuring organizational resilience. The existing organizational culture can influence how employee engagement impacts the human-centered security culture, well-being, job security, and operational resilience, as employees are more likely to align their efforts and enforce a human-centered security culture in an environment that supports engagement. Similarly, employees are more likely to experience positive effects on their well-being as their engagement is recognized and supported. By contrast, in a culture where recognition and advancement are inconsistent or perceived as unfair, job security may be jeopardized. Security culture also affects the relationship between employee engagement and operational resilience. A strong security culture enhances employee engagement by providing clear expectations and support for security practices, strengthening operational resilience through improved responsiveness and proactive problem-solving. The industry landscape is the second moderating variable in this framework, and it can severely impact the relationship security incidents in AI-driven environments might have upon the human-centered security culture. When the industry collaborates in establishing high-security standards, the impact of potential security/privacy incidents that are related to AI integrations on human-centered culture is minimal as organizations are well-equipped and prepared to mitigate risks. This results in a strong human-centered security culture while organizations maintain their focus on ethical and responsible AI integration. This also fosters employee well-being and increases the sense of job security as adequate preparation to handle security incidents reduces the level of stress that disruptions may cause. Additionally, the negative influence potential crises may have on organizational resilience heavily relies on the established standards in the broader environment of the organization. If standards are lacking or the broader environment is not supportive, crises can severely undermine resilience by exposing vulnerabilities and creating significant disruptions. In industries where leadership commitment is valued, organizations are more likely to prioritize a human-centered approach to security, as breaches can have severe consequences. Oppositely, in industries with deep-rooted traditions, the leadership commitment might be reduced, and changes aimed at improving employee well-being can sometimes face resistance. This can possibly impact the sense of job security among employees. If there is a lack of leadership commitment in industries that have complex supply chains, this can profoundly disrupt their organizational resilience efforts. Sectors like finance and healthcare are heavily regulated, and compliance is essential for maintaining business integrity.

Sometimes, heavy investments in infrastructure to comply with these regulations may shape a culture deeply reliant on technology, which takes precedence over human-centered approaches, negatively impacting employee well-being and job security. On the other hand, highly regulated industries improve their operational resilience in an effort to meet stringent compliance requirements. The relationship between employee engagement and human-centered security culture can also be influenced by industry-specific characteristics. In industries where security is a top priority, employee engagement fortifies the creation of a security-conscious environment with a focus on the human aspect. Alternatively, in industries with high turnover, even high engagement does not ensure employee well-being, while the sense of job security is limited. The impact on the relationship between employee engagement and organizational resilience can depend on the frequency of disruptions in a specific industry. Fast-moving industries with frequent changes, even with high employee engagement, might not be able to adapt quickly enough, resulting in limited organizational resilience.

Security Awareness, as a mediating variable, assists in explaining the relationship between the security/privacy incidents related to AI integrations with human-centered security culture. Higher levels of security awareness within an organization can assist in lowering the occurrence of security incidents and reinforce a human-centered security culture. Additionally, security awareness can help boost employees' well-being, as a reduced number of security incidents contributes to a safer and more secure workplace with lower stress levels. Job security can also be positively affected by high levels of security awareness that help mitigate risks related to security incidents. Security awareness can also help explain how security incidents affect organizational resilience, as low levels of awareness can result in business continuity issues. Leadership commitment enhances security awareness which in turn leads to a stronger human-centered security culture. Furthermore, increased leadership commitment and security awareness increase the sense of well-being and job security, while when employees are aware and vigilant about security issues, they help prevent events, improving the organization's resilience. Regulatory compliance can indirectly affect human-centered security culture through high levels of security awareness, while employee well-being and job security are also affected in a similar manner. High levels of security awareness about the regulatory requirements can help organizations build resilience and overcome crises. It is also evident in the visualization that employee engagement enhances security awareness which in turn enhances the human-center security culture. In a similar way, increased security awareness due to increased employee engagement enhances employee well-being, job security, and organizational resilience. The second mediating variable we see depicted on the diagram is employee trust. Employee trust in the organization can be a result of a decreased number of security incidents, while enhanced employee trust helps establish a strong human-centered security culture.

Similarly, increased employee trust promotes the feeling of well-being and job security while positively impacting organizational resilience. Leadership commitment acts as the starting point, influencing employee trust.

The enhanced trust, in turn, positively affects the human-centered security culture. When trust is increased, employees are more likely to engage in practices that promote security culture, employee well-being, job security, and organizational resilience. Regulatory compliance can also feed employee trust, as an organization that follows the rules and complies with all necessary regulations inspires its employees to be vigilant while giving them a sense of well-being, also influencing job security and organizational resilience. Finally, employee engagement increases employee trust in the organization as engaged employees are more likely to have a better understanding of the vision, and the leadership commitment and often benefit from open communications. This trust then enhances the level of security culture, as well as well-being, job security, and organizational resilience.

Even though the control variables (organizational size and geographic location) could potentially influence outcomes, these variables are kept constant and are not addressed in this research.

5 Interviews

To conduct the interviews for this research, I engaged directly with experts in the field, seeking insights from professionals specializing in security culture, AI technologies, and human resources. This approach allowed for a comprehensive understanding by integrating perspectives from both domains, ensuring that the study captured the human-centric aspect of security culture.

The complete transcripts are listed in the Appendix, allowing readers to review the full details of the data and gain a deeper understanding of the context and findings discussed in the study. Additionally, future researchers can use the same data and make their own conclusions. The transcripts are presented highlighting the codes (in bold letters) and extracting the emerging categories, themes, and concepts resulting from the coding process at the end of each interview. Below we present a summary of each interview as well as the emerging codes, categories, and themes.

Several challenges were encountered when transcribing interviews with participants from different nationalities and backgrounds. Accents, dialects, and varied speech patterns might have led to transcription errors, as the software used for transcription might not have captured all the spoken words accurately. To preserve the authenticity of the interviews, any grammatical or other errors have been left unchanged.

5.1 Participant Interviews

Interview 1:

Participant 1 does not distinguish security culture from the overall organizational culture, instead emphasizes the importance of conversation to enhance security. Adopting a holistic perspective, the participant explains the key elements of a human-centered culture, stressing that not everyone easily understands security practices. The way the message is communicated is crucial. Furthermore, the interviewee highlights the significant potential of AI but cautions that it must be managed carefully to avoid impacting human liberties. Below is the table that contains the codes, categories, and themes that emerged from interview 1.

Codes	Categories	Themes
Daily engagement	Security Culture and Engagement	Integration of Security in Daily Life
Low-level interest in security topics		
Terminology rejection		
Acknowledging existing security perceptions	Terminology and Perception	Language and Perception of Security
Human-centered approach in cybersecurity		
Embedding security features thoughtfully	Human-Centered Design and User Behavior	Human-Centered Approach
Planning and messaging for security changes		
Avoiding simplistic approaches in security tasks		
Achievability of security tasks		
Transparency and accountability in AI usage		
Managing AI's role in security	Communication and Implementation Strategies	Effective Communication and Management
Concerns about AI's impact on creativity		
AI's impact on job security	AI, Ethics, and Workforce Impact	Ethical Considerations of AI
AI's limitations due to data quality		
Task complexity	Emergent Behavior and Complexity	Emergent Outcomes from Security Practices
Emergent behaviors from security tasks		

Table 1.

Codes, Categories and Themes from Interview 1.

Interview 2:

Participant 2 emphasizes that changing culture is a challenging task; it requires both resources and time to be successful. Security teams must evolve to adopt a human-centered approach. According to the participant, AI offers potential but also poses risks, as criminals are already leveraging these technologies for their own gain. Privacy is a significant concern, and organizational leadership must have a strategy in place to mitigate emerging risks. For Participant 2, culture is shaped by small behaviors, and because security is a complex concept, people need to feel that they are integral to the overall strategy.

Codes	Categories	Themes
Early investment in security culture	Security Culture Development	Security Culture Development
Frequent and complex changes in the security landscape	Challenges in Security	
Fraudsters and criminals well-equipped with tools	Threat Landscape	
Phishing attacks and human involvement	Security Threats	
Security culture part of overall company culture	Long-term Approach	
Empowering employees to protect themselves	Employee Engagement	
Human-centered security culture	Human-Centered Approach	Human-Centered Approach
Need for diverse skills in security teams	Skills and Expertise	
Shift from mandatory compliance to a more engaging approach	Engagement Strategies	
Investment in measuring and improving security culture	Continuous Improvement	
Exploration and integration of AI in security practices	AI Utilization	AI Integration
Need for expert input and research	External Learning	
Collaboration and proper process in AI deployment	Collaboration and Process	
Experimentation with low-risk AI opportunities	Risk Management	
Unified culture encompassing security and company culture	Unified Culture	Cultural Integration
Prevention and strategic alignment of security culture	Strategic Alignment	
Customer trust and brand reputation	Reputation and Trust	

Demystifying complex security issues	Communication of Security	
Acknowledging and reinforcing correct security behaviors	Behavioral Reinforcement	
Open conversations and recognition of employee contributions	Employee Recognition	

Table 2.
Codes, Categories and Themes from Interview 2.

Interview 3:

Participant 3 supports that AI is a major disruptor for organizations, bringing with it numerous security and ethical considerations. Even with good intentions regarding AI usage, it is essential to remain cautious and prioritize people. Communication is crucial for fostering a human-centered security culture, as it has the power to shape behaviors. Finally, Participant 3 believes that AI integration is similar to any other innovation, and people need to adapt accordingly.

Codes	Categories	Themes
Security culture still developing	Evolving Security Culture	Security Culture Development
Initial security focus and organizational development	Security Framework Initiation	Organizational Security Culture Development
Historical focus and cultural shifts in security	Initial Security Focus	Cultural Shifts
Misconceptions about security as roadblocks	Security Misconceptions	Misconceptions and Conflict
Balancing development and security	Balancing Priorities	Integration of Priorities
Impact of security incidents	Risk Management	Risk Management
Ongoing development in R&D cooperation	Inter-departmental Collaboration	Collaborative Efforts
Emphasis on human-centered security culture	Human-Centered Approach	Human-Centered Approach
Awareness of biases and potential risks	Security Awareness	Awareness and Biases
AI as a disruptor and its implications	Technological Disruptions	Adapting to Technological Changes
Data privacy and security considerations with AI	Data Protection	Data Protection and Ethical Use
Skills and adaptation to AI	AI Integration and Job Dynamics	Skills and Adaptation

Communication between technical and non-technical teams	Cross-functional Communication	Effective Communication and Management
Balancing technical safeguards and human-centered behavior	Balancing Technical and Human Factors	Balancing Technical and Human Factors

Table 3.
Codes, Categories and Themes from Interview 3.

Interview 4:

Participant 4 believes that security should be integrated at all levels of an organization and that individuals have the power to influence and maintain security if they are adequately trained and empowered. The potential of AI is vast, as they can analyze large amounts of data and help identify threats more effectively. However, the participant also highlights the potential risks AI poses to human liberties and argues that the educational system should adapt to this new reality. Strong ethical standards and legal requirements must be established to ensure AI technologies complement human skills rather than replace them. While not overly optimistic about the future, the participant emphasizes the need for global cooperation to manage the impacts of technological advancements.

Codes	Categories	Themes
Security is part of corporate culture	Integration of Security Practices	Security Culture Development
Security must fit with corporate culture	Alignment with Corporate Culture	
Prioritizing security at all levels	Hierarchical Security Implementation	
Security as an organizational responsibility	Broad Organizational Responsibility	
Measuring security culture through compliance rates, security incidents, employee knowledge, etc.	Security Culture Metrics	
Leadership commitment to security	Leadership in Security	Human-Centered Approach
Human-centered security approach	Human-Centered Security	
Continuous education and awareness programs	Security Education and Awareness	Ethical Considerations of AI
Ethical concerns regarding AI deployment, including privacy, bias, and transparency	AI Ethical Considerations	
Balancing security enhancement with protecting individual rights	Ethical Balance in AI	

Ensuring transparency and accountability in AI-driven environments	AI Transparency and Accountability	
Concerns about human nature affecting the ethical use of AI	Human Nature and Ethics	
Preparing for Technological Singularity by establishing ethical and legal frameworks, and promoting understanding of AI	Technological Singularity Preparedness	
Global cooperation to manage societal impacts of rapid technological advancement	Global AI Ethical Standards	
Integration of AI technologies in security practices for threat detection, response, and efficiency improvements (e.g., Virtual Information Security Officer)	AI Integration in Security Practices	AI Integration
Designing AI to complement human skills and enhance collaboration	AI-Human Collaboration	
Future coexistence of AI and humans, with AI augmenting human capabilities	Human-AI Future Relationship	
Potential threats to human liberties and job security due to AI	AI's Impact on Employment	
Educational system adaptation to AI	Adapting Education for AI	

Table 4.
Codes, Categories, and Themes from Interview 4.

Interview 5:

Participant 5 notes that security has only gained significant importance over the past decade, and while it continues to evolve, most investments still focus on technical controls. Although it is still early in the process, organizations are beginning to take the right steps toward building a security culture. The human-centered aspect is closely linked to people's behaviors and attitudes, which have the most significant impact on various risks. Leveraging data from incidents and phishing simulations can help measure security culture and drive awareness initiatives. According to Participant 5, AI integration is inevitable, and organizations need to establish processes to address any ethical considerations. Taking advantage of AI's capabilities can help businesses protect themselves against increasingly sophisticated criminals. Additionally, AI can reduce the effects of human biases.

Codes	Categories	Themes
Worked 10 years with security awareness, behavior, and culture change	Experience and Expertise	Establishment and Evolution of Security Culture

Security gained importance and visibility over the past ten years	Evolution of Security	
90-95% of efforts go to the technical side	Focus on Technical Security	
Built a team of eight people to work on security culture	Building Security Culture	
Change in the right direction in the past few years	Positive Trends	
Knowledge, attitudes, behaviors	Measuring Security Culture	Measuring Security Culture
Measuring behaviors in simulated environments, using third-party tools	Methods for Measurement	
Data from third-party security tools like Microsoft Defender	Data Utilization	
AI tools for preventing attacks	AI in Security	AI's Role in Cybersecurity
Individual learning paths created by AI based on various factors	Personalized Security Training	
Ethical considerations with AI, including privacy and security	AI and Ethics	Ethical Considerations of AI
Ethical risks related to human biases	AI and Biases	
Hope AI will remove human biases but unsure if it will be possible	Addressing Human Biases with AI	
Not afraid of technological singularity in the next 10 years	Future of AI	

Table 5.
Codes, Categories, and Themes from Interview 5.

Interview 6:

Participant 6 emphasizes that security should be part of everyone's role and not seen as an additional activity. Organizational surveys and observing human behaviors can help assess an organization's security culture. According to Participant 6, the human-centered aspect should not be treated as separate, as humans, technology, and processes are interwoven. Regarding AI usage, the participant notes that since AI is fed with various types of data, the effects of biases cannot be entirely eliminated. While these technologies should be used, they must be approached cautiously, as they are not flawless. Lastly, the participant highlights that trust and transparency are the two most critical elements of a strong security culture.

Codes	Categories	Themes
Partnerships, Culture of trust, psychological safety	Organizational Practices	Security Culture Development
Informational interviews, Focus groups, Organizational health surveys, Campaigns,	Organizational Culture	
Behaviors, People-process-technology triangle	Performance Indicators	
Organizational health surveys, Informational interviews	Feedback Mechanisms	Measuring Security Culture
Behaviors, Campaigns	Performance Indicators	
Informational interviews,	Qualitative Measures	
AI technologies, Machine learning, Alerting, Tactical	Technology Integration	AI in Security Practices
Brainstorming, "Write it in this style", "Give me an idea for this", "Give me 10 names for a new website"	Creative Processes	
Tactical, Machine learning, Alerting	Operational Use	
Conflicts or ethical considerations, Biases, Legal assistant, AI-driven security systems, Human liberties,	Ethical Considerations	Ethical Considerations of AI
Blocking it, Internal tool, Speed bump,	Technology Deployment	
Freedom of choice, Technological singularity	Impact on Society	
Legal assistant	Role of AI	

Table 6.

Codes, Categories, and Themes from Interview 6.

Interview 7:

Participant 7 discusses the various approaches organizations take regarding security culture. The participant identifies a significant challenge in leadership, particularly when the strategy does not support security initiatives. The participant notes that, for culture to evolve, organizations need to focus on behaviors. Although AI is widely discussed, Participant 7 observes that not many companies are using it effectively. AI technologies should be leveraged to analyze human behaviors and holistically evolve the culture. The human element is crucial, as AI alone cannot be effective without the understanding and relationship-building that come from human communication. While moral dilemmas arise from the use of AI, humans are adaptable enough to address and overcome potential negative scenarios.

Codes	Categories	Themes
Security culture programs, Small businesses, Big brands, International retailers, Banking sector, Education sector, BIG4 consultancies	Different organizations & industries	Security Culture Development
Massive differences, understanding from a leadership perspective, Raise awareness,	Approaches to security culture	Challenges in implementing security culture
AI technologies, Integrated, Consultancy businesses, Vendors, People's behaviors, Communications,	AI in security culture	AI Integration
Catalyst for change, Conversations, Connect, Contextual, Relationship building,	Human-centered security strategies	Human-Centered Approach
AI, Human liberties, Replacing people, Moral dilemma, Large language models	AI and human roles	Ethical Considerations of AI
Risk-mitigating behaviors, Security strategy, Human intervention, Core risk-mitigating behaviors	Security strategy and human behavior	Aligning human behaviors with security strategy
Technological singularity, Short term, Lifetime, Unfamiliar position, Feeling-based, Rationally-based,	Future of AI	Perception of AI's future impact

Table 7.
Codes, Categories, and Themes from Interview 7.

Interview 8:

According to Participant 8, while the foundation for a secure organization is compliance with applicable rules and regulations, security culture is more than that. The participant notes that security culture should not be considered separate from the organization's culture. The first step to achieving a culture that values security is understanding the risk from people's behaviors. Once people realize the need for security, that is the tipping point for culture. Participant 8 supports that the shift happens when instead of the security team asking people to change their behaviors, people are addressing the security team, asking for recommendations. According to participant 8, 100% of security incidents are related to the human factor. Finally, accountability and responsibility are required for a human-centered culture to exist.

Codes	Categories	Themes
Security culture, Compliant culture	Culture	Organizational Values
Compliance is foundational	Foundational Importance	
Implementation of security culture	Security Culture Development	
Culture that values security	Cultural Integration	
Understands risk, Addressing specific risks	Risk Awareness	Organizational Practices
Situational to the organization	Contextual Adaptation	
Attitudes, Beliefs, Outward expression	Employee Perception	Employee Engagement
Interaction with security team	Employee Engagement	
Shift from push to pull	Behavioral Shift	
Trusted advisor, Pushing back on organization	Mutual Trust	
Human factor, Human-centric security	Human Factors	Human-Centered Approach
100% of incidents, Action or inaction of humans	Human Error	
Series of failures, Building resilient systems	Systemic Weaknesses	
Listening to mistakes, Non-judgmental approach	Error Management	
AI decision making, Accountability	AI Ethics	AI and Accountability
Human oversight, Just culture	Human Oversight	
Bias in AI, Misidentification	AI Bias	
Reversibility, Safeguards	AI Control Mechanisms	
Technological singularity, Societal shift	Future AI Concerns	

GenAI, Text prediction	Current AI Limitations	
Human execution, Reversibility	Extreme AI Risks	

Table 8.
Codes, Categories, and Themes from Interview 8.

Interview 9:

Participant 9 emphasizes that security culture extends beyond mere awareness and phishing campaigns; it requires a shift in behavior. To cultivate a human-centered security culture, prioritizing people and building trusting relationships is essential. The participant also highlights the importance of educating individuals about the privacy risks associated with AI technologies. Participant 9 believes that AI does not threaten job security but enhances creativity by taking over repetitive tasks.

Codes	Categories	Themes
Awareness program, Compliance, Regulations and laws	Security Culture	Current Practices in Security Culture
Home country, Europe, Maturity	Cultural Maturity	
Awareness initiatives, Reduction in real incidents, Anomalies proactively reported, Improved results in phishing campaigns	Measurement of Culture	Measuring Security Culture
SANS Maturity Model, Steps 4 and 5, Consistency, Financial investment, Change in management mindset	Program Evolution	Security Culture Development
Executive support, Limited number of staff, Human layer, People at the center	Resource Allocation	AI Integration
Initiatives underway, Hackathons, AI, Anomaly detection, Generating secure passwords, Defending against adversary attacks	AI Integration	
Privacy and data security problems, Educate about the best use	AI Ethical Concerns	Ethical Considerations of AI
Changing over the years, Repetitive jobs, Intellectual work, ChatGPT, Shallow and emotionless	Impact on Jobs	AI and Employment
Tools adapted to its reality, Customer data, Limit the sending of files, Clear education, Risks, Consequences in the event of non-compliance	AI Transparency and Accountability	AI and Accountability
Dismissing, Train AI tools, Open up the possibility, Repetitive tasks, Innovative solutions	Collaboration with AI	AI and Human Collaboration

Trusting relationships, Empathetic, Humans can make mistakes, Human-centered culture, Employees' contributions, Unique	Human-Centered Safety Culture	Human-Centered Approach
Reality, Education about AI, Security incidents, Technology as a facilitator	Future of AI and Humans	Future Trends in AI
Privacy, Non-discrimination, establishing regulatory frameworks, AI, Human rights, Laws and regulations, Transparency, Accountability,	Regulatory Measures and Public Awareness	AI and Human Rights

Table 9.
Codes, Categories, and Themes from Interview 9.

5.2 Interviewing the AI

To reiterate, the following "interview" is conducted solely for experimental purposes. While the results will be observed in order to form a better understanding on how AI technologies can be used in research, they will not be included in the framework.

The responses on the interview questions below were provided by ChatGPT.

Interview with AI:

The AI provided thorough responses when asked about its role and responsibilities. It clarified that its role is supportive, not authoritative, with decision-making ultimately in the hands of people. On security culture, the AI emphasized the importance of security awareness, compliance, and integrating security into daily operations. Its responses regarding ethical considerations of AI integration were noteworthy, pointing out that biases could result in unfair treatment of individuals and inadequate outcomes. According to AI, regular audits and accountability are essential for these technologies. Ethical frameworks and a focus on human rights are crucial to preventing potential challenges posed by AI.

Codes	Categories	Themes
Advisory and analytical tool, Analyze potential security risks, Supportive rather than authoritative	AI's Function in Security	AI's Role
Adherence to security policies, Incident reduction, employee engagement	Evaluating Security Culture	Measuring Security Culture

Privacy concerns, Potential biases in AI decision-making,	AI Ethics	Ethical Considerations of AI
Transparency and accountability, Regular audits	Ensuring AI Responsibility	Accountability and Transparency
AI can pose a threat to human liberties, Erosion of privacy and autonomy	AI's Impact on Society	AI and Human Liberties
Repetitive tasks, Opportunities for complex and creative work	AI's Impact on Employment	AI and Job Security
Culture of continuous learning, Employees trained to work alongside AI	AI and Human Coevolution	Collaboration and Coevolution
Empathy, trust, respect for contributions,	Core Values of Security Culture	Human-Centered Approach
AI handles routine tasks, Humans focus on strategic and creative aspects	AI and Human Integration	Future Coexistence
Protecting sensitive data, Encryption, access controls, Regular audits,	Data Protection	Safeguards in AI
Safeguarding human freedoms, Robust ethical frameworks	AI's Impact on Society	Technological Singularity

Table 10.
Codes, Categories, and Themes from Interview with ChatGPT.

6 Findings

In this chapter, we explore the main findings of our research, offering a thorough examination of the data we've gathered and the insights emerging from it. We are assessing whether we have addressed the research questions and will respond to those that remain unanswered.

6.1 Summary and Examination of Collected Data

In the previous chapter, we conducted in-depth interviews and presented the emerging codes, categories, and themes that resulted from our iterative coding process for each interview. In this chapter, we will examine the gathered data by consolidating the emerging themes based on their frequency of occurrence.

After consolidating the emerging themes per times of occurrence, we have the following:

Theme	Times of Occurrence
Human-Centered Approach	7
Ethical Considerations of AI	6
Security Culture Development	6
Measuring Security Culture	4
AI Integration	4
Effective Communication and Management	2
AI and Accountability	2

Table 11.
Consolidated Themes emerging from the interviews.

Human-Centered Approach: The "Human-Centered Approach" is the most prominent theme across all interviews, highlighting its central role in the research. Almost all interviewees emphasized the significance of a human-centered approach in sustaining a human-centered security culture. They stressed the necessity for diverse skills within security teams and highlighted the importance of ongoing education and awareness programs. Many, if not all, security incidents are linked to human factors. To build resilient systems, organizations must adopt a non-judgmental attitude and learn from mistakes. Trust is crucial, and recognizing that human errors are part of being human can help foster a more effective and compassionate security culture.

Ethical Considerations of AI: One of the most prominent themes from the in-depth interviews was the ethical considerations surrounding AI. Interviewees raised concerns about AI's limitations, particularly those stemming from the quality of data it relies on. They emphasized that ensuring transparency and accountability in AI-driven environments is crucial. Privacy and security were significant discussion points, while issues like freedom of choice and job security also occupied participants' thoughts. Despite the theoretical possibilities of technological singularity, it is not an immediate concern for the near future. Interviewees believe the technology still needs to advance vastly to warrant such concerns. Finally, addressing the ethical risks of integrating AI into business environments remains essential.

Security Culture Development: Another significant theme that emerged from the interviews was the development of security culture. Participants stressed the importance of investing early in security culture, noting that as fraudsters become increasingly sophisticated, employees must be empowered to protect themselves and their organizations. Integrating security culture into the broader corporate culture is essential. Effective tools for this integration include campaigns, focus groups, and organizational health surveys. A balanced approach involving the people-process-technology triangle should guide all efforts, with consistency being a critical factor in successfully developing an organization's culture.

Measuring Security Culture: Measuring security culture involves assessing the knowledge, attitudes, and behaviors of individuals within an organization. Third-party tools can be utilized to gather valuable data reflecting the organization's security culture. Key indicators include the frequency of security incidents and the level of employee engagement in security initiatives. To improve outcomes, organizations should implement awareness initiatives and encourage proactive reporting.

AI Integration: The participants discussed the multiple AI initiatives underway and the extent of AI integrations in security practices such as threat detection and response, highlighting the necessity of putting humans at the center and the importance of executive support. AI technologies should be designed to complement human skills and enhance collaboration in the future, as coexistence is inevitable. The interviewees flagged potential threats to human liberties and job security due to AI integration. They suggested experimentation with low-risk AI opportunities before moving to extended integrations.

Effective Communication and Management: While AI can boost efficiency and offer valuable insights, it's important to ensure that it complements rather than replaces human creativity. Participants highlighted that robust oversight is needed to manage AI's role in security.

Efficient communication among technical staff and non-technical team members is essential for bridging gaps in understanding and ensuring that technology solutions are implemented in ways that align with organizational goals.

AI and Accountability: Participants stated that sustaining a human-centered security culture within AI-driven environments requires careful consideration of accountability and human oversight to ensure ethical outcomes. In a just culture, mistakes are viewed as opportunities, while reversibility is a key measure to prevent unfair or inaccurate results. Clear education on AI's risks and consequences of non-compliance is essential.

It is important to note that the frequency of occurrence of themes does not necessarily indicate their relative importance. While some themes appear more prominently, this does not imply they are inherently more significant than those with lower frequency. The prominence of specific themes may reflect experts' current perspectives and priorities regarding security culture. Understanding why some themes are mentioned more often can provide valuable insights into prevailing viewpoints and emerging trends. Furthermore, examining the less frequently discussed themes can reveal underlying issues or areas that warrant further exploration, potentially guiding future enhancements and deeper investigations into security culture.

Although mentioned only once, the following themes are valuable and may reflect underlying factors that are not immediately apparent. Additionally, some of these themes are closely related and can be grouped together, suggesting they may play a more critical role than initially evident. The themes that emerge only once are the below:

Integration of Security in Daily Life, Language and Perception of Security, Emergent Outcomes from Security Practices, Cultural Integration, Cultural Shifts, Misconceptions and Conflict, Integration of Priorities, Risk Management, Collaborative Efforts, Awareness and Biases, Adapting to Technological Changes, Data Protection and Ethical Use, Skills and Adaptation, Challenges in Implementing Security Culture, Balancing Technical and Human Factors, Aligning Human Behaviors with Security Strategy, Technological Integration and Coevolution, Perception of AI's Future Impact, Organizational Values, Organizational Practices, Employee Engagement, AI and Employment, AI and Human Collaboration, Future Trends in AI, AI and Human Rights.

Interestingly, the interview with the large language model (ChatGPT) uncovered similar themes in the transcripts, with notable commonalities, especially among the most prominent ones. This alignment may stem from the influence of existing literature that is likely used to train the AI software.

Five of the seven most prominent themes from the human interviews also emerged directly or indirectly from the interview with the AI software. these themes are:

- Human-Centered Approach
- Ethical Considerations of AI
- Measuring Security Culture
- AI Integration
- AI and Accountability

As noted earlier, despite the commonalities, we will not incorporate this observation into our analysis and the refinement of the conceptual framework.

6.2 Refining the framework

In this chapter, we attempt to refine the conceptual framework by integrating the insights gained from the in-depth expert interviews. This refinement aims to enhance the framework's relevance and comprehensiveness by cross-analyzing the themes that emerged from the interviews with the initial variables and relationships outlined in the original model. Through this analysis, we will identify areas of alignment, uncover potential gaps, and introduce new dimensions that reflect the real-world complexities highlighted by the experts. The refined framework will therefore offer a stronger foundation for understanding and addressing the key challenges related to sustaining a human-centered security culture in AI-driven environments.

To reiterate, the framework variables are the below:

Independent Variables:

Security/Privacy Incidents related to AI integration
Leadership Commitment
Regulatory Compliance
Employee Engagement

Dependent Variables:

Human-Centered Security Culture
Employee Well-being and Satisfaction
Job Security
Organizational Resilience

Moderating Variables:

Organizational Culture
Industry Landscape

Mediating Variables:

Security Awareness
Employee Trust

Control Variables:

Organizational Size
Geographic Location

While the most frequently recurring themes are:

Human-Centered Approach
 Ethical Considerations of AI
 Security Culture Development
 Measuring Security Culture
 AI Integration
 Effective Communication and Management
 AI and Accountability

As mentioned earlier, the control variables are not being considered during the present research.

To refine the conceptual framework, we will perform a cross-analysis between the framework variables and the themes that emerged from the interviews, looking for overlaps, gaps, and potential new insights.

- **Overlaps:**

Human-Centered Approach (Theme) and Human-Centered Security Culture (Dependent Variable):

These two both emphasize the importance of focusing on the human element within security practices. The theme from the interviews aligns directly with the dependent variable, reinforcing its importance in the framework.

Ethical Considerations of AI (Theme) and Employee Well-being & Satisfaction/Job security (Dependent Variables):

The ethical considerations of AI are closely linked to the dependent variables: employee well-being and job security, particularly as AI's integration into the workplace can lead to job displacement and increased anxiety among employees. If left unchecked, bias in AI can lead to unfair treatment, undermining trust and well-being. Work-life balance is also significant, as AI-driven changes in the workplace could blur the lines between work and personal life, potentially causing burnout. Therefore, ethical AI practices are crucial to safeguarding job security and employees' overall well-being.

Security Culture Development (Theme) and Organizational Culture (Moderating Variable):

Developing a security culture is closely tied to the broader established organizational culture. The theme supports the idea that an organization's culture moderates the effectiveness of security practices and frameworks.

Measuring Security Culture (Theme) and Security Awareness (Mediating Variable):

One way of measuring security culture is through assessing security awareness, already identified as a mediating variable. This suggests that effective measurement practices are crucial for fostering security culture within the organization.

AI Integration (Theme) and Security/Privacy Incidents related to AI integration (Independent Variable):

AI integration is closely related to security and privacy incidents because the adoption of AI technologies can introduce new vulnerabilities and challenges that organizations must address. When integrating AI into systems, there is an elevated risk of security incidents stemming from the complex nature of AI solutions.

AI and Accountability (Theme) and Leadership Commitment/Regulatory Compliance (Independent Variables):

The theme of AI accountability, while not directly reflected in the framework, is strongly connected to regulatory compliance and leadership commitment as ensuring AI systems are accountable aligns with regulatory requirements that mandate transparency, fairness, and responsibility in AI deployment, and leadership commitment is essential for fostering a culture of accountability in AI usage.

- **Gaps:**

Effective Communication and Management (Theme):

While communication and management are critical to implementing security practices according to the interviewees, they are not explicitly captured in the current framework variables. This might suggest incorporating or emphasizing communication as a separate variable, as a new mediating/moderating variable.

- **New Insights:**

Human-Centered Approach:

The strong emphasis on the human-centered approach across both the themes and the framework highlights its critical importance. It suggests that all security-related efforts should be evaluated through their impact on the human experience, potentially leading to a better understanding of how to implement a human-centered security culture.

Ethical Considerations of AI:

The emergence of ethical considerations highlights the need to integrate ethical oversight into AI-related processes. This could suggest adding a new mediating variable focused on "Ethical AI Practices".

Employee Engagement:

While not among the most prominent themes in the interviews, employee engagement (an independent variable in the framework) remains highly relevant and important. Engaged employees are generally more committed, motivated, and aligned with the organization's values, which can significantly enhance the effectiveness of leadership commitment and ethical AI practices.

This cross-analysis has revealed substantial overlaps between the interview themes and the framework variables. However, it also identified gaps around communication and management, and the need for more explicit ethical practices within the framework.

The refined framework depicted below capture better the complexities and emerging challenges highlighted by the expert interviews:

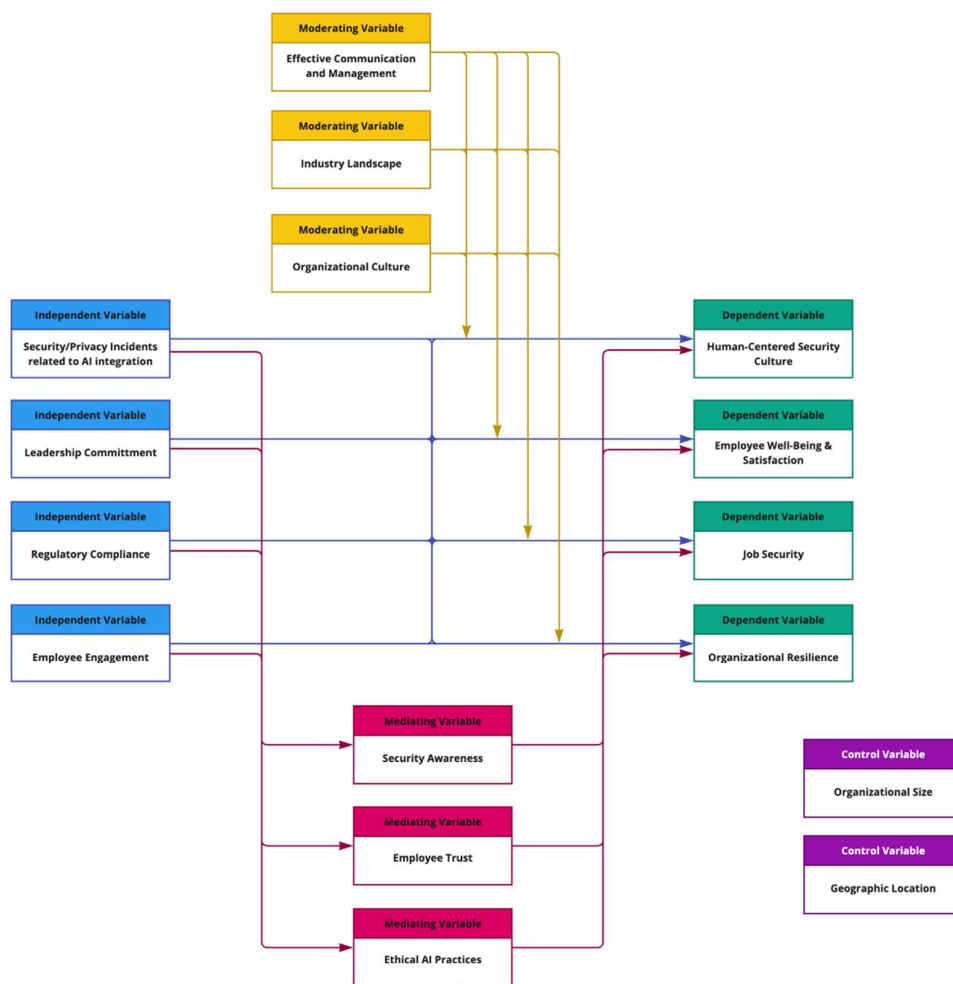


Figure 2.

Refined Framework for Sustaining a Human-Centered Security Culture in AI-Driven Environments

Organizations seeking to sustain a human-centered security culture in AI-driven environments can adopt this framework, which integrates critical components for fostering an environment that values both technological advancements and human factors, leading to a more secure and supportive workplace. Future research can further refine the framework by delving into additional themes identified from the expert interviews or by exploring new areas uncovered through subsequent studies.

6.3 Addressing the Research Questions

The first research question that this study attempted to answer was the following:

What are the key challenges and opportunities in integrating AI technologies into security culture methods while sustaining a human-centered approach?

This question was addressed through the literature review we conducted, identifying several key challenges and opportunities associated with integrating AI technologies into security culture. We explored the capabilities these technologies provide, as well as the ethical and legal implications of AI integration.

The second research question was the following:

What strategies can business organizations implement to ensure that AI-driven technologies prioritize human rights and well-being?

This question was addressed through a systemic process, starting with the development of our conceptual framework, then by conducting qualitative research through in-depth expert interviews, and finally by refining our framework with the data gathered from our qualitative research. The outcome is the refined framework for Sustaining a Human-Centered Security Culture in AI-Driven Environments.

The third and final research question which remains unanswered is the following:

What measurable Key Performance Indicators (KPIs) can be developed to evaluate the balance between AI-driven security solutions and human-centered values while accomplishing the organization's business goals?

To address this question, we propose adopting four KPIs designed to measure our framework's independent variables. By doing so, and given the established relationships between the different types of variables, we can effectively assess the overall efficiency of the framework.

The suggested KPIs are the below:

KPI Title: Reduction in Security Incidents

KPI Metric: Percentage Decrease in Security Breaches Detected by AI Systems.

Description: Measuring the reduction in the number of security incidents after implementing AI-driven threat detection compared to the baseline before AI integration.

KPI Title: Leadership Commitment

KPI Metric: Frequency of Leadership Involvement in Security Initiatives.

Description: Tracking the number of times leadership participates in or endorses security-related activities, such as meetings, training sessions, or policy updates, over a given period.

KPI Title: Employee Engagement

KPI Metric: Employee Participation Rate in Security Training and Initiatives

Description: Measuring the percentage of employees actively participating in security training programs and initiatives, indicating their engagement with the organization's security culture.

KPI Title: Compliance with Applicable Regulations

KPI Metric: Compliance Rate

Description: Evaluating the percentage of compliance with security regulations during audits, reflecting how well the organization adheres to applicable legal and regulatory requirements.

Additionally, organizations can utilize organizational surveys to improve the visibility and accuracy of the above KPIs. Organizational surveys can help measure overall employee satisfaction and well-being, providing valuable insights into how security culture impacts the workforce. These surveys can gauge employee perceptions of security culture, their confidence in the organization's protective measures, and their overall sense of job satisfaction, which are critical for maintaining a human-centered security culture.

6.4 Recommendations

Although this conceptual framework is comprehensive, it is not designed to be exhaustive. It provides a foundation for organizations to customize according to their specific needs and contexts. The framework offers a starting point for businesses to develop and refine their security practices. Future research will be essential in uncovering additional variables crucial for sustaining a human-centered security culture, offering further insights and enhancements to this framework. Organizations are encouraged to adapt and build upon this foundation to better align with their unique challenges and goals.

Our recommendation for organizations aiming to establish a human-centered security culture is to begin by conducting an audit based on this framework to assess their current situation and identify specific needs. Following this, organizations should develop tailored KPIs that align with their unique environment to track the progress of the framework's implementation effectively. This approach ensures that the framework is not only applied in a relevant and targeted manner but also allows for precise measurement and continuous improvement.

Another recommendation is to foster openness among organizations by encouraging the sharing of insights and collaboration. By exchanging ideas and experiences, organizations can help each other refine their processes for sustaining a human-centered security culture.

Finally, any recommendations from the reader's perspective are highly welcomed in an effort to continuously improve and refine the framework.

7 Discussion

Looking back at the beginning of this study, when I first selected the topic, I can now appreciate the valuable insights gained throughout the entire process. During the literature review, I had the opportunity to explore a range of publications spanning several decades, delving into theories and paradigms surrounding security culture and its evolution over time. Reflecting on the interviews, I find them enlightening. Despite my extensive experience in these discussions, each conversation brought fresh perspectives, and I believe the transcripts offer a wealth of new insights. I am eager to see where this research leads and the new avenues it may open for future studies. Human-centered security culture will undoubtedly remain relevant as technological advancements progress and ethical considerations continue to evolve.

To ensure the reliability and validity of this study, several measures were employed to enhance the credibility of the findings. Initially, the conceptual framework was developed based on my experience and the insights gained from the literature review. Analysis of the interview transcripts revealed consistency with the initial findings and also offered additional insights. By selecting a diverse group of experts from various fields, the study mitigated potential limitations that might have arisen from interviewing experts from only a single field. The use of coding methods allowed for the extraction of emerging themes, which were then compared with the framework to verify their validity.

I would like to thank all the people who participated in my research and shared their expert opinions. The framework would not have been the same without their contributions. Their insights and experiences have enriched the study and offered a more profound understanding of the topic. I am truly grateful for their time, effort, and valuable input, which have been crucial in shaping the findings and conclusions of this research.

Finally, I would like to thank the Laurea University of Applied sciences, and the Leading Transformational Change program specifically, for providing me with a solid foundation to understand the topics discussed. The knowledge I had already gained over the past couple of years in areas such as strategy, management, and transformational change greatly contributed to the depth and breadth of this research. The academic support and resources offered by the university have been invaluable in shaping my approach and analysis throughout this study. I would be remiss if I did not acknowledge the valuable recommendations and support that I received from my supervisor during this study.

References

Printed

- Alpaydin, E. 2016. Machine learning: The New AI. London: MIT Press.
- Bowen, H. 2013. Social Responsibilities of the Businessman. University of Iowa Press.
- Bryman, A. 2012. Social Research Methods (4th ed.). Oxford University Press.
- Carpenter, P. 2019. Transformational Security Awareness. 1st edition. Wiley.
- Carpenter, P., Roer, K. 2022. The Security Culture Playbook. 1st edition. Wiley.
- Cerra, A. 2019. The Cybersecurity Playbook. 1st edition. Wiley.
- Chrisley, R. 2020. A human-centered approach to AI ethics: a perspective from cognitive science. In: Dubber, M., Pasquale, F., Das, S. (eds.) The Oxford Handbook of Ethics of AI. Oxford University Press, 463-474.
- Crowther, D., Aras, G. 2008. Introduction to Corporate Social Responsibility. Ventus Publishing.
- Custers, B.H.M., Fosch-Villaronga, E. (eds.) 2022. Law and Artificial Intelligence. Springer.
- Denning, S. 2011. The Leader's Guide to Storytelling. 2nd edition. Wiley.
- Elliott, A. 2019. The Culture of AI: Everyday Life and the Digital Revolution. New York: Routledge.
- Friedman, M. 1970. The Social Responsibility of Business Is to Increase Its Profits. New York Times Magazine, 13 September 1970, 122-126.
- Gollan, P. 2000. Human resources, capabilities and sustainability. In: Dunphy, D., Benveniste, J., Griffiths, A., Sutton P. (eds.) Sustainability: Corporate Challenge for the 21st Century. Australia: Allen & Unwin Ltd, 55-77.
- Hadnagy, C., Fincher, M. 2015. Phishing Dark Waters. 1st edition. Wiley.
- Hayden, L. (2016). People-centric security: transforming your enterprise security culture. McGraw-Hill Education.

Kivunja, C. 2018. Distinguishing between Theory, Theoretical Framework, and Conceptual Framework: A Systematic Review of Lessons from the Field. *International Journal of Higher Education*, 7, 44-53.

Kuhndt, M., Tunçer, B. 2007. Sustainability as a Business Challenge: The Concept of Responsible Corporate Governance. In: Raimund B. (ed.) *Corporate Governance of Sustainability: A Co-Evolutionary View on Resource Management*. Edward Elgar, 8-25.

Kurzweil, R. 2008. *The Singularity Is Near: When Humans Transcend Biology*. Duckworth Overlook.

Liao S.M, (ed.) 2020. *Ethics of Artificial Intelligence*. Oxford University Press.

Miles, M. B., Huberman, A. M. 1994. *Qualitative data analysis: An expanded sourcebook*. 2nd edition. Sage Publications, Inc.

Read, V. 2000. Technologies and processes for human sustainability. In: Dunphy, D., Benveniste, J., Griffiths, A., Sutton P. (eds.) *Sustainability: Corporate Challenge for the 21st Century*. Australia: Allen & Unwin Ltd, 78-122.

Revett, K. 2008. *Behavioral Biometrics: A Remote Access Approach*. Wiley.

Roer, K. 2015. *Build a Security Culture*. IT Governance Ltd.

Russell, S. J., Norvig, P. (eds.) 2022. *Artificial intelligence: a modern approach*. 4th edition. Pearson.

Sharghivand, N., Derakhshan, F., Classification and Intelligent Mining of Anomalies in Industrial IoT. In: Karimipour, H., Derakhshan, F. (eds.) *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*. Springer, 163-180.

Sharghivand, N., Derakhshan, F., Data Security and Privacy in industrial IoT. In: Karimipour, H., Derakhshan, F. (eds.) *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*. Springer, 21-40.

Soyka, P.A. 2012. *Creating a Sustainable Organization: Approaches for Enhancing Corporate Value Through Sustainability*. FT Press.

Taticchi, P., Demartini, M. (eds.) 2021. *Corporate Sustainability in Practice: A Guide for Strategy Development and Implementation*. Springer.

Tegmark, M. 2017. *Life 3.0: being human in the age of artificial intelligence*. 1st edition. New York: Alfred A. Knopf.

Vinge, V. 1993. The coming technological singularity: How to survive in the post-human era. Whole Earth Review.

Weber, H. 2021. Hacking AI: Big and Complete Guide to Hacking, Security, AI and Big Data. Amazon Digital Services LLC.

Whitman, M.E., Mattord, H.J. 2012. Principles of Information Security. 4th edition. Boston: Thomson Course Technology.

Yavuzkilic, S., Akhtar, Z., Sengur, A., Siddique, K. DeepFake Face Video Detection Using Hybrid Deep Residual Networks and LSTM Architecture. In: Gaurav, J., Vivek, K., Raghavendra, R. (eds.) AI and Deep Learning in Biometric Security: Trends, Potential, and Challenges. CRC Press, 81-104.

Zeide, E. 2020. Robot Teaching, Pedagogy, and Policy. In: Dubber, M., Pasquale, F., Das, S. (eds.) The Oxford Handbook of Ethics of AI. Oxford University Press, 789-804.

Zhu, L., Xu, X., Lu, Q., Governatori, G., Whittle, J. 2022. AI and Ethics - Operationalizing Responsible AI. In: Chen, F., Zhou, J. (eds.) Humanity Driven AI: Productivity, Well-being, Sustainability and Partnership. Springer, 15-36.

Zinatullin, L. 2016. The Psychology of Information Security. IT Governance Ltd.

Online

Swaen, B., George, T. 2024. What Is a Conceptual Framework? | Tips & Examples. Scribbr. Accessed 20 August 2024. <https://www.scribbr.com/methodology/conceptual-framework/>

Appendix - Interview Transcripts

Interview 1:

Spiros Katiforis *The first question I have for you is if the organizations that you have worked for have established a security culture.*

Interviewee 1 Yes, I would say so. The one thing for me personally is I **don't use that terminology**, so I often don't think of it in that way, because if **you take the term security culture, it can seem like it's separate as an entity from other forms of culture**. And so, I tend to think about it more as the security part of the day-to-day activity, whether it's the X company I am working at currently, or, where I've worked previously. And yeah, **people think about it. People ask about it. They're intrigued about it.** We can ask questions and they react to posts or they will personally reach out, and there's just a level of low-level interest in the topic which promotes a lot of activity and people learning basically. It's the same wherever I would work, I **would never call it security culture specifically because I don't really enjoy the term**. But do we have an idea of it? Yes, yes, absolutely.

Spiros Katiforis *That's very interesting. And how about the human factor, how would you define a human-centered culture in general?*

Interviewee 1 So, for me, **the main focus is around the human factor and being people-centric and that is all about putting people at the center of a cybersecurity conversation** and that can be at any level. So, whether you're designing a product, it could be that, well, **how do we embed the security features? What is the effort of actually then taking part in doing the security activity and how do we better design for the security interaction?** Because if the security interaction isn't well thought through, then **people often don't use it or they might start using it and then not because it's too cumbersome**, and so forth.

So how do you plan ahead for those sorts of things? And if there is going to be a blocker, then **how do we message people** about the fact that, OK, this is a change, but there is a reason for it and how do we deal with that is important and **consider that whole journey from end to end instead of just pushing stuff out at people and thinking they can and will do it because I have told him to because people have busy lives and other things to do that security isn't there on the front of their mind**. Also acknowledge that when designing like I said, a product or when designing messages is **that to be people-centric is to actually appreciate that most people have already heard these messages**. They are adults

and they have seen security in many, many different ways in many different companies in the real life, in the jokes that people make on TV and so forth.

So, **they already have a preconceived idea of what security is and how do we work to that assumption and how do we work to that coping strategy that they've already created is really, really important** because what we often do is **we tend to tell people things about security as if they are children** and as if they just need to do it and then they're secure. And technically that isn't true because it depends on the situation and not all security activity is equal. Some things take longer. Some things do not require that much effort. And **what we do in security, we determine everything then to be well. It's just a list of 10 things, and they're all easy but easy for who? And easy for what purpose? And easy in what way?**

So to try and move away from being very conscious about this sort of language that we're using that sort of perceptions that we have internally as a security team as well as really important because if we feel that people are just lazy or things are easy, then that's what we project and they don't. And then **that's what security becomes to other people.** And then when they can't do it or they struggle, **they feel shame and they don't want to take part because you've made it so that they have nowhere to go with that conversation.**

So they're just like, well, I can't do it. I'm not technical, this isn't for me and I'm not taking part and the main thing with people and security is **how do you embed it into their everyday life?**

Spiros Katiforis *And now, with all these developments in AI technologies, do you identify any possible conflicts or ethical considerations in business environments?*

Interviewee 1 The main concern I have is **people's ability to use AI in a way that is useful.**

But that doesn't quite work for people in most organizations because it depends on the organization, **how you should say things to people, what's important to them, and getting that nuance is really, really important.** So using AI to help you think of something or to suggest an idea is fine, but what I worry about is **when that's used as a default.**

Well, this is then the answer because the computer said so and then **they don't invest in the creativity and ingenuity of the people in this space to actually add the for want of a better phrase, special source.** That is the thing that then connects people.

And then they can relate to it, and then it just becomes a very mundane and very static sort of messaging, which we already kind of have and doesn't particularly work very well.

But then that **will just get more and more embedded.**

So, **how do we make sure that it's balanced?** It's really, really important because, realistically, it just becomes more of a scale problem because more people have access.

Spiros Katiforis *That's leading to my next point. What measures can we facilitate to ensure transparency and accountability so that we can secure the human aspect?*

Interviewee 1 So I think **the one thing I would say to people is that if you like using AI or what have you or asking them to do extra tasks**, for example, you're moving to a password list, so you have to use two-factor authentication. **And these are things we've done and we've done it in this way for this purpose**, but hopefully this will help because and then say **it may take a moment to learn because we are asking you to change something** and then to say **this will probably take you 10 minutes, 30 minutes.**

So, **give yourself time. I don't expect you to do everything all at once.**

For example, you can do something if you're gonna do one thing. **Now this is the most important. Tell them. Don't give them a range of options.**

Just tell people what you expect in the moment.

Is this because for us right now this is the most important thing?

If there are lots of other security tasks **I can tell you not to do them, but at the moment do this and then we can move on to the next step** and think about just **being honest in how you communicate that to people.**

And like I said, this is where things like AI and so forth are quite difficult **because you need to know the culture of your organization more.**

You need to know the people and the work that they're doing to be able to add that honesty in.

So, this is where that balance is. You can get the general messaging and the concepts from if you're new, or if you're lacking imagination for a moment in your day, which may happen using that, but then also **remembering to add yourself as a person and remembering that kind of humanity in it.**

And balancing that so that **when people do it, they can feel the success for them.**

So, **they feel that they've achieved something and they feel that it's very approachable and doable.**

So, **you're not setting them up for failure, basically.**

Spiros Katiforis *And what would be in your opinion the key components of human-centric culture?*

Interviewee 1 So that's an interesting question. You know, it's really strange and I do consider this quite a lot because I wonder how I get the message that I say across to people and **the thing that I come back to all the time is how we are consciously considerate of others** and what I mean by that again is the time that **they need to take the learning journey may need to take** them on. And the fact that actually they're busy people already and **how do we fit in?**

So instead of saying and expecting them to become security experts, as the expert, **it's my responsibility to be able to give a message to them that they understand.**

So key component to me is **being really conscious about what you're asking, and being considerate about the thing you're asking.**

Achievable. **What does it mean to be achievable? How long does it take and then to be really realistic about actually when will they do it? At what point and how much can they get done at once?**

So **these are the elements that I think are so key, because if you don't consider those things,** what happens is people will do whatever they need to do and it **creates emergent properties and emergent behavior that you aren't planning for.**

But if you think things through in a slightly more logical way and you're very realistic about the fact that people will do things in a different way but you **don't dismiss them, you don't condemn them.**

For that, you just accept that it happens. You can plan better and you can take into consideration those elements and then you're more realistic and it means that **when people ask for things in the organization and they need reports, you can give them a more rounded view as well.**

And this has happened and phishing is probably the best example.

But **these are elements that then you can add in because it allows you to bring in conversation about how people interact and allows people then to see the world a bit differently about how to create support structures around people to make sure that they feel supported and not condemned.**

And that then is a **whole element of thinking instead of just doing that often.**

What you see as a transaction if I do something then they have to do it and then that's changed behavior and it hasn't that it doesn't work like that. Is not so straightforward.

There are loads of other **adjoining pieces and emergent properties, emergent behaviors that will affect the behavior**, and you just need to think that through and **be really conscious and considerate and realistic about how you're actually doing those things.**

Spiros Katiforis *This next one is more of a question influenced by the sci-fi literature, but do you foresee the evolution of AI and technology threatening human liberties, for example, job security?*

Interviewee 1 That's a bold question. Ah, **I think it will.** In the concept of it. AI is just the new thing. It's been said that this is the new savior to our world. This means that all of these companies are gonna save all of this money, and they are going to be able to streamline everything. But and that panics people because it **sounded really drastic and it sounded really deterministic that they're just gonna close things off.** But **do I think it will actually happen? I don't think it. I don't think it will have the impact that people think because, in actual fact, there are a lot of issues in the technology itself.** There's a lot of ways and **you see that already.** So for example, I tried **testing out AI. See what it can do.** Write me a fishing template, for example. Interestingly, **it tells you that this is a phishing simulation.** Don't misuse it and all of these sorts of things, and then it **puts phishing simulation in brackets throughout the entire email.** So, it doesn't just put like a header warning like don't misuse it but interestingly **puts the message throughout the email.** So, unless you don't read that, you could send that without realizing it. So, they are already thinking about the ramifications. The main issue that I see is that **AI allows specific scaling,** so things will become more frequent and quicker to the market, like with threats and so forth. Because, well, it's just quicker to achieve with an AI and I've no idea how that would ever be stopped. **But it does impact liberties.** It'll be impactful, but **I think it would be managed because just the technology as you see, the Internet is full of things that don't make sense.** So I think there will be a balance. It will be interesting to see how that develops, but I don't think it's quite at the point of being too concerning yet.

Spiros Katiforis *So what do you think about what is called "technological singularity"?*

Interviewee 1 **Don't get me wrong, I love that concept.** And the reason I say that is because **we know now that a lot of the data that exists on the Internet that businesses keep that that just exists in the world, that the quality**

and the and so forth, A is a very hard to manage and, B, the quality isn't very good.

So how would they construct something from it?

Because there'd have to be a lot of management around it and doing it wrong.

It's possible, but it I think it would just take a lot longer than people appreciate because there are lots of issues and we've seen it over the years like they've tried AI stuff before and where they've had to turn it on and then they have to turn it off and then things like that.

So that is all down to the quality of data that is being put into these systems and that is quite hard to manage because at the moment the data is everywhere and it could be anything.

And how do you make that manageable? So that you could make an AI that can work.

Spiros Katiforis *Thank you so much for all this information, and for the talk that we had today.*

Interviewee 1 Thank you.

[End of Interview 1]

Interview 2:

Spiros Katiforis *Has your organization already established a security culture?*

Interviewee 2 Yes. And I think this is something that my current organization and my previous organizations have invested in very early. And I think the security landscape changes so frequently and it's very, very complex.

And I think we're in a world now where even the fraudsters and the criminals are actually, well set up and in fact probably better set up than some organizations in terms of the tools that they use.

And you know, it's not something new when we read that many of the attacks are originating from phishing emails or from something that involves a human.

And I think from a culture perspective, my personal view and is that this is not something that could be done overnight or can be implemented and it's something that's considered done. And I also believe that security culture should be part of our overall company culture as well. So it's a way of working and ensuring that we're empowering our employees to set themselves up to be their best selves at work but also to protect themselves.

Spiros Katiforis *And would you define the security culture in your business environment or other business environments you have worked in as human-centered?*

Interviewee 2 Yes, I think so. I think it's predominantly human-centric however, I think we need to know what the problem is.

I think we've matured in recent years, whereas before, ten years ago you would have understood the threat and you would have pushed that comes to, a huge community almost assuming that everybody had the same passion for security and protection as the security teams. But I think we've learned in the last couple of years that's not the case at all.

So, you know, we've moved and progressed in terms of the critical skills of the security culture teams, and we need marketers, we need content, and digital creators to really create and nurture an environment that people want to follow.

And opposed to "you must do", "you can do".

And so, there is a huge investment and I find myself all the time that I need to challenge the way we do things in terms of how can we measure and our culture.

But I do think it is human centric and with a surrounding team that actually needs to support the security teams.

Spiros Katiforis *And has your organization or other organizations you have worked for integrated AI technologies into its security practices?*

Interviewee 2 I think the situation is that we are absolutely on board and we are looking at test cases and we're looking to see what we can do. If I'm being honest, it's still a little bit unknown.

Now, when you balance this against what we're seeing from an AI and a security threat perspective, and you can see where the criminals and fraudsters have already progressed.

They're using AI to harvest, and I think we absolutely have established that AI plays a part in security culture and security prevention.

We need to know how we can safely do it, considering ethical decision making which is getting a huge focus at the moment right now. And to figure out what we're going to do, yes.

Spiros Katiforis *Do you personally identify any conflicts or other ethical considerations in the deployment of AI-driven security systems in business environments?*

Interviewee 2 Yes, I think. AI is going to have huge potential for many of us in how we work but I also think as humans, we also need to make sure that, we create environments to ensure ethical decision making as part of that process.

So even if you think about products and services in telecoms, we've gone from 2G to 5G and already conversations are happening about 6G.

So, what are we doing to ensure that security and privacy and AI and decision making was part of our consideration right from the concept of what we're doing.

With **security by design** and **AI by design** and making sure that the **ethical consideration** is in there. And there's that balance between getting excited about what AI can help with.

But then the **privacy aspects** as well might need to be considered as well. So, I think the key here is ensuring that you've got **the right people in the room** for those conversations.

Spiros Katiforis *My next question is if you are anticipating AI to pose a threat to human liberties such as job security, and what measures do you believe are necessary to ensure transparency and accountability? And how can organizations foster collaboration and Co-evolution between AI and human personnel?*

Interviewee 2 Yeah, I think we're on a journey. I think **what we need to do is we need to learn, we need to learn externally.** We need to get absolute experts in. **We need to listen to what the research is telling us.**

We need to see where the opportunities are and then we **need to design the right way** and you know, if you think back 20 years ago when there was a myriad of other risks that we had to manage.

The key is collaboration and having the right process and the right information at that time and working together. I think it is key that we spend time, but we don't move too fast.

In organizations, I think **we also need to consider how we might experiment with some AI opportunities** that are not going to pose **inherent risks** that we should be concerned about.

So, **we see the benefits**, we see what we could do, but then we need to understand **what is the use case or what is it that we're working towards which might have more risk**, and how we can ensure that we've got the **right competent resources.**

Spiros Katiforis *So according to you personally, what would be the key components of a human-centric security culture?*

Interviewee 2 I think **when organizations have the right culture and tone from the top there is an understanding of what the risk is. Adequate oversight of the board in a way that it becomes part of our way of working is required.** What can happen in some organizations is that **when an event happens and then it's the enormity of that situation or that crisis event that actually negatively impacts our cultures.**

So, in my view it is prevention and ensuring that you are creating a culture. That's having one culture, not having a company culture or a security culture, but having one culture and actually ensuring that the security culture and the security behaviors underpin the strategic objectives of the organization. For many organizations, it's about customer trust. It's about ensuring that you know our reputation is seen to be a company where individuals that customers want to be with, want to be part of that brand. It's a trusted brand.

It's a loved brand, so with security culture, we need to be able to tell our stories in a way that wins the hearts and minds of our employees and our boards because quite frankly, security is quite complex.

It's ever changing and we're seeing it play out in media more now.

Look at the news and, you know, in terms of cyber attacks, State-sponsored national attacks, all of this. So, you know, it's to try and demystify, I guess, some of the more complex than topics that people resonate with because it's the small nudges.

It's the small behaviors. It's the small changes that organizations are working really, really hard with their employees and I think it's interesting because, the debate is, security, culture, security awareness, how effective is it, you know?

And I'm quite sure that if you were speaking to too many CISOs they don't really get it because you know, we should have a zero-trust environment.

We should have this, but in the way that we are progressing so fast through digitalization, we can't just switch the button off. So, we've got to figure out how we have all of our controls that are compensated controls. But having open conversations and moving to a stage where we're acknowledging employees in what they do right.

How many people in our organizations are doing the right thing or do they want to do the right thing? They want to talk, they want to speak up, and live by the security and spurs, as we call it here in our organization.

And so, we need to amplify that and make them feel and that they're playing a huge part to our overall strategic delivery.

Spiros Katiforis Thank you so much for this valuable information.

Interviewee 2 Thank you.

[End of Interview 2]

Interview 3:

Spiros Katiforis *Have you already seen in the business environment you have worked at a security culture being established?*

Interviewee 3 Yeah. And I think that our case is a bit interesting. It seems like the **security culture is still developing** as the company has been around since around 2000 or 2002.

However, it was still around three years ago when they had decided to start the group security, and so I mean, it's still a fairly developing security group, which means that with around **18 years or so of kind of it essentially just being a developer haven, then security wasn't at the forefront of their mind.**

So that's honestly still been a **very big challenge**, it's or at least was, in the beginning, kind of making sure that they **understand that security doesn't inherently mean that we want to serve as roadblocks.**

And I think that that can at first come into a bit of a conflict where you need to establish it.

No, **we actually want to make sure that development can go safely and securely and without disruption.**

And if you do have a **security incident, then that can be extremely disruptive.** And so I think that was more of the initial part and it definitely has been growing. And as far as security culture, where we've had more like **cooperation with R&D** for example, it's still a work in progress.

Spiros Katiforis *And how would you define a human-centered security culture?*

Interviewee 3 I think **for human-centered security culture**, that's also been something where especially in a more techie company, we really have only thought so much about **technical security** where we had it handling all of the security before and now. And I'm not from a technical background.

I'm very much from a **security and policy background**, so it is then **making sure that there is an awareness**, even though you may have technical competencies and everyone's extremely well versed in the technical aspects.

And a lot of people may think that since they know the technical aspects, they may be **immune to a lot of human risks.**

So, I think it is establishing the understanding that you can have technical competencies, but we still need to be aware of our **unconscious biases or potential blind spots.**

Spiros Katiforis *And do you foresee any conflicts or ethical considerations with the deployment of AI technologies in business environments?*

Interviewee 3 Yeah, I think, I mean, one of the biggest changes in the last year or like kind of biggest developments for companies was the creation of **ChatGPT**. I think that that was a **huge disruptor** especially when you are in a **more fast-paced environment** then you can see that and immediately think “oh my gosh this can be amazing, **this can help us develop really quickly**”. We can write code super well, and I think cases like the **Samsung data leak** as soon as ChatGPT came out. I also was like, “oh, great”. This is super helpful for policies, but then you look and you realize that there are a lot of **security considerations** and **a lot of risks when it comes to data privacy**.

And so, then when it came out, we kind of had to say, I know that we're all excited, but there does need to be some kind of ground rules for this as far as when you are analyzing code with an AI tool, we need to make sure that we are getting an actual **business model** for it so that we have the **data protection**.

So, I think there are a lot of **good intentions** and a lot of excitement about AI. But I think that there needs to be also a bit of taking a step back and looking at what actually can we do to make sure that we can utilize this and utilize really good tools while still being conscious of potential risks.

Spiros Katiforis *Do you foresee any threat to job security for people or other human liberties that might be threatened because of AI?*

Interviewee 3 I don't necessarily know if I think that **the human element is still incredibly important** also in technical aspects, but I think that one thing is that **we need to embrace the fact that AI is growing** and I think that it's **not necessarily jobs that will be replaced by AI** and but it might be that **people that know how to utilize AI tools in good ways will be replacing the ones who don't**. And I think that it's, yeah, the human element is always going to be needed in some dimension.

Spiros Katiforis *And what would be, in your opinion, the key elements of human-centered security culture?*

Interviewee 3 I think a huge part of it is **communication** and I think that that's one of the biggest things also with communicating between technical and non-technical people. Making sure that the people that do handle the cyber part of security are actually **communicating with people** like me who work in the **human-centered aspect** and that there needs to be a lot of **cooperation between the two**, you can't exist in a silo on your own.

Spiros Katiforis *If you could prioritize between policies, and other technical measures, what would be the most important?*

Interviewee 3 I mean, I think that when it does come down to it the **technical aspects** are probably **at the forefront** of being one of the more crucial, but also, we can have as many **technical safeguards** as possible, but if someone is not aware or if their behavior doesn't align with the more **human-centered aspect**, I think that it's even more important than just being aware of the technical risks. If someone is not behaving in a secure way then it doesn't matter how good we are technically, because that is a **huge gap**.

Spiros Katiforis *My last question is about the technological singularity. I'm not sure if you're aware of this term.*

Interviewee 3 No. Can you explain it a bit more?

Spiros Katiforis *It is the idea that someday, AI will progress to the extent that it will surpass human intelligence. And I was wondering, do you see that happening in the future with all the evolution of AI and technology? Do you see the human race threatened by technology?*

Interviewee 3 I do not necessarily see it being threatened, but definitely changed. We will have to start working in tandem with AI tools and I think that it's. It is just an evolution that's going to be happening. And I think that that evolution kind of happens all the time. For example, as far as working remotely, that's a **huge change** that happened, and people had to get on board with the fact that you aren't going to have in-person meetings all the time. So, I think that **we need to have adaptations**.

Spiros Katiforis Thank you so much for your participation in my survey.

Interviewee 3 Thank you.

[End of Interview 3]

Interview 4:

Spiros Katiforis *Has your organization/business environment already established a security culture?*

Interviewee 4 All companies have a security culture. It is a part of the corporate culture. The corporate culture influences the ideas, customs, and social behaviors within organizations. **Security should always fit with the corporate culture while prioritizing security at all levels of the organization**, from top management to entry-level employees, and **integrating security practices into daily workflows**. The key is recognizing that **security isn't solely a tech issue but a widespread organizational responsibility**.

Spiros Katiforis *How would you define security culture within your organization and how is it measured? Would you define it as human-centered?*

Interviewee 4 Security culture can be defined as the ideas, customs, and social behaviors of an organization that influence its security. A human-centered approach to security culture focuses on the role of individuals in maintaining security, emphasizing training, awareness, and empowerment.

It's measured through various metrics, including **compliance rates**, the **frequency of security incidents**, **employee knowledge levels**, the results of simulated phishing tests, **the opinion of employees about security in general**, behavioral observation by use of SIEM/SOC information, top management decisions, etc.

Spiros Katiforis *Has your organization integrated AI technologies into its security practices?*

Interviewee 4 Many organizations are currently **integrating AI technologies** to enhance their productivity, also in security. **AI can process large volumes of data to detect threats more efficiently** than traditional methods, automate responses to common security incidents, and predict potential vulnerabilities. For example, some clients build a **Virtual Information Security Officer (VISO)**. An A.I. that was trained to go through all 3rd party documents and come up with a summary of all relevant information to streamline the process of safely onboarding new clients in a faster way. **Efficiency increased from 1 month to 3 days.**

Spiros Katiforis *Do you personally identify any conflicts or other ethical considerations in the deployment of AI-driven security systems in business environments?*

Interviewee 4 The deployment of AI-driven security systems **raises several ethical considerations**, such as **privacy concerns**, **the possibility of bias in AI decision-making**, as well as **the transparency of AI operations**. There's a balance to be **struck between enhancing security and protecting individual rights**.

Spiros Katiforis *Do you anticipate AI posing a threat to human liberties and security within business environments? Do you foresee it affecting human job security?*

Interviewee 4 While AI can streamline and improve security measures, it also poses **potential threats to human liberties and job security**. The automation of surveillance and decision-making processes could infringe on privacy rights and reduce the need for human personnel in certain security roles. The challenge is to **leverage AI's benefits while mitigating its risks**. I also think there is a **threat for humanity and talent** in general. In the new A.I. age we will have new people coming into roles where they used A.I. in order to get a degree. In my opinion **the educational system should adapt** to this.

Focus on how to use A.I. how to verify the correct outcomes, how to verify the truth...

Spiros Katiforis *What measures do you believe are necessary to ensure transparency and accountability in AI-driven environments regarding security?*

Interviewee 4 **Transparency in AI-driven environments can be ensured through clear policies on AI use, accessible explanations of AI decision-making processes, and independent audits. Accountability involves establishing mechanisms for addressing any negative outcomes of AI deployment and ensuring that AI systems comply with ethical standards and legal regulations.**

Spiros Katiforis *How can organizations foster collaboration and coevolution between AI and human personnel?*

Interviewee 4 **Organizations can foster collaboration by designing AI systems that complement human skills, providing training for employees to work effectively with AI, and encouraging a culture of mutual learning and adaptation.**

Spiros Katiforis *What are the key components of a human-centered security culture?*

Interviewee 4 **Key components include continuous education and awareness programs, empowering employees to take proactive security measures, fostering an environment where security concerns can be openly discussed, and ensuring leadership demonstrates a commitment to security.**

Spiros Katiforis *How do you see the future coexistence of AI and humans in business environments?*

Interviewee 4 **I hope the future coexistence of AI and humans in business environments will likely be characterized by AI augmenting human capabilities rather than replacing them. Success will depend on careful management, ethical AI development, and fostering environments where humans and AI can complement each other's strengths. But when we look at human nature which is in my opinion destructive, I don't think the eventual outcome will be best for humanity. Our threat actors won't be doing all the above.**

Spiros Katiforis *How can humans safeguard their freedoms in the event of Technological Singularity?*

Interviewee 4 **Preparing for Technological Singularity involves establishing strong ethical and legal frameworks for AI development, promoting widespread understanding of AI capabilities and limitations, and ensuring that decision-making processes remain transparent and inclusive. It also requires global cooperation to manage the societal impacts of rapid technological advancement. The above is the perfect situation. But again, when we look at human nature I am not very positive about what is**

coming in the future. I hope A.I. will make us leap as Humanity... But it is going to be a 50/50 outcome.

Spiros Katiforis *Thank you for your responses*

Interviewee 4 Thank you.

[End of Interview 4]

Interview 5:

Spiros Katiforis *Have you experienced in the business environment that you have worked for an establishment of security culture already?*

Interviewee 5 I've worked very hard for this at least because I worked for close to 10 years now with security awareness, behavior, and culture change topics. That's really been my focus since the start, so I worked for large global companies in the manufacturing space as a consultant and then in retail. Four years as their head of security, culture, and competence. And what I can say is that I've I've seen that.

Of course, security has gained in importance and visibility over the past ten years, and still today most of the focus goes to the technical side of security.

You know, 90 percent, 95% of the efforts still go to the technical side, but I do see that there are more and more people realizing that, OK, it's not only about this, and yes, we also need to think about our people and what they do basically. And as you know, we can put as many technical layers as we want. We still need to also think about the people layer.

I worked very hard for this and I can just say then that at my previous company, at least when I started, there was just one security position. It was just me and I built a team of eight people to work specifically on security culture.

So that shows that, at least in this company, I was able to prove the importance and the impact of what we were doing. And when I talk to others in the field, I feel like, you know, of course, it's very certain organizations don't do this at all.

Some are just starting, so it's still a little bit early, but there's been a change in the right direction in the past few years for sure.

Spiros Katiforis *So you would say just to recap that security was not a focus until like 10 years ago? I would agree here with you because I have also experienced that. Also in the part that businesses have just started realizing the importance of a security culture. Do you have any experience with measuring security culture?*

Interviewee 5 Yeah, I have my own method here too. It's not something that is really published anywhere, but I think the simplified version of defining it is 3 components: knowledge: what people know about security, attitudes: how they feel about it, and behaviors: what they do about it. So with this, you have actually everything that is security culture and you can think that some elements that you might think about, they influence one of those three elements and so that you can specify to that. So I try to measure those three elements every time I join an organization or work with an organization. What are people feeling about security?

What do they think about this topic which is just having surveys and focus groups?

So that's the soft part of security culture. And then I focus a lot on behaviors because that's what is gonna have the biggest impact on the actual risk, right?

And so I measure behaviors either in simulated environments, doing phishing simulations for example, and looking at reporting rates, the classic using third-party tools.

Collecting data from third-party security tools like Microsoft Defender, if it's an organization that uses Microsoft, or the proxy, or the CASB so that we can find if people using shadow IT, or, who is having malware alerts on their devices.

Or if they are using USB sticks or all those kinds of things because security teams have a lot of telemetry basically on human behaviors. But these often stay with the SOC (Security Operations Center), right?

Actually, you can use this information to drive the security awareness.

So yeah, I try to get as much of this data as possible. If I can't get any data that is neither simulated nor based in real life but other third-party security tools, then I might just ask the question :

"Do you do this often or do people in your team do this?" You know, to try to collect as many insights as possible.

Spiros Katiforis *Do you personally identify any conflicts or other ethical considerations within security business environments now that AI technologies are starting to integrate within them? For example ChatGPT. How we can secure business environments from the wrong usage of AI systems?*

Interviewee 5 Yeah, it's a very wide question. You mentioned ChatGPT, so I will refer to specific examples about that. I think that it's impossible to go against the current, and people are gonna use AI so I would just strongly recommend companies pick one tool that they can offer to their

employees where they have a company subscription for it so that they make sure that the data that is put in there is only used for the company and it's not shared for training purposes or anything. But you know that AI is used in a lot of parts of most organizations nowadays.

So I was talking more about privacy. But with AI, its ethical considerations can go further than security and data protection. So I think there are concerns and there needs to be processes to address those concerns in organizations so that there's reasonable use of AI.

So that's just needs to be kind of framework I would say.

Spiros Katiforis *Do you anticipate any threats to human liberties? For example, do you foresee AI software start making decisions instead of people?*

Interviewee 5 **Yeah, but I think that can be a good thing. There's , of course, an opportunity in this, right?**

And giving the cliché answer here, when it comes to cybersecurity, we know that criminals could use AI to, for example, make more advanced phishing emails or make more of them in an easier way instead of having to create them, they just ask, you know, generally to create a lot of them. Or to create new malware, create deep fakes, right?

It can be used by the criminals, but I think there's lots of ways where it's already used also in different security tools to try to prevent some attacks. The CISOs of the companies I work with use AI for example in three different ways.

I'll talk about them very briefly, so , the 1st way is for training people.

Every single employee in your organization can receive individual learning paths that are created in part by AI based on where they are in the organization or how long they've been in the organization, their country, their language, their department, their job function, and their previous performance, their previous behaviors because we want to have training and coaching that is as relevant and targeted as possible.

If you're a security awareness team of one person, you cannot do that.

You're gonna do a massive training company or communication company for everyone that will be very generic. But with AI and with automation we can achieve much more targeted and relevant messages for everyone.

I don't even need to talk about the two other ways in which we can use AI as I think that's a really amazing way to save a lot of time both from the security team's perspective but also from the user's perspective by only getting things that are relevant to them and not generic training that they find boring and make them lose their time.

Spiros Katiforis *So what do you suggest? I agree with you that we need to embrace this technology and not just avoid it , or, be afraid of it in terms of seeing it as a threat for human liberties.*

It's an opportunity especially for security experts to be able to build more individualistic tools that can approach people in a way that a typical security awareness program, for example, cannot really, approach them.

Interviewee 5 **That's really from the security perspective.** And again, I would say **always embrace the change.** But of course, **there are ethical considerations and risks related for example to human biases.** That is something to think about during the development of these tools and to check regularly, to audit. But I would still use them.

Spiros Katiforis *So, just to take you to another dimension, mostly because you mentioned human biases and it's a very important part. So, I was wondering, do you believe that the usage of AI technologies can help prevent or avoid human biases?*

Can it resolve issues that we have because of human biases or not?

Because, as you know, we are feeding the AI technologies with, human data.

Interviewee 5 I hope it will, but it still has to be proven, to be shown. But I hope so, because I think that, **we have lots of human biases affecting the way we think the way we build things, the way we work and hopefully AI can come up with better solutions to remove the effects of these biases.** But since we are working with a lot of human data and actual people are reviewing the data and are making the decisions and the choices, I **don't know if it will be possible to remove them completely or enough.** So at this stage, I would say that's just the hope. I don't know if that will be the case.

Spiros Katiforis *This takes me to my last question because you have already answered a lot of questions I wanted to ask you. Are you aware of the term technological singularity, and if so, do you see that happening in the future?*

Interviewee 5 **Not in the short-term future. I don't know.**I'm not a sci-fi writer.I **don't really think about threats like this.** That feels very long-term. I feel that in the next 10 years I'm not afraid of this for sure. In the next 50 or 100 years, I don't know. I don't know if I can say more than this.

I'm not an expert on AI at all and this would be very much a speculation.

Spiros Katiforis Thank you very much.

Interviewee 5 Thank you.

[End of Interview 5]

Interview 6:

Spiros Katiforis *Has your organization established a security culture?*

Interviewee 6 Yes, I lead the security culture team.

Spiros Katiforis *How would you define security culture, and how can you measure it?*

Interviewee 6 Oh, that's hard. I think how I defined it is that everyone knows that it's a part, believes that it's a part of their role and it's just embedded into what they do.

So it's not something extra, it's not something on top of it, it's something that's just a part of what they do and in all areas in it at all levels and then.

How you measure it, that's the \$1,000,000 question and I think that's what everyone's trying to figure out and we've seen a lot of change within the security awareness industry and moving towards the human risk management space, which I think has been really interesting over the past couple of years to measure specific behaviors that people are doing and then trying to tie those to some of the campaigns that people do. I think that's one way to do it. Another way is through your organizational health surveys. I mean, if you don't have a overall culture of trust and psychological safety, I don't think you can have a true culture of security. So you need to measure those things as well, and then probably the the other way to measure it is just some informational interviews and focus groups just to get that qualitative piece in terms of when people are talking about their roles, are they bringing up the partnerships that they have with security or are they viewing, you know, security as the barrier?

Spiros Katiforis *And what about human-centered security culture? How how would you define that? How we can also measure it?*

Interviewee 6 I guess I don't view it differently than anything else. You know, I think the "people-process-technology" triangle has to be all together, you can't separate human versus technology versus process. It's all interwoven together.

Spiros Katiforis *And has your organization integrated AI technologies into its security practices already?*

Interviewee 6 Yeah. In some places they have machine learning and things like that with alerting.

And we do a little bit with security awareness using it to help us deploy faster when we're just about to get first drafts of something, you know, "write it in this style", or "give me an idea for this", or "give me 10 names for a new website", or something like that.

So we'll use it in that sense, **for brainstorming**, but then yeah, my other colleagues within the security organization would be using it **as well for more tactical things**.

Spiros Katiforis *Do you personally identify any conflicts or ethical considerations in the deployment of AI-driven security systems in business environments?*

Interviewee 6 For sure, I think **you have to be really careful about biases**. The way someone described AI to me in the beginning of it, kind of becoming, you know, splashing out, is that it's a really **good legal assistant**. Like if you worked for a law firm, It's your legal assistant, but it's not. It's not like you're gonna review that. **You're not just gonna take that and you know, go into court, you're going to review those documents**. And so that's how I view it too. **It's a really good intern that gave you a bunch of ideas and then you can take it from there**.

Spiros Katiforis *And do you anticipate AI posing a threat to human liberties within business environments? Do you foresee it affecting human job security?*

Interviewee 6 Can you give me an example of human liberties?

Spiros Katiforis *For example, freedom of choice and making decisions; job security. Will AI replace people in business environments?*

Interviewee 6 Hmm, yeah, I **certainly think it will eventually**. And whether I think that's the right idea or not, I **don't think at this point it's, you know, good enough**.

Like I said before, to just take it and run with it, I definitely think **there needs to be a human there**. To me, it's just a way to brainstorm and get started.

It's not a way to create a finished product and so you need that human element to really decide and give it context and creativity and things beyond just lists.

Spiros Katiforis *What measures do you believe are necessary to ensure transparency and accountability in AI-driven environments?*

Interviewee 6 It can be biased, it can be wrong. So you really have to do your due diligence. You have to **be really careful what you put into it, you know**. So if you're going out and using ChatGPT and you're putting in **your company's proprietary information**, that's a really bad move. If your company isn't **flat-out blocking it, a lot of companies will say don't do it, or they'll block it, or they'll put a speed bump to it**, a little warning that pops up or something like that. But yeah, you have to be really careful, and if you're if your company has an internal tool then that's great. **You do have a little bit more privacy there**, but you still have to watch for the biases and the correctness of it; **accuracy, I guess, is the word**.

Spiros Katiforis *And regarding the future, how do you see the coexistence of AI and humans in business environments?*

Interviewee 6 I think it'll be tricky because it's **exploded onto the scene really fast**. And then you'd read in the the news about the ChatGPT creator saying that **this wasn't a good idea after all**. I think that **we'll struggle with it as a human race**. And so I would say it's **concerning to see how we're going to integrate it**. In some places it's wonderful, with medical technology, it's **absolutely amazing to see it helping to detect for example polyps**. So that's incredible, and hopefully, it can continue to be used for those types of things.
But in other areas? I think it's **concerning and we really have to be diligent and not lazy with our use of it**.

Spiros Katiforis *I believe you're aware of the term technological singularity, right? How can we secure our human liberties in that case?*

Interviewee 6 I guess I would just say it again, **the ethics behind it**, you know, **why are you using it and how you are using it**, is really important; if you're using it to try and **go faster than everyone else** and not taking the time to **really ensure that the data is accurate and the responses are true and not biased**. Otherwise, it could be concerning.

Spiros Katiforis *What would be the key components for a human-centered security culture, maybe the two most important elements?*

Interviewee 6 The two most important elements in a security culture are **trust and transparency**.

Spiros Katiforis *Perfect. Thank you.*

Interviewee 6 Thank you.

[End of Interview 6]

Interview 7:

Spiros Katiforis *The first question that I have is about your experience in different business environments and if you have seen organizations building security culture programs.*

Interviewee 7 Over the years I've worked in lots of **different organizations** since 2000. Since then, I have worked in a lot of **small businesses**, but we were delivering to all of the **big brands**. So, I have worked with international retailers and grocery stores, the **BIG4 consultancies**, the **banking sector**, the **education sector**, etc.
So just to give you some context and background to my answer in terms of if I have seen **people doing security culture**, it's **massively varied**, and I don't think you can say for example, this organization does, because they're large

and because they look very mature on the outside, it means that they **take security culture seriously**. I've seen **massive differences from organizations with very few employees**. From a couple of hundred people who say we understand security culture and we want to do something about it, to the complete opposite, where you've got an organization of sort of **90,000 employees**, that **aren't really doing security culture at all**. The biggest challenge that I see actually is **understanding it from a leadership perspective**. I find that almost all organizations now will have something about it **in their strategy**.

But some organizations say we've got it in our strategy, and **actually what they've got is a load of risks and a load of technologies**, and they've got this little bubble on the side that says **we will raise awareness and it's through compliance training and we stick a few posters up and we maybe do an escape room for Cybersecurity Awareness Month**.

In my mind, there is **no culture change there**, versus other organizations where they look at their risks, they look at their **strategic initiatives**, and they ask themselves **what behaviors do we need, and what risk-mitigating behaviors we need** for every single line item of our technology change and **for our process change**, and they've built that in. And I do see some organizations doing that. Not many, though.

Spiros Katiforis *So what about AI technologies, though? Have you seen organizations integrating AI a lot?*

Interviewee 7 So I would say I haven't seen many organizations using AI effectively from a security culture perspective. I see organizations maybe dabbling in it, particularly the consultancy businesses. They're talking to their clients about it, but I don't think many organizations have integrated it yet into how they deliver security culture. I know that some vendors are starting to do it. I believe they build AI into the way their systems understand people's behaviors and then tailor and deliver their communications. So I think some organizations are starting to use it through some of the products that they are buying. There are obviously hundreds of thousands of organizations I don't work at all with, but the ones that I have seen **aren't really starting to do it**. Perhaps they're using it a little bit to develop some new **phishing templates**, but it's very much on the outskirts from what I've seen at the moment. But what I have seen, though, is that **security culture teams are talking about it, but often from a risk perspective**. This is how **AI can trick us better**. It can create, you know, deep fakes. Be careful about who you let record your voice. Because that could be used against you; all of

those sorts of things, I do find that they're talking about it and **raising awareness, but not integrating it.**

Spiros Katiforis *And do you personally identify any conflicts, related to the integration of AI and the human-centric aspect of security?*

Interviewee 7 I think one of the concerns that I've got is, and you probably looked at this when you looked at my profile and things that I do, is that obviously, I **understand security culture and security awareness kind of holistically**, but the bit that I'm really interested in is this concept is the **conversation that's the catalyst for change**, and we can have all of these technologies, we can have all of these really jazzy things, but actually, unless we as human beings, still make the time to talk to people, to understand people and have conversations, then you know that **light bulb moment**, if you like, that spark when people say "oh, I'd get this", that bit where you can connect.

You know, I could be talking to you; I could be a security awareness person in an organization; I could be talking to you, and you could have no interest in security at all, but then if I get to know you and if I find out what interests you, then perhaps I can make a link. Perhaps I can deliver something that's really **contextual** to you?

I probably don't understand enough about AI to understand whether it can do that. I'll be honest with you, but I think **my concern is that we miss that piece out.**

I also think if we only use AI to generate our awareness programs and our **culture change programs or to interact with our workforce**, then let's say I am the CISO or the lead culture person of an organization, and I go out and I find out some information about my audience through using AI. I can read that data or I can look at that data, **but I can't feel that data**, you know. And when you talk to people, when you **build relationships** with them, you **feel their problems, you feel their challenges**. And that's the bit that I think there's a little bit of a **conflict** with. I would like to see it in use. I would like to see it integrated, but I think it is about some **checkpoints** and ensuring that that conversation, that **relationship building**, that **feeling**, and that **understanding doesn't get lost in the process.**

Spiros Katiforis *Do you foresee AI posing a threat to human liberties? I will use job security as an example, in terms of replacing people within business environments and taking their role.*

Interviewee 7 Yeah, I think I already see the desire to do that, you know, I've already had people saying to me, well, why are you writing that? Why don't you **just get AI to write it for you?**

For example, **content writers and video producers** and all of those sorts of things.

I do think that there is a bit of a **moral dilemma** here because, as you know, at the moment, and again this is me sort of possibly talking from a **naïve understanding** of how AI and machine learning operate, but obviously, at the moment most of the content that these **large language models** are referencing, has been **human generated**. What happens in five fifteen-twenty years with the original content that was generated by humans, and the rest of the content? It's training itself. It's like me asking myself whether it's a good idea to do something. I'm gonna say yes. So who's checking that? If it's checking itself.

Spiros Katiforis *And what would be, in your opinion, the key components of human-centric security culture?*

Interviewee 7 I mean, for me, it's all **human-centric** because, whether you're making a decision about **technology or process or raising awareness**, actually, a human sits, you know, at the moment, and I'm sure **a person at some point will sit as part of deploying that process**.

I think the **key factor of having a really good human-centric strategy is understanding**. I call them **risk-mitigating behaviors**, and I sort of mentioned it at the beginning, but for any **Security strategy**, the **key is understanding where that human intervention lies**.

At what point are people going to be **interacting with your system**, your **piece of data**, or your **message**? And **what do you need to do**?

And I think it starts from there really because once you can understand **what those core risk mitigating behaviors are**, then you can **work on what are the things that we then do to raise awareness and change behavior**. And I think quite often it comes from the other.

Why is the **strategy just technology and risk based on the human pieces**, right?

We'll do an **annual training**. We'll **raise awareness** about some stuff, but it's not actually **these two aren't actually linked**. So yeah, I'm sort of repeating myself a little bit here, but hoping to make my sort of clarity on the point that I think it's about, you know, those **behaviors have to link back to strategic risks**, not just be random things like clicking on **phishing emails**.

Let me give you an example. OK, **the risk is that we might lose information from a data breach**. So, in my strategy, I put it. I decide that I'm going to **implement some DLP solutions**. Perhaps I'm going to. Say that we used to **hold our data all over the place**. We're now going to hold it all in SharePoint because Sharepoint's got all of these things. It means that we can **share**

information securely through role based access management. Great. The behaviors that are aligned with that are ” Do people actually know how to share so, you know, do **permission control** on SharePoint?” So with a couple of our clients, this exact thing has happened. And when you look at their service. They're the team that deals with IT incidents. All I can remember is the brand name, and I think you don't want the brand name, but they're IT helpdesk. So their IT helpdesk constantly says these are the calls that we get to the help desk on, etc. These are the calls that we get to the help desk about how to do SharePoint permissions. There's a kind of a **direct correlation between a risk, a strategic thing, a behavior, and that sort of thing gets missed out on**, you know, those compliance-based pieces, because it's **not linked to the security strategy**.

Spiros Katiforis *Do you personally believe that the technological singularity will happen?*

Interviewee 7 I guess I haven't thought about it deeply. My perspective on it is **that it's not going to happen in the short term, not in my lifetime**. And I think why do I make that judgment?

Maybe because it's a **very unfamiliar position**. Maybe it's **more feeling-based rather than rationally-based** because obviously, I've not sat down there and kind of analyzed it all and looked at, you know, the possibility. It's maybe a **little bit like a lot of humans**.

Do we bury our heads in the sand because we don't want to **envisage a reality where that's happening?** And yeah, I guess for that reason, I don't see that happening in my lifetime because I feel that **as human beings if that looks like it was becoming a possibility and you're in a sort of a Terminator scenario, the human beings are agile enough to change that scenario**.

Spiros Katiforis *Thank you for this valuable interview.*

Interviewee 7 Thank you.

Interview 8:

Spiros Katiforis *Has your organization already established a security culture?*

Interviewee 8 So I think the **security culture** questions are really important because I think, for me, it's the **obvious next step after you've got a compliant culture**, and in fact, it's **much more important**. **Compliance is important, it's very foundational**, but the **actual implementation of a security culture is really key**. So yeah, in pretty much all of the roles I've had. So, I've been working in security for eleven years now, ten years in three different, well, three or four different roles. In every case, I think that the **establishment of a security culture has been a goal**.

Spiros Katiforis *And how would you define security culture and how? How would you measure it within a business environment?*

Interviewee 8 OK, that's not a short answer. First I think there's a number of **different definitions**.

The one that I really like is that culture in general is the way we do things here, which I think came out of McKinsey a few years back.

So it's very much **situational to the organization**, but generally speaking, I think a security culture, well, I **don't like the phrase security culture for a start** because I **don't think you have individual cultures like that within an organization**. I much prefer to say we **have a culture that values security** and I know it may sound a little bit pedantic, but I think **you're what you're saying**, and **security is part of your overall culture, not a separate thing**. So, with that caveat, I'll probably just say security culture cause it's quicker, but every time I'm doing that I mean **a culture that values security**.

So I think that a really **key aspect of secure culture is, first, that it's an organization which understands risk**. So, it is looking not just to do what everybody else is doing, but actually **addressing individuals, behaviors that actually address specific risks**. So, some organizations will care a lot about **phishing**, others will care a lot about **passwords**. But you know, **there's no one size fits off**. That's the first situational part. I think the second thing is **any good definition of culture is about the attitudes, beliefs, and then the outward expression of those of the individuals involved**. And as they come together, that's your culture. So when we talk about security culture, what we're really talking about is **what do people think about security?**

Do they think it's important? Do they think it gets in the way? Do they think it's a drag?

Is it something that **adds friction** or is it something that **adds safety?** And the way that that comes out, I think, is **how people interact with your security team**. So certainly, when I've done security awareness and culture roles before, I think **there's a tipping point**.

We are telling you what you need to do: "I need you to come and talk to my team. I need to know about this." So there's that **shift**. What you've got is **people actually asking their own security questions**. They are coming to you and saying **"we want to be more secure"**.

"We want to do this properly but we believe this is important", not just "you tell us it's important", but **"we believe this is important"**. "And you

are the person who can **help us** and guide us to **make better security decisions.**"

So that's the second element, which is that **tipping point from push to pull**, and then I think the third element is when this happens after the two previous ones, which is when your **security awareness team starts pushing back on your organization.**

And by that, I mean that you become a **trusted advisor**, so somebody in your finance team says, "hey, we would love to do this securely, but this process, this technology, this thing stops us doing that" and that you're able to take that as a security awareness team back to the security team and say **we are causing people to break policy here.** So that's part of that pull to push. Sorry, **push to pull. Rather than telling people to change their behaviors, people are telling the security team, the technology team that there is a better way to do this** and when you have those three elements, I think then is when you're actually **starting to see a positive security culture.**

Spiros Katiforis *And what about the human-centric factor? Do you think security culture should be human-centered?*

Interviewee 8 **Absolutely.** You read the Verizon DBR every year, and it says 72% of incidents have the **human factor** involved, right? I don't believe that number. **I think it's 100%.**

I think **every security breach has the action or inaction of a human being**, or a series of human beings after it's called. Because, otherwise, you're just running something fully automated and it doesn't matter, right? **The problem that we have in security, and this counts against the security culture, is very often seems to be the end user.**

Who is that 72% when and there's a lovely quote from James Reason who writes an awful lot about **human error**, and he basically says that quite often, and I won't give you the whole quote because I can't remember it, but he basically says, you know, we have this thing about the end user and that was the point, the bad guys got in. Well, no, that's not true.

It was a **series of failures that allowed the bad guys to get in and we've just stopped looking when it gets to the end user.** And so for me **human-centric security**, which is a phrase, I'd really love the other one. I like the NCSC talk about **sociotechnical security**, which is literally **the interface between technology and society.**

But human-centric security for me is about saying **"are we building systems in such a way that they support and elevate the person at the core of security?"**

Because if we're not, if we're making them jump through hoops, we have to accept that at some point, they're gonna make a mistake.

If we had proper **human-centric security**, A, we would accept that **human error is inevitable** because it is, and B, we would **build resilient systems that didn't fall apart because somebody made a mistake** because we know that somebody's going to in the same way that if you drive a car and you don't do regular maintenance on it, your car at some point is going to fail. In fact, **you don't know which bits gonna fail, but some bit of bit is going to fail, right?**

A **good security culture** is like that. **Preventative maintenance** because you're listening to the sounds of the engine, metaphorically speaking, you're seeing people making a mistake and you're saying, OK, **why are they making a mistake?** Is it because we're putting too much pressure on them? Is it because we're asking them to remember too many things? Is it because we actually have a very **fragile system** that is **not resilient to failure?**

Because at some point, it's going to fail. That for me is **the core of human centric security** and that's **not absolving people of responsibility**. In fact, it adds much more.

So it's saying **everybody has the ability to act and to choose how they act**, what we need to be doing is **listening**, because if somebody says, "hey, I made this mistake and it's because of X", then what are we going to do about X? We can just fire you, right? That doesn't fix anything. It doesn't stop X from happening again, but in the same way, hearing a squeaky wheel probably means we need to put some oil on it.

Hearing somebody, when somebody makes a mistake, is telling us about a weakness in our system and we need to do something about that. And in a **non-judgmental way**. And that, for me, is the core of what I would call **human-centric security**.

Spiros Katiforis *Do you personally identify any conflicts or ethical considerations in the deployment of AI-driven security systems in business environments?*

Interviewee 8 Yeah, **absolutely**. I think one of the biggest **concerns** for me about AI and I'm very much ambivalent about it and this is one of the biggest concerns for me, is **accountability**.

So we have a phrase in British culture which comes out of a TV show which just says **computer says no**, and it's it's from a sketch show that used to be on TV and it's about **absolving of responsibility**; and ultimately I think we have to be very careful if something is able to make a decision, I mean again, we're **anthropomorphizing** a little bit there, but if an **AI system**

makes a decision and we **can't justify it**, then what can we do about it? So for me, if you're going to use AI in anything, it should be there **as a tool**, but **it shouldn't be making that final decision**.

There should be an **accountable person** or a **policy** or something, because again, what happens if it makes the wrong call? If you're my manager and you make a bad call, I can challenge you. If you aren't open to challenge, I can go to your boss and so on and so on and so on.

In the same way, if I make a bad call, you can challenge me, but if literally we put all the factors in, there's some AI generative model that throws an answer out and we go on that answer, **how do we challenge it** if that answer is wrong? So, at some point for me it's all about that accountability. **Who's actually signing off on that decision?**

Spiros Katiforis *So you anticipate AI posing a threat to human liberties. If there's no accountability, and if no measures are being taken, and if AI makes its own decisions nobody can take responsibility, for these decisions.*

Interviewee 8 Yeah, exactly. And there's a really strong example there. When you look at facial recognition technologies, which are using AI, we know that there are **inherent biases** in those systems because we've seen the results; we know in the UK, for example, they are much more likely to **misidentify** somebody with darker skin, right? So that's because of the models of how the light reflects, etc. But ultimately, there are people of color who are being picked up because they are being identified as being a person of interest on the basis of an **AI decision**.

If in some dystopic future that was all necessary, then that would be a **massive injustice**, whereas now at least we have the ability to say a human being can look at the original photo, can look at the person who's standing in front, **the AI got it wrong**, you're not this person, right? And so I think that for me, is a really key part of that **accountability**. Ultimately, we know that **no system is perfect**. We know **human beings make errors**. We know that **AI makes errors**, so there has to be some way of saying that was **unfair**, that was **unjust**. Whatever you want to call it, because that's the flip side for me, especially if you're talking about the **wider security culture**. **One of the things that's necessary for a secure culture is for a just culture to exist**. So if somebody knows that they've made a mistake and they **come forward** and they say "hey, I've told you about this, that should be taken into account". That's one of the key things that builds a **strong security culture**, strong safety culture, all of those things.

Spiros Katiforis *I believe you are aware of the term technological singularity, right?*

Interviewee 8 Yeah.

Spiros Katiforis *So, to safeguard our freedoms and to prevent something horrible from happening to the human race, do we need to establish policies? What kind of controls would you think we need to prevent this kind of thing?*

Interviewee 8 I'm aware of the concept of the singularity. I'm not sure I believe it, I don't necessarily think so.

One of the key things that I understand for the singularity is **that we would need to have actual artificial intelligence rather than what we currently call artificial intelligence. We're not going that way at all at the moment.** That's not the research that's been done.

What we basically have with GenAI, for example, is predictable, it is very good **text prediction**, right? But there's **no actual thinking going on there.** So I **don't know if that's ever gonna happen.** Having said that, if it did, I think that it would be such a **massive societal shift** if something like technological singularity was going to happen. I think there needs to be **safeguards** put in place. I think **human accountability** is key. Anything and **everything has to be reversible.**

I think that's the key thing for me. If we use a really extreme example, if you could have an **AI-driven justice system** that included the possibility of **human execution**, then there are a million ways that would go wrong. So yeah, I think everything has to be reversible.

Spiros Katiforis *I enjoyed our discussion and thank you for your valuable insights.*

Interviewee 8 That's my pleasure.

Interview 9:

Spiros Katiforis *Has your organization/business environment already established a security culture?*

Interviewee 9 Over ten years of working with awareness, I have dealt with **different scenarios.** Many companies had an **awareness program in place**, but it was **only based on compliance**, i.e., complying with **regulations and laws.** When I was in my home country, I thought it would be different here in Europe, but now I see a **very similar maturity.** I think that **treating security awareness with phishing simulations and mandatory training is not building a culture.** I mean, it can help you in this mission, but it **doesn't build a culture.** Especially **when you don't have a clear expectation of evolution or clear metrics.** I understand that **culture is a more extensive concept.** It's a **change in behavior.** So my answer is that most companies still **only do training and comply with regulatory requirements.**

Spiros Katiforis *How would you define security culture within your organization, and how is it measured? Would you define it as human-centered?*

Interviewee 9 Considering the way I like to work, I measure culture by drawing a parallel between awareness initiatives and the reduction in real incidents, the number of anomalies proactively reported by people, improved results in phishing campaigns, etc. Most of the companies I've worked with have only managed to reach step 3 of the SANS Maturity Model.

And speaking of measurement, this is the way I consider most applicable for measuring the evolution of an information security awareness program. Steps 4 and 5 require consistency, financial investment, and a change in management mindset. It is impossible to evolve a program without executive support and with a limited amount of staff to be 100% focused on the issue. As long as technology and processes are treated as more of a priority than the human layer, we won't have an area with people at the center.

Spiros Katiforis *Has your organization integrated AI technologies into its security practices?*

Interviewee 9 Speaking specifically about my area, there are many initiatives underway, such as hackathons, but nothing very advanced on the subject. But AI has long been used in several companies I've worked for anomaly detection, generating secure passwords and defending against adversary attacks.

Spiros Katiforis *Do you personally identify any conflicts or other ethical considerations in the deployment of AI-based security systems in business environments?*

Interviewee 9 AI can cause privacy and data security problems, so yes. However, it's a reality we can no longer escape. The way forward is to educate about the best use.

Spiros Katiforis *Do you foresee AI posing a threat to people's freedoms and safety in business environments? Do you foresee it affecting human job security?*

Interviewee 9 I don't believe it! I just believe that jobs are changing over the years. AI can help with more repetitive jobs, opening up opportunities for human beings to do more intellectual work. ChatGPT, for example, even produces texts, but they are shallow and emotionless. Do you know what I mean?

Spiros Katiforis *What measures do you believe are necessary to ensure transparency and accountability in AI-driven environments regarding security?*

Interviewee 9 I think it's important for each company to have tools adapted to its reality. For example, if we have customer data, the tool should be prepared to limit the sending of files with that data. And, of course,

clear education about what you can and can't do, with an explanation of the risks, including the consequences in the event of non-compliance.

Spiros Katiforis *How can organizations promote collaboration and coevolution between AI and human personnel?*

Interviewee 9 The question of millions! First and foremost, not by dismissing those who dedicate themselves to them and train AI tools. I believe that the important thing is to open up the possibility of developing better work. Since repetitive tasks can be carried out by a machine, people have more time to devote to more innovative solutions.

Spiros Katiforis *What are the main components of a human-centered security culture?*

Interviewee 9 The creation of trusting relationships. You have to be empathetic and understand that humans can make mistakes. A human-centered culture values and respects employees' contributions and considers each person as unique.

Spiros Katiforis *How do you see the future coexistence of AI and humans in business environments?*

Interviewee 9 I see it as a reality. And education about AI needs to start now. Otherwise, we'll have a lot of related security incidents. Security is no longer just about blocking. We need to create a future in which technology is a facilitator and not a threat.

Spiros Katiforis *How can humans safeguard their freedoms in the event of Technological Singularity?*

Interviewee 9 Privacy and non-discrimination must be safeguarded in the face of technological advances. Establishing regulatory frameworks for the development and deployment of AI is essential to guaranteeing these human rights. Laws and regulations can set limits, ensure transparency, and that developers and organizations are accountable for the ethical use of new technologies.

As well as promoting public education and awareness, their capabilities and their potential impact on society. An aware public is more prepared to defend initiatives that protect individual liberties.

Spiros Katiforis *Thank you for your participation.*

Interviewee 9 Thank you.

[End of Interview 9]

Interview with AI:

Spiros Katiforis *How do you define your role within the security culture realm? What would be your responsibilities in a business environment?*

ChatGPT Within the security culture realm, my role would be as an **advisory and analytical tool**. In a business environment, my responsibilities would include **helping to analyze potential security risks, educating employees on best security practices, and assisting in the development of security protocols**. However, my role is **supportive rather than authoritative**, meaning **decisions and accountability still rest with human stakeholders**.

Spiros Katiforis *How would you define security culture and how is it measured?*

ChatGPT Security culture refers to the **collective behaviors, beliefs, and practices** of an organization regarding security. It is measured by evaluating the organization's **adherence to security policies, the effectiveness of awareness programs, and the extent to which security considerations are integrated into daily operations**. Metrics such as incident reduction, employee engagement in **security initiatives**, and **proactive reporting** are also used.

Spiros Katiforis *Do you identify any conflicts or other ethical considerations in the deployment of AI-driven security systems in business environments?*

ChatGPT Yes, there are several **ethical considerations**, including **privacy concerns, potential biases in AI decision-making, and the risk of over-reliance on automated systems**. These issues can lead to **unintended consequences**, such as **unfair treatment of individuals or inadequate responses to complex security threats**.

Spiros Katiforis *What measures do you believe are necessary to ensure transparency and accountability in AI-driven environments regarding security?*

ChatGPT To ensure **transparency and accountability**, it's important to establish **clear guidelines for AI usage**, including the **requirement for human oversight** in critical decision-making processes. **Regular audits, bias assessments, and transparent reporting mechanisms** should be implemented to maintain accountability.

Spiros Katiforis *Do you anticipate AI posing a threat to human liberties and security within business environments? Do you foresee AI affecting human job security?*

ChatGPT AI can pose a **threat to human liberties** if not properly managed, particularly through the **erosion of privacy and autonomy**. In terms of **job security**, AI has the potential to **displace certain roles**, especially those involving **repetitive tasks**.

However, it can also **create opportunities for humans** to engage in more **complex and creative work**, provided there is adequate support for **transitioning roles**.

Spiros Katiforis *How can organizations foster collaboration and coevolution between AI and human personnel?*

ChatGPT Organizations can foster collaboration by promoting a **culture of continuous learning**, where employees are trained to **work alongside AI systems**. It's also important to **design AI tools** that **complement human skills** rather than replace them, ensuring that AI serves as an **enhancement to human decision-making**.

Spiros Katiforis *What are the key components of a human-centered security culture?*

ChatGPT Key components of a **human-centered security culture** include **empathy, trust, and respect for individual contributions**. It also involves recognizing the **inevitability of human error** and building systems that are **resilient to mistakes**. Additionally, **continuous education and open communication** are crucial.

Spiros Katiforis *How do you see the future coexistence of AI and humans in business environments?*

ChatGPT The future coexistence of **AI and humans** in business environments will likely involve a **partnership** where **AI handles routine tasks**, and **humans focus on strategic and creative aspects**. This coexistence will **require ongoing education, ethical guidelines, and adaptive organizational structures** to be successful.

Spiros Katiforis *What safeguards do you have in place to secure sensitive data and adhere to privacy regulations?*

ChatGPT Safeguards for **protecting sensitive data** include **encryption, access controls, regular audits, and compliance with relevant privacy regulations** such as **GDPR**. Moreover, AI systems should **incorporate privacy by design**, ensuring that **data is only used for its intended purpose** and is **protected from unauthorized access**.

Spiros Katiforis *How can humans safeguard their freedoms in the event of the Technological Singularity?*

ChatGPT Safeguarding **human freedoms** in the event of a **Technological Singularity** involves establishing **robust ethical frameworks, regulatory oversight**, and ensuring that **AI systems are designed to prioritize human rights**. **Public education and awareness** will also be key to ensuring that society is prepared to address the challenges posed by **advanced AI technologies**.

[End of Interview with ChatGPT]

Figures

Figure 1: Conceptual Framework for Sustaining a Human-Centered Security Culture in AI-Driven Environments	35
Figure 2: Refined Framework for Sustaining a Human-Centered Security Culture in AI-Driven Environments.....	58

Tables

Table 1: Codes, Categories and Themes from Interview 1.....	40
Table 2: Codes, Categories and Themes from Interview 2.....	41
Table 3: Codes, Categories and Themes from Interview 3.....	42
Table 4: Codes, Categories and Themes from Interview 4.....	43
Table 5: Codes, Categories and Themes from Interview 5.....	44
Table 6: Codes, Categories and Themes from Interview 6.....	46
Table 7: Codes, Categories and Themes from Interview 7.....	47
Table 8: Codes, Categories and Themes from Interview 8.....	48
Table 9: Codes, Categories and Themes from Interview 9.....	49
Table 10: Codes, Categories and Themes from Interview with ChatGPT.	50
Table 11: Consolidated Themes emerging from the interviews.....	52

Appendix

Appendix : Interview transcripts.....	67
---------------------------------------	----