LUISS

Degree Program in Global Management and Politics

Course of Corporate Strategy

Cyber-Proof Telecommunications:

The Characteristics of Leadership in Cyber Risk Management

Prof. Paolo Boccardelli

SUPERVISOR

Prof. Francesco Galietti

CO-SUPERVISOR

Chiara Leali
Mat. 783321

CANDIDATE

Academic Year 2024/2025

ABSTRACT

In an era of growing digital interconnectivity, cybersecurity has become a great concern, particularly for the telecommunications sector, a key component of national critical infrastructure. While data protection techniques are constantly evolving, the growing frequency, complexity, and sophistication of cyberattacks highlight the need for strategies that go beyond technical defenses and formal risk management frameworks. The ISO/IEC 27001 standard and the NIST Cybersecurity Framework provide essential guidance for building structured cybersecurity programs, yet they often place limited emphasis on the human factor. Research consistently shows that human behavior remains one of the greatest vulnerabilities, with many breaches stemming from lapses in judgment or awareness. This underscores the crucial role of leadership in fostering organizational resilience and cultivating a culture of cybersecurity vigilance.

Drawing on qualitative interviews with senior executives and cybersecurity leaders, as well as a review of classical leadership theories and recent literature on digital leadership, the present work aims to unveil the leadership traits and competencies required to manage cyber risks in today's telecommunications sector. The findings reveal that traditional leadership models are insufficient for the dynamic demands of cybersecurity, underlining the importance of competencies often overlooked in existing frameworks, including cybersecurity literacy, crisis communication, strategic foresight, rapid decision-making under uncertainty, multitasking, cross-functional collaboration, and continuous professional development.

Building on these insights, the research defines the Cyber Risk Leadership Model, which integrates strategic, technical, and human-centered competencies. The study further demonstrates the value of immersive cyberattack simulations and experiential exercises in strengthening both technical and interpersonal skills, thereby equipping leaders to respond effectively to evolving threats.

By developing this model, this thesis advances leadership theory while providing a foundation for targeted leadership development programs that address today’s cybersecurity risks. It offers implications for organizations and academic institutions in redesigning their curricula, contributing to the preparation of the next generation of cyber leaders and enhancing both organizational and societal resilience in the digital era.

TABLE OF CONTENTS

INTRODUCTION

Today's world is defined by rapid developments in technology, continuous innovation, and the constant evolution of business models, a period commonly referred to as the Fourth Industrial Revolution. While this dynamic environment generates remarkable avenues for growth and cutting-edge innovation, it also introduces significant vulnerabilities. Among the most pressing of these is cybersecurity, which has become a defining challenge for organizations, particularly those managing sensitive data and that are part of critical infrastructure. The heightened complexity and sophistication of cyber threats, coupled with the accelerated pace of digital transformation, requires organizations not only to adopt robust technical safeguards but also to cultivate effective leadership capable of fostering resilience and embedding a culture of cyber awareness across all levels of operation.

Chapter 1 situates this research within the broader context of the digital era, exploring the evolution of cybersecurity as both a technical and organizational concern. It examines the historical and technological origins of cyber threats, tracing their development alongside the increasing digitalization of society. The chapter further investigates the geopolitical implications of cyberattacks, underlining their possible influence on both international relations and national security. Narrowing to the European perspective, it provides a comprehensive overview of the continent's cybersecurity landscape, detailing emerging threats, strategic investments, and the evolving perception of risk. In addition, the chapter reviews regional and global governance frameworks, with particular emphasis on the initiatives of both the European Union and the United Nations, demonstrating how regulatory structures and international coordination shape the operational environment for organizations and influence their strategic priorities. This foundational analysis establishes the broader environment in which companies operate and illuminates the external pressures that define their risk landscape.

Recognizing the strategic importance of telecommunications as part of national critical infrastructure, the thesis focuses its analysis on this sector. Telecommunications companies are uniquely exposed to cyber risks, as they manage vast volumes of sensitive personal and commercial data and serve as the backbone of global digital connectivity. Their central role makes them frequent targets for malicious actors seeking to disrupt networks, compromise data integrity, or exploit vulnerabilities for geopolitical or economic gain. Consequently, enhancing cybersecurity within this sector is not only critical for protecting businesses and consumers but also essential for safeguarding the stability and security of nations.

Chapter 2 explores in detail the cybersecurity challenges that telecommunications operators face. It examines the specific threat landscape in Europe, presenting concrete examples of attacks that underscore the urgency of reinforcing resilience in this critical sector. To identify effective cyber threat mitigation strategies, the chapter reviews leading cyber risk management frameworks, including ISO/IEC 27001 and the NIST Cybersecurity Framework, and explores key data protection techniques such as encryption, firewalls, access control, and emerging tools including quantum key distribution and artificial intelligence. While these technical measures remain essential, evidence from recent C-suite discussions highlights a crucial reality: technology alone is insufficient. Security incidents are still predominantly caused by human error. Therefore, cultivating employee awareness and a vigilant organizational culture is fundamental to ensuring resilience. Acknowledging the critical role of the human factor in cybersecurity, this thesis emphasizes the importance of leadership in cultivating an organizational culture responsive to cyber risks. This focus on leadership, particularly on identifying the key characteristics that enable effective management and mitigation of cyber threats, shapes the central research question guiding this thesis: *What leadership characteristics are required for today's leaders in the telecommunications sector to effectively manage cyber risks in the context of digital transformation, and how can these characteristics enhance organizational resilience?*

To address this question, Chapter 3 provides an exploration of major leadership theories, examining both classical and contemporary frameworks in the context of the digital and cybersecurity era. Classical perspectives, including Trait Theory, Behavioral Theory, Contingency Theory, and Path–Goal Theory, as well as insights from the GLOBE Project on cultural influences, provide a foundational understanding of various leadership models and their underlying principles. Contemporary studies of leadership in the digital era further explore how innovation and digitalization reshape expectations for organizational leaders, while crisis leadership underscores the confusion, incomplete information, and rapidly evolving dynamics that define critical moments, highlighting leadership not as rigid planning but as embodied, situated action shaped by material, temporal, and social contexts. Despite these contributions, existing literature provides limited guidance on the specific competencies required to manage cyber risks effectively. Where leadership and cybersecurity intersect, discussions often remain general, failing to identify concrete traits and capabilities that enable leaders to enhance organizational resilience. This gap underscores the necessity of developing a new model of leadership tailored to the demands of the cybersecurity era.

To address this gap, semi-structured interviews were conducted with leaders from major Italian telecommunications companies, encompassing both managerial and technical roles, as well as cybersecurity experts from the Italian National Cybersecurity Agency. This diverse range of perspectives enabled a comprehensive understanding of the challenges faced by sector leaders and the skills required to navigate complex cyber risk landscapes. Chapter 4 details the methodological approach, including participant selection, data collection, and analytical procedures.

Chapter 5 presents the results of the interviews, highlighting the multifaceted nature of the cybersecurity environment and the critical leadership attributes that emerged as most relevant for managing risk effectively. Leaders described the operational and strategic challenges they face, from rapid technological changes and evolving threat landscapes to the necessity of fostering a security-conscious organizational culture. The interviews also emphasized that effective cyber risk management depends not only on technical acumen but on the ability to engage employees, promote awareness, and integrate cybersecurity considerations into broader organizational strategies. These insights laid the groundwork for the formulation of a novel leadership framework.

Building on these empirical findings, Chapter 6 introduces the concept of Cyber Risk Leadership, a new leadership model designed to capture the competencies, traits, and behaviours required of leaders in the cybersecurity era to effectively manage cyber threats.

The chapter details how these leadership characteristics can strengthen organizational resilience, mitigate human-related vulnerabilities, and guide decision-making under uncertainty. It also offers practical recommendations for leadership development in the telecommunications sector, emphasizing the need for targeted training, continuous learning, and the integration of both technical and human-centric strategies in leadership development programs and academic curricula. By articulating a structured model, this research not only advances theoretical understanding of leadership in the context of cybersecurity but also provides actionable guidance for organizations operating in one of the most strategically significant and exposed sectors of the modern economy.

Through this integrated examination of cybersecurity, organizational risk, and leadership, the thesis addresses a critical gap in the literature and provides a nuanced, empirically grounded perspective on how leaders can enhance resilience in telecommunications companies. The work thereby contributes to both academic research and practical policymaking, offering insights relevant to organizations, regulators, and educators seeking to prepare leaders for the complex challenges of the digital age.

CHAPTER 1.

DIGITAL ERA AND CYBER RISK

1.1 Digital Transformation: Opportunities, Disruptions, and the Rise of Cybersecurity

The digital era presents both unprecedented opportunities and significant disruptions for businesses operating in a fast-evolving global economy.[1] The integration of cutting-edge technologies such as AI, cloud computing, big data analytics, and IoT has allowed firms to transform traditional business models and create new avenues for value generation.[2] These tools, in fact, enable organizations to personalize customer experiences through data-driven insights, automate and streamline operational processes, and expand market reach via digital platforms and e-commerce ecosystems. Digital transformation further strengthens organizational competitiveness by enhancing flexibility, improving efficiency, and enabling timely responses to shifting market needs.[3] However, on the other hand, alongside the advantages it offers, digital transformation introduces substantial challenges that could disrupt an organization's stability and strategic focus.[4] First, the speed of technological change forces companies to continuously adapt, requiring significant investments in digital infrastructure, employee training, and cultural realignment. his continuous transformation can place a significant burden on financial resources, especially for small and medium-sized enterprises that may not have sufficient capital to implement advanced technologies as rapidly as

[1] Khanom, T. M. (2023). *Business strategies in the age of digital transformation.* Journal of Business, 08(01), 28-35. https://www.researchgate.net/publication/370708380_Business_Strategies_in_The_Age_of_Digital_Transformation

[2] Feliciano-Cestero, M. M., et al. (2022). *Is digital transformation threatened? A systematic literature review of the factors influencing firms' digital transformation and internationalization.* Journal of Business Research, *157*, 113546. https://doi.org/10.1016/j.jbusres.2022.113546

[3] Ibidem.

[4] Charter Global (2024). *Digital transformation for SMEs: Overcoming challenges & Embracing growth*. Charter Global. Digital transformation for SMEs

larger competitors.[5] At the same time, digital transformation disrupts labor markets by automating routine tasks and reshaping job roles, creating both opportunities for high-skilled employment and risks of displacement for workers whose skills become obsolete.[6] This imbalance highlights the importance of reskilling and upskilling initiatives to ensure inclusivity and sustainability in the digital economy.[7] Furthermore, the proliferation of digital platforms intensifies competition by lowering entry barriers, enabling new players and startups to challenge established firms, which may destabilize traditional industries.[8] While this fosters innovation, it also generates market volatility and shortens product life cycles, requiring organizations to remain agile and adaptive. Another disruption stems from the cultural challenges of digital adoption: transforming mindsets, encouraging risk-taking, and overcoming organizational resistance can prove more difficult than implementing technology itself.[9] In addition, the uneven pace of digital adoption across sectors and regions exacerbates the digital divide, widening inequalities between firms, industries, and societies that can access and benefit from digitalization and those that cannot.[10]

Moreover, as digital innovation advances, it brings substantial risks. Businesses and institutions that increasingly depend on digital tools face heightened exposure to cybersecurity threats, data breaches, and privacy concerns, becoming a critical concern for governments, organizations, and societies at large.[11] The following chapter will be dedicated to the exploration of cybersecurity

[5] Ibidem.

[6] Charles, L., et al. (2022). *Digitalization and Employment: A Review*. International Labour Office. Digitalization and Employment

[7] Ibidem

[8] Singh, P. (2021). *Impact of digital platforms on traditional businesses*. Impact of Digital Platforms on Traditional Businesses

[9] Baumann, B. (2024). The key challenges in aligning corporate culture with digital transformation. *Panorama Consulting Group*. Key Challenges in Aligning Corporate Culture with Digital Transformation

[10] World Bank Group. (2024) Digital Progress and Trends Report 2023. World Bank.

[11] Greco, E., Marconi, F. (2024). *Technological innovation and cybersecurity: The role of the G7.* Istituto Affari Internazionali (IAI).

origins and historical evolution from the 1940s to the present, highlighting key technological milestones, emerging threats, and the rise of new challenges such as AI- and quantum-powered attacks. The analysis will then shift to the geopolitical implications of cyberattacks, showing how cyberspace has become a domain of international rivalry and strategic competition. Building on this, the focus will narrow to Europe, examining its cybersecurity landscape, perceived risks, and strategic investments to address emerging cyber threats. Attention will also be given to the main regulatory frameworks developed at both the UN and EU levels, which aim to establish governance mechanisms in the digital realm. Finally, the discussion will turn to the telecommunications sector, a critical infrastructure at the core of the digital economy given its role in managing sensitive data, ensuring connectivity, and facing heightened exposure to sophisticated cyber threats. The paragraph thus makes the case for the thesis's focus on telecoms, which will be examined in greater depth in the next chapter.

1.2 Cybersecurity: Origins and Evolution

The concept of *Cybersecurity* encompasses measures taken to secure computers, networks, programs, and data against cyberattacks, unauthorized intrusions, and potential damage or loss.[12]

Cybersecurity has gained importance due to the proliferation of digital technologies and the escalating dependence on interconnected networks. It aims to protect the confidentiality, integrity, and availability of information against a growing threat landscape, where malicious actors, from

[12] For the definition of cybersecurity refer to Hogan, M., Newton, E. (2015b). *Supplemental information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S.* Objectives for Cybersecurity. https://doi.org/10.6028/nist.ir.8074v2.

individual hackers to nation-states, exploit vulnerabilities in software, hardware, and human behavior.[13]

The story of cybersecurity began in the mid-20th century, at a time when the digital landscape was barely recognizable compared to today.[14] In 1945, the first general-purpose electronic computer, ENIAC (Electronic Numerical Integrator and Computer), was introduced.[15] While the concept of networks and cyber threats was non-existent, visionary thinkers were already planting the seeds of what would eventually become C*ybersecurity*. John von Neumann, for instance, theorized about self-replicating mechanical organisms, an idea that later informed the development of computer viruses.[16] Though his groundbreaking work would not be published until the 1960s, it represented an early theoretical exploration of the challenges to come.

In the 1940s and 1950s, the focus was on building and refining large mainframe computers.[17] These machines were employed mainly for scientific and military applications, with security measures limited to controlling physical access.[18] A locked room was often all that was required to secure a

[13] According to ISO standards, cybersecurity protects the "confidentiality, integrity, and availability of information in cyberspace" (ISO/IEC, 2012, section 4.2). Bay, M. (2016). *What is cybersecurity? In search of an encompassing definition for the post-Snowden era.* French Journal for Media Research, 6, 2264-4733.

[14] For a comprehensive historical overview of the evolution of cybersecurity, refer to Smith, K. (2024). *A History of Cybersecurity and cyber threats.* Coro Cybersecurity. A History of Cybersecurity and Cyber Threats

[15] ENIAC, the first programmable general-purpose computer, was developed during WWII by John Mauchly, J. Presper Eckert, and their team at the University of Pennsylvania, with support from the U.S. Army. For further insights see Freiberger, P. A., & Swaine, M. R. (2025, January 25). *ENIAC | History, Computer, Stands For, Machine, & Facts.* Encyclopedia Britannica. https://www.britannica.com/technology/ENIAC

[16] The roots of the modern computer virus go back to 1949, when computer pioneer John von Neumann, a renowned mathematician, presented a paper on the "Theory and Organization of Complicated Automata," in which he postulated that a computer program could reproduce. Reed, E., (2023, December 1). *The Origins of Computer Viruses: A journey back to 1949 - Eric Reed Cybersecurity training*. Eric Reed Cybersecurity Training. The Origins of Computer Viruses:

[17] Smith, K. (2024). *A History of Cybersecurity and cyber threats.* Coro Cybersecurity. A History of Cybersecurity and Cyber Threats

[18] The Harvard Mark I, designed in 1937, was the first mainframe computer and was used by the US Navy during WWII for solving complex mathematical problems. Susnjara, S., & Smalley, I. (2024). *What is a mainframe?* IBM. What is a Mainframe

computer. The absence of interconnected systems meant that the concept of cyberattacks, as it is known today, was still far off.[19]

By the 1960s, however, the landscape began to change. Computing systems grew more widespread, and early hacking incidents emerged.[20] Such activities were frequently motivated by curiosity rather than harmful intent, with hackers attempting to access systems merely to explore their vulnerabilities.[21] Still, the idea of cybersecurity as a distinct field was not yet established. The priority was on securing physical systems, as computing resources remained limited and costly.

Nevertheless, this era saw the birth of foundational security measures. Password systems and access controls were introduced, albeit inconsistently.[22] The decade also marked the rise of mainframe computers in business and scientific applications, bringing with them a new wave of security concerns.[23]

The 1970s heralded a transformative period with the creation of ARPANET in 1969, the precursor to the modern internet.[24] This groundbreaking network was designed to facilitate communication

[19] Smith, K. (2024). *A History of Cybersecurity and cyber threats.* Coro Cybersecurity. A History of Cybersecurity and Cyber Threats

[20] *History of computer hacking and cybersecurity threats: From the 50s to today (2023). Mayhem.* https://www.mayhem.security/blog/history-of-computer-hacking-and-cybersecurity-threats-from-the-50s-to-today

[21] Ibidem.

[22] In 1961, MIT computer science professor Fernando Corbato created the first digital password as a project problem-solver. Cempaka Sari, A., et al. (2022). *Review Of Text Based Password And Other Authentication Methods For E-Commerce Data Protection.* In Bina Nusantara University, Journal Of Theoretical And Applied Information Technology (Vol. 100, Issue 6, Pp. 1604–1605) [Journal-Article]. Little Lion Scientific. https://Www.Jatit.Org

[23] In 1951, the Eckert-Mauchly Computer Corporation (EMCC) began building the first commercial mainframe, UNIVAC. Soon after, in 1953, IBM introduced its first mainframe designed for commercial business use, the IBM Model 701 Electronic Data Processing Machine. The company's first electronic computer, the 701 was about 25 times to 50 times faster than its predecessors, with rapid advancements in computing power, memory capacity and smaller size. Susnjara, S., & Smalley, I. (2024). *What is a mainframe?* IBM. What is a Mainframe

[24] Packard, N. (2020). *The ARPANET into the Internet: A tale of two networks.* Studies in Media and Communication, 8(1), 37. https://doi.org/10.11114/smc.v8i1.4783

and resource sharing between researchers. However, as interconnected systems emerged, so did the need for more sophisticated security solutions.

It was during this decade that the first computer virus was developed. Bob Thomas, a computer engineer working at BBN Technologies, created a program called *Creeper*, which moved across ARPANET terminals, displaying the message *I'm the creeper: catch me if you can*.[25] In response, in 1971, Ray Tomlinson, a computer programmer, developed *Reaper*, the first antivirus program, to counteract *Creeper*.[26] These developments highlighted the growing importance of protecting digital systems from unauthorized intrusions.

Government agencies, recognizing the potential risks of interconnected computing, began prioritizing cybersecurity. Projects like the US ARPA (Advanced Research Projects Agency) laid the groundwork for securing systems that were becoming integral to national infrastructure and defense.[27]

The 1980s witnessed the democratization of computing.[28] Personal computers became increasingly available to the general public, and with them came an explosion of connectivity through systems

[25] Nilupul, S. A. (2024). *Evolution and Impact of Malware: A Comprehensive Analysis from the First Known Malware to Modern-Day Cyber Threats*. Cyber Security. Evolution and Impact of Malware: A Comprehensive Analysis from the First Known Malware to Modern-Day Cyber Threats

[26] Chebitko, R. (2024). *The first antivirus was called*. MS.Codes. The First Antivirus Was Called

[27] The Advanced Research Projects Agency (ARPA), established in 1958, was a U.S. government agency dedicated to fostering high-risk, high-reward research and development projects. Its mission was to expand the frontiers of technology and science, aiming to achieve breakthroughs that were not readily attainable through traditional research channels. ARPA played a pivotal role in the development of early computer networks, including the ARPANET, which laid the foundation for the modern internet. In 1972, ARPA was renamed the Defense Advanced Research Projects Agency (DARPA) to emphasize its focus on defense-related research. DARPA continues to drive innovation in various technological fields, including cybersecurity, by funding advanced research projects. Dennis, & Aaron, M. (2025, February 15). *Defense Advanced Research Projects Agency (DARPA)*. Encyclopedia Britannica. https://www.britannica.com/topic/Defense-Advanced-Research-Projects-Agency

[28] *History of computer hacking and cybersecurity threats: From the 50s to today (2023). Mayhem.* https://www.mayhem.security/blog/history-of-computer-hacking-and-cybersecurity-threats-from-the-50s-to-today

like Bulletin Board Systems (BBS).[29] This newfound accessibility also brought new vulnerabilities, as viruses and malware began to proliferate.

Notable examples from this era include the Elk Cloner virus (1982), targeting Apple II computers,[30] and the Brain virus (1986), which infected IBM-compatible PCs.[31] The infamous Morris Worm of 1988 marked one of the first widespread instances of malware, disrupting thousands of computers across the nascent internet.[32]

Governments also began taking cybersecurity more seriously. In 1983, U.S. President Ronald Reagan signed National Security Decision Directive 145,[33] which emphasized safeguarding telecommunications and computer systems. In the same year, the launch of the Domain Name System (DNS) eased internet navigation while simultaneously introducing new security concerns..[34]

The 1990s marked the beginning of a new era of connectivity, with the internet expanding quickly and the World Wide Web becoming increasingly commercialized.[35] Personal computing became ubiquitous, and with it came an exponential increase in cyber threats. Online platforms like America

[29] Bulletin-board systems (BBS) were computerized systems used to exchange public messages or files. The Editors of Encyclopaedia Britannica. (2025, January 24). *Bulletin-board system | Online Forum, Message Board, Networking*. Encyclopedia Britannica. https://www.britannica.com/technology/bulletin-board-system

[30] Nilupul, S. A. (2024). Evolution and Impact of Malware: A Comprehensive Analysis from the First Known Malware to Modern-Day Cyber Threats. Cyber Security. Evolution and Impact of Malware: A Comprehensive Analysis from the First Known Malware to Modern-Day Cyber Threats

[31] Schneider, J., (2023). *The history of malware: A primer on the evolution of cyber threats.* IBM blog https://www.ibm.com/think/topics/malware-history.

[32] Ibidem.

[33] The White House. (1984). *National Security Decision Directive Number 145: National policy on telecommunications and automated information systems security*. https://irp.fas.org/offdocs/nsdd145.htm

[34] The Domain Name System (DNS) constitutes a fundamental component of the Internet, which serves as the primary medium for most modern communications. One of its main functions is to convert human-readable domain names into machine-readable IP addresses. In this way, DNS acts as a translator, linking the names people use to access websites with the numerical addresses that computers require to locate and communicate with those sites. See Khormali, A., et al. (2021). *Domain name system security and privacy: A contemporary survey.* Computer Networks, 185, 107699.

[35] Smith, K. (2024, June 3). *A History of Cybersecurity and cyber threats.* Coro Cybersecurity. A History of Cybersecurity and Cyber Threats

Online (AOL)[36] and Internet Relay Chat (IRC)[37] became popular, but they also introduced new avenues for cyberattacks, including unauthorized access, social engineering, and distributed denial-of-service (DDoS) attacks.[38]

The rise of Microsoft Windows as the dominant operating system made it a prime target for cybercriminals. High-profile incidents, such as the rise of ransomware and the theft of sensitive information, highlighted the vulnerabilities of both individuals and organizations.[39]

As we entered the 21st century, the proliferation of technologies like 5G, cloud computing, and the Internet of Things (IoT) drastically expanded the attack surface for cybercriminals. In recent decades, the rise of automated cyberattacks, driven by artificial intelligence and machine learning, has enabled threat actors to compromise systems with minimal human intervention.[40] Further compounding these challenges, the emergence of quantum computing poses a significant threat to existing cybersecurity frameworks, with the potential to render many current encryption methods obsolete.[41] The looming capability to retroactively decrypt sensitive data intercepted today raises urgent concerns about long-term data confidentiality. Together, AI and quantum technologies not

[36] AOL was one of the earliest and most popular internet service providers (ISPs) and online platforms in the 1990s and early 2000s. It offered dial-up internet access, email services, instant messaging (AOL Instant Messenger or AIM), and online chat rooms. AOL played a major role in popularizing the internet for everyday users but declined in relevance with the rise of broadband internet and modern social media platforms. Burgelman, R. & A., Meza P., E., (2003). *AOL: The Emergence of an Internet Media Company*. Stanford Graduate School of Business. AOL

[37] IRC is a text-based communication protocol that enables real-time chat between multiple users in channels (chat rooms) or private messages. It was widely used in the 1990s and early 2000s for online discussions, tech support, and even early forms of hacking communities. While its popularity has diminished, IRC is still used today, particularly in niche communities and by developers. Rintel S. E., et al. (2001). *First Things First: Internet Relay Chat Openings*, Journal of Computer-Mediated Communication, Volume 6, Issue 3. https://doi.org/10.1111/j.1083-6101.2001.tb00125.x

[38] Smith, K. (2024, June 3). *A History of Cybersecurity and cyber threats.* Coro Cybersecurity. A History of Cybersecurity and Cyber Threats

[39] Ling, X. & Wu, L. (2023). *Adversarial attacks against Windows PE malware detection: A survey of the state-of-the-art.* Computers & Security *128*, 103134. https://doi.org/10.1016/j.cose.2023.103134

[40] Adewuyi, N. A., et al. (2024). T*he convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems.* World Journal of Advanced Research and Reviews, 23(1), 379–394. https://doi.org/10.30574/wjarr.2024.23.1.1993

[41] Weigand, S. (2025, January 2). *2025 Forecast: AI to supercharge attacks, quantum threats grow, SaaS security woes*. SC Media. https://www.scworld.com/feature/cybersecurity-threats-continue-to-evolve-in-2025-driven-by-ai

only elevate technical risks but also introduce profound regulatory, ethical, and strategic challenges, demanding new cryptographic standards, forward-looking governance, and specialized expertise to ensure digital resilience in a rapidly evolving threat landscape.

Having examined the origins and evolution of cybersecurity, the next section will turn to the underlying purposes of cyberattacks, exploring the diverse motivations and strategic objectives that drive them.

1.2.1 The Purpose and Consequences of a Cyber Attack

With the continuous evolution of digital technologies and the growing sophistication and frequency of cyberattacks, internet security has emerged as one of the most pressing challenges of the twenty-first century.[42] Advances in information and communication technologies have revolutionized the way data is created, transmitted, and stored, but this very transformation has also exposed critical vulnerabilities. As societies and businesses become increasingly reliant on interconnected systems, the protection of information and digital assets has become not only a technical necessity but also a strategic imperative for economic stability, public trust, and national security.[43]

The purpose of a cyberattack can vary depending on the attackers' objectives. In today's digital landscape, one of the primary motivations behind cyberattacks is data theft as data has become one of the most valuable assets, often referred to as the "new currency".[44] Data thefts can involve stealing a business's financial information, customer financial details such as credit card data,

[42] World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. Global Cybersecurity Outlook 2025

[43] Ibidem.

[44] Ablon, L. (2018). *Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data.* Testimony before the Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance, United States House of Representatives. RAND Corporation. Data Thieves

sensitive personal data, email addresses and login credentials, client databases, intellectual property including trade secrets or product designs.

Beyond data theft, cyberattacks may also be motivated by other factors. Some cybercriminals engage in hacktivism, using cyberattacks to promote a social or political cause, often by disrupting services or leaking sensitive information[45]. Others carry out cyber espionage, using hacking techniques to spy on competitors, governments, or organizations to gain an unfair advantage in business, politics, or international affairs. In addition, some attacks are driven by financial motives, such as ransomware, where hackers steal data, encrypt it to block access, and demand payment for its release, sometimes threatening to leak the data unless the ransom is paid.[46]

Beyond data theft, cyberattacks can also compromise critical national infrastructure, posing serious threats to national security.[47] By stealing sensitive government information or disrupting and sabotaging essential systems, these attacks can cause significant operational downtime and destabilize key services. This type of attack is particularly significant in cyber warfare, where adversaries target critical infrastructure such as power grids, communication networks, or military systems to weaken a nation's defenses or disrupt essential services. The following paragraph will examine the role of cybersecurity in international relations and its impact on diplomatic and strategic interactions between states.

1.3 The Geopolitical Implications of cyberattacks on International Relations

[45] Vaidya, T. (2015). *2001-2013: Survey and analysis of major cyberattacks.* arXiv (Cornell University). https://doi.org/10.48550/arxiv.1507.06673

[46] Connolly, L. Y., et al. (2020). *An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability.* Journal of Cybersecurity, *6*(1). https://doi.org/10.1093/cybsec/tyaa023

[47] Geers, K. (2009). *The cyber threat to national critical infrastructures: Beyond theory.* Information Security Journal: A Global Perspective, *18*(1), 1–7.

As mentioned in the previous paragraph, cybersecurity threats are one of the main national security, and public safety challenges every nation faces in the twenty-first century. The content of international security has expanded over the years. Today it covers a variety of interconnected issues including the protection of national critical infrastructure from cyberattacks.[48]

Cyberattacks in fact have become a critical threat to national security, as they increasingly target the essential systems and infrastructures that sustain modern societies. Critical infrastructure - including energy, water, communications, transportation, healthcare and finance - forms the backbone of a nation's economy and public safety.[49] These infrastructures are considered crucial because their disruption or destruction could have a devastating impact on national security, economic stability, and the well-being of citizens.

With the rapid expansion of the Internet in the 1990s, it became evident that illicit activities in the digital domain could yield significant financial gains and organized crime groups increasingly established their presence in cyberspace. In some instances, these criminal enterprises appeared to operate with the tacit approval or even direct support of the governments within whose jurisdictions they were based, further complicating efforts to combat cybercrime at an international level.[50]

The geopolitical implications of cyber risks on international relations are profound and multifaceted, as the digital domain increasingly shapes the interactions between nations.[51] In an interconnected world, cyberspace has emerged as a critical frontier where power dynamics, security

[48] Maglaras, L., et al. (2022). *Cybersecurity of critical Infrastructures: challenges and solutions.* Sensors, *22*(14), 5105. https://doi.org/10.3390/s22145105

[49] Ribeiro, A. (2025c). *NERC 2025 RISC report finds cybersecurity, supply chain, critical infrastructure interdependencies among top reliability risks*. Industrial Cyber. NERC 2025 RISC Report

[50] Tran, D. (2018). *The law of attribution: Rules for attributing the source of a cyber-attack.* Yale Journal of Law & Technology, 20(1), 376. Interesting for the problem of attribution.

[51] Foulon, M., & Meibauer, G. (2024). *How cyberspace affects international relations: The promise of structural modifiers.* Contemporary Security Policy, *45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

concerns, and statecraft converge. Cyber risks not only challenge national security but also influence diplomatic relationships, economic stability, and global governance structures.

One significant geopolitical implication of cyberattacks is the erosion of trust between nations. Cyberattacks attributed to state actors, such as hacking government systems or targeting critical infrastructure, fuel suspicions and escalate tensions.[52] These incidents often lead to a breakdown in diplomatic relations, with accusations and retaliatory actions becoming a norm. This cycle of mistrust can destabilize regions and undermine international cooperation.

Furthermore, the weaponization of cyber tools has introduced a new dimension to modern warfare, fundamentally altering the nature of conflict and national security.[53] Cyber operations, including espionage, sabotage, and disinformation campaigns, have become key instruments of statecraft, allowing nations to assert influence, gather intelligence, and disrupt adversaries without resorting to conventional military action. Unlike traditional warfare, cyberattacks can be executed remotely, often with anonymity, making attribution challenging and enabling states to engage in hostilities while maintaining plausible deniability.

The war in Ukraine has brought this reality into sharp focus, demonstrating how cyberattacks have become a critical feature of modern warfare. On December 12 2023, Ukraine's largest mobile network, Kyivstar, suffered a cyberattack that disrupted essential services, including air raid sirens and text alerts warning citizens of Russian air assaults.[54] The UK's Ministry of Defense labeled the incident as "one of the highest-impact disruptive cyberattacks on Ukrainian networks" since

[52] Azubuike, C. F. (2023). *Cyber security and international conflicts: An analysis of state-sponsored cyber attacks.* Nnamdi Azikiwe Journal of Political Science (NAJOPS), 9(1). ISSN: 2992-5924.

[53] Cyberspace has moved from the realm of political competition to a domain permanently involved in warfare, a battlefield on which actors generate combat power to combine with forces in other domains. Theorists have speculated on the nature of cyber warfare and how it will affect future wars, but the 2022 Russian invasion of Ukraine provides an important look into how cyber operations actually integrate into a conventional war. Pickle, C. (2024). *The changing character of cyber warfare.* Proceedings, 150(6), 1-456. U.S. Naval Institute.

[54] Hunder, M., et al. (2023, December 12). *Ukraine's top mobile operator hit by biggest cyberattack of war.* Reuters.

Russia's full-scale invasion.[55] Responsibility for the attack was claimed by Solntsepyok, a group linked by Ukrainian officials to Russian military intelligence.[56]

Oleksandr Komarov, CEO of Kyivstar, underscored the broader context of the attack, describing it as a consequence of the war with Russia.[57] This incident illustrates the dual nature of contemporary conflicts, where physical and digital battlegrounds are deeply intertwined and war is also happening in cyberspace.

Cyberattacks in this context are not merely technical disruptions; they have profound implications for national security, civilian safety, and international law. The International Criminal Court (ICC) has begun to explore the potential for cyberattacks to be prosecuted as international crimes.[58] According to ICC Prosecutor Karim Khan, while cybercrimes are not explicitly mentioned in the Rome Statute, such acts could fulfill the elements of core international crimes, including war crimes, crimes against humanity, genocide, and the crime of aggression. Khan has stated the Court's intention to investigate cybercrimes, recognizing their role in exacerbating the human toll of conflict.[59]

Cyberattacks also have global economic implications. Cyber risks threaten the stability of global trade and financial systems, as cyberattacks targeting supply chains, financial institutions, and

[55] Verbruggen, Y. (2024). *Cyberattacks as war crimes.* International Bar Association.Cyberattacks as War Crimes

[56] Ibidem.

[57] Hunder, M., et al. (2023, December 12). *Ukraine's top mobile operator hit by biggest cyberattack of war.* Reuters.

[58] Verbruggen, Y. (2024). *Cyberattacks as war crimes.* International Bar Association.Cyberattacks as War Crimes

[59] In a statement from January 2024, Prosecutor Khan addressed the issue of cyber-enabled crimes, emphasizing the Court's commitment to addressing these challenges within the framework of the Rome Statute system. For further details see *Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system,* (2024). International Criminal Court. Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system

intellectual property disrupt economic activity.[60] These incidents exacerbate existing inequalities between nations, as wealthier states are better equipped to invest in cybersecurity measures, while developing countries remain vulnerable. This digital divide not only hampers economic growth but also deepens geopolitical rivalries, as nations compete for technological dominance.[61]

Disinformation campaigns and the manipulation of public opinion through digital platforms have further strained international relations. The ability of state and non-state actors to influence elections, sow discord, and destabilize societies challenges the principles of sovereignty and self-determination.[62] These activities blur the lines between internal and external threats, prompting nations to adopt defensive measures that may infringe on privacy and human rights.

The lack of a comprehensive international framework to govern cyberspace exacerbates these challenges. Unlike traditional domains of conflict, such as land, sea, and air, cyberspace operates without clear boundaries or universally accepted norms.[63] This regulatory vacuum fosters ambiguity, making it difficult to attribute cyber incidents and hold perpetrators accountable. As a result, nations often resort to unilateral actions, further complicating efforts to establish a stable and cooperative digital environment.

The following paragraph will focus on the European cybersecurity landscape, assessing the scale of cyber threats facing the region and highlighting how businesses increasingly rank cyber risks

[60] Natalucci, F., et al. (2024, April 9). *Rising cyber threats pose serious concerns for financial stability. I*nternational Monetary Fund. Rising Cyber Threats Pose Serious Concerns for Financial Stability

[61] Geopolitical tensions, the rapid adoption of emerging technologies, and the increased reliance on interdependent supply chains contribute to the growing complexity of cyberspace. This complexity exacerbates the digital divide between countries, widening the gap between wealthy nations with advanced cybersecurity measures and developing countries facing greater vulnerabilities. World Economic Forum. (2025). *Global Cybersecurity Outlook 2025.* https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[62] In 2023, Polish officials reported a disinformation campaign targeting the Polish public, with recipients receiving anti-Ukrainian refugee disinformation via email. These activities were attributed to Russia-linked hackers. *Significant Cyber Incidents | CSIS*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents?

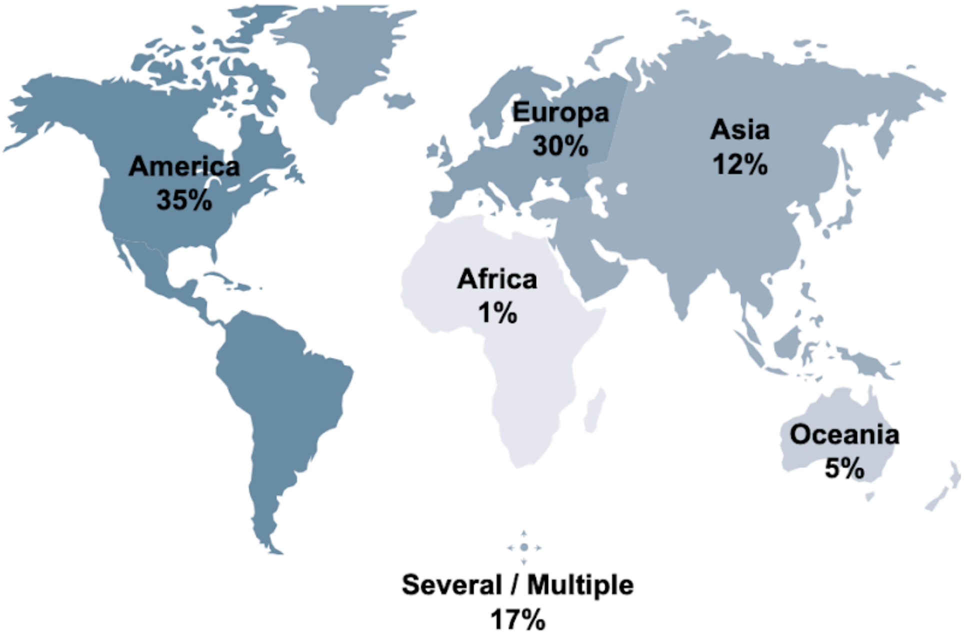
[63] Hofmann, S. C., & Pawlak, P. (2023). *Governing cyberspace: policy boundary politics across organizations*. Review of International Political Economy, 30(6), 2122–2149. https://doi.org/10.1080/09692290.2023.2249002

among the most significant global threats. It will also explore how some selected EU member states are addressing these challenges to strengthen both national and corporate cyber resilience.

1.4 Europe's Cybersecurity Landscape: Threat Trends and Investments

According to the Security Navigator 2025, published by Orange Cyberdefense, Europe has become the leading target for hacktivism, with over 6,600 attacks by a single pro-Russian group since March 2022, 96% of which were aimed at European countries, particularly Ukraine, the Czech Republic, Spain, Poland, and Italy.[64]

Figure 1.1 Geography of victims 2024



© Clusit - Rapporto 2025 sulla Cybersecurity

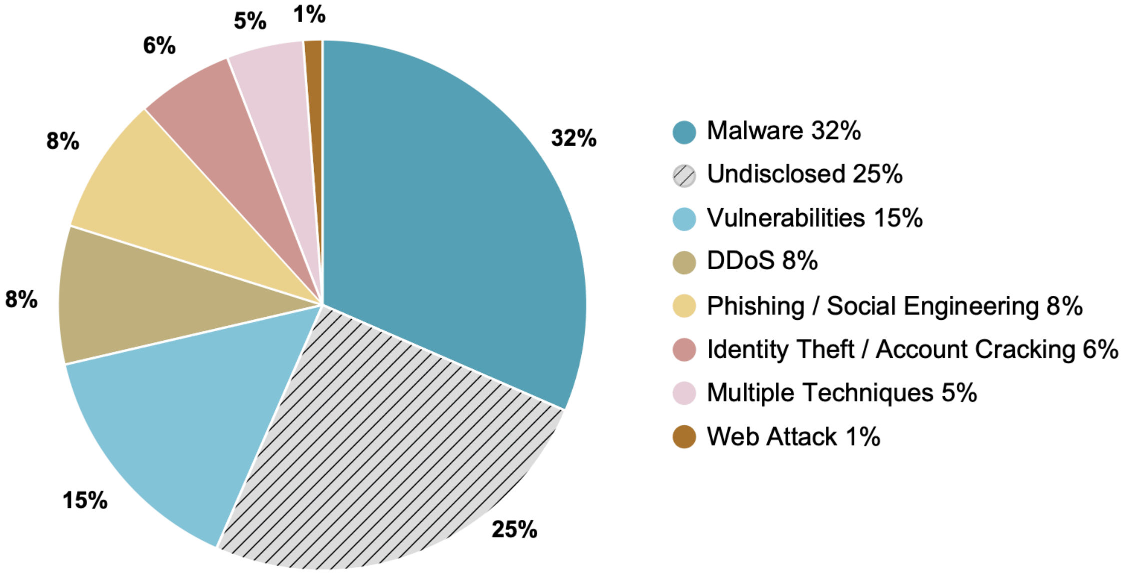
The Clusit 2025 report highlights a concerning rise in cyberattacks. In 2024, the number of serious cyber incidents increased by 27% worldwide and by 15% in Italy.[65] Despite contributing only 1% to

[64] *Security Navigator 2025 reveals Europe as top target of hacktivism groups shifting focus to cognitive attacks.* (2024). Orange Business. Security Navigator 2025 reveals Europe as top target for hacktivism, with groups shifting focus to cognitive warfare

[65] *Clusit: Rapporto 2025 sulla Cybersecurity in Italia e nel mondo. 2025. Clusit.* Clusit Report

global GDP, Italy suffered 10% of all global cyberattacks, underscoring a significant imbalance and vulnerability.[66] The most common threats in 2024 included ransomware and malware, marking a shift from the previous year's predominance of Denial of Service attacks. Phishing also remained a major issue, accounting for 35% of cybersecurity incidents in the country.[67] A notable increase in attacks targeted the public sector, which experienced a 90% surge in Europe, with Italy among the most affected nations.[68]

Figure 1.2 Distribution of cyberattack techniques in 2024



© Clusit - Rapporto 2025 sulla Cybersecurity

Additionally, cyber extortion incidents rose by 18% year-on-year across Europe, with Italy and Germany each accounting for 19% of victims, France 16%, Spain 13%, and Belgium 8%.[69] The

[66] Ibidem

[67] Ibidem

[68] Ibidem

[69] *Security Navigator 2025 reveals Europe as top target of hacktivism groups shifting focus to cognitive attacks.* (2024). Orange Business. Security Navigator 2025 reveals Europe as top target for hacktivism, with groups shifting focus to cognitive warfare

EU's ENISA Threat Landscape report further corroborates the growing threat, documenting approximately 2,580 cyber incidents across member states in 2024, including 220 cross-border attacks.[70]

Critical infrastructure across Europe, such as government, healthcare, telecommunications, and energy, has increasingly been targeted by sophisticated threats ranging from AI-driven fraud to state-sponsored espionage. In the UK, for instance, the 2025 Cyber Security Breaches Survey found that 67% of medium and 74% of large businesses reported cyber breaches or attacks, with phishing being the most prevalent form (affecting 93% of businesses and 95% of charities that experienced cybercrime).[71]

Data from the AXA Future Risks Report shows that companies increasingly perceive cyber risk as one of the top global threats.[72] Alongside climate change and geopolitical instability, cyber threats are now considered among the most significant dangers facing businesses. In Europe, cyber risk is frequently ranked as the most pressing concern, and companies express growing concern about the complexity and unpredictability of attacks, especially as they are increasingly facilitated by artificial intelligence and advanced digital tools. This convergence of statistical trends and business perception underscores the urgent need for stronger cybersecurity strategies and investment.

The global cybersecurity market is projected to reach approximately USD 309 billion by 2029, up from an estimated USD 201 billion in 2025, reflecting a compound annual growth rate (CAGR) of 10.6%. [73] This expansion is being driven by stricter regulations, accelerated digital adoption, and the

[70] *Threat landscape. (2025). ENISA*. https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

[71] *Cyber security breaches survey 2025*. (2025). GOV.UK. Cyber security breaches survey 2025

[72] *AXA Future Risks Report 2024*. AXA.com. https://www.axa.com/en/news/2024-future-risks-report

[73] Cimmarusti, I. (2025, July 8). *Cybersecurity, investment in the euro area to reach EUR 75 billion.* Il Sole 24 ORE. https://en.ilsole24ore.com/art/cybersecurity-in-the-euro-area-investments-the-75-billion-AH47W3RB?refresh_ce=1

emergence of new cyber threats. In Europe, the trend is similarly positive: cybersecurity expenditure in the eurozone is currently around €50 billion and is expected to rise to €75.6 billion by 2029, maintaining a steady CAGR of 10–11%.[74]

In particular, the European Commission has committed substantial resources to strengthening cybersecurity across the European Union, allocating €145.5 million (approximately US$170 million) to support public administrations and small and medium-sized enterprises in adopting advanced cybersecurity solutions and research-driven innovations.[75] This effort is being implemented through two major funding initiatives managed by the European Cybersecurity Competence Centre. The first, under the Digital Europe Programme, has a budget of €55 million, with €30 million specifically dedicated to enhancing cybersecurity in hospitals and healthcare providers.[76] This initiative aims to help these institutions detect, monitor, and respond effectively to threats such as ransomware, strengthening resilience in the healthcare sector amid ongoing geopolitical tensions. The program also funds pilot projects that bring together stakeholders, including hospital networks, professional associations, and cybersecurity service providers, to assess needs, implement technical solutions, and provide staff training.[77]

Complementing this, the Horizon Europe Programme provides approximately €90.5 million to advance cybersecurity research and innovation.[78] Its focus includes the development of operational tools, generative AI applications, privacy-enhancing technologies, and post-quantum cryptography,

[74] Ibidem.

[75] *EU allocates €145.5 million to boost European cybersecurity, including for hospitals and healthcare providers*. (2025). Shaping Europe's Digital Future. European Commission

[76] Ibidem.

[77] Ribeiro, A. (2025). *EU invests €145.5 million to strengthen cybersecurity across healthcare systems and public institutions*. Industrial Cyber. EU invests €145.5 million to strengthen cybersecurity across healthcare systems and public institutions

[78] *EU allocates €145.5 million to boost European cybersecurity, including for hospitals and healthcare providers*. (2025). Shaping Europe's Digital Future. European Commission

alongside frameworks and services that support cross-sector and cross-border operational cooperation.[79] Proposals are expected to address outcomes such as improved situational awareness, enhanced cyber threat intelligence, risk assessments for critical EU supply chains, expanded functionality for Security Operations Centres (SOC/CSIRTs), and the development of digital twins for critical infrastructure.[80] The funding also supports the creation of cyber crisis management frameworks and tools to bolster EU-wide preparedness for cyber and hybrid threats.

These initiatives are designed to foster a stronger European cybersecurity ecosystem by supporting SMEs, start-ups, and scale-ups, facilitating market access across the EU and internationally, and promoting innovation through incubators, accelerators, and technology transfer programs.[81] Additionally, the Commission emphasizes raising cybersecurity awareness among citizens, students, and professionals to reduce the likelihood of incidents and data breaches.[82] Complementing these investments, the EU recently formalized the Cyber Blueprint for cyber crisis management, establishing a coordinated framework for detection, response, and recovery across member states during large-scale cybersecurity events.[83] Together, these strategic investments and initiatives reflect the EU's commitment to building a resilient, innovative, and secure digital environment that safeguards both public and private sector entities while promoting the growth of a competitive cybersecurity market.

[79] Ribeiro, A. (2025, June 13). *EU invests €145.5 million to strengthen cybersecurity across healthcare systems and public institutions*. Industrial Cyber. EU invests €145.5 million to strengthen cybersecurity across healthcare systems and public institutions

[80] Ibidem.

[81] Ibidem.

[82] Ibidem.

[83] Ribeiro, A. (2025a, June 6). *EU Cyber Blueprint unifies crisis management, sets joint response framework, enhances cross-border coordination*. Industrial Cyber. EU Cyber Blueprint unifies crisis management, sets joint response framework, enhances cross-border coordination

Despite EU-level investment plans and national initiatives aimed at enhancing cybersecurity resilience, projections for 2025 indicate a possible slowdown, as weak economic growth, geopolitical tensions, trade disputes, and the impact of US tariff policies lead many European companies to reconsider or postpone their cybersecurity spending.[84] Companies are increasingly faced with the strategic choice of either strengthening their cyber defenses or postponing expenditure. In Italy, for instance, a Deloitte survey indicates that 52% of companies anticipate increasing their cybersecurity budgets over the next two years, driven both by the growing frequency of cyberattacks targeting private organizations and by ongoing geopolitical uncertainties, as highlighted by Bruno Frattasi, Director of the National Cybersecurity Agency.[85]

1.5 Regional and Global Cybersecurity Governance: The European Union and the United Nations.

1.5.1 The European Union's Legislative Framework For Data Protection

The EU upholds privacy as a fundamental human right, enshrined in its Charter of Fundamental Rights[86] and has established itself as a global leader in data protection and cybersecurity by implementing a comprehensive and stringent regulatory framework designed to safeguard users' data.[87]

[84] Ibidem.

[85] Deloitte. (2025). *Future of Cyber Survey 2025: La cybersecurity come chiave per la creazione del valore aziendale, nel percepito delle imprese italiane.* Deloitte Italia.

[86] Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. *Recital 1 - Data protection as a Fundamental right - General Data Protection Regulation (GDPR).* (2019, September 2). General Data Protection Regulation (GDPR). Recital 1 Data Protection as a Fundamental Right

[87] The extraterritorial reach of the EU General Data Protection Regulation (GDPR) has significant global implications, as it applies to any company processing the personal data of EU citizens, regardless of where the company is based. This has profound consequences for international relations, particularly in the context of transatlantic data flows and regulatory alignment. A notable example is the ongoing discussion regarding U.S. data protection standards and their alignment with the GDPR framework. For an overview of EU GDPR and USA regulations read Bakare, S. S., et al.,

At the core of this framework is the General Data Protection Regulation (GDPR), a groundbreaking piece of legislation that not only reinforces individuals' rights to access, correct, and delete their personal information but also imposes strict obligations on organizations to ensure transparency, accountability, and robust security measures in handling data, thereby setting a global benchmark for privacy and cybersecurity standards. The EU's strong stance on data protection reflects its broader commitment to digital trust, consumer rights, and the prevention of data misuse in an increasingly interconnected world.

Among national critical infrastructure, the telecommunications sector, as a major processor of vast amounts of personal data, is inevitably impacted by the several EU regulations and directives. This section provides an overview of the key regulations, directives, and legislative acts that govern data protection in the EU, specifically those relevant to the telecommunications sector. [88]

On January 25, 2012, the European Commission proposed a comprehensive revision of the EU's 1995 data protection rules, with the goal of enhancing individuals' rights over their personal information.[89]

(2024). *Data Privacy Laws And Compliance: A Comparative Review Of The EU GDPR And USA Regulations.* Computer Science & IT Research Journal.

[88] At the European level, legislation distinguishes between regulations and directives, each with distinct legal effects. A regulation is a binding legislative act that applies directly and uniformly across all EU member states without the need for national implementation. In contrast, a directive establishes objectives that EU countries must achieve, but it allows each member state to determine the specific legal measures required to reach those goals. This distinction ensures both harmonization and flexibility within the EU's legal framework for data protection. *Types of legislation.* European Union. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en?

[89] A "Data Subject" is the individual the personal data relates to. See European Data Protection Board (EPDB). *Key GDPR Definitions.*

To improve upon the standards set by Directive 95/46/EC[90] and address its limitations, the Commission determined that a Regulation would be the best legal tool to establish a unified framework for personal data protection across the Union. Because a Regulation is directly applicable under Article 288 TFEU, it helps minimize legal inconsistencies, enhances legal clarity, strengthens individual privacy rights, and facilitates the smooth movement of personal data within the EU.[91]

The European Union's General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, which became enforceable on May 25, 2018, is a pivotal advancement in the global approach to data privacy.[92] As a binding legislative act, the GDPR is directly applicable and enforceable across all EU Member States. It represents a uniform framework that harmonizes data protection laws across the region, replacing the earlier Data Protection Directive (DPD) of 1995.

The GDPR is built upon six foundational principles that govern the processing of personal data.[93] First, data must be processed in a lawful, fair, and transparent way, ensuring that individuals are fully informed about how their information is collected and used. Second, data must be collected for specified, explicit, and legitimate purposes, with restrictions on further processing to prevent misuse. This principle, known as "purpose limitation," allows exceptions for public interest, scientific, or historical research, provided safeguards are in place to protect data subjects. Third, the

[90] European Parliament and Council of the European Union. (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Official Journal of the European Communities, L 281, 23 November 1995, 31-50. Today it is no longer in force.

[91] European Union. (2012). *Consolidated version of the Treaty on the Functioning of the European Union, Article 288*. Official Journal of the European Union, C 326, 26 October 2012, 47–390.

[92] Albrecht, J. P. (2016). *How the GDPR will change the world.* European Data Protection Law Review (EDPL), 2(3), 287-289.How the GDPR will change the world.

[93] Art. 5 - Principles relating to processing of personal data - *General Data Protection Regulation (GDPR)*. (2018). https://eur-lex.europa.eu/eli/reg/2016/679/oj. For an analysis of the six GDPR's principles see Gay, C. (2019). *The GDPR's effect on transatlantic relations*. University of Chicago Law School, Chicago Unbound.

principle of “data minimization” mandates that only the personal data essential for achieving the specified purpose is collected, thereby mitigating the risks tied to handling excessive information.

Additionally, the GDPR emphasizes the importance of data accuracy. Organizations must ensure that personal data remains accurate and up to date, implementing measures to rectify inaccuracies promptly. The regulation also addresses the duration for which data can be retained, adhering to the principle of “storage limitation.” Personal data should only be stored for as long as necessary to fulfill its intended purpose, with exceptions made for research or public interest projects subject to robust safeguards. Finally, the principle of “integrity and confidentiality” requires organizations to adopt appropriate technical and organizational measures to protect data against unauthorized access, loss, or damage, ensuring a high level of security.

Beyond its foundational principles, the GDPR introduces several innovative concepts, such as *privacy by design* and *privacy by default*.[94] These concepts require organizations to integrate data protection measures into their systems and processes from the outset rather than as an afterthought. The regulation also imposes stringent requirements for obtaining consent,[95] which must be clear, affirmative, and withdrawable at any time, ensuring that individuals retain control over their data throughout its lifecycle. Additionally, the GDPR requires organisations handling personal data to systematically identify and document all the personal data they gather and process.[96] For every

[94] Goddard, M. (2017). *The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact.* International Journal of Market Research, 59(6), 703-705. https://doi.org/10.2501/IJMR-2017-050

[95] Internet Service Providers (ISPs) must ensure that consumer information is stored and used only with explicit user consent and, where possible, in a manner that does not allow for easy identification of individuals. Consumer consent plays a crucial role in determining how data is stored and processed throughout the data processor supply chain. Furthermore, telecom operators are required to delete any personally identifiable information (PII) upon a user’s request (Art. 17 GDPR - Right to erasure) and must ensure that PII datasets are portable (Art.20 GDPR - Right to data portability) meaning they should be structured in a standardized format that allows users to access and transfer their data upon request. These stringent regulations reinforce the GDPR’s commitment to empowering users with greater control over their personal data while imposing strict compliance measures on companies operating in the telecommunications sector. Art.7 - *Conditions for consent* - General Data Protection Regulation (GDPR). (2018).

[96] Article 30 - *Records of processing activities* - General Data Protection Regulation (GDPR). (2018).

processing activity, organizations are required to document the types of data involved, the reasons for processing, and the technical and organizational safeguards in place to protect the data, as well as details of any data transfers. Moreover, the GDPR imposes a strict obligation to notify authorities of any data breaches within 72 hours, ensuring timely response and transparency to safeguard individuals' rights and minimize potential harm.[97]

Non-compliance with GDPR can result in penalties reaching as high as €20 million or 4% of the global annual revenue of the business or group, depending on which amount is greater.[98] In addition to these financial penalties, non-compliance can also lead to claims and class actions from data subjects. The fines are scaled according to the severity of the infringement, underscoring the critical importance of adhering to the regulation and ensuring robust data protection practices.

The General Data Protection Regulation (GDPR) has a particularly significant impact on telecommunications companies, as handling sensitive customer data is central to their operations. This has required telecom operators to reorient their business processes, revamp governance mechanisms, and even explore new revenue streams to ensure compliance. Given the ever-increasing risk of network breaches in the digital domain, telecom companies providing services within the European Union must restructure the way they collect, store, and analyze vast amounts of customer data within the GDPR framework. To achieve full compliance, they must conduct a thorough reassessment of their entire business operations, including Business Support Systems (BSS), which manage customer interactions, billing, and service orders, as well as Operational Support Systems (OSS), which oversee network management and service provisioning.

[97] Art. 33 - *Notification of a personal data breach to the supervisory authority* - General Data Protection Regulation (GDPR). (2018).

[98] Art. 83 - *General conditions for imposing administrative fines* - General Data Protection Regulation (GDPR). (2018).

Additionally, telecom companies are required to appoint a Data Protection Officer (DPO) as mandated by Article 37 of the GDPR.[99] Internet Service Providers (ISPs) must also ensure that consumer information is stored and used only with explicit user consent and, where possible, in a manner that does not allow for easy identification of individuals.[100] Consumer consent plays a crucial role in determining how data is stored and processed throughout the data processor supply chain. Furthermore, telecom operators are required to delete any personally identifiable information (PII) upon a user's request and must ensure that PII datasets are portable, meaning they should be structured in a standardized format that allows users to access and transfer their data upon request.[101] These stringent regulations reinforce the GDPR's commitment to empowering users with greater control over their personal data while imposing strict compliance measures on companies operating in the telecommunications sector.

Apart from the General Data Protection Regulation (GDPR), the European Union has introduced a comprehensive set of policies that reflect not only its commitment to data protection but also its determination to strengthen cybersecurity strategies across Europe.

A notable example is the NIS2 Directive, which took effect in January 2023 as an updated version of NIS1 (Directive 2016/1148). NIS2 represents the EU's first extensive legislation designed to enhance the cybersecurity of network and information systems, with the goal of protecting essential

[99] The General Data Protection Regulation (GDPR) has established the concept of a Data Protection Officer (DPO) in Europe. Unlike common assumptions, the obligation to appoint a DPO does not depend on the company's size. Instead, it hinges on the core processing activities that are critical to the company's objectives. If these central activities involve processing sensitive personal data on a large scale or include data processing that significantly impacts individuals' rights, the organization must designate a DPO. See Art. 37 - *Designation of the data protection officer* - General Data Protection Regulation (GDPR). (2018).

[100] GDPR mandates explicit consent as a freely given, specific, informed, and unambiguous indication of user wishes, requiring a clear affirmative action like ticking a box or signing a statement (GDPR Recitals 32 and 42, Articles 4(11), 7, and 9). This consent must be separate from other terms, revocable, documented, and cover specific data processing purposes.

[101] GDPR Article 17 (Right to erasure) grants individuals the right to have their personal data deleted without undue delay when certain conditions apply, such as withdrawal of consent or unlawful processing.

services critical to the EU's economy and society.[102] The NIS2 directive establishes a unified legal framework to uphold cybersecurity in critical sectors across the EU including energy, transport, healthcare, banking and finance and providers of public electronic communication services.[103]

To address the growing cyber threats facing Europe, the NIS2 Directive requires Member States to strengthen their cybersecurity capabilities. It introduces obligations such as implementing risk management practices, establishing reporting protocols, and setting rules to foster cooperation, information sharing, oversight, and enforcement of cybersecurity standards.[104] The directive requires timely notifications of significant cybersecurity incidents to relevant national authorities.[105]

The NIS2 Directive particularly impacts telecommunications companies, requiring them to implement robust risk management practices to detect and mitigate cyber threats effectively, ensuring resilience against potential nation-state attacks and other external adversaries.[106]

[102] Member States had until 17 October 2024 to transpose the NIS2 Directive into national law, with NIS2 officially repealing NIS1 on 18 October 2024. The NIS2 Directive introduces strengthened cybersecurity requirements, expanding the scope of covered entities, enhancing risk management measures, and improving coordination among EU Member States. Compared to NIS1, which primarily focused on critical infrastructure sectors, NIS2 broadens its application to include a wider range of essential and important entities, ensuring a higher level of resilience across the EU. Additionally, NIS2 establishes clearer enforcement mechanisms, stricter incident reporting obligations, and improved oversight by national authorities. *NIS2 Directive: new rules on cybersecurity of network and information systems*. (2025, January 15). Shaping Europe's Digital Future. NIS2 Directive: securing network and information systems

[103] *NIS2 Directive: new rules on cybersecurity of network and information systems*. (2025). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[104] Art. 21 - *Cybersecurity risk-management measures* - Directive (EU) 2022/2555 (NIS2 Directive) - Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555

[105] Art. 23 - *Reporting obligations* - Directive (EU) 2022/2555 (NIS2 Directive) - Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555

[106] Art. 3 of the NIS2 Directive designates "providers of public electronic communications networks or publicly available electronic communications services" as essential and important entities. Member States are required to implement national cybersecurity strategies addressing supply chain security for ICT products and services used by these entities. Additionally, they must establish cybersecurity requirements for ICT products and services in public procurement, covering areas such as cybersecurity certification, encryption, and open-source cybersecurity solutions. These provisions directly impact telecommunication companies, driving them to adopt robust cybersecurity strategies. See Art. 3 - *Essential and important entities* - Directive (EU) 2022/2555 (NIS2 Directive) - Official Journal of the European Union and Art. 7 - *National cybersecurity strategy* - Directive (EU) 2022/2555 (NIS2 Directive) - Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555

As mentioned in this chapter, telecommunications infrastructure plays a vital role in national security and economic resilience, making it a primary focus for proactive cyber threat evaluation. As a result, the NIS2 Directive places more rigorous responsibilities on telecom providers compared to other sectors. These providers are required to deploy cutting-edge encryption technologies to protect communications from evolving cyber threats. Taking this proactive approach is crucial to preserving the confidentiality and integrity of data flowing through telecom networks.[107]

The directive requires each Member State to develop a national cybersecurity strategy that outlines strategic objectives and includes policies focused on securing supply chains, managing vulnerabilities, and promoting cybersecurity education and awareness.[108] Additionally, Member States must maintain and periodically update a register of essential service operators to ensure these entities adhere to the directive's standards.[109]

Another important piece of legislation with a significant impact on the telecom sector is the *ePrivacy Directive* which refers to Directive 2002/58/EC on Privacy and Electronic Communications, as amended by Directive 2009/136/EC.[110]

The ePrivacy Directive aligns closely with the broader European data protection framework and plays a crucial role in regulating privacy and electronic communications within the European Union, particularly affecting the telecommunications sector.[111] One of its primary objectives is to

[107] Art. 21 - *Cybersecurity risk-management measures* - Directive (EU) 2022/2555 (NIS2 Directive) - Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555

[108] Art. 7 - *National cybersecurity strategy* - Directive (EU) 2022/2555 (NIS2 Directive) - Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555

[109] Art. 7 (f) - *National cybersecurity strategy* - Directive (EU) 2022/2555 (NIS2 Directive) - Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555

[110] Art 3 - *Services Concerned - Directive 2002/58/EC (ePrivacy Directive).* Official Journal of the European Union, L 201, 37-47. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058

[111] The ePrivacy Directive complements the GDPR and sets specific rules regarding direct marketing communications, and the placement of cookies and similar identifiers in users' equipment (computers, laptops, smartphones and other devices). European Union. (2002). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July*

ensure the confidentiality of electronic communications by imposing strict obligations on telecom providers regarding the handling of traffic data, routing data, and location data.[112] These forms of metadata, which reveal sensitive information about user behavior and movement, can only be processed under specific conditions, such as with the explicit consent of the user or when necessary for billing, network security, or law enforcement purposes.[113]

In addition to confidentiality rules, the Directive sets forth clear requirements for direct marketing practices, directly impacting how telecom companies can engage with their customers. In principle, the use of automated calling systems, emails, and SMS for marketing purposes requires the prior consent of the recipient, which is typically obtained through an opt-in mechanism.[114] This means that users must take an active step, such as ticking a box or clicking a confirmation button, to agree to receive marketing communications.[115]

2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive). Official Journal of the European Union, L 201, 37-47 https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng?

[112] Article 6 regulates the processing of traffic data, which must be erased or anonymized when no longer needed for communication transmission, except for billing and interconnection payments. Article 9: Stipulates that location data other than traffic data can only be processed if anonymized or with the user's consent, specifying the processing's purpose and duration. Art. 6 - *Traffic data - Directive 2002/58/EC (ePrivacy Directive).* Official Journal of the European Union, L 201, 37-47 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058

[113] Article 10 allows exceptions to the directive's provisions for national security, defense, public security, and the prevention, investigation, detection, and prosecution of criminal offenses. Art. 10 - *Exceptions - Directive 2002/58/EC (ePrivacy Directive).* Official Journal of the European Union, L 201, 37-47 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058

[114] Art. 11 - *Automatic call forwarding* - Directive 2002/58/EC (ePrivacy Directive). Official Journal of the European Union, L 201, 37-47 and Art. 13 - *Unsolicited communications* - Directive 2002/58/EC (ePrivacy Directive). Official Journal of the European Union, L 201, 37-47. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[115] However, the Directive introduces a limited exception, allowing companies to send marketing emails to existing customers without explicit consent, provided that such communications relate to similar products or services and that customers are given a clear and easy option to opt out. This exemption is particularly relevant for telecommunications providers seeking to promote new service plans or additional features to their current subscribers while maintaining compliance with privacy regulations.

Furthermore, the Directive establishes stringent rules regarding the use of cookies and similar tracking technologies, requiring that users grant their consent before such technologies are deployed on their devices.[116] This provision has significant implications for telecom operators, particularly those offering digital services, as it restricts their ability to track user behavior online without obtaining explicit permission. While certain exceptions apply, such as cookies that are strictly necessary for the functioning of a website or service, the general principle reinforces the need for transparency and user control over personal data.

In addition, the ePrivacy Directive imposes obligations on providers of electronic communication services (ECS) to ensure the proper handling of communications. Since the European Electronic Communications Code (EECC) came into effect at the end of 2021, the scope of ECS has expanded beyond conventional services like mobile phones and Internet connections. It now also includes platforms such as instant messaging apps, VoIP services, web-based email, and video conferencing tools, commonly known as Over-the-Top (OTT) services.[117]

Because the ePrivacy Directive is a directive rather than a regulation, it does not automatically apply in all countries. Each EEA Member State is responsible for incorporating its provisions into national legislation, which has led to differences in how ePrivacy rules are implemented across the region. Unlike the GDPR, the directive does not specify exact fines or penalty levels, only that any sanctions should be effective, proportionate, and capable of deterring violations.[118] As a result, the

[116] Article 5(3) of the ePrivacy Directive sets out the rules governing the use of cookies and other comparable tracking technologies. European Data Protection Board. (2024). *Guidelines 2/2023 on technical scope of Art. 5(3) of ePrivacy Directive.* European Data Protection Board. Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

[117] Cox A., (2024). *Changes for 'Over The Top' communications services following their inclusion within the European Electronic Communications Code.* Arthur Cox LLP. Changes for 'Over The Top' communications services following their inclusion within the European Electronic Communications Code

[118] Art. 5 - *Application of certain provisions of Directive 95/46/EC* - Directive 2002/58/EC (ePrivacy Directive). Official Journal of the European Union, L 201, 37-47. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

amount of maximum fines varies from one EEA Member State to another. However, there are ongoing discussions on turning the ePrivacy directive into a regulation to enforce its applicability.[119]

Another directive that significantly impacts the telecommunication sector was adopted in December 2018, when the European Union approved a new set of rules known as the European Electronic Communications Code (EECC). This comprehensive framework applies to all electronic communication services within the EU and aims to meet Europe's growing connectivity needs.[120] By updating and merging existing telecommunications regulations, the EECC seeks to enhance connectivity while ensuring better protection for users across the continent. Regarding data protection, the Code safeguards consumers regardless of whether they use traditional communication methods, such as calls and SMS, or online services, ensuring, among other things, enhanced protection against cyber threats.[121] Before being amended by the adoption of the NIS2 Directive, the European Electronic Communications Code primarily focused on improving connectivity, enhancing competition, and protecting consumers within the telecommunications sector. It set out rules to harmonize regulations across EU member states, aiming to create a more integrated digital single market and encourage investment in next-generation networks.[122]

Another essential piece of legislation in the EU's regulatory framework for cybersecurity and data protection is the EU Cybersecurity Act. Originally adopted in 2019, the EU Cybersecurity Act was the subject of a targeted amendment proposed by the European Commission on April 18, 2023,

[119] European Commission. (2017). *Commission staff working document: Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*. SWD(2017) 5 final. Official Journal of the European Union. Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

[120] *EU Electronic Communications Code*. (2024). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/eu-electronic-communications-code?

[121] Ibidem.

[122] Ibidem.

aimed at facilitating the future adoption of European certification schemes for managed security services. These schemes will address critical areas such as incident response, penetration testing, security audits, and consultancy, ensuring high levels of quality and reliability in these essential services that help organizations prevent, detect, respond to, and recover from cyber incidents.[123]

The amendment also enhances the responsibilities of the EU Agency for Cybersecurity (ENISA), positioning it as a key player in developing and maintaining the European cybersecurity certification framework. ENISA is tasked with laying the technical groundwork for specific certification programs, supporting consistent and reliable cybersecurity standards across the EU.[124]

Under the EU Cyber Resilience Act, telecommunications companies will be required to take a more active role in safeguarding their customers, both residential and business, from cyber threats. This expands their traditional role in providing connectivity to include proactive, carrier-grade cybersecurity as a core part of their service offering, reinforcing the EU's broader strategy to enhance digital resilience across sectors.[125]

As technologies continue to evolve, the EU's legal framework for data protection and cybersecurity must remain agile to address new challenges. A notable example of this is the 5G cybersecurity initiative. In January 2020, following an EU-wide risk assessment of 5G networks, the NIS

[123] The EU Cybersecurity Act establishes a unified certification framework for ICT products, services, and processes across the EU. This allows companies operating within the EU to obtain certification for their ICT offerings just once, with the resulting certificate being accepted throughout all Member States. *The EU Cybersecurity Act*. (2025, January 15). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[124] ENISA will be responsible for publicizing the certification schemes and the certificates issued via a dedicated platform. The agency is also tasked with enhancing operational collaboration across the EU, assisting Member States upon request in managing cybersecurity incidents, and supporting the EU's coordination in responding to large-scale, cross-border cyberattacks and crises. *The EU Cybersecurity Act*. (2025, January 15). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[125] Recital 3 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification, and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), emphasizes the need for actions to improve cybersecurity across the Union, ensuring that network and information systems, communications networks, digital products, services, and devices used by citizens, organizations, and businesses - ranging from SMEs to operators of critical infrastructure - are better protected from cyber threats. https://eur-lex.europa.eu/eli/reg/2019/881/oj

Cooperation Group, supported by the European Commission and ENISA, developed the 5G Toolbox.[126] This set of guidelines offers strategic, technical, and supporting measures to mitigate cybersecurity risks related to 5G networks. ENISA, building on its expertise in telecom security, is actively working to support the implementation of these measures, helping ensure that the EU's cybersecurity standards evolve in line with the rapid advancements in digital technologies.[127]

The regulations, directives, and acts discussed in this section highlight the European Union's steadfast commitment to data protection and its continuous efforts to strengthen cybersecurity across member states.

On one hand, cyber-resilient infrastructure is essential to ensuring data protection, a fundamental right recognized by the EU. However, the need to strengthen cybersecurity strategy extends beyond protecting personal data; it is also vital for safeguarding national security in an increasingly interconnected world where cyberattacks are emerging as significant tools of modern warfare. In this context, cybersecurity frameworks are becoming increasingly important in discussions of global governance and the quest for global dominance in the cybersecurity arena.

The EU has established a leading role in data protection, notably with the General Data Protection Regulation (GDPR), which applies not only within the EU but also to entities outside its borders that process EU citizens' data. This regulation applies not only to businesses within the EU but also to any company, regardless of its location, that processes the data of EU citizens. The reach of the GDPR has significantly influenced global regulatory approaches, underscoring the EU's global influence in shaping the future of data protection and cybersecurity standards worldwide.

[126] *Report on the EU 5G Toolbox Implementation by Member States published.* (2020) *ENISA*. https://www.enisa.europa.eu/news/enisa-news/member-states-report-on-eu-5g-toolbox-released-today
[127] *Telecom sector and Digital Infrastructure* (2024). *ENISA*. Telecom sector and Digital Infrastructure

Moreover, robust cybersecurity measures are becoming increasingly essential for remaining competitive in today's business environment. As businesses face mounting cyber threats, especially in the telecommunications sector, strong security practices not only prevent fines but also build trust and enhance brand reputation. In industries that handle vast amounts of sensitive data and are frequent targets of cyberattacks, such as telecommunications, cybersecurity is critical for ensuring both corporate success and national security.

1.5.2 The UN's Role in Shaping Global Cyber Norms and Digital Regulation

Recognizing the profound influence of emerging technologies and artificial intelligence on global development, employment, and the Sustainable Development Goals (SDGs), the UN has developed multiple initiatives to mitigate the risks posed by malicious cyber activities while promoting responsible state behavior and protecting fundamental rights in the digital sphere. UN Secretary-General António Guterres has played a key advocacy role, calling for stronger regulation of cyberspace and AI, regular Security Council reviews, and greater global cooperation.

The UN Framework for Responsible State Behavior in Cyberspace which outlines 11 voluntary norms aimed at reducing the risk of conflict and enhancing trust in digital interactions, was formally endorsed by the United Nations General Assembly in 2015, following work by the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.[128] The 11 voluntary norms were elaborated by the 2015 GGE report and later reaffirmed in subsequent UN resolutions and reports,

[128] United Nations General Assembly. (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). https://undocs.org/A/70/174

including the 2021 OEWG final report, which emphasized their continued relevance and encouraged their implementation.[129]

In 2020, the United Nations General Assembly initiated a five-year Open-Ended Working Group (OEWG) focused on the security of information and communication technologies (ICTs). This group is scheduled to operate from 2021 through 2025, aiming to address key issues related to ICT security on a global scale.[130] This group was created to advance the development of international norms, rules, and principles guiding responsible state behavior in cyberspace. It also aims to create an inclusive platform for regular institutional dialogue among UN Member States on matters related to ICT security. The OEWG's mandate includes analyzing existing and emerging cyber threats, particularly in areas such as information and data security, in order to foster shared understandings. It also seeks to explore avenues for international cooperation to prevent cyber incidents, and to evaluate how international law applies to state use of ICTs. Confidence- and capacity-building are core elements of the OEWG's work, aimed at reinforcing global cybersecurity collaboration.

In 2024, the UN General Assembly adopted the Convention on Cybercrime, the first global treaty focused on prosecuting cyber offenses such as financial fraud, online child exploitation, and money laundering, while also addressing the capacity gaps in developing nations, though it has faced scrutiny over potential misuse by authoritarian regimes.[131] The United Nations Institute for Disarmament Research (UNIDIR) further supports global dialogue through its annual Cyber Stability Conference, fostering interdisciplinary cooperation on emerging cyber threats.

[129] United Nations General Assembly. (2021). Final substantive report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (A/75/816). https://docs.un.org/en/A/75/816

[130] UNIDIR. *Open-Ended Working Group on security of and in the use of ICTs and UNIDIR side events. Building a More Secure World.* https://unidir.org/un-open-ended-working-group-and-unidir-side-events

[131] *United Nations Convention against Cybercrime*. (2024). United Nations : Office on Drugs and Crime. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

Adopted at the UN Summit of the Future in September 2024, the Global Digital Compact (GDC) is a landmark multilateral initiative aimed at establishing shared principles for global digital governance.[132] Developed through inclusive consultations with governments, civil society, the private sector, and the technical community, the Compact sets out a vision for an open, secure, and rights-respecting digital future. Central to its framework is the commitment to uphold international law and human rights online, including privacy, freedom of expression, and protection from harmful content. The GDC prioritizes the ethical regulation of artificial intelligence and responsible data governance, calling for the creation of an International Scientific Panel on AI and exploring a Global Fund on AI to ensure equitable access and capacity-building, especially in developing countries. It sets ambitious goals to bridge the digital divide, ensuring universal internet connectivity and promoting digital public goods, with a focus on women, youth, and small enterprises. The Compact also institutionalizes a multistakeholder model, emphasizing collaboration between states, industry, academia, and civil society to address digital challenges collectively. To combat internet fragmentation and online disinformation, it promotes access to factual information and a globally stable internet infrastructure. Positioned within the broader Pact for the Future, the GDC aligns with the Sustainable Development Goals, offering a comprehensive framework to shape a fairer, more inclusive digital era.

Complementing the UN's normative efforts, the International Telecommunication Union (ITU) has played a pivotal and evolving role in advancing global cybersecurity. As the United Nations' specialized agency for ICTs, the ITU initially focused on foundational aspects of global telecommunications, such as radio spectrum allocation and the development of international standards for telephony and broadband. However, with the rapid digital transformation and the

[132] United Nations. (2024). Global Digital Compact. Global Digital Compact.

emergence of complex cyber threats, the ITU's mandate has significantly expanded to encompass cybersecurity as a critical priority.

Since the early 2000s, the ITU has been instrumental in fostering international cooperation and capacity-building to strengthen the cybersecurity posture of its Member States, particularly focusing on developing countries that face resource and expertise constraints. One of the ITU's flagship initiatives is the Global Cybersecurity Agenda (GCA), launched in 2007, which established a comprehensive framework to coordinate international efforts in legal, technical, organizational, capacity-building, and international cooperation domains.[133] This agenda laid the groundwork for subsequent cybersecurity activities by promoting a multi-stakeholder approach that involves governments, private sector, academia, and civil society.

Building on the GCA, the ITU introduced the Global Cybersecurity Index (GCI) in 2014, a benchmarking tool that assesses national cybersecurity commitments across five key pillars: legal measures, technical capabilities, organizational structures, capacity development, and international partnerships.[134] The GCI provides a transparent mechanism for tracking progress, identifying gaps, and fostering peer learning among countries. The annual reports not only highlight leaders in cybersecurity maturity but also spotlight vulnerabilities and areas where support is most urgently needed. The 2024 edition revealed that while 46 countries have reached Tier 1 status, many nations, especially in the Global South, still face significant challenges in securing their digital environments.[135]

[133] International Telecommunication Union. Global Cybersecurity Agenda (GCA). GCA

[134] International Telecommunication Union. Global Cybersecurity Index (GCI). GCI

[135] International Telecommunication Union. (2024). Global Cybersecurity Index 2024 (GCI 2024). https://www.coit.es/sites/default/files/uit_global_cybersecurity_index_2024.pdf

Beyond benchmarking, the ITU actively delivers tailored capacity-building programs through its Cybersecurity Centres of Excellence, which offer training, technical assistance, and policy guidance to Member States. These centers help countries develop national cybersecurity strategies, establish Computer Security Incident Response Teams (CSIRTs), and build legal and regulatory frameworks aligned with international best practices. The ITU also facilitates global forums such as the Global Forum on Cyber Expertise (GFCE), which promotes knowledge exchange and coordinates efforts to combat cybercrime, cyber terrorism, and other malicious activities.

Moreover, the ITU works closely with other international organizations, including INTERPOL, the World Bank, and the United Nations Office on Drugs and Crime (UNODC), to harmonize global cybersecurity initiatives and support the implementation of international cyber norms. Through its Telecommunication Development Sector (ITU-D), the agency advocates for cybersecurity integration into broader digital development goals, emphasizing the protection of critical infrastructure, the promotion of secure digital identities, and the fostering of trust in emerging technologies such as 5G and the Internet of Things (IoT).

Despite these efforts, major challenges persist: the borderless nature of the internet complicates jurisdiction, many developing countries lack adequate resources and infrastructure, and existing frameworks are largely voluntary and non-binding, limiting enforcement.

1.6 The Case for Cybersecurity Management in the Telecommunications Industry

As analysed in the first paragraph of this chapter, the modern digital era has transformed how businesses, governments, and individuals generate, process, and utilize data. Amid this transformation, certain industries are inherently more vulnerable to cyber threats due to the nature of the services they provide and the sensitive information they manage. As mentioned in this chapter, the telecommunications sector stands out as one of the most critical and frequently targeted industries in the digital ecosystem. This is due not only to its essential role in national and international communications infrastructure but also to the vast and highly sensitive data it handles on a daily basis. Telecommunications companies are custodians of personal user information, call records, financial transactions, and network configurations, all of which represent highly valuable targets for cybercriminals engaged in identity theft, financial fraud, corporate espionage, and even state-sponsored cyber operations.[136]

The value of data within the telco sector stems from its centrality to economic activity, innovation, and strategic advantage.[137] Telecommunications providers leverage data analytics to understand consumer behavior, optimize services, and develop competitive strategies.[138] Beyond business purposes, data plays a crucial role in other sectors. In finance, it underpins secure transactions and fraud detection[139], while in healthcare, it facilitates personalized medical treatments, research breakthroughs, and efficient patient management[140]. Governments, too, rely on telecom data for national security, public administration, and the delivery of critical public services.[141] Consequently, the protection of such data is not merely a regulatory requirement but a strategic necessity. The

[136] Kumar, M. J. (2023) Privacy-Preserving Technologies in Telecom Data Analytics: Implementing Privacy-Preserving Techniques Like Differential Privacy to Protect Sensitive Customer Data During Telecom Data Analytics . Available at SSRN: https://ssrn.com/abstract=5136773 or http://dx.doi.org/10.2139/ssrn.5136773

[137] Viktor Mayer-Schönberger predicts that "data capitalism" will eventually replace finance capitalism as the global economy's organizing principle. Rosenbach, E., & Mansted, K.,(2019). *The Geopolitics of Information.* Belfer Center for Science and International Affairs, Harvard Kennedy School.

[138] McGuire, T. (2017, December 4). *Why Big Data is the new competitive advantage - Ivey Business Journal*. Ivey Business Journal. Why Big Data is the new competitive advantage

[139] Udeh, N. E. O., et al. (2024). *The role of big data in detecting and preventing financial fraud in digital transactions.* World Journal of Advanced Research and Reviews, 22(2), 1746–1760. https://doi.org/10.30574/wjarr.2024.22.2.1575

[140] Batko K, & Ślęzak A., (2022). *The use of Big Data Analytics in healthcare.* J Big Data. doi: 10.1186/s40537-021-00553-4. PMID: 35013701; PMCID: PMC8733917.

[141] Government reliance on data significantly increased following COVID-19. For further insights see Karkera, A., et al., (2022, April 1). *Data-fueled government*. Deloitte Insights. Data-fueled government Breaking down silos with turbo-charged data

repercussions of data breaches extend far beyond individual companies, affecting interconnected sectors, service delivery, and broader societal trust in digital infrastructure.

Cybercriminals recognize the immense value of this data and exploit it for financial gain, corporate advantage, or political leverage. Personal information can be sold on the dark web, used to commit identity theft, or manipulated to facilitate financial fraud. Sensitive corporate or governmental data may be leveraged for espionage, blackmail, or geopolitical influence.[142] As telecommunications companies handle such high-value information, the stakes of inadequate cybersecurity are enormous, underscoring the need for a proactive, comprehensive approach to risk management. In this context, the telco sector exemplifies the industries most vulnerable to sophisticated cyberattacks, making it an appropriate focus for an in-depth analysis of cybersecurity requirements.

The financial and operational consequences of cyberattacks in telecommunications are profound.[143] Direct costs associated with data breaches and system intrusions include forensic investigations, IT remediation, infrastructure repairs, and emergency security upgrades.[144] These measures often necessitate hiring specialized cybersecurity personnel, implementing real-time monitoring systems, and replacing compromised hardware and software. Operational disruptions, such as network outages or service interruptions, exacerbate financial losses, particularly for providers that rely on subscription models or service-level agreements. The theft or compromise of sensitive data can trigger further costs, including regulatory fines, legal liabilities, and customer compensation initiatives like credit monitoring programs.[145] In the EU, where stringent regulations govern the

[142] Rosenbach, E., Mansted, K., (2019). *The Geopolitics of Information*. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/geopolitics-information

[143] Wang, P., e al. (2019). *Economic costs and impacts of business data breaches.* Issues in Information Systems, 20(2), 162-171.

[144] Ibidem.

[145] Noah, A., et al. (2024, December 4). *The consequences of non-compliance with data protection regulations on business analytics.* ResearchGate.

protection of citizens' data, violations can result in multi-million-dollar penalties, compounding the financial impact.[146] Finally, the aftermath of an attack often necessitates major investments in security enhancements and compliance measures. Strengthening cybersecurity infrastructure, updating protocols, and implementing more advanced monitoring systems require continuous financial commitment, adding to the long-term cost of a breach.[147] These direct financial repercussions highlight the urgent need for telecom companies to adopt proactive cybersecurity strategies to mitigate risks and ensure business continuity.

Indirect costs of cyberattacks are equally significant.[148] Breaches can erode trust in a telecommunications company's services, damage brand reputation, and result in customer attrition.[149] The loss of confidence may extend to investors and partners, increasing the company's cost of capital and insurance premiums. Additionally, disruptions in the telco supply chain can affect downstream businesses, amplifying the economic ripple effects of a single security

[146] In October 2015, the UK-based telecommunications company TalkTalk suffered a significant cyberattack. Hackers exploited a vulnerability on the company's website to access sensitive user information. Approximately 157,000 customers had their personal and financial data compromised, including names, addresses, dates of birth, and bank account details. The overall financial impact of the breach, including both direct and indirect costs, was estimated at £77 million. Subsequently, on 5 October 2016, the Information Commissioner's Office imposed a £400,000 fine on TalkTalk for failing to adequately protect customer data. Smith, J. (2016). *The TalkTalk Data Breach: Lessons Learned*. Journal of Cybersecurity, 3(2), 87-102. See previous paragraphs on regulatory fines imposed on companies processing EU citizens' data.

[147] Post-breach costs include detection, investigation, forensic analysis, documentation, network restructuring, access adjustments, protocol modifications, remedial training, and control enhancements. Friedman, A., et al. (2020). *Cost of A Cyber Incident: Systematic Review And Cross-Validation*. Cybersecurity and Infrastructure Security Agency (CISA) | Defend Today, Secure Tomorrow.

[148] Wang, P., et al. (2019). *Economic costs and impacts of business data breaches.* Issues in Information Systems, 20(2), 162-171.

[149] The reputational damage suffered by telecommunications companies after a cyberattack can be severe. A single breach can lead to a loss of customer trust, causing clients to migrate to competitors with a more robust security posture. Negative media coverage and public perception can lead to long-term brand erosion, further weakening the company's position in an increasingly competitive market. Moreover, the reputational fallout from a cyberattack can extend to business partnerships. Other organizations, especially those that rely on secure communication channels, may hesitate to form or continue partnerships with a company that has proven vulnerable to cyber threats. The damage to a company's credibility can take years to repair and may have lasting effects on its ability to attract new customers or maintain existing contracts. Wang, P., et al. (2019). *Economic costs and impacts of business data breaches*. Issues in Information Systems, 20(2), 162-171.

incident.[150] Although these costs are often less tangible than direct financial losses, their long-term implications for competitiveness and market position are substantial, highlighting that cybersecurity is not merely a technical concern but a strategic business issue.

The increasing digitalization of telecommunications infrastructure, particularly with the rollout of technologies such as 5G, the Internet of Things (IoT), and artificial intelligence (AI), has amplified both opportunities and vulnerabilities.[151] These technologies enable advanced services, higher network efficiency, and innovative applications but simultaneously expand the attack surface available to cybercriminals. AI-driven cyberattacks, automated intrusion methods, and vulnerabilities in connected devices illustrate the sophisticated threats that telecommunications providers must anticipate. Without robust cybersecurity defenses, companies risk severe operational, financial, and reputational consequences. Protecting customer data, ensuring network integrity, and maintaining uninterrupted service are essential to sustaining competitiveness and trust in a highly connected digital society.

Moreover, the telco sector occupies a strategic position in national infrastructure. Telecommunications networks underpin not only private communications but also emergency services, public administration, and critical industrial operations. Any disruption or compromise in this sector can cascade through other economic and social systems, amplifying the consequences of security lapses. As a result, ensuring the cybersecurity resilience of telecommunications companies is not only a corporate priority but also a matter of national and regional security.

[150] A notable example is the 2013 Target data breach, which originated from a third-party HVAC vendor. Attackers gained access to Target Corporation - a major American retail chain - through the vendor's compromised credentials, ultimately exposing the credit and debit card information of over 70 million customers. Steinberg, S., Adam, Neary, K., & Picker Center Digital Education Group. (2021). *Target cyber attack: A Columbia University case study.* In G. Rattray & J. Healey (Eds.), *SIPA* [Case study].

[151] The deployment of 5G networks represents a major advancement in telecommunications, providing faster speeds, lower latency, and improved connectivity. At the same time, the intricate and widespread structure of 5G networks brings significant cybersecurity risks. See Bellamkonda, S. (2021). *Strengthening cybersecurity in 5G networks: Threats, challenges, and strategic solutions.* Journal of Computational Analysis and Applications, *29*(6), 1159-1173.

Regulatory compliance further underscores the need for stringent cybersecurity in telecommunications. EU legislation, including directives such as NIS2 and frameworks like the Cyber Resilience Act, imposes rigorous requirements for data protection, incident reporting, and system security. Compliance is essential not only to avoid financial penalties but also to maintain operational integrity and public trust. By adopting proactive cybersecurity strategies, telecommunications companies can meet regulatory obligations while also reinforcing resilience against evolving threats, safeguarding both their business operations and the broader digital ecosystem.

In summary, the telecommunications sector occupies a pivotal position in the digital economy, given its management of highly sensitive data, its central role in ensuring connectivity, and its exposure to increasingly sophisticated cyber threats. As emerging technologies enhance capabilities while simultaneously introducing new vulnerabilities, and as regulatory and geopolitical pressures intensify, telecom companies must treat comprehensive cybersecurity management as a top strategic priority. Protecting data and securing networks is therefore essential not only for maintaining trust and competitive advantage but also for ensuring long-term operational resilience in an interconnected and increasingly vulnerable digital landscape.

The next chapter will explore the telecom sector in greater depth, analyzing its role as national critical infrastructure and its cyber threat landscape, thereby laying the groundwork for a discussion on cyber risk management frameworks, techniques and best practices aimed at strengthening the cybersecurity resilience of telecommunications industries.

CHAPTER 2.

TELECOMMUNICATIONS AND CYBER RISK MANAGEMENT

2.1 The telecommunication Industry as Critical National Infrastructure

The telecommunications sector has evolved significantly since its inception in the 1830s with the invention of the electrical telegraph, the first mechanical communications device.[152] The telegraph revolutionized communication by reducing the time required to transmit messages from days to mere hours. However, its functionality was heavily dependent on a vast infrastructure and a network of highly skilled operators who relayed messages using Morse code. This early innovation laid the foundation for a rapidly evolving industry that would transform the way information is exchanged.

The development of the telephone in 1876 marked a significant milestone by enabling the direct transmission of the human voice, thereby diminishing reliance on Morse code operators.[153] Over the following decades, the introduction of radio and television further broadened the telecommunications landscape, allowing for wireless transmission of information and reducing the need for physical networks. The emergence of cellular and satellite communication in the late 20th century continued this trajectory, minimizing reliance on fixed telephone infrastructure and enabling global connectivity. Finally, the advent of computers and the internet ushered in an era of instantaneous data transmission, fundamentally altering the industry's focus from voice communication to digital data exchange.

[152] McGillem, & D, C. (2025, August 23). *Telegraph | Invention, History, & Facts*. Encyclopedia Britannica. https://www.britannica.com/technology/telegraph

[153] Ibidem.

As the industry evolved, so too did its structure. Initially dominated by a small number of large, state-owned entities that controlled infrastructure and service provision, the sector has gradually become more decentralized. Deregulation, privatization, and technological advancements have lowered barriers to entry, allowing for increased competition and innovation.[154] Today, major public corporations provide core services, while smaller specialized companies manufacture and maintain critical infrastructure components, such as routers, switches, and network equipment.

Although telephone services historically represented the primary revenue source for the industry, technological progress has shifted the focus towards data-driven communication.[155] The demand for high-speed internet, multimedia services, and cloud-based applications has reshaped telecommunications.[156] The sector's fastest-growing segment now lies in mobile and wireless communication services, which provide seamless connectivity and facilitate the proliferation of data-intensive applications worldwide.

The telecommunications sector can be broadly categorized into three sub-sectors: telecommunications equipment, telecommunications services, and wireless communication.[157] Telecommunications equipment, the largest of the three, includes the development and manufacturing of hardware essential for network functionality. Telecommunications services

[154] Fransman, M. (2001). *Evolution of the telecommunications industry into the internet age.* Communications and Strategies, vol. 43, pp. 57-113.

[155] Traditionally, the telecom sector generated most of its revenue from voice calls and SMS. However, the emergence of Over-the-Top (OTT) services is shifting the industry toward a model focused on data-driven services. This study examines the shift from the voice and SMS era to a business model centered on data. Dahal, M. S. (2023). *Transforming Telecom Revenue- The impact of OTT Service.* Research Square. https://doi.org/10.21203/rs.3.rs-3084516/v1

[156] Digital Subscriber Line (DSL) is a modem technology being widely deployed in North America and parts of Europe. By leveraging existing telephone lines, and considering there are over 750 million lines worldwide, copper wiring seems to offer the most practical infrastructure for expanding global access to infocommunication services. Savino, S. (2002). *Digital subscriber line: leading technology revolutionizing access to the information highway.* Proceedings of the 2000 IEEE Engineering Management Society. EMS - 2000 (Cat. No.00CH37139), 453–457. https://doi.org/10.1109/ems.2000.872545

[157] Sadiku, M. N. O., et al. (2024). *Telecommunications industry: An overview.* International Journal of Trend in Scientific Research and Development (IJTSRD), 8(6), 503-510.

encompass a wide range of offerings, including long-distance and domestic telecom services, foreign telecom operations, and diversified communication solutions. Wireless communication, the most rapidly expanding segment, is at the forefront of the industry's future, driving the shift towards mobile devices, cloud computing, and next-generation network technologies.[158] The continued evolution of telecommunications remains critical in shaping global connectivity, economic development, and digital transformation.

As mentioned in the previous chapter, telecommunications constitute a fundamental pillar of modern society, enabling the seamless transmission of data and information across diverse sectors on a global scale. These networks connect governments, businesses, emergency services, utilities, and individuals, ensuring the continuous functioning of essential services and infrastructure.[159] Due to their indispensable role, telecommunications are classified as part of national critical infrastructure and are integral to national security and cybersecurity.[160] Any disruption in communication networks can have profound consequences, impairing a country's ability to respond to security threats, conduct military operations, and maintain public order.

The significance of telecommunications is particularly evident in times of crisis or emergency, where they serve as the backbone for disaster response, security operations, and the dissemination of vital public information.[161] Additionally, these networks play a crucial role in sustaining financial

[158] Ibidem.

[159] The COVID-19 pandemic highlighted the essential role of technology and telecommunications in keeping societies connected and functional. Confronted with severe social and economic disruptions, people worldwide increasingly relied on the internet, cloud services, and virtual communication. In this context, telecoms became a cornerstone for enabling remote work, information access, and social interaction during the global crisis. Khan, M.K. (2022) *Technology and telecommunications: a panacea in the COVID-19 crisis.* Telecommun Syst 79, 1–2. https://doi.org/10.1007/s11235-022-00880-8

[160] Cardenes, W. (2025, August 28). *National Critical Infrastructure*. Enea. National Critical Infrastructure

[161] Carreras-Coch, A., et al. (2022). *Communication technologies in emergency situations.* Electronics, *11*(7), 1155. https://doi.org/10.3390/electronics11071155

systems by facilitating transactions and enabling secure data exchange.[162] In the healthcare sector, telecommunications support telemedicine, health data sharing, and coordination among medical professionals, thereby enhancing healthcare accessibility and efficiency.[163] Furthermore, they drive economic growth by underpinning global trade, e-commerce, and the digital exchange of information. Given their far-reaching impact, any disruption in telecommunications infrastructure can severely affect business operations, supply chains, and economic stability.

Due to their strategic importance, telecommunications companies have become prime targets for cyberattacks, facing an array of sophisticated threats that jeopardize network security and the continuity of critical services.[164] Among the most prevalent threats are malware attacks, in which cybercriminals deploy malicious software designed to infiltrate systems, steal sensitive data, or cause damage to digital infrastructure. Phishing scams represent another significant risk, involving fraudulent communications that appear to originate from legitimate sources to deceive individuals into disclosing confidential information, such as login credentials or financial details, or inadvertently installing malicious software. Additionally, denial-of-service (DoS) attacks pose a critical challenge, as they seek to overwhelm network resources with excessive traffic, thereby disrupting operations and rendering services unavailable.

Telecommunications companies manage vast amounts of sensitive data, including network configurations, customer information, and billing records, making them attractive targets for

[162] The rapid growth of digital financial services offers the telecom industry a crucial opportunity to expand into new markets and diversify its revenue sources. *Telecoms and banks connect to create mobile financial services*. IBM. Telecoms and banks connect to create mobile financial services.

[163] Haleem A, et al. (2021). *Telemedicine for healthcare: Capabilities, features, barriers, and applications.* Sens Int. 2021;2:100117. doi: 10.1016/j.sintl.2021.100117. PMID: 34806053; PMCID: PMC8590973.

[164] Manukonda, K. R. R. (2019). *Cyber attack on telecommunications company*. European Journal of Advances in Engineering and Technology, *6*(12), 113-120.

cybercriminals engaged in espionage or financial fraud.[165] As digital threats evolve in complexity, safeguarding telecommunications networks against data breaches, tampering, and unauthorized access presents an increasingly formidable challenge.[166] Strengthening cybersecurity frameworks within the telecommunications sector is therefore imperative to mitigate risks, protect critical infrastructure, and ensure the resilience of global communication networks in the face of emerging cyber threats.

2.2 Telecommunications' Cyberthreat Landscape

As discussed in the previous chapter, advancements in information technology have also driven the evolution of cybersecurity threats, resulting in increasingly sophisticated attack methods. The surge in high-profile data breaches has heightened businesses' concerns about cybersecurity, as the financial and reputational impacts are becoming more severe.

Today, cybersecurity has become a vital component of enterprise risk management, as the rising number of cyber breaches continues to impose significant and multifaceted costs on both organizations and individuals.[167]

Cyberattacks on telecommunications companies in Europe have escalated significantly in recent years, driven by geopolitical tensions, rapid digitalization, and the increasing sophistication of

[165] Kumar, M. J. (2023). *Privacy-Preserving Technologies in Telecom Data Analytics: Implementing Privacy-Preserving Techniques Like Differential Privacy to Protect Sensitive Customer Data During Telecom Data Analytics* . Available at SSRN: https://ssrn.com/abstract=5136773 or http://dx.doi.org/10.2139/ssrn.5136773

[166] Sadiku, M. N. O., et al. (2024). *Telecommunications industry: An overview.* International Journal of Trend in Scientific Research and Development (IJTSRD), 8(6), 503-510.

[167] For a better understanding of cyberattacks costs refer to Chapter 1 of the present work and to Wang, P., e al. (2019). *Economic costs and impacts of business data breaches.* Issues in Information Systems, 20(2), 162-171.

cybercriminals, with several high-profile breaches exposing the sector's systemic vulnerabilities.[168] Between July 2023 and June 2024, the telecommunications sector in Europe faced a sharp rise in cyber threats. A study by Cloudflare revealed that 40% of European organizations experienced a cybersecurity incident within a year, with 84% of these reporting an increase in the frequency of attacks.[169] Alarmingly, 16% of organizations suffered an attack every 6 to 11 days. The most common attack methods included phishing (59%), web attacks (58%), and DDoS attacks (37%). Ransomware was particularly prevalent, accounting for 26% of all attacks in Europe during this period, followed by server access attacks (12%) and data theft (10%).[170]

The European Union Agency for Cybersecurity (ENISA) has warned that the frequency and sophistication of cyberattacks against telecom providers are escalating, emphasizing the need for enhanced resilience measures.[171]

The urgency of implementing robust cybersecurity strategies is widely recognized across the industry. According to the *State of Public Cloud Security Report*, 95% of telecommunications companies identify cybersecurity as a top concern, driven by the rapid pace of digital transformation and the increasing reliance on cloud-based infrastructure.[172] Without adequate safeguards, cyberattacks have the potential to disrupt essential communication services, compromise sensitive consumer data, and undermine public confidence in telecommunications providers.

[168] European Commission. (2024). *Cybersecurity and resiliency of Europe's communications infrastructures and networks: Follow-up to the Nevers Call of 9 March 2022.* NIS Cooperation Group. Cybersecurity and resiliency of Europe's communications infrastructures and networks

[169] *European businesses anticipate more cybersecurity attacks, but feel unprepared for them. Cloudflare*. European Businesses Anticipate More Cybersecurity Attacks, But Feel Unprepared for Them

[170] Ibidem

[171] Lule, M.-L., (2024) *Telecom Security Incidents 2022. Annual Report.* European Union Agency for Cybersecurity.

[172] Devry, J. (2024). *The state of cloud security - cybersecurity insiders*. Cybersecurity Insiders. The State of Cloud Security

For instance, Vodafone Portugal suffered a sophisticated cyberattack in 2022 that disrupted mobile services, television, and emergency communications, demonstrating the widespread consequences of telecom security breaches.[173] In Germany, major telecom operators have also reported an increase in phishing, distributed denial-of-service (DDoS) attacks, and data exfiltration attempts targeting critical network infrastructure.[174] Italy has witnessed a sharp increase in cyberattacks in recent years, with the telecommunications sector being one of the primary targets. In August 2024, Telecom Italia Mobile S.p.A. (TIM), the country's largest telecommunications provider, suffered a significant ransomware attack orchestrated by the Stormous group. The attackers claimed to have exfiltrated 100GB of sensitive data, highlighting the persistent threat facing critical national infrastructure.[175]

In the UK alone, BT Group reported detecting over 2,000 potential cyberattacks per second in 2024, translating to more than 200 million threats daily.[176] Many of these attempts targeted vulnerabilities in connected devices and critical infrastructure. The company also observed a staggering 1,234% increase in new malicious IP scanners over the year, highlighting the growing automation and scale of these threats.[177] This surge aligns with findings from Nokia's Threat Intelligence Report, which

[173] *Cyberattack on Vodafone Portugal*. Vodafone Portugal. Cyberattack on Vodafone Portugal

[174] Reuters. *Cybercrime and sabotage cost German firms $300 bln in past year.* (2024). Reuters. Cybercrime and sabotage cost German firms $300 bln in past year

[175] Ellis, A., (2024). *Cyber chaos: Pro-Russian hackers hit Italian airports.* Euro Weekly News. Cyber chaos: Pro-Russian hackers hit Italian airports

[176] Aruna, A. (2024, December 13). BT's Eye-Opening Data on Daily Cyber Threats and Emerging Risks. *Telecom Review Europe*. BT's Eye-Opening Data on Daily Cyber Threats and Emerging Risks

[177] Desmarais, A. (2024, September 16). UK telecoms provider records 2,000 possible cyber-attacks every second. *Euronews*. UK telecoms provider records 2,000 possible cyber-attacks every second

noted that DDoS attacks on telecom networks increased from one or two per day to over 100 per day across many European networks between mid-2023 and mid-2024.[178]

These attacks are not only growing in frequency but also in their financial and operational impacts.[179] The financial costs of these attacks are substantial. While specific figures for the telco sector are not always disclosed, the broader economic impact of cybercrime in Europe is estimated to reach billions annually. For instance, ransomware attacks often demand payments ranging from hundreds of thousands to millions of euros, while the costs of mitigating DDoS attacks or recovering from data breaches can be equally high. Additionally, as mentioned in the previous chapter, regulatory fines for failing to protect customer data further exacerbate financial losses.

Geopolitical factors have also played a significant role in increasing cyber threats. The European Union Agency for Cybersecurity (ENISA) reported that cyberattacks linked to Russian-based groups doubled between late 2023 and early 2024.[180] These attacks are part of broader digital warfare strategies tied to conflicts like the ongoing war in Ukraine. Such state-sponsored campaigns often target telecom infrastructure for espionage or disruption.[181]

Despite these challenges, many European telcos remain underprepared for such threats. Only 29% of organizations surveyed by Cloudflare felt highly prepared to defend against cyberattacks.[182] This

[178] *Nokia Threat Intelligence Report finds cybercriminal attacks on telco infrastructure are accelerating, driven by Generative AI and automation*. (2024). Nokia.com. Nokia Threat Intelligence Report finds cybercriminal attacks on telco infrastructure are accelerating, driven by Generative AI and automation.

[179] Imber, D. (2025, April 9). The Latest Cyber Crime Statistics (updated April 2025) | AAG IT Support. *AAG IT Services*. https://aag-it.com/the-latest-cyber-crime-statistics/

[180] Euronews. (2024, May 29). Disruptive attacks double in EU in recent months, cybersecurity chief says. *Euronews*. https://www.euronews.com/next/2024/05/29/disruptive-attacks-double-in-eu-in-recent-months-cybersecurity-chief-says

[181] Desmarais, A. (2024, September 16). UK telecoms provider records 2,000 possible cyber-attacks every second. *Euronews*. UK telecoms provider records 2,000 possible cyber-attacks every second

[182] *European businesses anticipate more cybersecurity attacks, but feel unprepared for them. Cloudflare*. European Businesses Anticipate More Cybersecurity Attacks, But Feel Unprepared for Them

lack of preparedness is concerning given that two-thirds of respondents anticipated even more frequent attacks in the coming year.[183]

The rising frequency and sophistication of cyberattacks on European telcos underscore the urgent need for enhanced cybersecurity measures. Companies must invest in robust defenses, including AI-driven threat detection systems, comprehensive incident response plans, and employee training programs to mitigate risks effectively. Without such proactive steps, the financial and operational consequences will continue to escalate across Europe's telecommunications landscape.

According to a recent report by Moody's, companies in the Telecommunications, Media, and Technology (TMT) sector have significantly increased their cybersecurity budgets, with spending rising by 125% between 2019 and 2023.[184] This surge underscores the growing importance of robust cybersecurity measures in response to the ever-evolving landscape of digital threats.[185]

In addition to boosting budgets, TMT companies report higher levels of cybersecurity expertise at the board level compared to the global median, with many organizations appointing dedicated cyber managers and ensuring more frequent reporting on cybersecurity issues to both CEOs and boards.[186]

Reflecting the sector's increased focus on security, the telecom cybersecurity solutions market is projected to grow from $38.15 billion in 2024 to $44.85 billion in 2025, marking a substantial

[183] Ibidem

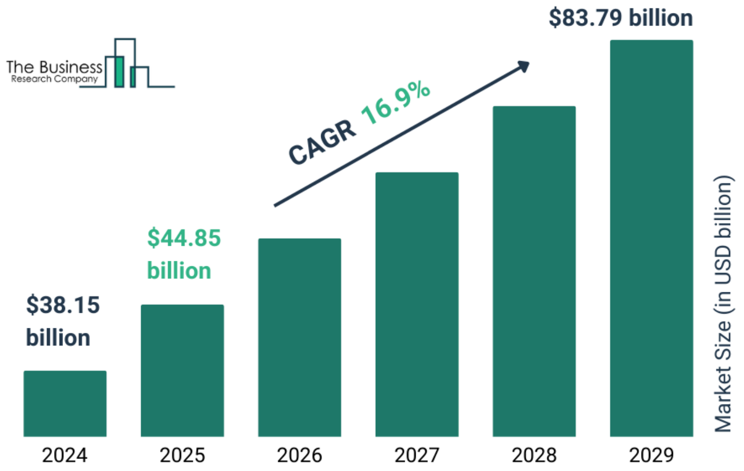
[184] Adams, H. S. (2024, June 15). *Cybersecurity budgets rise for telecommunications & tech.* Mobile Magazine. Cybersecurity budgets rise for telecommunications & tech.

[185] Ibidem.

[186] Adams, H. S. (2024, June 15). *Cybersecurity budgets rise for telecommunications & tech.* Mobile Magazine. Cybersecurity budgets rise for telecommunications & tech.

year-over-year increase and further highlighting the critical role of cybersecurity in safeguarding telecommunications infrastructure.[187]

Figure 2.1 Telecom Cyber Security Solution Global Market Report 2025 [188]



2.3. Cyber-risk Analysis and Cyber-risk Management

Given the growing importance of implementing robust cybersecurity strategies to prevent data breaches and their wide-ranging consequences, telecommunications companies must establish effective mechanisms for cyber risk analysis and management. This process is essential to safeguard critical infrastructure, protect sensitive data, and maintain business continuity in an increasingly hostile cyber environment.

Cyber risk analysis involves identifying, evaluating, and understanding potential sources of cyber threats that could impact the company.[189] This includes assessing vulnerabilities in digital systems,

[187] Grand View Research. I*T and Telecom Cyber Security Market Size, share & Trends Analysis Report by component (Hardware, software, services), by deployment (On-premise, Cloud), by enterprise size, by region, and segment Forecasts, 2025 - 2030.* Market Analysis Report

[188] The Business Research Company. (2025). *Telecom Cyber Security Solution Global Market Report 2025.* The Business Research Company. Telecom Cyber Security Solution Global Market Report 2025

[189] Finio, M., Downie, A. (2024). *What is a cybersecurity risk assessment?* IBM. https://www.ibm.com/think/topics/cybersecurity-risk-assessment

determining the likelihood of different types of cyberattacks, and estimating the potential impact on the company's operations, finances, and reputation. By thoroughly analyzing these risks, telco companies can gain a clearer picture of their threat landscape and prioritize their cybersecurity efforts accordingly.

Cyber risk management, on the other hand, focuses on implementing strategies and controls to mitigate the identified risks.[190] This involves selecting appropriate cybersecurity frameworks, best practices, and technologies to reduce vulnerabilities, strengthen defenses, and minimize the likelihood and impact of cyberattacks.

To better explore these concepts, in the following sections the most important cybersecurity frameworks and data protection techniques will be analysed. Firstly, the two leading cybersecurity frameworks will be introduced, namely the National Institute of Standards and Technology, known as NIST, and the International Organization for Standardization, known as ISO, focusing on how they guide cyber risk assessment and management. Then, the key data protection techniques that telco companies can implement to mitigate cyber risks and enhance their overall cybersecurity posture will be examined.

2.3.1 NIST & ISO Cybersecurity Frameworks

The National Institute of Standards and Technology (NIST), a non-regulatory agency within the U.S. Department of Commerce, issued the NIST Cybersecurity Framework (CSF) following Executive Order 13636, which aimed to strengthen national and economic security by advancing the safeguarding of critical infrastructure against cyber threats.[191] On February 12, 2014, NIST released

[190] Forescout Technologies, Inc. (2025, February 10). *What is Cybersecurity Risk Management?* Forescout.

[191] National Institute of Standards and Technology. (2024b). The NIST Cybersecurity Framework (CSF) 2.0. In *NIST CSWP 29*[Report]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

the "Framework for Improving Critical Infrastructure Cybersecurity", developed through a collaborative public-private partnership.[192] This framework leverages industry standards and best practices to provide voluntary, risk-based measures that help organizations identify, assess, and mitigate cyber risks. Though designed for critical infrastructure protection, the CSF is technology-neutral and flexible enough to be applied by organizations of any size, sector, or risk level. It serves as both a guideline for building or improving cybersecurity programs and a valuable tool for executives to understand their organization's security posture, identify vulnerabilities, and prioritize opportunities for improvement.[193]

The evolution of this framework led to the release of NIST CSF 2.0, which introduced several significant updates to enhance its relevance and effectiveness.[194] Notable changes include the introduction of a new "Govern" function, an expanded focus on supply chain risk management, improved usability, and broader applicability beyond critical infrastructure to guide both government agencies and private sector organizations in managing cybersecurity risks.

At the core of the NIST Cybersecurity Framework is a taxonomy of high-level cybersecurity outcomes designed to help organizations understand, assess, and communicate their cybersecurity efforts. The CSF consists of three primary components: the CSF Core, CSF Organizational Profiles, and CSF Tiers.[195]

The CSF Core, which forms the foundation of the framework, is structured around a hierarchy of Functions, Categories, and Subcategories.

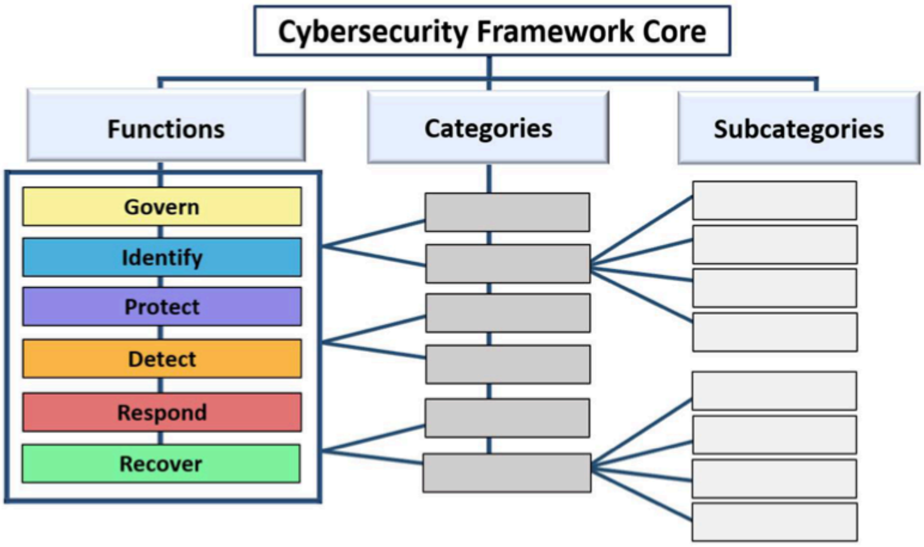
[192] National Institute of Standards and Technology. (2018, April 16). *Framework for improving critical infrastructure cybersecurity* (Version 1.1).

[193] Ibidem

[194] Ibidem

[195] Ibidem

Figure 2.3 CSF Core structure [196]



This structure helps organizations manage cybersecurity risks across diverse environments and technologies, including IT, the Internet of Things (IoT), and operational technology (OT). It revolves around five fundamental functions: Identify, Protect, Detect, Respond, and Recover. These functions represent critical cybersecurity practices that organizations should implement to build a robust and adaptable security program. The newly introduced "Govern" function focuses on establishing a risk management strategy, aligning cybersecurity policies with the organization's broader mission, and understanding the organizational context. The "Identify" function emphasizes recognizing cybersecurity risks and prioritizing efforts accordingly. The "Protect" function involves implementing safeguards to prevent cyber incidents, including identity management, data security, and platform resilience. The "Detect" function focuses on identifying potential cyberattacks and compromises, enabling timely incident response. "Respond" and "Recover" cover actions taken during and after an incident, including mitigation, communication, and restoration of affected assets.

[196] Ibidem

Each Function is divided into Categories that describe related cybersecurity outcomes, which are further detailed in Subcategories. These outcomes are intended to be sector-neutral and technology-agnostic, offering flexibility for organizations to adapt them based on their unique risks, technologies, and strategic priorities. The framework's forward-looking nature ensures its applicability to evolving technologies, including artificial intelligence (AI) and cloud environments.

CSF Organizational Profiles are another critical component of the framework, designed to help organizations describe and manage their cybersecurity posture. These profiles can reflect an organization's current cybersecurity outcomes ("Current Profile") or its desired outcomes based on strategic objectives and anticipated changes ("Target Profile"). By comparing these profiles, organizations can identify gaps, set priorities, and develop action plans to improve cybersecurity over time. Profiles are particularly useful for aligning cybersecurity efforts with mission objectives, stakeholder expectations, and changes in the threat landscape.

CSF Tiers provide a mechanism for organizations to assess the maturity and rigor of their cybersecurity risk management practices. These Tiers help contextualize an organization's approach to risk, including the processes and governance mechanisms in place. Organizations can use Tiers to inform both their current and target profiles and to evaluate how cybersecurity fits into broader risk management strategies.

While the NIST CSF is not prescriptive, it offers supplemental online resources that provide detailed guidance on achieving the framework's desired outcomes.[197] These resources help

[197] Ibidem

organizations understand and adopt the framework while offering practical advice on controls, best practices, and implementation.

The framework's flexibility allows it to be applied in various ways, including internal management of cybersecurity capabilities and external oversight or communication with third parties. By integrating cybersecurity with other enterprise risks - such as financial, reputational, and privacy risks - organizations can make informed decisions about cybersecurity investments and strategies.

Cybersecurity risk management is essential for safeguarding the confidentiality, integrity, and availability of sensitive information, especially when dealing with advanced technologies like artificial intelligence. AI introduces new cybersecurity and privacy risks, which are addressed through the NIST AI Risk Management Framework (AI RMF).[198] This framework complements the CSF by applying similar principles - Functions, Categories, and Subcategories - to manage AI-related risks. By treating AI risks as part of an integrated enterprise risk management approach, organizations can enhance efficiency and resilience across their operations.

The NIST Cybersecurity Framework (CSF) provides a flexible, risk-based approach to managing cybersecurity that can be applied across diverse industries. However, organizations seeking to implement a more structured and detailed information security management system may benefit from aligning with the ISO/IEC 27000 series, which is widely regarded as a global benchmark for information security best practices.[199] While the NIST CSF focuses on key cybersecurity outcomes to enhance resilience and guide risk management, the ISO/IEC 27000 series offers a more

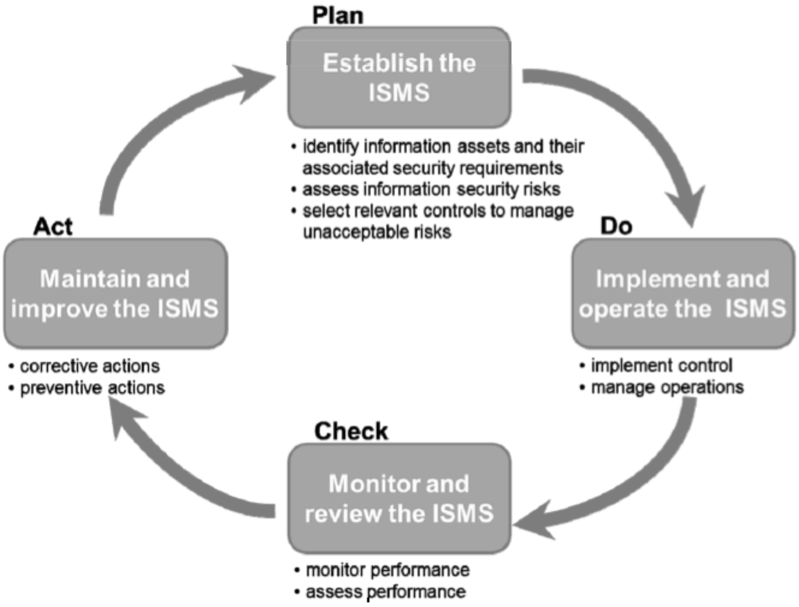
[198] U.S. Department of Commerce, Raimondo, G. M., et al. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. In *NIST Trustworthy and Responsible AI*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

[199] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

comprehensive, systems-based approach, particularly through the ISO/IEC 27001 standard, which provides detailed guidance on implementing and maintaining an Information Security Management System (ISMS).[200]

The ISO/IEC 27001 standard, which is part of the broader ISO/IEC 27000 series, specifies the requirements for creating, implementing, maintaining, and continuously enhancing an Information Security Management System (ISMS). This framework is particularly applicable to all industries, including telecommunications companies, which manage vast amounts of sensitive customer data, critical communications infrastructure, and operational technology. In today's fast-changing digital environment, continuous improvement and optimization of cybersecurity measures are essential to address dynamic and adaptive cyber threats. To achieve this, ISO/IEC 27001 employs the Plan-Do-Check-Act (PDCA) cycle as a key principle, promoting iterative improvements in information security management and risk control.

Figure 2.4 PDCA cycle in ISO 27000 [201]


Plan
Establish the ISMS
• identify information assets and their associated security requirements
• assess information security risks
• select relevant controls to manage unacceptable risks
Do
Implement and operate the ISMS
• implement control
• manage operations
Check
Monitor and review the ISMS
• monitor performance
• assess performance
Act
Maintain and improve the ISMS
• corrective actions
• preventive actions

[200] Ibidem

[201] Ibidem

The PDCA cycle forms the backbone of the ISMS by enabling a continuous process of planning, implementing, monitoring, and refining security measures. This cyclical approach ensures that an organization's information security posture evolves to meet new challenges, just as the NIST CSF encourages ongoing improvements in cyber risk management. The four PDCA steps align as follows:[202]

1. Plan: This step involves the planning and design of an ISMS, including defining the scope, establishing security policies, and identifying potential security risks and organizational vulnerabilities. It may include initial risk assessments based on ISO/IEC 27005, which provides detailed guidelines for information security risk management. This planning stage mirrors the "Identify" and "Govern" functions in the NIST CSF, which emphasize assessing cyber risks, determining organizational priorities, and aligning security efforts with broader business objectives.

2. Do: The implementation phase focuses on putting the planned ISMS measures into practice, including security controls, training programs, and operational safeguards to protect critical information assets. This phase aligns closely with the "Protect" function of the NIST CSF, which aims to develop safeguards that limit or contain the impact of a cybersecurity event.

3. Check: Once the ISMS is operational, organizations must regularly monitor, measure, and review the effectiveness of their security policies and controls. This is essential for identifying gaps, evaluating performance, and ensuring compliance with established security objectives. In terms of the NIST CSF, this step corresponds to the "Detect" function, which

[202] Ibidem

emphasizes timely identification of anomalies, potential breaches, and system vulnerabilities.

4. Act: Based on the findings from the monitoring phase, organizations initiate corrective actions to address identified deficiencies, strengthen their ISMS, and enhance overall cybersecurity resilience. This phase reinforces the NIST CSF's "Respond" and "Recover" functions, which focus on mitigating the impact of cyber incidents and restoring normal operations while learning from past events to improve future resilience.

A critical element of effective ISMS implementation under the ISO/IEC 27000 series is the identification and management of cyber risks. ISO/IEC 27001 emphasizes the importance of understanding an organization's business model and core assets to identify potential threats, vulnerabilities, and consequences of cyber incidents. These assets may include information (e.g., sensitive customer data), software, hardware (e.g., routers, servers), IT infrastructure (e.g., data centers), and intangible assets such as intellectual property or organizational reputation.[203]

To assess risk comprehensively, firms can utilize ISO/IEC 27005, which provides detailed methodologies for identifying cyber threats, evaluating vulnerabilities, and determining the potential impact on critical assets.[204] This risk identification process must consider both internal and external factors, including the organization's dependence on digital systems, existing risk controls, and exposure to evolving cyber threats.

[203] Disterer, G. (2013). *ISO/IEC 27000, 27001 and 27002 for information security management.* Journal of Information Security, 04(02), 92–100. https://doi.org/10.4236/jis.2013.42011

[204] Agrawal, V.. (2016). *Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard.* HAISA.

For example, e-commerce companies, which rely heavily on digital platforms and customer data, may have a higher cyber risk exposure than firms with less digital dependence. Consequently, organizations with significant cyber risk exposure must behave proactively by continuously identifying, assessing, controlling, and monitoring vulnerabilities. This proactive approach is necessary to manage emerging risks effectively and minimize the potential for financial, operational, or reputational losses.

ISO/IEC 27001 recommends adopting either a top-down or bottom-up approach to risk assessment. The top-down approach focuses on strategic risks and may be faster to implement but may overlook specific vulnerabilities or risk correlations.[205] The bottom-up approach, in contrast, is more comprehensive, capturing detailed information about enterprise processes, systems, and potential cyber risks. Given the complexity and interconnectivity of modern cyber environments, the bottom-up approach is often advisable for a thorough evaluation of risk exposure.

Once risks have been identified, organizations can classify them based on categories such as actions of people (e.g., insider threats), failed internal processes (e.g., system misconfigurations), technical failures (e.g., hardware malfunctions), or external events (e.g., natural disasters or cyberattacks). Alternatively, risk classifications can be based on broader categories, including natural risks, technical risks, and human-related risks.[206]

Ultimately, the ISO/IEC 27000 series' emphasis on continuous improvement through the PDCA cycle provides a robust framework for managing cyber risks and enhancing information security. By

[205] Disterer, G. (2013). *ISO/IEC 27000, 27001 and 27002 for information security management.* Journal of Information Security, 04(02), 92–100. https://doi.org/10.4236/jis.2013.42011

[206] Posthumus, S., Von Solms, R. (2004). *A framework for the governance of information security.* Computers & Security, *23*(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.006

integrating ISO/IEC 27001's ISMS principles with the NIST CSF's outcome-driven approach, organizations can build resilient, adaptive cybersecurity programs that address both immediate threats and long-term strategic challenges. This integrated approach is particularly relevant for telcos, which must balance cybersecurity resilience with service continuity, data protection, and compliance in a highly dynamic digital ecosystem.

2.3.2 Main data protection techniques

Beyond cyber risk frameworks that can help identifying industry specific and systemic risks of a company, its vulnerabilities and loopholes and make it subject to cyber attacks, and after having seen steps and practices available for companies to manage cyber risk, telco have at their disposal a series of cybersecurity techniques that can be implemented to protect their networks, their computers and therefore the amount of sensitive data.

In this paragraph the main data protection techniques will be presented. There are techniques that can be implemented to block the access to the data, namely that build a sort of cushion surrounding the data itself to lower the risk of data theft. These are typically referred to under the umbrella of "preventive security controls" or "access control mechanisms" as they focus on stopping unauthorized access in the first place. Otherwise there are other techniques that are specifically applied to data to make it difficult to steal them or that make them unusable once stolen. These are techniques applied to the data directly, to make it difficult to steal, understand, or use even if accessed. These fall under "data-centric security" or "data protection mechanisms". Preventive security controls and data-centric security techniques can be also used together to implement different layers of protections.

a) Preventive Security Controls

One of the most important, yet classical, security techniques for protecting both information and physical assets is access control. This technique is fundamental in safeguarding resources by regulating who can access specific data, information processing services, or restricted physical locations. Access control refers to the process of granting or denying specific requests to obtain and use information or to enter protected environments. By ensuring that only authorized individuals are permitted to perform certain actions within a system or facility, access control plays a crucial role in minimizing security risks and preventing unauthorized access.[207]

Access control consists of two main components: authentication and authorization.[208] Authentication verifies an individual's identity before granting access, typically through credentials such as passwords, biometric scans (fingerprint or facial recognition), smart cards, or multi-factor authentication, which combines multiple verification methods for enhanced security. Authorization, on the other hand, determines what actions an authenticated user is allowed to perform, ensuring they can only access resources necessary for their role or privileges.

Access control encompasses several models, each offering varying degrees of security and adaptability. Discretionary Access Control (DAC) grants resource owners the authority to set access permissions. Mandatory Access Control (MAC) imposes strict, policy-driven access rules based on security labels, commonly used in military and governmental contexts. Role-Based Access Control (RBAC) assigns access rights according to an individual's job role within an organization, ensuring access aligns with their responsibilities. Attribute-Based Access Control (ABAC) builds upon

[207] *Personal identity verification (PIV) of federal employees and contractors*. (2022). https://doi.org/10.6028/nist.fips.201-3

[208] Shoemaker, P. (2025). *Authentication vs. Authorization: Key Roles in Access Control*. Identity. https://www.identity.com/the-role-of-authentication-and-authorization-in-access-control/

RBAC by considering additional factors such as user location, time of access, and device type before allowing entry. [209]

Access control is widely implemented in both physical and digital security. In physical security, it restricts entry to buildings, data centers, and secure rooms through keycards, biometric scanners, or PIN codes. In information security, it controls access to databases, cloud services, and sensitive company files, protecting against unauthorized data breaches and cyber threats.

With the increasing complexity of cybersecurity threats, modern access control systems integrate artificial intelligence and machine learning to detect anomalies, enforce adaptive security policies, and provide real-time threat assessments. Ensuring robust access control mechanisms is essential for maintaining data confidentiality, integrity, and availability in any secure system.

Another technique is the firewall, a critical network security device that serves as a protective barrier, separating a trusted internal network from untrusted external networks such as the internet.[210] It monitors and controls incoming and outgoing network traffic based on predefined security rules, determining whether to allow or block specific data packets. Firewalls have served as a fundamental defense mechanism in cybersecurity, protecting systems from unauthorized access, malware, and other cyber threats.

Firewalls can be implemented in various forms, including hardware, software, and cloud-based solutions.[211] A hardware firewall is a physical device that filters traffic between a network and external sources, commonly used in enterprise settings for large-scale protection. A software

[209] Fathauer, M. (2025). *Mandatory & Discretionary access control: Which to choose?. Ping Identity.* https://www.pingidentity.com/en/resources/blog/post/access-control.html

[210] *Cisco Secure Firewall: first line of defense*. (2025, February 3). Cisco. What is a Firewall?

[211] Ibidem.

firewall, on the other hand, is an application installed on individual devices to monitor and control network traffic at the host level. Cloud-based firewalls, available as Software-as-a-Service (SaaS) solutions, provide scalable and flexible security, often used in hybrid or multi-cloud environments. Additionally, virtual firewalls are deployed in public and private cloud infrastructures to secure cloud-based applications and workloads.

There are various types of firewalls, each offering different levels of security. Packet-filtering firewalls offer basic security by analyzing individual data packets and making decisions based on criteria like IP addresses, ports, and protocols. Stateful inspection firewalls enhance security by tracking active network connections and assessing the context before allowing or denying traffic. Proxy firewalls act as intermediaries at the application layer, inspecting the content of communications to detect threats. Next-generation firewalls (NGFWs) combine traditional firewall capabilities with advanced features such as deep packet inspection, intrusion prevention, and sophisticated threat detection to offer a more comprehensive defense.[212]

Firewalls are essential in preventing unauthorized access, mitigating cyber threats, and ensuring secure communication across networks. They are widely used in businesses, government agencies, and personal computing to enforce security policies and protect sensitive data from cyberattacks. With the rise of sophisticated threats, modern firewalls integrate artificial intelligence, machine learning, and behavioral analytics to enhance threat detection and response, making them an indispensable component of modern cybersecurity frameworks.

[212] Teach Me Networking & by Teach Me Networking. (2024, November 3). Understanding the 5 different types of firewalls: A comprehensive guide. *teachmenetworking.tech*. Understanding the 5 Different Types of Firewalls: A Comprehensive Guide

With the rise of increasingly sophisticated cyber threats, preventive controls have evolved beyond traditional access control models and firewalls. One of the most significant modern advancements in this area is the Zero Trust Architecture (ZTA), which extends and redefines classical approaches to access management. ZTA is a cybersecurity framework built on the principle that no user, device, or application, whether inside or outside an organization's network, should be trusted by default.[213] Instead, it enforces strict identity verification, continuous authentication, and least-privilege access for every access request. Unlike traditional perimeter-based security, Zero Trust reduces the risk of breaches by segmenting networks, validating device compliance, and granting access based on real-time contextual factors such as user identity, device health, and location. This approach not only prevents unauthorized access but also limits the lateral movement of threats, making it particularly effective in securing today's hybrid environments characterized by cloud services, mobile devices, and IoT. As the traditional notion of a secure network perimeter becomes obsolete, ZTA is increasingly recognized as a cornerstone of preventive cybersecurity strategies.

b) Data-centric Security Techniques

Encryption is one of the oldest and most fundamental methods of data protection, transforming plaintext into ciphertext to ensure that only authorized recipients can access the original information.[214] This process is a key component of cryptography, which involves designing secure systems for data transmission and storage. However, encryption is not infallible - this is where cryptanalysis comes in. Cryptanalysis is the practice of breaking encrypted messages without knowing the key or algorithm used, often by finding weaknesses in cryptographic methods.

[213] *What is Zero Trust Architecture (ZTA)? Benefits and best practices | Fortinet*. Fortinet. ZTA

[214] Pandya, D., et al. (2015). Brief history of encryption. In *International Journal of Computer Applications* (Vol. 131, Issue No.9, pp. 28–29). Brief History of Encryption

Together, cryptography (the art of securing data) and cryptanalysis (the art of breaking encryption) form the broader field of cryptology, which encompasses the study of both creating and breaking secure communication systems.[215]

The term "encryption" originates from the Greek word *kryptos*, meaning "hidden." Since ancient times, humans have sought ways to safeguard sensitive information from unintended recipients. The need for secure communication dates back thousands of years, leading to the development of cryptographic techniques. Early methods included substituting parts of a message with symbols, numbers, or images. Different civilizations used cryptography for various purposes—Assyrians to protect pottery manufacturing secrets, the Chinese to safeguard silk production methods, and the Germans for military confidentiality.[216]

With the advent of the internet and digital communication, the need for information security has grown significantly. Online activities such as email, messaging, e-commerce, and banking require robust encryption to prevent unauthorized access. As computers and the internet advanced, businesses, industries, and organizations increasingly relied on encryption to protect sensitive data from cyber threats and intrusions.[217]

Modern cryptography relies on computers and mathematical functions to secure data effectively. Over time, various encryption techniques have been developed, which can be broadly categorized into symmetric and asymmetric encryption.[218]

[215] Ibidem

[216] Ibidem

[217] Ibidem

[218] Ibidem

As already said, encryption is a cryptographic process designed to prevent unauthorized access to plaintext by transforming it into an unreadable format. Only those with the appropriate decryption key can revert the ciphertext back to its original form. In symmetric encryption, the same key is used for both encryption and decryption.[219] This means that both the sender and the recipient must share and securely store the key, making key distribution a potential security challenge.

In contrast, asymmetric encryption, also known as public key cryptography, operates with a pair of keys: a public key and a private key. The public key, which can be shared openly, is used to encrypt data, while the private key, kept confidential, is used to decrypt it.[220] The security of this system relies on the fact that, even if someone has access to the public key, they cannot derive the private key from it. This approach is widely used in secure communications, as it enables encrypted messaging, secret key exchange over insecure networks, and digital signature authentication. Asymmetric cryptography plays a crucial role in many cryptographic applications, including internet security protocols, secure email communication, and blockchain technology.

Over time, encryption methods have evolved, with Homomorphic Encryption (HE) emerging as a breakthrough technique in cryptography. HE enables computations to be carried out directly on encrypted data without needing to decrypt it first. The output of these computations remains encrypted, and once decrypted, the result matches what would have been obtained if the operations were performed on unencrypted data. This capability is particularly valuable for scenarios where a third party, such as a cloud provider, is entrusted with data processing but should not have access to

[219] Badman, A., Kosinski, M. *What is asymmetric encryption?* IBM Think.

[220] Badman, A., Kosinski, M. *What is asymmetric encryption?* IBM Think.

the underlying sensitive information. Even if such a provider's system is compromised, the data remains protected. [221]

For many years, homomorphic encryption faced two main challenges: restricted computational capabilities and high computational resource demands, leading to slower processing and larger energy consumption. The first challenge was addressed with the development of Fully Homomorphic Encryption (FHE), which supports arbitrary computations on encrypted data. Meanwhile, advancements in software optimization have helped reduce the performance overhead, making homomorphic encryption increasingly feasible for practical use.[222]

Quantum computers, a new generation of computing technology, are anticipated to have the capability to compromise many of today's widely used encryption techniques, putting secure communications at risk.[223] Because of their potential to break current cryptographic systems, researchers are actively developing post-quantum cryptography, new methods designed to protect data from such quantum-enabled attacks. This means future data security will require fundamentally different approaches.[224]

[221] Métayer, D. L., et al. (2015). Privacy and Data Protection by Design - from policy to engineering. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1501.03726

[222] Fully homomorphic encryption (FHE) is a cryptographic breakthrough that enables computations on encrypted data without decrypting it first, preserving privacy while allowing data utility. Unlike traditional encryption methods, which require decryption for processing, FHE ensures sensitive information remains protected even during complex operations like machine learning inferences or statistical analyses. *A High-Level Technical Overview of fully homomorphic encryption*. (2024). Math ∩ Programming. A High-Level Technical Overview of Fully Homomorphic Encryption.

[223] IndustryTrends, & IndustryTrends. (2025, March 10). *Quantum Cryptography: A new era of Encryption*. Analytics Insight. https://www.analyticsinsight.net/white-papers/quantum-cryptography-a-new-era-of-encryption?

[224] Sabani, M., et al. (2022). *Quantum Key Distribution: Basic Protocols and Threats.* In 26th Pan-Hellenic Conference on Informatics (PCI 2022), November 25–27, 2022, Athens, Greece. ACM, New York, NY, USA 6 Pages. https://doi.org/10.1145/3575879.3576022

One promising approach is Quantum Key Distribution (QKD), which has gained traction recently as quantum technology becomes more practical.[225] Globally, isolated point-to-point QKD links are being connected into larger networks as they move toward commercial viability. QKD transmits quantum bits (qubits) using the quantum states of single photons, enabling two communicating parties to establish a shared symmetric key securely.[226] This method leverages principles from quantum mechanics, such as the no-cloning theorem, which prevents exact copying of photons, and the uncertainty principle, which causes disturbances when photons are measured, to detect potential eavesdropping. When paired with a trusted authentication channel, these laws give legitimate users an advantage over attackers.

By processing the measured qubits through post-processing techniques, the users can create a matching bit sequence known only to them, which serves as a secure encryption key for symmetric cryptography. Unlike classical encryption that depends on the complexity of mathematical problems, QKD's security is grounded in physical quantum laws, making it resilient against both classical and quantum computational attacks, and thus considered future-proof.

A mention should also be made of recent advancements in applying artificial intelligence to cybersecurity defense. While the rise of AI-powered attacks has been analyzed in the previous chapter, AI-driven defensive techniques are equally transforming how organizations detect, respond to, and mitigate threats.[227] By leveraging machine learning and advanced analytics, these platforms provide real-time visibility, automated detection, and rapid response capabilities that significantly outperform traditional manual methods. AI can identify subtle patterns and anomalies across vast

[225] Peel, M. (2025, April 23). *Secure 'quantum messages' sent over telecoms network in breakthrough*. Financial Times. https://www.ft.com/content/51a65e45-302c-45fa-8bd1-c828a66b012d?

[226] Ibidem

[227] Lewis, C., Kristensen, I., Caso, J., & Fuchs, J. (2025). *AI is the greatest threat—and defense—in cybersecurity today. Here's why*. McKinsey & Company. AI is the greatest threat—and defense—in cybersecurity today. Here's why.

and complex networks, enabling early detection of malicious activity and the automation of containment and remediation processes to minimize impact. Cutting-edge tools now support behavioral analysis, predictive risk modeling, and adaptive defenses, fostering a powerful synergy between human expertise and technological innovation. This convergence is becoming indispensable to building resilient cybersecurity systems in 2025 and beyond.

2.4 The importance of Human Factor in Cyber Risk Management

While telecommunication companies have access to mature cybersecurity frameworks, such as ISO/IEC 27001 and the NIST Cybersecurity Framework, and a range of advanced data protection techniques, the reality is that cyberattacks continue to occur with alarming frequency. Despite the availability of sophisticated tools, defensive architectures, and regulatory incentives, many telecom operators remain underprepared, suggesting that technical solutions alone are insufficient.[228] This highlights that, despite the most advanced techniques and frameworks, something essential remains overlooked. A review of the literature on cyber risk management reveals a critical insight: cybersecurity is not merely a technical issue but, at its core, a human and organizational challenge. Even when high-quality preventive measures are deployed, human error can render these defenses ineffective, compromising the integrity, availability, and confidentiality of sensitive information.

Human error is widely recognized as one of the greatest vulnerabilities in any cybersecurity program. Research consistently demonstrates that up to 90–95% of breaches involve some form of human factor, whether through negligence, misconfiguration, social engineering, or a lack of

[228] Only 29% of organizations surveyed by Cloudflare felt highly prepared to defend against cyberattacks. Pandya, D., et al. (2015). Brief history of encryption. In *International Journal of Computer Applications* (Vol. 131, Issue No.9, pp. 28–29). Brief History of Encryption

awareness.[229] Employees may inadvertently use weak passwords, click on phishing emails, mishandle confidential data, or fail to follow established security protocols. These mistakes are rarely isolated incidents; instead, they reflect systemic gaps in organizational culture, training, accountability, and communication.[230] In the telecommunications sector, where sensitive customer information, financial transactions, and network configuration data are processed and stored, such errors can have cascading consequences, affecting not only the organization but also customers, business partners, and national infrastructure.

Analysing the literature on how to improve employee awareness leadership emerged as a critical factor to promote organizational culture, make employees aware of risk, set the strategy and training programs. Leadership is therefore the linchpin in mitigating human risk.[231] Leaders shape organizational culture, establish accountability, and define the strategic priorities that govern cybersecurity practices. Beyond drafting policies, effective leaders foster an environment of vigilance, ensuring that employees are trained to recognize threats, understand the consequences of breaches, and adopt secure behaviors.[232] They also facilitate open communication channels, encouraging staff to report suspicious activity without fear of reprisal. By embedding cybersecurity into organizational culture, leaders can transform employees from potential vulnerabilities into proactive participants in risk management.[233]

[229] Aksoy, C. (2025b). Building Effective Cybersecurity Leadership: The Crucial Role Of Leaders In Protecting Businesses Against Cyber Threats. *Kalite Ve Strateji Yönetimi Dergisi*, *5*(1), 33–49. https://doi.org/10.56682/ksydergi.1539408

[230] Triplett, W. J. (2022). *Addressing human factors in cybersecurity leadership*. Journal of Cybersecurity and Privacy, 2(3), 573–586.

[231] Ibidem.

[232] Puhakainen, P., Siponen, M. (2010). *Improving employees' compliance through information systems security training: An action research study.* MIS Quarterly, 34(4), 757-778; Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983-988.

[233] National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*(Version 1.1). U.S. Department of Commerce.

Even when organizations adopt advanced technological tools, such as AI-driven cybersecurity agents, the effectiveness of these solutions is contingent on informed oversight.[234] AI agents can monitor networks, detect anomalies, and respond to incidents with a speed and scale that far exceeds human capabilities. However, they rely heavily on the quality of the data on which they are trained and the parameters established by human operators.[235] Without leaders who fully understand the organization's risk landscape, these AI systems may be poorly configured or fail to recognize emerging threats. As a result, the most advanced technological solutions cannot compensate for a lack of awareness, leadership engagement, or strategic risk management.

An illustrative concepts, the "Watermelon Effect", highlights the challenges posed by inadequate risk awareness. The Watermelon Effect refers to situations where risks appear benign on the surface (green) but are, in reality, critical beneath the exterior (red).[236] In telecommunications, this can occur when superficial security metrics suggest that systems are secure, while hidden vulnerabilities remain unaddressed. If risks are not recognized or monitored early, they may only become apparent at critical stages, leaving insufficient time for effective mitigation. This concept underscores that technical controls alone are insufficient; without informed leadership and a deep understanding of potential threats, organizations are unlikely to identify, assess, and respond to vulnerabilities in a timely manner. Leadership therefore plays a vital role in reducing the frequency and impact of human error.

Therefore, cybersecurity in the telecommunications sector is not simply a matter of deploying firewalls, encryption, or zero-trust architectures. While these technologies are indispensable, they

[234] *The Ultimate Guide to AI Agents in Cybersecurity 2025.* (2025). Cyble. AI Agents

[235] Ibidem.

[236] Zeijlemaker, S., Pal, R., & Siegel, M. (2025). *Perusing Watermelon Risks to Strengthen Cyber Resilience: Combatting the illusion of control that fosters unintended lapses of control.* Massachusetts Institute of Technology, CAMS

must be supported by a workforce that is both trained and aware, and by leadership capable of translating awareness into strategic action.[237] Protecting telecom networks, customer data, and national critical infrastructure requires a holistic approach in which human factors are integrated into risk management, policy enforcement, and technology adoption. Only through a combination of informed leadership, continuous education, and a culture that prioritizes cybersecurity can telecommunication companies effectively reduce human error, close vulnerabilities, and achieve operational resilience against increasingly sophisticated cyber threats.

Given the central role of leadership in defining strategy and fostering a culture of vigilance, the necessity of individuating the best leadership able to reduce human error is crucial. The next chapter will focus on leadership theories, examining the literature to identify the characteristics most effective in managing cyber threats. A leader's ability to assess vulnerabilities, communicate risks, and guide employees is indispensable to building true cyber resilience within telecommunications organizations.

[237] Nobles, C. (2018). *Botching human factors in cybersecurity in business organizations.* Holistica–Journal of Business and Public Administration, 9(3), 71-88.

CHAPTER 3.

OVERVIEW OF LEADERSHIP THEORIES AND MODELS

3.1 What is Leadership?

The idea of leadership has fascinated people for centuries, going as far back as the time of Greek philosophers like Plato and Socrates. Even though we widely acknowledge its importance, there's still no clear-cut definition of what leadership truly is. One of the reasons for this is that leadership tends to mean different things to different people. Everyone brings their own perspective shaped by personal experiences, cultural background, and education, making it hard to pin down a universal definition.[238]

Another factor that complicates things is that our understanding of leadership often depends on the theoretical lens used. For instance, leadership has been described as the act of guiding and influencing a group of individuals toward accomplishing a common objective.[239] While this definition is widely accepted and straightforward, it still places the focus squarely on the individual leader.

On the other hand, a broader and more collective perspective suggests that leadership is a social process involving intentional influence, exerted at times by an individual, and at other times by a group, with the aim of shaping actions and relationships within an organization or team.[240] However, even this version leaves room for questions: What does this "influence" really look like in

[238] Bolden, R., (2004) *What is Leadership?*, Leadership South West Research Report 1, University of Exeter.

[239] Northouse, P.G., (2004), *Leadership: Theory and Practice*, 3rd ed., London, Sage Publications Ltd.

[240] Yukl, G.A., (2002), *Leadership in Organizations*, 5th ed., Upper Saddle River, NJ, Prentice-Hall.

practice? How exactly does it shape group dynamics? And who, in a group setting, is considered the true leader?

Ultimately, leadership is a multi-layered concept that intersects with many other areas, including organizational behavior, social interaction, and individual motivation. At its core, leadership is about influencing others to move toward shared goals, not through force or authority, but by inspiring and engaging them.

In the following paragraph, some of the most influential theories of leadership will be explored, including trait theory, behavioral theory, and contingency theory.

3.2 Classical Theories of Leadership

3.2.1 Theory of Traits: A Leader is Born

Throughout much of the early twentieth century, leadership was commonly viewed through the lens of identifying specific traits believed to distinguish leaders from others. This approach focused primarily on how prominent, often male, historical figures attained and retained positions of power. The prevailing assumption was that these individuals were naturally born to lead, excelling by virtue of inherent personality qualities rather than acquired skills or experiences.

At the heart of trait theory lies a straightforward idea: certain personality characteristics are unique to leaders and set them apart from followers. This perspective holds that leadership is an innate quality, something leaders are born with, not made. As one of the earliest attempts to explain leadership effectiveness, trait theory sought to pinpoint the attributes that define potential leaders. Its foundations can be traced back to mid-19th century thinkers like Thomas Carlyle[241] and Sir

[241] Carlyle, T. (1841). *On Heroes, Hero-Worship and The Heroic.* History. London: James Fraser.

Francis Galton[242]. These scholars analyzed great leaders of history, such as military commanders and political figures, to identify common traits like charisma and persuasiveness, encapsulated in the *Great Man Theory.*"[243]

As leadership studies evolved, the focus broadened beyond exceptional historical figures to include an analysis of psychological and physiological traits influencing leadership effectiveness. For example, an overview of this evolution illustrates how the study of leadership traits has moved from simplistic assumptions to more complex interpretations.[244] The origins of trait theory, in particular, can be linked to Galton's 1869 book *Hereditary Genius*, where he proposed two key ideas: first, leadership is a rare quality possessed by extraordinary individuals whose choices shape history; and second, these qualities are inherited genetically, implying that leaders are born, not made.[245] Galton's view suggested that leadership traits are fixed and immutable, unaffected by learning or development, a perspective that dominated leadership research into the twentieth century.

However, despite extensive research across military, business, and educational settings, no universally consistent set of traits has been identified that reliably predicts effective leadership. While intelligence, education, and self-confidence have been considered as possible indicators, no single trait guarantees leadership success. It has been emphasized that possessing a particular personality trait alone does not ensure effective leadership or suitability across all leadership roles.[246]

[242] Galton, F.(1869). *Hereditary Genius*, London: Macmillan.

[243] Carlyle T.. 1841. *On Heroes, Hero-Worship and The Heroic.* History. London: James Fraser.

[244] Zaccaro, M. (2017). *Trait-Based Leadership: Early Theories and Recent Advances.* Journal of Leadership Studies.

[245] Galton F., (1869). *Hereditary Genius*, London: Macmillan.

[246] Bass B.M., 2008, *The Bass Handbook of Leadership: Theory, Research, and Managerial Applications,* 4th ed., New York: Free Press.

Critical reviews[247] challenged the narrow focus on traits, paving the way for behavioral theories that emphasized what leaders do, their actions and behaviors, rather than who they are. These studies exposed the limitations of attributing leadership exclusively to personal qualities and underlined the importance of learned skills and behaviors.

Despite this shift, trait theory did not fall entirely out of favor. By the 1980s, leadership research began to reincorporate traits into broader leadership models, recognizing that personality characteristics play a meaningful but not exclusive role in effective leadership. The ongoing importance of individual traits was acknowledged, particularly when combined with situational factors that influence leadership outcomes.[248]

More recently, researchers have applied frameworks like the Big Five personality model to explore traits commonly associated with leadership. Certain traits, such as extraversion, marked by sociability, assertiveness, and comfort in social interactions—are consistently linked to effective leadership.[249] Additionally, conscientiousness, which reflects diligence and responsibility, and openness to experience, indicative of creativity and vision, are significant predictors of leadership success. Conversely, traits like agreeableness and neuroticism appear less relevant in predicting leadership effectiveness.

Another important dimension of leadership traits involves motivation, as outlined by McClelland's model[250], which identifies three key drivers among leaders:

[247] Stogdill R.M.,(1948). *Personal Factors Associated with Leadership: A Survey of the Literature.* Journal of Psychology, vol. 25, pp. 35–71. D. Mann, 1959, A Review of the Relationship Between Personality and Performance in Small Groups, Psychological Bulletin, vol. 56, no. 4, pp. 241–270.

[248] House R.J., (1988). *Leadership Research and Theory: A Functional Integration.* Psychological Bulletin, vol. 103, no. 3, pp. 41–47.

[249] Judge T.A., et al. (2002). P*ersonality and Leadership: A Qualitative and Quantitative Review.* Journal of Applied Psychology, vol. 87, no. 4, pp. 765–780.

[250] McClelland D.C., (1975). *Power: The Inner Experience*, New York: Irvington Publishers.

- Power: The desire to influence others and hold positions of authority.
- Achievement: The drive to accomplish goals and gain recognition.
- Affiliation: The need to develop strong interpersonal relationships and promote team unity.

Research suggests that successful leaders often have a dominant power motivation but balance it with self-control and responsibility, enabling them to meet leadership demands effectively.

Adding a contemporary perspective, the Principle-Centered Leadership model[251] highlights eight essential qualities that effective leaders possess:

- Continuous learning: A commitment to ongoing personal and professional growth.
- Service orientation: Ethical responsibility and a focus on serving others.
- Positive energy: Optimism and enthusiasm that inspire followers.
- Trust in followers: Patience and resilience that nurture confidence in the team.
- Balanced judgment: The ability to assess situations with nuance and avoid extremes.
- Courage: Vigilance and innovation in anticipating challenges.
- Synergy: Viewing the organization as a whole and promoting collaboration.
- Self-renewal: Maintaining physical, mental, emotional, and spiritual well-being to sustain effectiveness.

Finally, leadership attributes can be categorized into five broad groups that predict success[252]:

- Skills: Including knowledge, creativity, communication, and problem-solving abilities.
- Results: Demonstrated personal achievements above the norm.
- Drive: Traits like confidence, persistence, and competitiveness.

[251] S.R. Covey, 2009, The 8th Habit: From Effectiveness to Greatness, New York: Free Press.

[252] A. Nahavandi, 2015, *The Art and Science of Leadership*, 7th ed., Upper Saddle River, NJ: Pearson.

- Participation and involvement: Approachability, empathy, flexibility, and active engagement with followers.
- Status: Leaders often have higher social and economic standing compared to followers or less effective leaders.

3.2.2 Behavioural Theory: Leader you Become

The behavioral approach to leadership represents a pivotal change in leadership studies, shifting the focus away from inherent personality traits and toward the actual actions and behaviors of leaders. Instead of concentrating solely on who leaders are, this perspective examines what leaders do to guide, motivate, and manage their teams effectively. The fundamental goal is to identify specific, practical behaviors that can be learned and applied by anyone who assumes a leadership role, emphasizing that effective leadership is not an innate gift but a set of skills that can be developed.

This transition from trait-based explanations was driven by a growing understanding that leadership can be taught and shaped through experience and learning, rather than being a fixed attribute possessed from birth. Whereas earlier theories suggested leaders are naturally born with certain characteristics, the behavioral viewpoint regards leadership as a dynamic process grounded in observable and replicable actions. Leadership, from this standpoint, is essentially a subset of human behavior that can be studied scientifically, taught, and imitated.[253]

Central to behavioral theory is the analysis of leaders' conduct and interactions, especially how they influence group dynamics and organize efforts within an organization. Scholars have primarily focused on three domains of leader behavior: how power is distributed among group members, the management of tasks and leader responsibilities, and social behaviors within the group context. According to this view, effective leadership arises when leaders demonstrate appropriate behaviors

[253] Hunt R., Larson C., (1977). *Leadership as Behavior.* Journal of Applied Psychology.

across these areas, which in turn shapes followers' perceptions of their competence and effectiveness.

Historical research in this field offers valuable insights into what behaviors distinguish effective leaders. For instance, mid-20th century work by scholars such as Bass and Stogdill categorized leadership styles based on the degree to which leaders involve their followers in decision-making.[254] They identified three principal leadership styles:

- Autocratic leadership, where the leader centralizes authority and makes decisions independently, often disregarding input from followers. This style tends to occur when leaders lack trust in their teams and prefer to tightly control group activities. Studies generally associate autocratic leadership with lower employee satisfaction and decreased performance.
- Participative leadership, in which the leader actively seeks followers' opinions and includes them in goal-setting and decision processes. Although the leader retains final decision-making power, involving followers tends to enhance engagement and typically leads to improved outcomes.
- Laissez-faire leadership, characterized by the leader's hands-off approach, allowing followers to make most decisions and set their own objectives. While this style grants autonomy, it often results in a lack of guidance and direction, potentially causing lower performance and follower dissatisfaction.

Further foundational research, notably from Ohio State University, identified two critical dimensions of leadership behavior[255]:

[254] Bass B.M. and Stogdill, R.M. (1990). *Handbook of Leadership: Theory, Research, and Managerial Applications,* 3rd ed., New York: Free Press.

[255] Sujan. (2025, April 13). *The Ohio State Leadership Studies.* TheMBAins. The Ohio State Leadership Studies.

- Consideration, reflecting the leader's attention to followers' needs, well-being, and emotional support. Leaders high in consideration foster trusting relationships and maintain open, two-way communication.

- Initiating structure, which involves organizing tasks, clarifying roles, and setting expectations. Leaders who excel in initiating structure provide clear direction and maintain control over group processes.

Empirical evidence suggests that leaders who demonstrate high consideration typically enjoy greater follower satisfaction, while those emphasizing initiating structure often see better performance results. However, these outcomes are nuanced and heavily dependent on the situational context.

Similarly, research from the University of Michigan highlighted two predominant leadership orientations: production-oriented leadership, focused on task completion and goal achievement, and employee-oriented leadership, emphasizing relationships and follower welfare.[256] These findings complement the Ohio State dimensions, reinforcing the importance of balancing task management and interpersonal sensitivity.[257]

More recent studies have broadened the behavioral approach by integrating emerging leadership styles such as transformational and passive leadership.[258] Transformational leadership, in particular, has gained prominence in the face of contemporary challenges such as globalization, technological

[256] Kenton, W. (2022). *Michigan Leadership Studies: History and Criticism*. Investopedia. Michigan Leadership Studies

[257] Boje, D. (2000). *The Isles Leadership: The Voyage of the Behaviorists.* The Leadership Box. Northern Michigan State University

[258] Derue S.L., et al., (2011). *A Meta-Analytic Review of Leadership Behavior and Effectiveness.* Journal of Applied Psychology, vol. 96, no. 3.

innovation, and economic uncertainty[259]. This style is characterized by behaviors that inspire and motivate followers beyond routine task accomplishment. Transformational leaders articulate compelling visions, encourage creativity and risk-taking, and guide followers through change and growth processes rather than focusing solely on short-term performance targets.

Contemporary research reveals several key patterns related to leadership behaviors:

- Both task-oriented and transformational leadership behaviors tend to show stronger positive relationships with organizational performance compared to relationship-oriented or passive styles.
- Relationship-focused and transformational behaviors correlate more closely with follower satisfaction and contribute to a positive organizational climate.
- Except for passive leadership, which is generally linked to poorer outcomes, most leadership behaviors positively impact leadership effectiveness in terms of both objective results and follower perceptions.

Despite these insights, behavioral theories have faced criticism for insufficiently accounting for the impact of situational factors. The effectiveness of a particular leadership behavior may vary dramatically depending on the organizational environment, follower characteristics, or external conditions. This shortcoming has led to the development of contingency or situational leadership theories, which stress the importance of adapting leadership behaviors to fit specific contexts for optimal effectiveness.

In summary, the behavioral perspective reframes leadership as a set of actions and conduct rather than inherent traits. It highlights the importance of observable, teachable behaviors and provides a

[259] Bass B.M., (1999). *Two Decades of Research and Development in Transformational Leadership.* European Journal of Work and Organizational Psychology.

framework for categorizing leadership styles based on these actions. Most importantly, it underscores that leadership effectiveness depends not only on behavior but also on the context in which leadership is practiced, pointing to the necessity of flexibility and adaptation in leadership roles.

3.2.3 Contingency Theory: Adapting Leadership to Context

Contingency theory offers a flexible approach to leadership, emphasizing that no single leadership style is universally effective in all situations. Unlike earlier frameworks such as trait theory, which centers on the personal attributes of leaders, or behavioral theory, which emphasizes specific leadership actions, contingency theory argues that the effectiveness of leadership is heavily shaped by the context in which it is practiced. In this view, a strategy that succeeds in one setting may fail in another due to variations in organizational structure, team dynamics, or external pressures.

This perspective marks a notable shift in leadership studies. Where trait theory suggests that individuals are naturally predisposed to lead due to inherent characteristics, and behavioral theory posits that effective leadership can be taught and replicated through consistent behaviors, contingency theory insists on adaptability. The underlying message is clear: leaders must remain responsive to shifting conditions and tailor their approaches accordingly, rather than adhering rigidly to one preferred style. Minor variations in context, such as the nature of the task, the experience level of the team, or even interpersonal dynamics, may necessitate completely different leadership strategies.

As Daft points out, leadership effectiveness is fundamentally determined by how well a leader's style aligns with the environment they are navigating.[260] Leaders who succeed are those who can

[260] Daft R.L. (2011). *The Leadership Experience*, 5th ed. Mason, OH: Cengage Learning

read the room, understand the nuances of their context, and respond with behaviors that best suit the moment. This means that situational awareness and strategic flexibility are essential components of good leadership.

One of the earliest and most influential models within this school of thought is Fred Fiedler's Contingency Model, developed in the 1960s.[261] Fiedler developed the Least Preferred Coworker (LPC) scale, a tool used to determine whether a leader is more focused on tasks or relationships:

- Task-Oriented Leaders prioritize organization, planning, and goal achievement. They perform best in situations with either very high or very low levels of control.
- Relationship-Oriented Leaders emphasize trust and team morale, and they are most effective when control is moderate.

He further identifies three key contextual elements that shape leadership outcomes:

- Leader–Member Relations: the quality of interactions and trust between the leader and team members.
- Task Structure: how clearly defined and organized the group's goals and responsibilities are.
- Leader's Position Power: the extent of formal authority and influence the leader has.

These variables interact to determine which style of leadership is most likely to succeed in a given scenario. Fiedler's model is foundational in highlighting that effectiveness cannot be divorced from situational complexity.

[261] Fiedler F.E., (1965). *A Contingency Model of Leadership Effectiveness*. Advances in Experimental Social Psychology, vol. 1, ed. L. Berkowitz (New York: Academic Press, 1965), 149–190.

Another significant contribution to contingency theory comes from Robert House and Terence Mitchell through their development of the Path–Goal Theory.[262] Drawing inspiration from Vroom's Expectancy Theory,[263] this model shifts the focus to the relationship between motivation, leadership behavior, and task accomplishment. The theory suggests that leaders help their team achieve success by adapting their behavior to match both the team's needs and the requirements of the task. It is based on the idea that:

- Team members' effort contributes to effective performance (expectancy),
- Good performance produces results or rewards (instrumentality),
- The rewards or outcomes are meaningful and desirable to the team (valence).

Leaders, in this view, must facilitate their team's "path" to success by choosing behaviors that match both the characteristics of their followers and the nature of the tasks. The Path–Goal Theory outlines four primary leadership styles:

- Directive: Clarifies tasks, roles, and expectations. Best used when tasks are ambiguous.
- Supportive: Focuses on building relationships and addressing team members' emotional needs.
- Participative: Involves followers in decision-making; effective when team members are capable and motivated.
- Achievement-Oriented: Involves setting ambitious goals and encouraging team members to perform at their best.

[262] House R.J., Mitchell T.R.(1974). *Path-Goal Theory of Leadership.* Journal of Contemporary Business 3, no. 4: 81–97.

[263] Vroom V.H., (1964). *Work and Motivation,* New York: Wiley

The theory also emphasizes that follower characteristics play a key role in determining which leadership approach will be most effective. Leaders must, therefore, be adept at reading both the task environment and their team's psychological makeup to inspire optimal performance. Key follower traits influencing leadership effectiveness are:

- Competence: More skilled team members often prefer participative leadership.
- Authoritarianism: Some prefer clear hierarchy and directive leadership.
- Locus of Control: Internally motivated individuals prefer autonomy; externally motivated ones may favor more structured leadership.

Leaders must, therefore, be adept at reading both the task environment and their team's psychological makeup to inspire optimal performance.

Hersey and Blanchard's Situational Leadership Theory further advances the contingency approach by introducing the concept of follower maturity.[264] Rather than viewing followers as a homogeneous group, this theory assesses their readiness based on two criteria: competence and commitment. The model suggests four leadership styles that correspond to varying levels of follower maturity:

- Delegating (High competence, high commitment): Minimal direction and support; leader acts as a facilitator.
- Supporting (High competence, low commitment): Focus on emotional support and encouragement.
- Coaching (Low competence, high commitment): Directive leadership combined with support to build skills.

[264] Hersey P., Blanchard K.H., (1988). *Life Cycle Theory of Leadership.* Training and Development Journal 23, no. 5 (1969): 26–34. P. Hersey and K.H. Blanchard, Management of Organizational Behavior: Utilizing Human Resources, 5th ed. (Englewood Cliffs, NJ: Prentice Hall, 1988).

- Directing (Low competence, low commitment): Clear instructions and close supervision.

This approach underlines the flexible nature of leadership, suggesting that as team members become more skilled and self-assured, leaders should correspondingly reduce their level of direct involvement and adjust their support. Hersey and Blanchard emphasize that team maturity isn't merely the sum of individual abilities; rather, it also reflects shared elements such as interpersonal trust, unity within the group, and the intricacy of tasks. Effective leadership, therefore, requires sensitivity to both individual and group dynamics, adapting to evolving needs and situational demands.[265]

Contingency theory reinforces the idea that leadership success is highly dependent on context. Rather than relying on fixed traits or static behaviors, leaders must assess factors like their team's experience, the nature of the task, and environmental uncertainty to determine the most suitable approach.

Whether referencing Fiedler's methodical analysis of situational control, House and Mitchell's emphasis on motivation and team alignment, or Hersey and Blanchard's model based on developmental stages, the central message remains consistent: leadership should be tailored to context.

These frameworks offer valuable tools for navigating the leadership challenges of fast-paced, digitally driven sectors like telecommunications, where technological disruption and cyber threats demand adaptive, informed, and responsive leadership strategies.

3.2.4 The GLOBE Project: Understanding the Cultural Foundations of Leadership

[265] Ibidem.

Interesting to be mentioned in a discussion on leadership is the GLOBE (Global Leadership and Organizational Behavior Effectiveness) Project originated in the early 1990s as a major, multidisciplinary research initiative aimed at understanding how culture impacts leadership and organizational practices worldwide. The project was launched by Robert J. House and a team of over 170 researchers from 62 countries, making it one of the largest studies of its kind.[266]

The GLOBE research team defined leadership as an individual's ability to influence, inspire, and enable others to contribute effectively to organizational success.[267] They expanded the concept of implicit leadership theory by incorporating the role of national culture, proposing that people's expectations of leaders vary according to the cultural values prevalent in their societies. This means that leadership attributes and behaviors considered effective in one culture may differ in another, highlighting the importance of cultural context in leadership effectiveness.[268]

The impetus behind GLOBE was to move beyond traditional leadership theories, which were largely developed in Western contexts, and to explore how leadership behaviors and effectiveness vary across diverse cultural environments. Researchers wanted to identify which leadership attributes are universally valued and which are culturally specific.

To do this, the GLOBE Project collected extensive data from thousands of middle managers across multiple industries in different societies. It examined how people in various cultures perceive leadership, what leadership styles are most effective, and how societal cultural dimensions influence leadership preferences.

[266] GLOBE Project. (2011, April 1). 2004, 2007 Studies - GLOBE Project: An overview of the 2004 study: Understanding the relationship between national culture, societal effectiveness and desirable leadership attributes. https://globeproject.com/study_2004_2007.html

[267] House, R. J., et al. (Eds.). (2004). Culture, leadership, and organizations: The GLOBE study of 62 societies. Sage Publications.

[268] Lord, R. G., Maher, K. J. (1991). Leadership and information processing: Linking perceptions and performance. Unwin Hyman.

The GLOBE study built on earlier work in cross-cultural research, such as Hofstede's cultural dimensions theory, but expanded it by directly linking cultural factors to leadership behaviors.[269] Through rigorous statistical analysis, GLOBE identified nine cultural dimensions:

- Performance Orientation: Refers to the extent to which a group values and incentivizes improvement and excellence in individual and collective performance.
- Assertiveness: Describes how strongly individuals express themselves in interactions, including being direct, confrontational, or competitive when appropriate.
- Future Orientation: Captures the degree to which individuals or organizations plan ahead, invest in long-term goals, and delay immediate rewards for future benefits.
- Humane Orientation: Reflects the emphasis a group places on fairness, altruism, generosity, and caring behavior toward others, rewarding those who demonstrate these qualities.
- Institutional Collectivism: Measures the degree to which societal or organizational institutions encourage collaboration, shared resource distribution, and collective action.
- In-Group Collectivism: Represents the pride, loyalty, and cohesion individuals show toward their families or organizations, highlighting the importance of close group bonds.
- Gender Egalitarianism: Indicates how strongly a society or organization works to reduce gender disparities and promote equality between men and women.

[269] Shi, X., Wang, J. (2011). Interpreting Hofstede Model and GLOBE Model: Which way to go for Cross-Cultural research? *International Journal of Business and Management*, *6*(5). https://doi.org/10.5539/ijbm.v6n5p93

- Power Distance: Captures the extent to which hierarchical differences, authority, and unequal status are accepted and legitimized within a group or community.

- Uncertainty Avoidance: Refers to the degree to which people rely on rules, procedures, and established norms to manage the unpredictability of future events. Higher uncertainty avoidance leads to greater emphasis on order, structure, formal regulations, and consistent practices in daily life.

GLOBE designed a questionnaire with 112 leader attributes and behaviors items which included a wide variety of traits, skills, behaviors, and abilities potentially relevant to leadership emergence and effectiveness.[270] The statistical analysis produced 21 primary dimensions of leadership which with further analysis produced a set of 6 global leadership dimensions. The six global dimensions and their associated 21 primary leadership dimensions constitute the notion of culturally endorsed leadership theory (CLT) and are briefly defined as follows:

- Charismatic or Value-Based Leadership focuses on motivating and inspiring others to achieve high performance by adhering to deeply held values. Its key traits include being visionary, inspirational, willing to make personal sacrifices, acting with integrity, making decisive choices, and maintaining a performance-oriented approach.

- Team-Oriented Leadership prioritizes building effective teams and fostering shared goals among members. It emphasizes collaboration, integrating team efforts, diplomatic behavior, administrative competence, and the avoidance of harmful behaviors (reverse scored).

[270] Psychology iResearchNet. GLOBE study: Cultural dimensions and leadership. GLOBE

- Participative Leadership concerns the extent to which leaders involve others in decision-making and implementation. It ranges from nonparticipative to autocratic tendencies, with both extremes being reverse scored.

- Humane-Oriented Leadership reflects a supportive and considerate approach, emphasizing compassion, generosity, and modesty, with a focus on human-centered values.

- Autonomous Leadership highlights independence and individuality, valuing traits such as self-reliance, uniqueness, and autonomous decision-making.

- Self-Protective Leadership is centered on maintaining personal and group security, often through status awareness and face-saving behaviors. Key characteristics include self-centeredness, status consciousness, conflict induction, procedural adherence, and efforts to preserve reputation.

In sum, the GLOBE Project's origin was rooted in the need to understand leadership within the rich diversity of global cultures, recognizing that leadership effectiveness is deeply influenced by cultural norms, values, and expectations that differ significantly from one region to another.

3.3 Leadership in the Digital Era

Given the theories and different types of leadership that have been developed, a question that might arise is if leadership has changed over the years given the incredible revolutions brought by digitalization.

In the ever-evolving landscape of the 21st-century digital economy, leadership is being reshaped by the rapid integration of digital technologies into all aspects of business operations. The concept of digital leadership has emerged as a critical framework that encompasses the strategic and human-centric competencies leaders must possess to navigate the complexities of digital transformation. This shift demands a departure from traditional leadership models, which emphasized control, structure, and continuity, toward more dynamic, agile, and visionary styles capable of fostering innovation, enabling continuous learning, and managing uncertainty. Digital leadership is not just about adopting new technologies; it is about reimagining the way organizations function, make decisions, engage with stakeholders, and create value in a volatile, uncertain, complex, and ambiguous (VUCA) world.

The digital revolution, driven by rapid technological advancements, has had profound implications on leadership. Digital disruption alters the fabric of how individuals live, work, and interact, thereby reshaping organizational cultures and business models. Digital disruption changes how people socialize and operate within professional settings, demanding adaptive responses from leaders.[271] Moreover, the digitalization of products and services is a global megatrend that fundamentally transforms value chains across industries.[272] Businesses across sectors are actively exploring and implementing digital technologies to innovate and enhance value delivery.[273] These technologies, embedded within core operations and offerings, necessitate comprehensive changes in leadership practices.[274]

[271] Nyagadza, B. (2022). *Sustainable digital transformation for ambidextrous digital rms: A systematic literature review and future research directions.* Sustainable Technology and Entrepreneurship 100020.

[272] Collin, J. (2015). *Digitalization and dualistic IT. IT Leadership in Transition - The Impact of digitalization on Finnish organizations (pp. 29−34).* Aalto University.

[273] Matt, C., Hess, T., & Benlian, A. (2015). *Digital transformation strategies.* Business & Information Systems Engineering, 57(5), 339–343. doi:10.1007/s12599-015-0401-5.

[274] Yoo, Y., et al. (2012). *Organizing for innovation in the digitized world.* Organization Science, 23, 1398–1408. doi:10.1287/orsc.1120.0771.

However, many companies are still ill-equipped to manage the challenges posed by digitalization, such as the acceleration of innovation cycles, the need for organizational agility, and employee adaptation.[275] In this context, leadership becomes the linchpin for successful transformation.

Leadership in the digital era requires a specific skill set and mindset tailored to address the complexities of technological change. Leaders must act as visionaries, crafting and articulating a compelling digital future for their organizations.[276] This vision must be not only inspiring but also actionable, guiding employees toward shared objectives.[277] Effective communication is central to this process, as it fosters alignment and motivation across diverse teams.[278] In addition to vision, digital leaders need the strategic capability to translate ideas into executable plans, leveraging digital tools to achieve business goals.[279]

Transformational leadership theory provides a foundational framework for understanding digital leadership. Originating from Burns (1978) and expanded by Bass (1985), transformational leadership emphasizes the role of leaders as change agents who inspire, innovate, and mobilize teams toward a collective purpose. This contrasts with transactional leadership, which focuses on maintaining the status quo. The dynamic nature of digital transformation aligns more closely with transformational leadership, which prioritizes adaptability, creativity, and forward-thinking.[280]

[275] Almeida, F.,et al. (2020). *The challenges and opportunities in the digitalization of companies in a post-COVID-19 World.* IEEE Engineering Management Review, 48(3), 97–103. Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital transformation: An overview of the current state of the art of research. Sage Open, 11,(3) 21582440211047576

[276] Westerman, G., Bonnet, D., & McAfee, A. (2014b). The nine elements of digital transformation. MIT Sloan Management Review, 55(3), 1–6.

[277] Guzmán, V. E., Muschard, B., Gerolamo, M., Kohl, H., & Rozenfeld, H. (2020). Characteristics and skills of leadership in the context of Industry 4.0. Procedia Manufacturing, 43, 543–550.

[278] Ivančić, L., Vukšić, V. B., & Spremić, M. (2019). Mastering the digital transformation process: Business transformation 4.0 as a new paradigm. Business Systems Research Journal, 10(1), 37–48.

[279] Kazim, F. (2019). Digital transformation and leadership style: A multiple case study. The ISM Journal of International Business, 1(1), 1–12.

[280] Kotter, J. P. (2000). What leaders really do. Harvard Business Review, 79(11), 24–33.

The emergence of terms such as "digital leadership" and "leadership in a digital age" reflects a growing recognition of the new competencies required in the digital era.[281]

Digital leaders must exhibit a range of competencies, starting with visionary leadership. They must anticipate market trends, interpret technological shifts, and guide organizations toward sustainable growth.[282] Creativity and curiosity are vital, allowing leaders to challenge norms and explore innovative solutions.[283] The importance of a "growth mindset," which emphasizes continuous improvement and a willingness to embrace change is also underscored among the characteristics that leadership in the digital era must possess.[284]

Agility is another cornerstone of digital leadership. In the face of rapid technological and market changes, leaders must make swift decisions and pivot strategies as needed.[285] Agility encompasses both organizational flexibility and personal resilience, enabling leaders to respond effectively to uncertainty. The VUCA framework - Volatility, Uncertainty, Complexity, Ambiguity - captures the environmental conditions that necessitate agile leadership.[286] In such contexts, leaders must be comfortable with ambiguity and capable of guiding teams through complexity.[287] A critical element

[281] El Sawy, O. A., et al. (2016). *How LEGO built the foundations and enterprise capabilities for digital leadership.* MIS Quarterly Executive, 15(2), 141–166 and Araujo, L. M., et al. (2021). *Digital leadership in business organizations.* International Journal of Educational Administration, Management, and Leadership, 2(1), 45–56. doi:10.51629/ijeamal.v2i1.18.

[282] Kane, G. C., et al. (2019). *How digital leadership is (n't) different.* MIT Sloan Management Review, 60(3), 34–39

[283] Larjovuori, R.-L., et al. (2018). *Leadership in the digital business transformation.* In Proceedings of the 22nd International Academic Mindtrek Conference (pp. 212–221). doi:10.1145/3275116.3275122.

[284] Nadella, S., & Euchner, J. (2018). *Navigating digital transformation: An interview with Satya Nadella.* Research Technology Management, 61(4), 11–15. doi:10.1080/08956308.2018.1471272.

[285] Berman, S. (2012). Digital transformation: *Opportunities to create new business models.* Strategy & Leadership, 40(2), 16–24. doi:10.1108/10878571211209314 and Kohli, R., & Johnson, S. (2011). *Digital transformation in latecomer industries: CIO and CEO leadership lessons from Encana Oil & Gas (USA) Inc.* MIS Quarterly Executive, 10(4), 141–156.

[286] Bennett, N., & Lemoine, G. J. (2014). What a difference a word makes: Understanding threats to performance in a VUCA world. Business Horizons, 57(3), 311–317. doi:10.1016/j.bushor.2014.01.001.

[287] Guzman, V. E., Muschard, B., Gerolamo, M., Kohl, H., & Rozenfeld, H. (2020). Characteristics and skills of leadership in the context of industry 4.0. Sustainable manufacturing - hand in hand to sustainability on globe. In

of digital leadership is digital literacy or digital savviness. While leaders may not require deep technical expertise, they must understand how digital tools impact business models and operations.[288] This includes familiarity with data analytics, cloud computing, artificial intelligence, and other emerging technologies. Digital leaders must be able to leverage data for decision-making and strategic planning.[289]

Collaboration is equally essential in digital environments. Leaders must cultivate a culture of teamwork, knowledge sharing, and cross-functional collaboration. Cross-functional teams, comprising members from diverse departments, foster innovation and holistic problem-solving.[290]

Continuous learning and development are also foundational to digital leadership. The concept of lifelong learning, or continuous learning, reflects the need for ongoing skill enhancement to remain competitive in the digital economy.[291] Leaders play a pivotal role in enabling learning opportunities, providing training programs, and encouraging knowledge acquisition among employees.[292]

Soft skills complement technical and strategic competencies in digital leadership. Traits such as empathy, humility, emotional intelligence, and resilience are frequently cited as crucial for effective

Proceedings of the 17th Global Conference on Sustainable Manufacturing (pp. 543−550). doi:10.1016/j.promfg.2020.02.167.

[288] Imran, F., et al. (2020). Leadership competencies for digital transformation: Evidence from multiple cases. International Conference on Applied Human Factors and Ergonomics (pp. 81−87). doi:10.1007/978-3-030-50791-6_11.

[289] Eberl, J. K., Drews, P. (2021). *Digital leadership–mountain or molehill? A literature review.* Wirschaftsinformation 2021 Proceedings (pp. 223−237). doi:10.1007/978-3-030-86800-0_17; Kane, G. C., et al. (2015). *Strategy, not technology, drives digital transformation:* 14 (pp. 1−25). MIT Sloan Management Review and Deloitte University Press.

[290] Guinan, P. J., et al. (2019). *Creating an innovative digital project team: Levers to enable digital transformation.* Digital Transformation & Disruption, 62(6), 717–727. doi:10.1016/j.bushor.2019.07.005.

[291] Eberl, J. K., & Drews, P. (2021). *Digital leadership–mountain or molehill? A literature review. Wirschaftsinformation 2021 Proceedings (pp. 223−237). doi:10.1007/978-3-030-86800-0_17.*

[292] Wrede, M., et al. (2020). *Top managers in the digital age: Exploring the role and practices of top managers in rms' digital transformation.* Managerial & Decision Economics, 41(8), 1549–1567. doi:10.1002/mde.3202.

leadership in digital contexts.[293] These attributes enhance a leader's ability to connect with employees, manage stress, and foster inclusive work environments. Motivating and inspiring teams through authentic engagement is key to driving digital transformation.[294]

Cultural awareness and inclusivity are increasingly relevant in digital leadership. Virtual teams and global workforces require leaders to manage cultural diversity and ensure equitable participation.[295] Intercultural competence enables leaders to navigate differences and build cohesive, high-performing teams. Additionally, multigenerational workforces present unique challenges, particularly in digital fluency. Leaders must bridge generational gaps by offering targeted support and promoting inclusive digital practices.[296]

Ethical responsibility is another pillar of digital leadership. As organizations adopt technologies that collect and process vast amounts of data, leaders must uphold ethical standards in data privacy, transparency, and fairness.[297] The ethical dimension of leadership extends to ensuring that digital transformation does not exacerbate inequalities but rather supports inclusive growth and societal well-being.

In summary, digital leadership is an evolving construct that integrates vision, strategy, empathy, agility, and technical awareness. It responds to the unique challenges and opportunities presented by

[293] Babin, R., Grant, K. (2019). *How do CIOs become CEOs?* Journal of Global Information Management, 27(4), 1–15. doi:10.4018/JGIM.2019100101; Cresnar, R., & Nedelko, Z. (2020). Understanding future leaders: How are personal values of generations Y and Z tailored to leadership in industry 4.0? Sustainability, 12(11), 4417. doi:10.3390/su12114417

[294] Larjovuori, R.-L., et al. (2018). *Leadership in the digital business transformation.* In Proceedings of the 22nd International Academic Mindtrek Conference (pp. 212−221). doi:10.1145/3275116.3275122.

[295] Schwarzmüller, T., et al. (2018). *How does the digital transformation affect organizations? key themes of change in work design and leadership.* Management Revue, 29(2), 114–138

[296] Chuang, S., & Graham, C. M. (2020). *Contemporary issues and performance improvement of mature workers in industry 4.0.* Performance Improvement, 59(6), 21–30. doi:10.1002/p .21921.

[297] Herold, G. (2016). *Leadership in the fourth industrial revolution.* Stanton Chase Business Journals, 22(12), 1–15. https://www.stantonchase.com//wp-content/uploads/2016/09/Leadership-in-Fourth-Industrial-Revolution-1.pdf last accessed 2022-02-06.

digital transformation. Leaders must be equipped to anticipate change, inspire teams, drive innovation, and build adaptive, learning-oriented organizations. As digitalization continues to redefine the contours of the modern workplace, the need for effective digital leadership will only intensify.

The transition from traditional leadership models to digital leadership is not merely a shift in tools or platforms; it is a transformation in mindset and organizational philosophy. It requires embracing a future that is uncertain, dynamic, and technology-driven, and positioning leadership as the catalyst for positive change. By fostering a culture of innovation, inclusion, and continuous development, digital leaders can unlock the full potential of their organizations and ensure long-term resilience and relevance in the digital age.

3.4 Crisis Leadership and Cybersecurity

The leadership models analyzed in this chapter highlight a wide array of characteristics, from classical theories to those considering specific contexts, cultures, and organizational settings. The previous paragraph instead, dedicated to the evolution of leadership in the digital era, showed how new traits and approaches have become increasingly important as organizations undergo rapid transformation. Leadership is no longer static; it must adapt to unprecedented uncertainty, technological disruption, and cross-functional interdependence.Despite these developments, a significant research gap persists in understanding leadership competencies specifically suited to managing cyber crises.

Crisis leadership can be considered as a starting point for the definition of the leadership model related to cyber crisis. Crisis leadership has traditionally been defined as the exercise of influence and agency during periods of acute uncertainty, disruption, and threat, where leaders are expected to restore order, minimize damage, and guide organizations toward recovery.[298] Crises share defining features of unpredictability, urgency, and escalation risk, though they differ from disasters in terms of scale and broader societal impact. Whereas disasters are dangerous events causing substantial human and economic loss, crises are often specific, unexpected events that create acute uncertainty for organizations, threatening high-priority goals and demanding immediate action.[299]

Over the years, scholars have developed models to systematize the crisis management process. Coombs' three-stage model (precrisis, crisis, and postcrisis), Fink's four-stage framework (prodromal, acute, chronic, resolution), and Mitroff's five-stage cycle (signal detection, prevention, damage containment, recovery, and learning) remain among the most influential.[300] While these frameworks offer valuable guidance, they tend to conceptualize crises in sequential or linear terms. Such approaches risk underplaying the improvisational, recursive, and relational nature of leadership as it unfolds in practice. However, crises are characterized by confusion, incomplete information, and emergent dynamics, which means effective crisis leadership depends less on rigid plans than on organizational context, collective sensemaking, and improvisation.[301] Yet empirical studies capturing these dynamics remain limited, leaving open important questions about how leaders *actually* navigate crises in practice.

[298] Lehtonen, S., et al. (2025). *Rethinking Crisis Leadership through Leadership-as-Practice: A Narrative Review and Future Directions.* International Journal of Disaster Risk Reduction, 105671. https://doi.org/10.1016/j.ijdrr.2025.105671

[299] Ibidem.

[300] Ibidem.

[301] Gilpin, D.R., Murphy, P.J. (2008). *Crisis Management in a Complex World.* Oxford University Press, New York.

Against this backdrop, the Leadership-as-Practice (L-A-P) perspective has emerged as a promising alternative.[302] Rooted in practice theory, L-A-P shifts the focus away from individual leaders and their traits or styles toward the collective, situated practices through which leadership emerges. Leadership is understood not as a static attribute of a person but as an ongoing process of activities, improvisations, and interactions between human and non-human actors.[303] This approach rejects traditional dualisms such as structure versus agency or mind versus body, instead framing leadership as embodied, situated action shaped by material, temporal, and social contexts.

In crisis settings, L-A-P provides a particularly valuable lens. Rather than attributing success or failure to heroic individuals, it foregrounds the collective, improvisational, and distributed practices through which organizations make sense of and respond to crises. This post-heroic perspective resonates with the reality of complex crises where no single leader can marshal the expertise, information, and authority required to manage the situation alone. Instead, leadership emerges from the collective accomplishments of multiple actors, adapting dynamically to the unfolding context.[304]

Although L-A-P has been applied across diverse fields, including education, health care, the military, and international development, it has not yet been systematically explored in crisis or disaster contexts.[305] However it becomes particularly relevant when turning to the field of cybersecurity, which increasingly exhibits the characteristics of crisis contexts. Cyber threats are

[302] For a complete analysis of the L-A-P model see Lehtonen, S., et al. (2025). Rethinking Crisis Leadership through Leadership-as-Practice: A Narrative Review and Future Directions. *International Journal of Disaster Risk Reduction*, 105671. https://doi.org/10.1016/j.ijdrr.2025.105671

[303] Carroll B., et al. (2008). *Leadership as practice: challenging the competency paradigm.* Leadership 4 (4) 363–379, https://doi.org/10.1177/1742715008095186.

[304] Crevani, L., Endrissat, N., (2016), *Mapping the leadership-as-practice terrain: comparative elements,* in: J.A. Raelin (Ed.), Leadership-as-Practice: Theory and Application, Routledge, New York, pp. 21–49.

[305] Lehtonen, S., et al. (2025). *Rethinking Crisis Leadership through Leadership-as-Practice: A Narrative Review and Future Directions.* International Journal of Disaster Risk Reduction, 105671. https://doi.org/10.1016/j.ijdrr.2025.105671

marked by unpredictability, urgency, and the potential for cascading escalation. The rise in frequency and severity of cyberattacks demands organizational responses that are not only technically sophisticated but also strategically adaptive and socially embedded. It can be considered as a starting point for the cyber risk leadership, extending it to cybersecurity to reveal how leadership practices are enacted under conditions of high uncertainty, improvisation, and collective sensemaking.

Traditional crisis leadership frameworks have not been extensively validated for cyber-related events, even though the frequency and severity of cyberattacks, particularly ransomware, have risen sharply. This surge underscores the pressing need for effective organizational crisis management in the cyber domain. Studies reveal, however, that leadership effectiveness in cybersecurity remains strikingly low, with only around 12% of leaders rated as "very effective".[306] This highlights the necessity of rethinking leadership education, shifting toward more holistic approaches that blend fairness, consistency, and emotional intelligence with technical expertise. These human-centered traits are essential in building trust, fostering collaboration, and enabling agile and innovative responses to cyber threats.

Yet, the literature linking leadership to cybersecurity remains fragmented. Most research continues to privilege technical solutions, treating leadership dimensions as secondary or implicitly assumed. As a result, there is still no consolidated framework identifying the soft skills and leadership competencies most critical to fostering cyber resilience. A growing body of case-based studies, however, demonstrates the potential value of adapting crisis leadership theories to cyber contexts.

[306] Burton, S. L., et al. (2023). Exploring the nexus of cybersecurity leadership, human factors, emotional intelligence, innovative work behavior, and critical leadership traits. *Scientific Bulletin*, *28*(2), 162–175. https://doi.org/10.2478/bsaft-2023-0016

For example, the 2019 ransomware attack on Norsk Hydro has been analyzed through the crisis leadership competency model developed by Wooten and James.[307] Before the incident, Norsk Hydro exhibited both technical and organizational weaknesses, including poor collaboration and low cyber awareness, factors that underscored the urgent need for better prevention and preparation. During the crisis, leadership traits such as organizational alignment, creativity, decisive action under pressure, transparent communication, and ethical conduct proved crucial in navigating the disruption. Trust, clear role definition, and effective coordination within the crisis management team accelerated response efforts, while open communication with employees, customers, and external stakeholders reinforced credibility. Importantly, creativity and organizational agility allowed operations to continue despite the paralysis of normal IT systems. In the post-crisis stage, the company embraced organizational learning, embedding new cybersecurity and resilience strategies to strengthen defenses. Acting with transparency and integrity from the outset further enhanced stakeholder confidence and aided recovery.

This case illustrates that effective cyber crisis management requires a hybrid model: combining traditional crisis leadership competencies with cyber-specific elements such as heightened risk awareness, cross-actor collaboration, organizational agility, and ethical openness.[308] The Norsk Hydro experience also highlights the absence of a comprehensive framework that systematically captures these competencies, underlining the urgent need for a cyber risk leadership model. Such a model would systematize the traits, soft skills, and competencies most effective in fostering cyber resilience. It would also help reframe cybersecurity from being seen purely as a technical or

[307] For further information see Salviotti, G., et al. (2023). Understanding the role of leadership competencies in cyber crisis management: A case study. Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS).

[308] Ibidem.

compliance-driven function into a strategic leadership imperative that builds trust, enables innovation, and strengthens long-term resilience. Such a model could guide leaders in proactively embedding resilience, fostering organizational trust, and transforming cyber risk management from a purely technical exercise into a strategic leadership imperative. Leaders in high-risk sectors like telecommunications, where exposure to advanced persistent threats, insider risks, and regulatory pressures is acute, require precisely this integrated approach, combining technical understanding with strategic foresight, cultural influence, and continuous learning.

Ultimately, leadership can serve as a "force multiplier" in cybersecurity, amplifying the effectiveness of technical controls through organizational alignment and behavioral change. As cyber threats grow more sophisticated, leaders must not only mitigate risks but also transform cybersecurity into a source of strategic advantage. Doing so requires moving beyond fragmented understandings and toward a consolidated framework of cyber risk leadership.

To advance the development of a cyber risk leadership model, the present work adopts a qualitative research design, as outlined in the following chapter. This approach seeks to uncover the concrete competencies, behaviors, and leadership traits that underpin effective cyber risk management, moving beyond abstract frameworks to capture the lived experiences and practices of leaders operating in high-stakes digital environments. In this way, cybersecurity is framed not merely as a technical domain, but as a central leadership challenge—one that is essential for cultivating resilience, fostering trust, and enabling innovation in an increasingly interconnected world. With a focus on the telecommunications sector, the study addresses two key questions: Which leadership characteristics are required to effectively manage cyber risks in the context of digital transformation? And which traits enable leaders to strengthen organizational resilience against evolving cyber threats? By engaging with these questions, the research aims to generate insights that are both academically rigorous and practically applicable, offering a meaningful contribution to leadership development in an era defined by complex cybersecurity challenges.

CHAPTER 4.

METHODOLOGY

4.1 Purpose Statement and Research Question

In recent decades, the business landscape has undergone profound transformations, largely shaped by the Fourth Industrial Revolution and the rapid pace of technological innovation. Digital transformation has unlocked remarkable opportunities for organizations, such as operational efficiency, cost reductions, and the development of innovative products and services.[309] At the same time, it has introduced unprecedented challenges, the most critical of which concerns cybersecurity.[310] As companies increasingly rely on interconnected digital systems, the scale, frequency, and sophistication of cyber risks have intensified, making cybersecurity a central concern for business strategy and governance.[311]

This issue is particularly pronounced in the telecommunications sector. Telecommunication companies form part of a nation's critical infrastructure, enabling the exchange of information, ensuring connectivity, and supporting essential services across societies and economies.[312]

[309] Schwab K. (2016). The Fourth Industrial Revolution: what it means, how to respond. World Economic Forum. https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ and Admin, I. (2025, June 29). The 4IR Impact on Business: Navigating Innovation and Opportunities in a Digital Era - Fourth Industrial. *Fourth Industrial Revolution*. The 4IR Impact on Business: Navigating Innovation and Opportunities in a Digital Era

[310] Ukwandu E, Hewage C, Hindy H. Editorial: Cyber security in the wake of fourth industrial revolution: opportunities and challenges. Front Big Data. 2024 Feb 21;7:1369159. doi: 10.3389/fdata.2024.1369159. PMID: 38449565; PMCID: PMC10915258.

[311] Adewuyi, N. A., et al. (2024). The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems. World Journal of Advanced Research and Reviews, 23(1), 379–394. https://doi.org/10.30574/wjarr.2024.23.1.1993

[312] Cardenes, W. (2025, August 28). *National Critical Infrastructure*. Enea. Securing National Critical Infrastructure

The sector handles massive volumes of sensitive personal and corporate data while operating highly complex networks.[313] These characteristics make telco companies frequent and attractive targets for cyberattacks.[314] The consequences of such attacks extend well beyond financial loss, reputational damage, or temporary service disruption; they also pose risks to national security and the trust of the wider community.[315]

The telecommunications industry is experiencing a profound transformation. Companies that once focused primarily on providing voice and data services are now evolving into key facilitators of advanced technologies. This transition is reshaping how both consumers and businesses operate, while positioning telecom providers as an essential foundation for industry, government, and society at large.[316]

The dual force of technological innovation and escalating cyber risks creates an environment often described as VUCA: volatile, uncertain, complex, and ambiguous. While innovations and digital transformation present major opportunities for telecommunications companies, they also introduce new risks and responsibilities in the field of cybersecurity.[317] To maintain customer trust, comply with evolving regulatory requirements, and meet shareholder expectations, telcos must effectively address these challenges. This requires reinforcing governance structures, building greater

[313] Manukonda, K. R. R. (2019). *Cyber attack on telecommunications company*. European Journal of Advances in Engineering and Technology, *6*(12), 113-120.

[314] Ibidem.

[315] Wang, P., e al. (2019). *Economic costs and impacts of business data breaches.* Issues in Information Systems, 20(2), 162-171; Noah, A., et al. (2024, December 4). *The consequences of non-compliance with data protection regulations on business analytics.* ResearchGate.

[316] Gupta, A., Verbree, M., Rica, F., Michaux, D., & KPMG International Cooperative. (2019). *Global Perspectives on Cyber Security in Telco: A roundtable discussion on the state of cyber security management in the telco sector.* KPMG. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/02/global-perspectives-on-cyber-security-in-telco.pdf

[317] Saeed, S., et al. (2023). *Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations.* Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666

resilience, integrating cybersecurity into core business strategies, and rethinking the role and scope of the cybersecurity function itself.[318]

In this environment, organizations must not only embrace digital transformation to remain competitive but also strengthen their resilience against growing cyber threats. Cybersecurity has thus become a crucial pillar for protecting the confidentiality, integrity, and availability of data and systems. Yet despite increasingly sophisticated technological defenses and risk management frameworks, organizations remain vulnerable. This is due in large part to the dynamic nature of cyber threats, which are exploited by a diverse array of actors, including lone hackers, organized criminal networks, and state-sponsored groups.[319]

At the outset of this thesis, the research interest was centered on identifying strategies that enable telecommunications companies to manage cyber risk effectively and strengthen resilience against the operational, financial, and reputational damage caused by cyberattacks. Initial explorations included analyzing existing technical protection measures, cybersecurity frameworks such as ISO and NIST, and relevant global and regional regulations designed to mitigate cyber risks.[320] Discussions were also conducted with software developers with experience in cybersecurity, and professionals from the International Telecommunication Union, with the aim of identifying practical measures that could render telco companies more cyber resilient.

Through these exploratory discussions, one critical insight emerged: while existing literature and practice devote significant attention to technical defenses and risk management frameworks, the

[318] Ibidem.

[319] FortiGuard Labs (2025). *Fortinet Global Threat Landscape Report.* Fortinet Global Threat Landscape Report.

[320] For further information see chapters 1 and 2 of the present work.

role and the importance of the human factor remains comparatively often underexplored.[321] Statistics show that a significant portion of cyber attacks is directed towards employees[322] and that incidents originate from human vulnerabilities, including inadequate employee training, lack of awareness, and, crucially, insufficient leadership guidance.[323] Even the most advanced technological safeguards cannot ensure cybersecurity if the organizational culture does not promote awareness, accountability, and resilience. In this context, leadership emerges as a decisive factor. Leaders shape organizational priorities, allocate resources, and influence employee behavior.[324] Their ability to foster a culture of cybersecurity, encourage vigilance, and ensure preparedness directly determines how effectively an organization can withstand cyber threats.[325]

This realization reframed the purpose of the thesis. Rather than focusing solely on technical and procedural mechanisms for cyber protection, the present research concentrates on the role of leadership in managing cyber risk. Specifically, it explores which leadership characteristics make individuals most effective at guiding organizations through the complexities of cyber risk in an era defined by rapid digital innovation. The underlying curiosity is to identify what makes leaders in the telecommunications sector "fit for purpose" in navigating extreme uncertainty, and how leadership can complement technical measures to strengthen organizational resilience.

[321] Colabianchi, S., et al. (2025). *Transforming threats into opportunities: The role of human factors in enhancing cybersecurity.* Journal of Innovation & Knowledge, 10(3), 100695. https://doi.org/10.1016/j.jik.2025.100695

[322] Nagar, G. (2024). *The role of human factor in cybersecurity: Behavioral insights and training strategies.* International Research Journal of Modernization in Engineering, Technology and Science, *6*(3), 5723–5730. https://www.irjmets.com

[323] Aksoy, C. (2025b). *Building Effective Cybersecurity Leadership: The Crucial Role Of Leaders In Protecting Businesses Against Cyber Threats.* Kalite Ve Strateji Yönetimi Dergisi, 5(1), 33–49. https://doi.org/10.56682/ksydergi.1539408

[324] Lemieux, R. (2025, August 12). *Leadership's role in enabling cyber operational resilience*. DVMS Institute. https://dvmsinstitute.com/2025/02/03/five-steps-leadership-can-take-to-enable-organizational-cyber-resilience-through-culture/

[325] Iovan, S., & Iovan, A.-A. (2016). *From cyber threats to cyber-crime.* Journal of Information Systems & Operations Management, 10(2), 425–434 https://web.rau.ro/websites/jisom/Vol.10 No.2 - 2016/JISOM-WI16-A15.pdf

The decision to focus on the telecommunications sector is particularly relevant for several reasons. First, telcos play a strategic role in national security, and their infrastructure is indispensable for the functioning of modern economies and societies.[326] Second, the sensitive data managed by these companies makes them primary targets for cyberattacks.[327] Third, their exposure to constant cyber threats makes leadership capability not only an internal organizational concern but also a matter of collective safety and resilience at the national and international levels. Examining leadership in this sector thus offers insights with both organizational and societal significance.

From these considerations, the research is guided by the following central questions:

1. What are the leadership characteristics that today's leaders in the telecommunications sector need to possess in order to effectively manage cyber risks in the context of digital transformation?
2. Which characteristics should leaders have to improve organisation's resilience in respect to cyber risk?

These questions aim to move the discussion beyond technical solutions and into the realm of leadership studies. By addressing them, the thesis seeks to contribute to both leadership research and cybersecurity management scholarship. It argues for the integration of leadership characteristics into cyber risk management frameworks as a crucial dimension of organizational resilience.

[326] Cardenes, W. (2025). *National Critical Infrastructure*. Enea. National Critical Infrastructure. Refer to chapter 2 for a comprehensive analysis of the telecommunications sector as critical national infrastructure.

[327] Cybersecurity has emerged as a critical component of the telecommunications sector, driven by the increasing complexity of digital infrastructure and the growing volume of sensitive data being transmitted across networks. Olaoluwa F. Samuel, et al. (2024). Ensuring Cybersecurity in telecommunications: Strategies to protect digital infrastructure and sensitive data. Computer Science & IT Research Journal, 5(8), 1855-1883. https://doi.org/10.51594/csitrj.v5i8.1448.

The anticipated contribution of this research is twofold. First, from an academic perspective, it contributes to filling a gap in the literature by positioning leadership as a critical, though often overlooked, factor in cybersecurity resilience. Existing studies tend to emphasize technological innovation, compliance with regulatory frameworks, and the implementation of risk management systems. This thesis highlights that without effective leadership, capable of fostering awareness, ensuring employee training, and guiding organizational culture, these measures may fall short. Second, from a practical perspective, the findings aim to provide actionable insights for executives, policymakers, and cybersecurity practitioners. They point to the need for leadership development programs that specifically address cyber risk management, including training for decision-making under uncertainty, cross-disciplinary collaboration, and crisis communication.

Ultimately, the thesis underscores that cybersecurity cannot be understood solely as a technical issue; it is also a human and strategic challenge. Leadership plays a pivotal role in aligning organizational culture with cybersecurity priorities, ensuring that resilience is embedded into both strategy and daily operations. By focusing on leadership characteristics in the telecommunications sector, this research aspires to inform strategies that strengthen not only organizational security but also broader societal trust in critical infrastructure.

4.2 Interviewee Sample and Recruitment

To investigate which characteristics are most relevant for today's leaders to effectively manage cyber risks, interviews were conducted with high-level management professionals and experts in the telecommunications sector. These interviewees were selected to provide insights into the role of leaders in addressing cybersecurity threats and to highlight best practices and essential qualities for fostering cybersecurity awareness. The telecommunications industry was selected because of its high exposure to cyber threats, stemming from the vast amount of sensitive data it manages and its strategic role in national infrastructures.[328] This sector therefore offers particularly valuable perspectives on the leadership skills necessary to address cybersecurity challenges.[329]

The selection of interviewees was carried out according to their leadership positions within major Italian telecommunications companies and their professional experience in cybersecurity at the national level. The targeted job positions included Chief Executive Officers (CEOs), Chief Technology Officers (CTOs), Chief Information Security Officers (CISOs), Chief Security Officers (CSOs), Chief Information Officers (CIOs) and board members. These roles were chosen as they combine both strategic decision-making authority and direct responsibility for cybersecurity, providing insights that are highly relevant for the research objectives.

In addition to industry leaders, experts from the Italian National Cybersecurity Agency (ACN) were contacted, in order to integrate a national security perspective and assess leadership awareness and capacity beyond the corporate dimension.

The recruitment process proved challenging due to the typically low response rate in high-level professional outreach. Initially, more than fifty potential participants were contacted via LinkedIn. Out of these, twelve responded positively, while three declined to participate. Two others missed their scheduled interviews and, given the difficulties in rescheduling, were excluded from the final sample. To expand participation, a snowball sampling strategy was used by asking each interviewee to refer me to additional relevant contacts. This method proved successful and enabled me to reach the final number of participants.

[328] Kumar, M. J. (2023) Privacy-Preserving Technologies in Telecom Data Analytics: Implementing Privacy-Preserving Techniques Like Differential Privacy to Protect Sensitive Customer Data During Telecom Data Analytics. http://dx.doi.org/10.2139/ssrn.5136773

[329] Gupta, A., Verbree, M., Rica, F., Michaux, D., & KPMG International Cooperative. (2019). Global Perspectives on Cyber Security in Telco: A roundtable discussion on the state of cyber security management in the telco sector. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/02/global-perspectives-on-cyber-security-in-telco.pdf

The final sample consisted of eleven individuals: two CEOs, one board member, three experts from the National Cybersecurity Agency, two CISOs, two CTOs, and one cybersecurity and leadership development expert. The two CEOs and the board member, all from leading Italian telecommunications companies, offered critical insights into leadership perspectives at the highest levels of decision-making. Both CEOs and the board member had over thirty years of professional experience, with more than a decade in top leadership roles, providing a robust understanding of leadership practices in long-term organizational contexts.

The perspectives of the CTOs and CISOs enriched the study by highlighting the role of technical leadership in managing cyber risks. Unlike top executives, these leaders are directly responsible for the operational management of cybersecurity within their organizations. Their contributions shed light on the importance of technical expertise, problem-solving, and the ability to translate complex security challenges into actionable strategies. This allowed us to compare managerial and technical leadership skills, distinguishing which abilities are critical in shaping cybersecurity strategy and which are more relevant to day-to-day operational resilience.

To mitigate the potential bias inherent in self-assessment from company leaders, three experts from the National Cybersecurity Agency were included. Their input was essential in contextualizing leadership practices within the broader business and policy environment. They provided an external evaluation of how the sector has evolved, the types of risks and opportunities that telecommunications companies face, and the behavioral patterns observed among leaders in the field. This triangulation reduced the risk of overestimating or misrepresenting the qualities leaders perceive as important.

Finally, the interview with a cybersecurity expert, specialized in leadership development through cybersecurity training, offered a practical perspective on how leaders perform in high-stakes contexts. This expert designs and conducts cybers attacks simulations, enabling leaders to experience crisis scenarios in real time. Their observations contributed significantly to validating my findings by highlighting where leadership capacity is currently lacking, what challenges emerge during simulated crises, and which interventions may strengthen leaders' preparedness. This interview was conducted after the initial data collection and analysis phases, with the specific purpose of evaluating and consolidating the results.

To deepen my understanding of the impact of these cyberattack simulations, one session was attended, which allowed me to engage with experts and observe participants' reactions, behaviors, and problem-solving approaches, providing first-hand insight into the skills required for effective cyber risk management and also informing strategies, best practices and learning experiences to strengthen leadership development.

Overall, the final sample represented a diverse mix of perspectives, spanning strategic, operational, and expert viewpoints. The group included two women and nine men, with an average age of fifty-four years. Their breadth of experience, both in leadership and in cybersecurity, ensured that the insights gathered reflected not only the realities of managing cyber risks within telecommunications companies, but also the broader expectations of national and professional communities. This combination of voices allowed for a balanced and multidimensional understanding of what makes a leader fit to manage cyber risks in today's complex digital environment.

4.3 Data Collection

The data collection process was based on a semi-structured interview approach, supported by a guided questionnaire that was specifically designed for this research. The questionnaire included eleven core open-ended questions, structured around several key dimensions: (1) background information on the interviewee, (2) challenges, and risks associated with the digital era and cybersecurity, (3) characteristics of effective leadership in today’s context, (4) limitations of existing leadership models, and (5) possible future directions for reshaping leadership in relation to cyber risk management.

Table 4.1 Guided Questionnaire

Guided Questionnaire
1. Background and Role Could you briefly describe your current role and key responsibilities? How long have you held this position?
2. Awareness of Digital and Cyber Risks What are the main risks that telecommunications companies face in relation to digital transformation and cybersecurity?
3. Cyber Risk Management Challenges What, in your opinion, are the main challenges for leaders today with regard to cyber risk management?
4. Relationship with Technical Leadership How would you describe your working relationship with key technical leaders such as the CISO and CTO? How involved are you in discussions around cybersecurity and technology strategy?
5. How Leadership Expectations Have Changed How have digital technologies and cyber threats changed what is expected from todays leaders in the telecommunication sectors in comparison to the leaders of the past? To what extent is cybersecurity reshaping leadership traits?
6. Leadership and Cybersecurity Awareness How important is leadership in building a culture of cyber awareness and prevention?

7. Key Leadership Qualities in a Cyber Crisis What characteristics are generally required of contemporary leaders to navigate cybersecurity challenges? When a cyber incident occurs, which leadership qualities are most critical to manage the crisis successfully?
8. Nature of Leadership: Innate or Developed? Do you believe effective leadership mainly comes from natural traits, or can it be developed through experience and training?
9. Importance of Continuous Learning How important is ongoing learning and skill development for leaders to keep up with fast-changing digital and cyber environments?
10. Digital Understanding and Soft Skills How important is it for leaders to understand digital technologies and cyber risks? Beyond technical knowledge, which soft skills (e.g., communication, resilience, decision-making) are essential?
11. Leadership Challenges and Gaps What are the main challenges in developing an effective cyber risk leadership? Where do you think current leadership falls short in the telecom sector?
12. Future Leadership Needs Looking ahead, what suggestions would you give to enhance the ability of today's leaders to manage cyber risks?

The primary objective of the questions was to uncover the leadership characteristics most relevant to managing cyber risks in the telecommunications sector. However, they were also designed to elicit broader insights into the contextual drivers shaping today's leadership, as well as the challenges that leaders face in an increasingly digitalized environment. This twofold purpose ensured that the interviews captured both descriptive and analytical perspectives, while still remaining flexible to adapt to the specific expertise of each interviewee.

While the guiding framework was consistent across all interviews, some questions were adjusted depending on the participant's role. For example, in addition to the questions in *Table 4.1*, some role-specific questions were included to explore issues in greater depth. For technical experts such as Chief Technology Officers (CTOs) and Chief Information Security Officers (CISOs), some questions were adapted to further explore the degree of involvement of top management in cybersecurity matters. These included: *How is cybersecurity positioned within your organization's strategic priorities? Does it have board-level visibility? Who do you report to, and how often do you engage with the executive board or CEO on cyber matters? In your experience, how informed and engaged is your board of directors when it comes to cybersecurity risks?* By asking these questions, the aim was to uncover whether a disconnect exists between the strategic leadership level and the technical specialists responsible for implementing cybersecurity measures.

The ten interviews were conducted over a two-month period and took place virtually via Google Teams, with each interview lasting approximately one hour. English was used as the primary language, ensuring consistency across interviews despite the diverse backgrounds of participants. While the response rate to my initial outreach was relatively low, I considered the final number of interviews sufficient for the purposes of this study. This conclusion was based on the observation that recurring themes began to emerge across different participants, indicating a certain level of data saturation. In practice, this meant that while each participant contributed valuable individual insights, the range of ideas began to overlap and converge, suggesting that additional interviews might not have introduced substantially new perspectives. Nevertheless, I acknowledge that a larger sample size, particularly with more participants from the same professional categories, could have further reinforced the findings.

During the entire data collection phase, ethical principles were carefully observed. Prior to each interview, participants were provided with an informed consent document that clearly explained the study's objectives, the procedures they would be involved in, and their rights throughout the process. The document stressed that participation was entirely voluntary and that individuals could withdraw from the study at any time without facing any negative consequences. It also highlighted confidentiality measures, assuring participants that their identities would be anonymized in the reporting of results. Consent forms were sent to each participant once an interview was scheduled and confirmed, and all participants returned a signed form before their interview took place. This process ensured that the research adhered to ethical standards and respected the autonomy and privacy of participants.

In summary, the data collection process combined a structured yet flexible interview framework with careful attention to ethical requirements. The use of open-ended questions enabled participants to articulate their perspectives freely, while the tailored role-specific questions allowed for deeper exploration of leadership dynamics in relation to cybersecurity. Although the sample was relatively limited, the consistency of emerging themes across interviews provides confidence in the robustness of the data and its relevance for answering the research questions guiding this thesis.

4.4 Data Analysis

A concurrent analysis approach was adopted, beginning the analysis while interviews were still being conducted. Concurrent analysis, also known as simultaneous data collection and analysis, is a core feature of grounded theory in which data is analyzed as it is being collected rather than after all data has been gathered.[330] This approach allows researchers to adjust subsequent data collection

[330] Grant M.J, (2024). *Concurrent data collection and analysis in grounded theory*. The Grounded Theorist. Concurrent Data Collection

based on emerging insights, explore connections across datasets, and refine research questions iteratively, while remaining cautious to avoid introducing bias into the process. The main benefit is that it produces richer, more nuanced findings, keeps the study closely grounded in the data, and helps identify gaps or new directions in real time.[331] After each interview, the discussions were transcribed and the coding process was initiated. Once all the ten interviews had been completed, the codes were compiled to capture all elements mentioned across the data, without imposing any pre-existing structure. At this stage, each interview generated an average of fifty codes, resulting in a total of 494 codes.

Subsequently, the dataset was refined by excluding from each interview the codes that did not provide relevant insights for addressing the research question. This process reduced the number of codes to 273. Once irrelevant elements had been removed, codes were compared across interviews, revealing that they could be meaningfully organized into three overarching categories: (i) characteristics of leadership, which comprised 137 codes; (ii) drivers, risks, and challenges shaping leadership today, which accounted for 79 codes; and (iii) background and others relevant information, which included 47 codes and served mainly to contextualize the findings, provide interesting examples about interviewees' companies or personal experiences, and sharing best practices and future leadership development insights. This categorization facilitated the analysis and interpretation of the data.

To deepen the analysis, a comparative examination of the codes within each category across the different interviews was conducted. This comparison revealed recurring patterns and similarities, as several concepts were repeated multiple times by different interviewees. To capture these patterns systematically, a thematic frequency analysis was carried out by counting how many times a given concept was mentioned in the interviews, helping me to highlight patterns, recurring ideas, or

[331] Ibidem.

dominant issues in participants' responses.[332] Thematic frequency analysis provides a structured way to quantify qualitative information, assessing how often specific themes appear across different datasets. This enhances the consistency and reliability of the results, enabling researchers to capture the core messages of interviews, focus groups, or other qualitative sources.[333]

Nevertheless, some concepts emerged only once in the data. For example, regarding the characteristic of leadership, concepts such as "creativity", "positivity", and "humility" were mentioned one time as well as "globalization" and "geopolitical context" under the category of risks and challenges. In order to maintain analytical consistency and focus on the most robust findings, I excluded these concepts from further consideration, restricting the analysis to those that appeared at least twice across the dataset. As a result of this refinement, the final set of codes amounted to 204, divided as follows: 111 for leadership characteristics, 53 for risks, and challenges, and 40 for background information.

This systematic process of coding, categorization, and thematic frequency analysis enabled me to identify the most significant and recurrent themes, providing a solid foundation for the subsequent interpretation of results.[334]

4.5 Strengths and Limits

The methodology adopted in this research offers several strengths. First, the extensive review of the literature on cyber risk management allowed for the identification of significant gaps, particularly concerning the human and leadership dimensions of cybersecurity. Similarly, the analysis of

[332] Williams, B. (2024). *Summative content analysis in qualitative research*. Insight7 - AI Tool for Call Analytics & Evaluation. https://insight7.io/summative-content-analysis-in-qualitative-research/

[333] Ibidem.

[334] Ahmed, S. K., et al. (2025). *Using thematic analysis in qualitative research.* Journal of Medicine Surgery and Public Health, 100198. https://doi.org/10.1016/j.glmedi.2025.100198

leadership theories raised new questions about the characteristics required of today's leaders, especially in the telecommunications sector, and whether novel traits could be observed in practice compared to what is highlighted in existing scholarship.

Second, the decision to combine interviews with a diverse set of participants, including CEOs, CISOs, CTOs, a board member, and experts from the National Cybersecurity Agency, ensured a broad and balanced range of perspectives. This diversity strengthened the validity of the findings by integrating both managerial and technical insights, while also mitigating potential biases that could emerge from leaders' self-assessments. The inclusion of external experts, in particular, provided an independent viewpoint that contextualized and complemented the perspectives of organizational leaders. Moreover, presenting the results to a cybersecurity and leadership development expert at the conclusion of the data collection process reinforced the credibility of the findings and offered further validation.

Third, the concurrent and iterative process of data collection and analysis enhanced the flexibility and responsiveness of the study. Interview questions were refined throughout the process, allowing the exploration of themes that emerged in earlier discussions. This adaptive approach ensured that the interviews remained relevant and targeted as the research progressed. In addition, the systematic coding of data, followed by a frequency analysis of recurring themes, strengthened the rigor of the research. This approach provided transparency in how results were derived and highlighted not only the most common patterns but also those that held particular significance across participants.

Despite these strengths, the methodology is subject to certain limitations. The most evident constraint lies in the relatively small sample size, which relied on voluntary participation. Although the final group represented a rich variety of profiles, it cannot fully capture the diversity of leadership practices across the wider telecommunications sector. As such, the findings should be interpreted as indicative rather than fully generalizable.

Another limitation stems from the methodological choice to exclude concepts that were mentioned only once by participants. While this decision was necessary to ensure analytical focus on robust and recurring themes, it may have led to the omission of potentially valuable but less widely acknowledged insights. Some unique perspectives, even if not shared by others, could still reflect emerging trends or highlight niche but important challenges in the sector.

Finally, the interviews were conducted in English, which, although effective as a common language for communication, may have constrained participants' ability to express nuanced perspectives. For those whose first language is not English, subtle elements of meaning, cultural connotations, or context-specific expressions may have been lost, potentially limiting the richness of the data.

Taken together, these limitations suggest directions for future research. Expanding the sample size and ensuring greater diversity, both in terms of professional roles and geographical coverage, could reinforce the generalizability of the findings. Comparative case studies across different national or cultural contexts would also be valuable, as they could reveal how leadership characteristics in managing cyber risks vary depending on organizational culture, regulatory environments, or societal expectations.

In conclusion, while the methodological choices of this study provided a strong foundation for exploring the intersection of leadership and cybersecurity in the telecommunications sector, acknowledging its limitations is important for contextualizing the results and pointing the way toward future research that can build on these findings.

CHAPTER 5.

RESULTS

5.1 Overview of the Main Findings

The ten interviews provided valuable insights into the risks and challenges that today's telecommunications companies face in the realm of digital transformation and cybersecurity. They offered a clearer understanding of the rapidly evolving environment, in which new technologies emerge alongside new risks, highlighting the challenges of continuous rapid innovation, particularly for telco companies, and the critical necessity of keeping pace to remain competitive. They also underscored a crucial aspect that served as the starting point of this research: the identification of human error as one of the greatest risks in cybersecurity, and the pivotal role of leadership in fostering a culture of cyber awareness capable of protecting and safeguarding telecommunications companies.

Moreover, the interviews contributed to answering the research question regarding the leadership characteristics that today's leaders in the telecommunications sector need to effectively manage cyber risks in the context of digital transformation, therefore underlining which characteristics enhance organizational resilience to cyber threats. The interviewees identified traits previously discussed in the literature, as well as new characteristics that have become increasingly relevant in the context of cybersecurity and digital transformation. The participants included leaders in various roles: CEOs and one board member responsible for overall strategy and management direction in telco companies; CISOs and CTOs directly managing cybersecurity strategies; and experts from ACN coordinating and implementing national cybersecurity strategies while providing insights into telco cybersecurity risks and their impacts. The diversity of these backgrounds shed light on multiple perspectives, offering a comprehensive understanding of what is required today to be a leader in cyber risk and providing relevant data to support the definition of the characteristics necessary to foster cybersecurity awareness and make telco companies more cyber-resilient.

Thanks to these contributions, and recognizing a gap in the literature that does not yet address the emergence of cyber risk leadership, a new model of leadership can be proposed, one that departs from current frameworks, which often consider leadership in digital transformation but overlook the cyber risk dimension.

To better visualize the results obtained in the interviews, two tables were created: one summarizing risks in the cybersecurity era, and the other outlining the main leadership characteristics. As mentioned in the methodology chapter, I applied a thematic frequency analysis, considering only concepts that appeared at least twice across the dataset to maintain analytical consistency. The main results, along with the number of times they recurred in the interviews, are summarized in the following two tables:

Table 5.1 Risks In The Cybersecurity Era.

RISKS IN THE CYBERSECURITY ERA	**FREQUENCY**
Frequency of Cyberattacks	10
Employee Awareness/ Human Error	10
Cyberthreat Evolution	9

Digital Interconnectivity	8
Regulatory Compliance	6
Breach Impact	5
Lack of Skills	3
Big Tech Competition	2

Table 5.2 Leadership Characteristics

LEADERSHIP CHARACTERISTICS	FREQUENCY
Rapid Decision-Making	10
Multitasking	6
Effective Crisis Communication	10
Empathy	6
Ability to Delegate	4
Continuous learning	6
Digital and Cybersecurity Literacy	10

Calmness Under pressure	5
International Experience	8
Open-mindness	7
Ability to Navigate Uncertainty	10
Adaptability	6
Strategic Foresight	5
Collaboration	4
Risk-awareness	10
Visibility and Accessibility	4

Table 5.1 summarizes the primary risks associated with operating in the digital and cybersecurity era, as identified by the interviewees. These risks and challenges were crucial for understanding the business environment in which leaders must operate, highlighting threats not only from technological advancements but also from human error, and emphasizing the role of leaders in raising employee awareness. At the same time, the interviews helped identify which risks are more widely shared among personnel in telco companies. Understanding these risks set the stage for identifying the leadership characteristics best suited to address and manage these challenges.

As shown in Table 5.2, the interviews revealed a set of leadership characteristics that were particularly relevant for addressing the research questions. These traits arose not only from direct questions about leadership characteristics but also throughout broader conversations exploring other dimensions. Some of these characteristics, as visible in the table, recurred across all interviews, highlighting their consistency and underscoring the importance of specific leadership requisites.

To analyze the interview results systematically, two separate sections will follow: one focused on the main risks of the cybersecurity era, and the other on the key leadership characteristics. The next section will examine the primary risks to contextualize the environment in which today's leaders operate, helping to explain why certain leadership traits have emerged and what factors drive their development. During the interviews, participants were asked: *"What are the main risks that telecommunications companies face in relation to digital transformation and cybersecurity?"* This question aimed to gauge awareness of digital and cyber risks, exploring what leaders perceive as the greatest threats and what cybersecurity experts, such as CISOs, CTOs, and ACN professionals, consider critical. Participants were also asked: *"What, in your opinion, are the main challenges for leaders today with regard to cyber risk management?"* This sought to identify challenges not only for the organization but also for leaders themselves, revealing the leadership characteristics required to navigate these risks effectively.

The second paragraph focuses on the main leadership characteristics, as identified through questions such as: *"How important is leadership in building a culture of cyber awareness and prevention? What characteristics are generally required of contemporary leaders to navigate these challenges? How have digital technologies and cyber threats changed what is expected from today's leaders in the telecommunications sector compared to leaders of the past? To what extent is* *cybersecurity reshaping leadership traits? And what suggestions would you give to enhance the ability of today's leaders to manage cyber risks?"*

These questions were instrumental in establishing the relevance of this study by highlighting human error as a key factor in cyber risk management and emphasizing the crucial role of leaders in mitigating such errors. They also guided the exploration of leadership characteristics directly related to the risks identified during the interviews, illustrating how cybersecurity challenges influence the expectations and behaviors of modern leaders. By addressing the evolution of leadership in response to emerging risks, the questions enabled a comparison with classical leadership models, highlighting differences in traits and approaches shaped by contemporary contexts and the specific pressures faced by today's telecommunications leaders.

An additional focus of these questions was to uncover challenges in developing effective cyber risk leadership, including inquiries such as: *What are the main challenges in cultivating this type of leadership? Where do current leadership practices fall short in the telecom sector?* These prompts revealed gaps in current leadership capacities and provided insights into what is still required for leaders to manage cyber risks effectively, offering valuable guidance for future leadership development initiatives.

It is important to emphasize that the findings presented here are drawn directly from the interviews, including participant quotes and examples, which corroborate the coding choices and provide richer context. These firsthand insights illustrate not only the leadership traits deemed essential by experts but also practical experiences and perspectives that shape effective leadership in managing cybersecurity challenges. By grounding the analysis in empirical evidence, this section demonstrates how leadership must evolve in response to both technological and human factors, offering a nuanced understanding of the competencies needed to strengthen cyber awareness and organizational resilience in telecommunications.

5.1.1 Main Risks In The Cybersecurity Era

Among the most significant risks faced by telecommunications companies in the cybersecurity era, all interviewees consistently highlighted the frequency and intensity of cyberattacks. One CEO shared a striking account: *"My company experiences over 100 attacks per day. It's a lot, and every time you never know if you are safe".* This testimony reflects the heightened vulnerability of telcos, which are increasingly targeted due to the critical role they play in national and international infrastructure.[335]

Data provided by ACN experts further contextualized this threat, citing the *Operational Summary for the First Semester of 2025* on cyber risks in Italy. In the first half of 2025 alone, 1,549 cyber events were identified, representing a 53% increase compared to the same period in 2024.[336] Of these, 346 incidents had a confirmed impactful effect, nearly double (+98%) from the previous year. June 2025 marked an unprecedented peak, with 433 cyber events registered, a 115% increase compared to June 2024, making it the most intense month ever recorded.[337] Particularly concerning was the sharp rise in Distributed Denial of Service (DDoS) attacks, which jumped from 336 incidents in early 2024 to 598 in 2025 (+77%).[338] During this period, telco companies ranked third most targeted sector, after local and central public administrations.

[335] Cardenes, W. (2025, August 28). *National Critical Infrastructure*. Enea. Securing National Critical Infrastructure

[336] Agenzia per la Cybersicurezza Nazionale. (2025). *Operational summary: First semester 2025 [Report].* https://www.acn.gov.it/portale/w/operational-summary-1-semestre-2025

[337] Ibidem.

[338] Ibidem.

A particularly noteworthy insight emerging from both ACN experts and company executives was the prevalence of spear phishing attacks. Unlike general phishing campaigns that target large numbers of individuals with generic messages, spear phishing is highly personalized.[339] It involves extensive reconnaissance by attackers to craft emails that appear authentic and trustworthy, exploiting social engineering techniques to deceive specific individuals or organizations. The ultimate aim is to steal login credentials, financial information, or to trick victims into downloading malware, often by creating a false sense of urgency or familiarity.[340]

Both CEOs and cybersecurity officers (CISOs and CTOs) stressed that companies, particularly larger ones, are inundated daily with dozens of phishing attempts, ransomware threats, and fraudulent communications. As interviewees emphasized, the larger the organization, the greater the difficulty in maintaining oversight and ensuring effective detection. This reality underlines the necessity for leaders and employees alike to develop the capacity to recognize, prevent, and respond to these sophisticated and persistent threats.

The evolution of cyberthreats emerged as another major concern, with interviewees stressing the growing sophistication of hacker techniques. Several noted the increasing use of deepfake voice messages and advanced social engineering strategies. The CEO of a major Italian telecom company remarked: *"There are plenty of videos of me on YouTube. It is very easy for a hacker to send a voice message replicating my voice and asking for money or a specific code or password."* Similarly, leaders highlighted how fake emails are becoming almost indistinguishable from legitimate communications, making detection ever more challenging.

[339] Check Point Software. (2025, March 24). *What is spear phishing?* What is Spear Phishing?

[340] Ibidem.

ACN experts drew particular attention to the accelerating use of Artificial Intelligence and Machine Learning in cyber operations. These technologies allow threat actors to automate attacks, refine phishing techniques, and enhance cyber-espionage activities.[341] The threat landscape increasingly resembles strategic, militarized cybercrime, with pro-Russian hacker groups coordinating through gamified and incentivized campaigns that resemble military logic more than traditional cybercrime.[342]

Adding to this complexity, a CISO emphasized the challenge of delayed detection: breaches often occur unnoticed and are discovered only after significant time has passed—sometimes too late to prevent serious damage.

Despite the sophistication of external threats, interviewees agreed that the human factor remains the greatest vulnerability. As the board member explained: *"Employees answer emails that may raise suspicion, but because they are unaware of the consequences, they respond."* ACN experts echoed this point, stressing that most successful breaches occur because employees inadvertently enable them: *"The human factor is a huge risk, as it is the one that opens the door to the hackers."*

All participants emphasized the critical responsibility of leaders and boards to address this issue by cultivating a strong culture of cyber-awareness. Continuous vigilance, employee training, and awareness programs were seen as essential to reducing human error and strengthening organizational resilience against evolving threats.

[341] World Economic Forum. (2025). *Global cybersecurity outlook 2025 (in collaboration with Accenture).* https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[342] Aljazeera (2025, July 16). *Joint global operation takes down pro-Russian hacking group. Al Jazeera.* https://www.aljazeera.com/news/2025/7/16/joint-global-operation-takes-down-pro-russian-hacking-group

Digital interconnectivity was mentioned by eight interviewees in different contexts. Participants emphasized that interconnected devices, networks, and services significantly increase potential entry points for cybercriminals. Technologies such as the Internet of Things (IoT), 5G, and cross-border connectivity further complicate network security.[343] Telcos, in particular, depend heavily on external vendors for hardware and software solutions, ranging from routers and switches to cloud services, meaning that a vulnerability in a partner's system can compromise entire infrastructures. Interconnectivity also facilitates the rapid spread of malware, ransomware, or distributed denial-of-service (DDoS) attacks. A single breach in one operator's core network can cascade to roaming partners, amplifying the impact.[344] One CEO stressed the challenge of third-party risk management: *"We have more than a thousand vendors across Italy—imagine ensuring each of them is safe and keeping control of all of them."*

Regulatory compliance was highlighted by six interviewees, who noted the growing weight of legal obligations and breach reporting requirements. For telcos, compliance with EU regulations is particularly demanding. As ACN experts explained, operators are required to notify competent authorities in the event of a data breach, with failure to do so resulting in sanctions. Key instruments include the ePrivacy Directive 2002/58/EC, Commission Regulation (EU) No 611/2013, and the General Data Protection Regulation (GDPR), all of which establish strict deadlines for reporting. Failure to respect these deadlines can lead to substantial fines.

[343] Carter, E. (2025, August 1). *5G Security Risks 2025: Mitigation Plan.* Online Hash Crack. https://www.onlinehashcrack.com/guides/cybersecurity-trends/5g-security-risks-2025-mitigation-plan.php

[344] An example of coordinated cyberattacks by threat actors is the "Salt Typhoon" campaign, which targeted major U.S. telecommunications companies in 2024. This sophisticated cyber-espionage operation, attributed to a Chinese state-sponsored group, compromised critical network infrastructure of firms such as Verizon, AT&T, T-Mobile, and Lumen Technologies. The attackers exploited vulnerabilities in routers and switches to gain access to sensitive metadata and wiretapping systems, posing significant national security risks. Such incidents highlight the escalating complexity and strategic nature of cyber threats facing the telecommunications sector. Ribeiro, A. (2024). *US Congressional Research Service reports on PRC state-sponsored Salt Typhoon hacks on telecoms*. Industrial Cyber. https://industrialcyber.co/threat-landscape/us-congressional-research-service-reports-on-prc-state-sponsored-salt-typhoon-hacks-on-telecoms/

A further complication, as underlined by ACN experts, is that breaches are often detected months after they occur, giving attackers extended time to remain hidden within systems and extract sensitive data. This delay not only escalates the damage caused but also makes compliance with reporting deadlines even more challenging, underscoring the dual difficulty of managing both technical and regulatory dimensions of cybersecurity.

The impact of cyber breaches, spanning economic, operational, and reputational risks, was highlighted by five participants. One CEO recounted a recent ransomware incident in which attackers infiltrated systems undetected, causing prolonged internal damage before eventually demanding a ransom. Although the specific amount was not disclosed, the CEO described it as substantial. Such incidents illustrate the severe financial strain breaches can impose. Supporting this, ACN estimates place the economic impact of cybercrime in Italy at over €66 billion by 2025, equivalent to approximately 3.5% of national GDP, with projections rising to €160 billion by 2026.[345] These figures underscore the escalating threat that cyberattacks pose to both businesses and the broader economy.

A smaller number of interviewees, two in total, raised the issue of competition from big tech companies. They noted that telcos increasingly face challenges from lightly regulated digital platforms that encroach on their traditional business lines. For instance, services such as WhatsApp, originally designed for messaging, now also offer voice calls, thereby eroding telcos' customer base. Due to their transnational nature, these companies are often not subject to the same EU data protection rules, despite operating with European users. This creates an uneven playing field,

[345] Lirosi, M. (2025). *Cybersecurity in Italy 2025, the threat grows: cyber attacks up 53%, record data breaches, and websites down - FIRSTonline*. FIRSTonline. Cybersecurity in Italy

forcing telcos to compete in an increasingly crowded market where differentiation is both difficult and costly.

5.1.2 Main Leadership Characteristics

Through the thematic frequency analysis of the ten interviews conducted, a set of leadership characteristics emerged as particularly relevant for managing cybersecurity challenges. These traits were synthesized from the terminology used by interviewees into coherent categories while retaining the nuances expressed. For instance, the characteristic "rapid decision-making" encompassed multiple expressions such as "taking decisions in a short time," "decide fast," and "thinking quickly under pressure." As described in the methodology chapter, only elements mentioned at least twice across different interviews were included, ensuring consistency and robustness in the findings. Figure 2 illustrates the frequency of each leadership characteristic and the number of times it emerged across interviews.

The results reveal that all interviewees emphasized the critical importance of rapid decision-making. Leaders are expected to act promptly, particularly during cyber incidents or technological disruptions, where even short delays can significantly escalate risks. An additional nuance that emerged is the necessity of making rapid decisions under conditions of limited information. One CEO explained: *"When cyberattacks happen, you realize you have to prioritize certain actions, put in place a cybersecurity framework and internal policies, and respond quickly—or the problem will escalate."*

This perspective was echoed by other CEOs, a board member, and ACN experts, who stressed that hesitation not only increases technical and operational damage but also intensifies reputational risks. A delayed response can create the perception that a company is unable to detect or resolve problems effectively, undermining trust among customers and stakeholders.[346] As participants noted, such reputational damage is inseparable from financial losses, as it can result in operational breakdowns, reduced competitiveness, and diminished market confidence. Overall, the findings highlight that rapid, informed, and decisive leadership is indispensable in the cybersecurity era, where threats evolve faster than traditional decision-making cycles allow.

Similarly, effective crisis communication was universally cited as a critical leadership trait. Interviewees consistently stressed the importance of being able to "communicate complex topics, such as technical or cybersecurity issues, in a clear and accessible way." Leaders are expected to share information transparently and break down organizational silos, which otherwise hinder timely responses to cyber incidents. CEOs interviewed mentioned that they had taken courses in strategic communication and public speaking to strengthen their ability to convey messages effectively to diverse audiences. Technical experts, such as Chief Information Security Officers (CISOs) and Chief Technology Officers (CTOs), emphasized the need to translate highly technical concepts into language that board members and non-technical colleagues can understand, ensuring informed and timely decision-making.

What emerged across all interviews is the growing necessity for technical roles to be coupled with strong crisis communication skills. For professionals aspiring to leadership positions such as CISO, the ability to articulate risks, explain mitigation strategies, and foster information sharing during crises is increasingly indispensable. This evolution is partly driven by regulatory developments,

[346] CodeHunter. (2025). Cybersecurity incident response: Time is of the essence. Cybersecurity Incident Response

which mandate that companies designate a person responsible for security[347], but also by the recognition that cybersecurity is now a central element of business strategy. As a result, roles like the CISO are no longer confined to technical oversight during incidents; they are increasingly present in the boardroom and actively shape corporate strategies. Effective communication was also regarded as essential for raising employee awareness and fostering a culture of cyber vigilance throughout organizations.

Another universally recognized characteristic was a solid understanding of digital technologies and cybersecurity. ACN experts underscored the need for leaders to stay informed about the latest cybersecurity techniques and evolving regulatory frameworks. CEOs pointed out that awareness of the regulatory landscape is crucial not only for compliance but also for knowing which steps to take when a cyberattack occurs. Beyond regulations, several CEOs highlighted the importance of understanding the different modalities of attacks, both to anticipate threats and to promote a company-wide culture of prevention.

CISOs and ACN experts further emphasized that strong leadership requires the ability to assess risks, detect vulnerabilities, and prioritize remediation strategies. This involves not only technical knowledge but also a deep understanding of the company's core business and its most sensitive assets, those areas where an attack would cause the greatest harm. Leaders must therefore integrate

[347] The European Union's cybersecurity regulations, particularly the NIS 2 Directive and the EU Cyber Resilience Act, place significant cybersecurity obligations on telecommunications companies recognized as essential entities within critical infrastructure. These companies must implement comprehensive cybersecurity strategies and risk management processes. Specifically, the NIS 2 Directive requires telecom operators to deploy security measures aligned with advanced cyber threats, designate a responsible cybersecurity officer, and comply with strict reporting and risk management duties. This directive consolidates various sector-specific laws into a unified regulatory framework addressing cybersecurity responsibilities across sectors in the EU. European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

cybersecurity awareness with strategic foresight, ensuring that protective measures align with both operational needs and long-term business goals.

Interviewees consistently highlighted the importance of accepting unpredictability and making informed decisions even when information is incomplete. One CEO remarked, *"Always be on guard, as something will happen, never feel safe."* This sense of constant vulnerability and the need for continuous prevention and protection was a recurring theme across the interviews. Leaders today, participants agreed, must be able to navigate uncertainty, particularly in a context marked by rapid technological and environmental change.

Closely linked to this is adaptability, which was mentioned six times across interviews. Leaders are expected to adjust strategies, identify alternative solutions, and ensure business continuity in the face of unforeseen circumstances, such as cyberattacks, technological shifts, or external crises. The capacity to remain flexible and respond quickly to emerging challenges was seen as an indispensable trait of effective leadership in the digital age.

Another critical characteristic identified is risk awareness. All interviewees emphasized that leaders must be able to identify, evaluate, and prioritize risks, particularly those tied to cybersecurity and digital transformation. This involves defining a comprehensive cybersecurity strategy that includes establishing internal policies, conducting normative assessments of processes, adopting technologies to monitor and prevent attacks, and investing in employee training. Leaders must consider risks in both technological systems and human behavior, identify vulnerabilities, and address weak points that could expose the company to serious harm.

Finally, strategic foresight was highlighted as essential. This refers to the ability to anticipate future risks and trends and to prepare organizations to mitigate their impact.[348] Participants stressed that effective leaders move beyond reactive management, embedding risk anticipation into their decision-making processes. By incorporating forward-looking perspectives, leaders enable proactive long-term planning, thereby enhancing resilience and ensuring that organizations are not merely defending against present threats but also preparing for those on the horizon.

Open-mindedness was highlighted by seven participants as an essential trait for contemporary leaders, particularly in the context of cybersecurity and digital transformation. Interviewees stressed the importance of welcoming new perspectives, listening to diverse opinions, and engaging constructively with a wide range of stakeholders. This characteristic was closely connected to international experience, which eight participants linked to the ability to operate effectively in multicultural and complex environments. Many interviewees, especially CEOs and CISOs, had extensive professional experience abroad, particularly in the United States, and often across different sectors before entering the telecommunications industry.

Reflecting on this, one CISO explained: *"My international experiences allowed me not only to learn different ways of working and thinking but also to develop a range of soft skills, such as quickly adapting to new environments and languages, and integrating into unfamiliar settings. When I returned, I brought with me a kind of double experience, both professional and personal."* When asked how this shaped his leadership role, he added: *"My international experiences helped me interact with people from different cultures and understand their diverse approaches to work. I learned how to manage and coordinate these differences effectively—an invaluable skill in my*

[348] *Strategic foresight / Trend research readiness*. ITU. Strategic Foresight / Trend Research Readiness

current job." These insights reinforced the idea that exposure to diverse contexts enhances leaders' flexibility, cultural sensitivity, and problem-solving abilities.

Multitasking was another trait emphasized by six interviewees. Leaders in the telco sector are often required to juggle multiple priorities, balancing strategic oversight with hands-on operational responsibilities. One CEO noted: *"The pace of work is very fast, and knowing that we are always reachable, through phone calls and emails, adds pressure. We constantly have to manage multiple tasks at the same time."*

However, interviewees also underlined that multitasking must be paired with the ability to delegate. Leaders cannot handle every responsibility alone; instead, they must trust their teams and rely on others' expertise. Delegation, therefore, emerged as a connected and equally critical trait. As several participants observed, effective leadership in cybersecurity depends not only on managing multiple responsibilities but also on dividing tasks strategically and building trust across the organization.

Another important theme emerging from the interviews was the visibility and accessibility of leaders within the organization. Effective leaders were described as those capable of both "directing from above" and "being present on the ground" with employees. Several participants stressed that remaining confined to an office limits a leader's perspective, whereas engaging directly with staff provides a clearer picture of ongoing challenges and organizational dynamics. One CEO explained that spending time with employees, talking and listening to them, often reveals issues that might otherwise remain unnoticed. Similarly, a CISO emphasized the importance of working on-site rather than remotely, highlighting that in-person presence fosters stronger interaction, trust, and oversight.

This visibility was strongly linked to the trait of collaboration, which four participants identified as essential. Interviewees underlined that collaboration must occur not only within teams but also across departments, requiring leaders to actively support teamwork, dismantle silos, and encourage collective problem-solving. According to participants, leadership in the cybersecurity era cannot rely solely on a hierarchical, top-down approach; rather, it must be inclusive and participatory, strengthening resilience through shared responsibility.

Closely connected to this was empathy, cited by six interviewees. Leaders were described as needing to connect with teams on a personal level, understand their concerns, and provide reassurance during periods of uncertainty or high pressure. Empathy was often mentioned alongside the ability to remain calm under stress, ensuring that leaders not only manage crises effectively but also maintain the trust and confidence of their employees.

Another widely cited characteristic was curiosity and continuous learning, highlighted by six participants. In an environment marked by rapid technological change, leaders must proactively seek knowledge, remain updated on sectoral developments, and anticipate emerging trends. This commitment to learning ensures relevance and adaptability in a constantly evolving landscape.

When asked whether leadership is innate or acquired, all interviewees agreed that, while certain qualities may come naturally, leadership is largely a learned skill developed through experience and growth. Interestingly, however, when questioned about training, most CEOs and the board member admitted they had undertaken only limited formal training, primarily in public speaking, with little directly related to cybersecurity or risk management. Instead, they reported staying informed through newspapers, social media, and personal networks, suggesting that much of their knowledge acquisition remains self-directed and informal.

Composure under pressure was identified by five participants as a fundamental requirement for cybersecurity leadership. Leaders must remain calm, rationally analyze information, and synthesize diverse inputs while projecting stability to their teams. This composure, as one CISO explained, is essential: *“When a cyberattack happens, we must remain lucid and calm, as this helps us make rapid decisions and prioritize what needs to be done.”* Maintaining clarity under pressure enables leaders to inspire confidence and guide their teams effectively through crises.

Alongside composure, continuous innovation and readiness to act swiftly were highlighted as ongoing imperatives. Interviewees repeatedly stressed that leaders must remain vigilant in the face of uncertainty, adapting quickly to evolving threats and technological change. This constant emphasis on uncertainty and evolution reflects the dynamic environment in which leaders operate today.

A recurring theme across all interviews was the evolution of leadership models. Participants observed that earlier leadership styles tended to be more autocratic and top-down, characterized by limited collaboration and minimal employee engagement. By contrast, contemporary leadership in the digital and cybersecurity era prioritizes inclusivity, visibility, and meaningful interaction with teams. This evolution underscores the growing importance of adaptive, communicative, and resilient approaches over rigid or hierarchical ones.

In summary, the findings point to a multi-dimensional leadership model essential for navigating the cybersecurity era. Leaders must combine technical expertise with interpersonal skills, strategic foresight, and operational agility. Certain characteristics, such as composure, effective communication, and rapid decision-making, were unanimously highlighted, while others emerged from at least two interviewees. Together, these traits define a leadership style capable of managing cyber risks, fostering innovation, and safeguarding organizational resilience in an increasingly interconnected and high-risk digital landscape.

5.2 Best Practices for Leadership Development

Other insights from the interviews relevant to this analysis concern best practices and strategies companies use, or would need to use, to support effective leadership while enhancing cyber risk management. One key question posed to interviewees was: *"What suggestions would you give to enhance the ability of today's leaders to manage cyber risks?"*

Respondents consistently emphasized the importance of cultivating leadership skills specifically tailored to the cybersecurity context, providing practical examples of initiatives implemented within their organizations. Several interviewees noted the use of cybersecurity newsletters distributed to all employees to maintain awareness and provide updates on emerging threats and techniques. CEOs and CISOs highlighted the value of regular board-level meetings—weekly or monthly—dedicated to cybersecurity strategy, enabling leaders to remain informed about organizational methods, threats, and mitigation approaches.

While CEOs, board members, and CISOs mostly focused on strategies to enhance cyber awareness among employees, some also addressed leadership development directly. For example, a board member described simulations of phishing attacks and scams for employees to test their responses and subsequently provide targeted training, helping staff recognize and prevent cyber incidents. However, when specifically asked about leadership programs for themselves, one CEO admitted that formal programs were absent, while another emphasized that training programs and practical simulations, often involving mock cyberattacks or crisis scenarios—were particularly effective. These exercises allow leaders to practice decision-making, crisis management, and rapid response in a controlled setting, thereby enhancing both personal leadership capabilities and overall organizational resilience.

Interviewees also discussed the current challenges in developing leaders for cyber risk management. CEOs highlighted a significant skills gap, noting that cybersecurity is increasingly complex and requires specialized expertise. Communication challenges were emphasized, particularly the need for cybersecurity leaders to translate technical information into strategic insights for the business, including risk assessment, operational impact, and economic considerations. Additionally, the growing regulatory pressure within the telecommunications sector was identified as a challenge, requiring leaders to stay informed and compliant while maintaining effective strategic oversight.

These insights collectively suggest that leadership development in the cybersecurity era requires a combination of technical knowledge, practical experience, communication skills, and regulatory awareness, reinforced through targeted training, simulations, and continuous engagement with emerging cyber risks.

Following the ten interviews, a cybersecurity and leadership development expert was consulted to validate the findings and ensure their alignment with current leadership development practices and research. This expert, who oversees training programs and cyberattack simulations for leaders in the cyber risk domain, provided insights based on extensive professional experience. After identifying the main leadership characteristics from the interviews, a validation phase was conducted in collaboration with this expert to confirm the relevance and consistency of the traits with contemporary leadership studies and practical applications. Additionally, participating in one of these cyberattack simulations offered a first-hand perspective on which leadership qualities are most critical in high-pressure scenarios. This process reinforced the robustness of the research and highlighted the practical implications of effective cyber risk leadership.

CHAPTER 6.

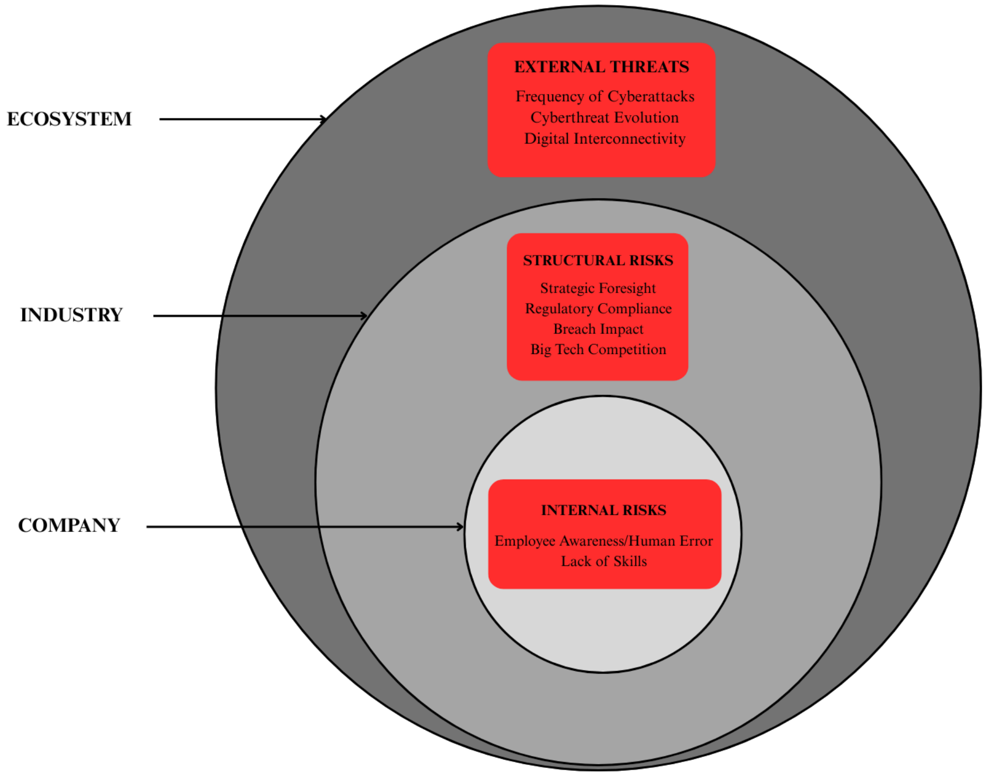
DISCUSSION

6.1 The Complexity of the Cyber Threat Era

The interviews offered valuable insights into how cyber threats are reshaping leadership roles, highlighting the need for a new model of leadership, the *Cyber Risk Leadership*, which specifically addresses the management of cyber threats. As discussed in the previous chapter, existing leadership models fail to fully capture the complexity and transformative impact of cybersecurity challenges. This study thus highlights the importance of recognizing and systematizing leadership traits specific to cyber risk, which is essential for targeted leadership development and designing focused training programs. Existing frameworks often list isolated characteristics without consolidating them into a clear model, making it difficult to translate theory into practice. A structured model not only guides effective leadership development but also aligns these traits with sector-specific risks, a necessity given the rapidly changing threat landscape in telecommunications.

The emergence of new risks related to the cybersecurity era calls for a shift in organizational paradigms, strategy formulation, and managerial decision-making, to enable companies to operate successfully in a complex and rapidly evolving environment. The risks identified from the interviews can be systematized as follows:

Figure 6.1 Risk Dimensions and Key Challenges in the Digital and Cybersecurity Era



Starting from external threats, all interviewees underscored that telecom companies face an overwhelming volume of cyberattacks daily, given their role as managers of critical infrastructure and custodians of vast amounts of sensitive customer data. Frequent cyberattacks require leaders to remain constantly vigilant, anticipate potential breaches, and respond with rapid, well-informed decisions. As one CEO of a telecommunications company highlighted, their organization faces more than 100 attacks every day, a striking figure that illustrates the persistent insecurity of the sector and the necessity of being prepared at all times for potential breaches. Such insights from industry leaders reinforce existing data and future projections, underscoring the urgent need for strong leadership commitment and preparedness in managing cyber risks. Moreover, cybersecurity experts from ACN confirmed a broader awareness that the threat landscape will intensify in the coming years, with cyberattacks projected to increase year after year. Recent authoritative research and sector-specific analyses confirm a steep upward trajectory in the frequency and sophistication of cyberattacks against telecom firms. For instance, Check Point Research's Q2 2025 report highlights telecommunications as one of the three most targeted industries globally, with a 38% year-on-year increase in weekly cyberattacks per organization.[349] EY's 2025 telecommunications risk report likewise emphasizes this sector's expanding threat landscape, driven by geopolitical tensions, regulatory complexities, and the critical nature of telecom infrastructure.[350] Similarly, KPMG's 2025 analysis elaborates on the intensifying threats from both state-sponsored actors and financially motivated cybercriminals targeting telecom firms.[351] These sources collectively affirm that telecom companies inhabit a uniquely high-risk cyber environment that demands tailored, robust risk management strategies.

Another significant global risk, referenced by nine of the interviewees, is the evolving nature of cyber threats.[352] The interviews highlighted the growing sophistication of ransomware, phishing, malware, and AI-driven attacks, as well as the potential future impact of quantum computing on both attack and defense strategies. Leaders must therefore maintain a proactive stance, continuously monitoring threat landscapes and adapting corporate defenses to counter emerging risks. This requires staying informed about the latest technological developments and fostering an organizational culture capable of agile and rapid response.

[349] Check Point Software Technologies Ltd. (2025, July 21). Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions. Check Point Research. Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions

[350] Ernst & Young Global Limited. (2025, January 21). Top 10 Risks for Telecommunications in 2025. EY. Top 10 risks for telecommunications in 2025

[351] KPMG International. (2025). Cybersecurity considerations for Technology, Media & Telecommunications (TMT) companies 2025. KPMG. Strategic Foresight / Trend Research Readiness

[352] Kuzior, A., et al. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal Of International Studies, 17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

Digital interconnectivity was also identified as a major external risk, as companies face not only direct attacks but also vulnerabilities stemming from third-party partners, whose exposure can in turn compromise the companies themselves. This confirmed the literature: recent studies highlight that supply chain management represents a critical challenge for large organizations in achieving cyber resilience.[353] According to the literature, 54% of such organizations perceive supply chain vulnerabilities as the main obstacle to strengthening their cybersecurity posture. This is largely due to the increasing complexity of supply networks and the limited visibility over the security practices of suppliers. Key areas of concern include weaknesses in third-party software and the potential for cyberattacks to propagate throughout interconnected systems, affecting multiple stakeholders within the ecosystem.[354]

While technological advancements, including new cybersecurity tools and emerging solutions such as quantum computing, offer enhanced protective measures, the human factor remains represent ons of the greatest organizational risks, central to effective cyber risk management. Literature consistently highlights that human error accounts for a substantial proportion of cybersecurity incidents, with estimates reaching up to 95% of breaches.[355] This perspective was strongly reflected in the interviews, where respondents recognized employee behavior as one of the greatest sources of vulnerability. In fact, among global risks, employee awareness emerged as the most frequently cited

[353] World Economic Forum. (2025). *Global Cybersecurity Outlook 2025: Insight Report.* Global Cybersecurity Outlook 2025: Insight Report.

[354] Ibidem

[355] Ibidem

concern, standing out as one of the most critical vulnerabilities. This aligns with recent cybersecurity research, which increasingly recognizes the human factor as a principal risk vector.[356]

For instance, the 2025 Fortinet[357] and SANS Institute[358] reports underscore that a significant portion of cyber incidents stem from human error or lack of security awareness, making continuous and behaviorally relevant employee training indispensable to organizational security posture. Interviewees emphasized that a significant proportion of cyber incidents originate from employee actions, such as failing to update passwords, responding to phishing emails, or engaging in unsafe digital practices. Several participants shared data from internal phishing simulations, which measure employee responses to simulated cyberattacks. For instance, one CEO noted that five years ago, the rate of employee responses that could compromise security was approximately 50%; this rate has now dropped to 5% due to increased training and awareness, yet it still represents a critical vulnerability. These findings reinforce the thesis's emphasis on the human factor as a central element in designing effective cyber risk management strategies and reveal that while technical controls are essential, cultivating informed, vigilant employees through effective security awareness programs is critical to preventing cyberattacks, a theme that has only recently gained more prominence in cyber risk literature.

The interviewees consistently emphasized the crucial role of leaders in cyber risk management strategies, reinforcing the idea that the human factor is fundamental to effective mitigation of cyber threats. Their responses to questions about the importance of leadership in this domain were

[356] Interesting is also this perspective that considers the human factor as both threat and opportunity. Colabianchi, S., Costantino, F., et al. (2025b). *Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. Journal of Innovation & Knowledge*, *10*(3), 100695. https://doi.org/10.1016/j.jik.2025.100695

[357] Fortinet. (2025). 2025 Global Threat Landscape Report. Fortinet. 2025 Global Threat Landscape Report

[358] SANS Institute. (2025). SANS 2025 SOC Survey. SANS Institute. SANS 2025 SOC Survey

overwhelmingly positive, underlining that leadership commitment not only determines the prioritization of cybersecurity initiatives but also shapes organizational culture by embedding cyber risk awareness across all levels of the company. Leaders are therefore expected to actively promote cybersecurity awareness, provide continuous training, model best practices, and communicate the importance of digital hygiene consistently. This finding is consistent with recent expert analyses, such as the *Gartner Leadership Vision for 2025*, which stresses that executive involvement, from CEOs to board members, is essential to position cybersecurity as a strategic business enabler rather than a purely technical safeguard.[359] Engaged leadership fosters proactive decision-making, ensures appropriate resource allocation, and cultivates a culture of security awareness, all of which are key to strengthening organizational resilience. Thus, the evidence underscores that the human element, and particularly leadership, remains pivotal in managing cyber risks in today's complex technological environment.

One of the most pressing organizational challenges highlighted by the ANC experts is the critical shortage of skills in cybersecurity and digital literacy. As emphasized by the World Economic Forum, the cybersecurity industry is facing a global shortfall of nearly four million professionals, a gap that continues to widen each year as demand for qualified practitioners grows.[360] This shortage is not confined to one sector or region but affects nation-states and industries worldwide, with projections indicating that by 2030 the global talent gap could surpass 85 million workers, potentially resulting in $8.5 trillion in unrealized annual revenue.[361] Such figures underscore the urgency of the issue: at a time when cyberthreats are becoming increasingly sophisticated and

[359] Gartner, Inc. (2025, January 13). Gartner Leadership Vision for 2025: Security and Risk Management by Tom Scholtz and Lisa Neubauer. Absolute Software. Key Imperatives for SRM Leader in 2025 by Gartner®

[360] World Economic Forum. (2024). *Strategic Cybersecurity Talent Framework. World Economic Forum.* Strategic Cybersecurity Talent Framework

[361] Ibidem.

frequent, organizations are left dangerously understaffed, undermining their ability to safeguard digital infrastructures and harness the benefits of the Fourth Industrial Revolution. The lack of skilled professionals in this field not only exposes organizations to heightened vulnerabilities but also jeopardizes economic growth and innovation. Addressing this talent crisis is therefore not optional but a strategic imperative, requiring decision-makers to invest in cybersecurity education, workforce development, and long-term talent management strategies.

Turning to the analysis of structural threats, regulatory pressure emerged as a significant challenge highlighted by most interviewees, particularly in regions such as the European Union. Here, the continuous evolution of cybersecurity and data protection frameworks compels organizations to navigate a complex landscape of compliance obligations while simultaneously managing operational risks. Companies are thus required to strike a delicate balance: ensuring adherence to stringent regulatory standards without undermining efficiency, innovation, or competitiveness. While regulatory demands affect many sectors, they represent a distinct risk for telco companies, given their role as critical infrastructure providers, their handling of vast volumes of sensitive personal data, and their reliance on complex cross-border networks that are subject to multiple regulatory regimes. Leaders must integrate regulatory requirements into strategic planning and decision-making processes, balancing legal obligations with operational efficiency.[362]

The impact of cyber breaches is also a profound structural threat, encompassing reputational, operational, and financial consequences.[363] Multiple interviewees, including CEOs, board members,

[362] EY. (2025). Top 10 risks for telecommunications in 2025. EY. Top 10 risks for telecommunications in 2025

[363] The impact of cyber breaches can be understood as a structural risk because it extends far beyond the immediate technical event. Unlike internal risks such as human error or external risks like malicious attacks, the consequences of a breach unfold within broader economic, regulatory, and technological structures. Its severity is shaped by contextual factors such as the organization's sector, national regulatory frameworks, and interdependencies with other actors in the ecosystem.

and security officers, emphasized that breaches erode public trust, damage corporate credibility, and invite intense regulatory scrutiny. These consequences are well-documented in both recent case studies and industry reports. For example, high-profile breaches at companies like T-Mobile, Optus, and Deutsche Telekom have led to massive data exposures, public backlash, regulatory investigations, and significant remediation costs. The IBM Cost of a Data Breach Report 2025 quantifies the financial impact, with average breach costs rising sharply, stressing the economic imperative for robust cybersecurity measures.[364]

Competition from big tech companies, although mentioned less frequently, represents a significant and growing structural concern for telecommunications firms. Three interviewees highlighted how the agility, innovation, and expansive ecosystems of large technology companies place substantial pressure on telcos to innovate continuously while maintaining robust cybersecurity defenses. Specifically, leaders mentioned cases where messaging platforms and digital services offered by Big Tech are encroaching on core telco activities such as voice communication and customer engagement, effectively disintermediating traditional revenue streams and forcing telcos to rethink their business models. This competitive landscape requires leadership that can foster a culture of innovation, anticipate rapid market shifts, and sustain operational resilience amidst external threats and disruption. Industry analyses echo these concerns, emphasizing that telcos must evolve from pure connectivity providers to technology-driven service innovators, leveraging AI, cloud computing, and 5G to compete effectively. Without such adaptability, telcos risk losing relevance in a digitally converging ecosystem increasingly dominated by Big Tech players.

[364] IBM Security. (2024). Cost of a Data Breach Report 2025. IBM. Cost of a Data Breach Report 2025

The discussion of risks, categorized as external, internal, and structural, provides essential context for understanding the complexity of an era characterized by rapid technological development and pervasive cyber threats. In this environment, innovation is constant, but so are risks. Analyzing these risks offers a clear perspective on the challenges faced by telecommunications companies within the global cybersecurity landscape, highlighting both the opportunities and the negative consequences associated with digital transformation.

The three dimensions of risk place leaders in a particularly challenging position, requiring the ability to harness technological evolution, manage associated risks, and promote organizational innovation while ensuring resilience. This risk analysis serves as a foundation for the next section, which introduces the leadership characteristics necessary to manage cyber risks and to develop a new leadership model, termed *Cyber Risk Leadership*. By directly linking these risks to leadership traits, this research addresses an intersection that is rarely explored in current leadership studies.[365]

6.2 The Cyber Risk Leadership Model

As discussed in Chapter 3, the literature on leadership presents a wide range of models. However, these frameworks prove insufficient for addressing the challenges posed by cyber risk. This limitation stems largely from the fact that many classical leadership theories were developed prior to, or at the early stages of, the Fourth Industrial Revolution and therefore reflect different priorities. More recent approaches place greater emphasis on digital innovation and the ability of leaders to leverage digital opportunities, yet they still tend to overlook the critical dimension of cybersecurity and the unique demands it entails. While certain traits identified in existing leadership theories also

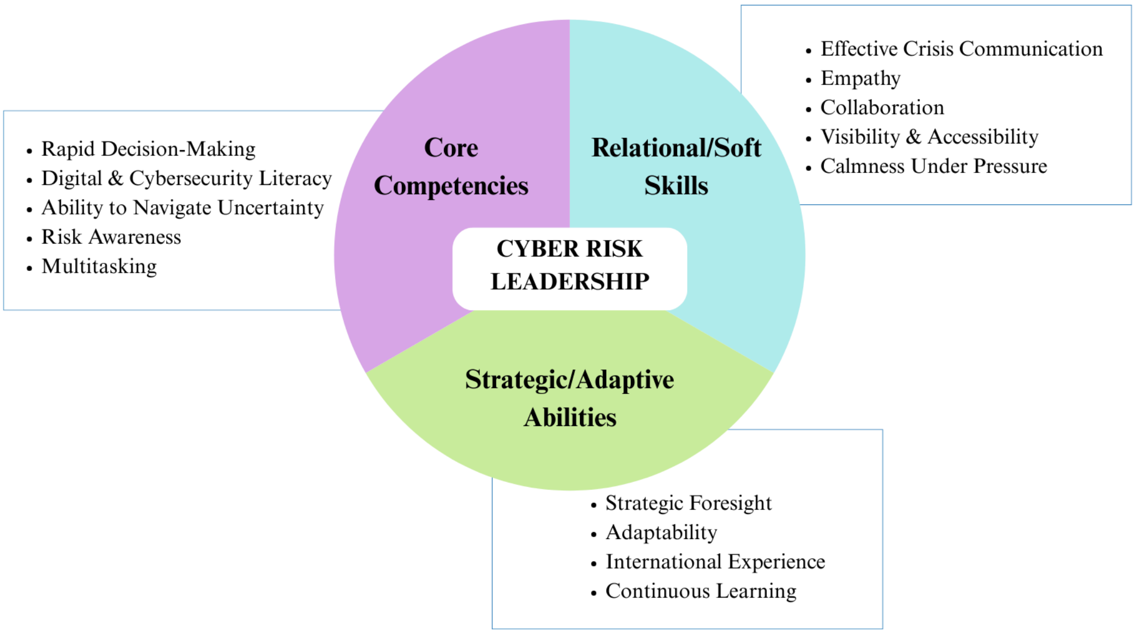
[365] World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

appear relevant in the context of cyber risk leadership, their meaning and significance shift considerably when applied to risk management, reflecting the distinctive requirements of today's rapidly evolving digital environment.[366]

The risks and challenges faced by telecommunications companies, as outlined in the previous paragraph, act as powerful push factors driving the development of new skills and competencies that were not previously required of leaders. These findings underscore the need for a leadership framework specifically designed to address the realities of cyber threats. In this sense, the Cyber Risk Leadership Model takes shape directly from the risks that emerged in the interviews: the vulnerabilities and pressures identified by practitioners reveal the gaps in existing approaches and point to the capabilities that leaders must now develop. The model is therefore not an abstract exercise but a context-sensitive framework rooted in empirical evidence, one that both incorporates elements of established leadership styles and extends beyond their traditional boundaries. At the same time, the findings highlight new dimensions and interpretations of leadership qualities that remain largely absent from current literature. Together, these insights provide the foundation for a comprehensive model that articulates the competencies and behaviors required to navigate uncertainty, manage rapid technological change, and confront the complex organizational challenges posed by cybersecurity. As was done previously for the risks of the digital and cybersecurity era, the key characteristics of cyber risk leadership emerging from the interviews can be systematically organized as follows:

[366] Le Thi Bich Tram, & Nguyen Chau Bich Tuyen. (2025). *Transformation of traditional to modern leaderships in the VUCA environment. Journal of Business Review*, 10(3). https://doi.org/10.26668/businessreview/2025.v10i3.5325

Figure 6.2 Cyber Risk Leadership Model: Dimensions and Competencies


CYBER RISK LEADERSHIP
Core Competencies
Relational/Soft Skills
Strategic/Adaptive Abilities
• Rapid Decision-Making
• Digital & Cybersecurity Literacy
• Ability to Navigate Uncertainty
• Risk Awareness
• Multitasking
• Effective Crisis Communication
• Empathy
• Collaboration
• Visibility & Accessibility
• Calmness Under Pressure
• Strategic Foresight
• Adaptability
• International Experience
• Continuous Learning

Starting from the analysis of the core competencies in the context of cyber risk leadership, the interviews strongly emphasized that cybersecurity literacy, rather than general digital literacy, represents a fundamental competency. While prior literature on digital-era leadership tends to highlight broad digital skills or familiarity with data analytics, it rarely considers the need for leaders to understand cybersecurity concepts, incident response protocols, or international regulatory frameworks. This finding marks a significant departure from existing models: leaders are not expected to become technical experts but must acquire sufficient knowledge to guide organizational responses, make informed strategic decisions, and communicate effectively across both technical and non-technical domains. The growing complexity of the cyber landscape means that sustained engagement with cybersecurity issues, through continuous learning and strategic awareness, is indispensable.

The interviews also revealed risk awareness as a defining trait. Unlike standard leadership theories, which often stress risk-taking or innovation as desirable qualities, cyber risk leadership requires a more cautious and informed orientation. Leaders must develop a deep understanding of potential threats, geopolitical dynamics, regulatory pressures, and organizational vulnerabilities. Staying informed, whether by reading specialized reports, participating in industry briefings, or consulting with experts, was consistently highlighted as central to maintaining this awareness. This dimension goes beyond the innovation-driven focus of many digital leadership frameworks, reframing leadership around vigilance and anticipation of risks rather than only opportunity-seeking.

Equally critical are rapid decision-making and multitasking under conditions of uncertainty. Traditional models such as transformational or adaptive leadership acknowledge decisiveness and flexibility but seldom explore the pressures of operating with scarce, fragmented, or rapidly changing information. The interviews conducted in this study, but also the participation in the cyber attacks simulation, confirmed that leaders facing cyberattacks must act quickly, prioritize business-critical assets, and coordinate multiple tasks simultaneously, often in the absence of full visibility. This situational demand, absent from much of the leadership literature, underscores the need for cognitive agility and composure under pressure. It also highlights the importance of balancing innovation with precaution, a nuance often overlooked in frameworks that prioritize entrepreneurial or opportunity-driven approaches.

An interesting interpretation of the findings is that external threats, such as the high frequency of cyberattacks, the constant evolution of threats, and increasing digital interconnectivity, can be understood as push factors shaping the core competencies required of leaders in the telecommunications sector. These risks appear to drive the need for rapid decision-making, stronger cybersecurity literacy, and heightened risk awareness. For instance, the escalation of sophisticated attacks seems to compel leaders not only to make quick, high-stakes decisions under uncertainty but also to acquire sufficient technical understanding to guide coordinated organizational responses. In this sense, external threats may be seen as directly influencing the emergence of leadership competencies that extend beyond traditional models and reflect the specific demands of cybersecurity.

Beyond technical competencies, the interviews made clear that relational skills are indispensable for effective cyber risk leadership. Among these, effective communication emerged as one of the most frequently cited traits, consistent with both classical and contemporary leadership theories. Yet the interviews and participation in cyberattack simulations underscored an important nuance absent from much of the literature: the critical role of crisis communication. Unlike charismatic communication, which often focuses on inspiration and persuasion, crisis communication requires the ability to translate complex technical information into simple, clear, and actionable messages under intense time pressure. This capacity to reduce complexity while maintaining credibility proved decisive for managing cyber risk effectively.

The interviews also revealed the importance of delegation, trust, and collaboration. Leaders in the telecommunications sector cannot rely on dominance or unilateral decision-making, as such approaches would weaken resilience and undermine the cross-functional teamwork required to counter cyber threats. At the same time, the findings suggest that cyber risk leaders are not fully participative in the traditional sense: while they listen, engage, and communicate with teams, they retain a strong central responsibility for guiding the organization and do not delegate strategic decision-making to all employees. This positions cyber risk leadership closer to participative models[367] than to laissez-faire leadership, but with a distinct emphasis on cross-functional coordination and accountability at the top.

[367] Bass B.M., Stogdill R.M., (1990). *Handbook of Leadership: Theory, Research, and Managerial Applications*, 3rd ed., New York: Free Press.

A further skill highlighted by the interviews, and largely absent from leadership literature, is calmness under pressure. In high-stakes cyber incidents, the leader's ability to remain composed directly influences the organization's collective response, preventing panic, fostering trust, and enabling effective crisis management. This relational quality reinforces other competencies such as crisis communication and trust-building, while also distinguishing cyber risk leadership from the other models that do not account for sustained high-stress environments.

Taken together, these relational traits resonate with aspects of transformational leadership, which emphasizes motivating teams, fostering trust, and guiding organizations through uncertainty and change. However, the findings also indicate a shift toward a more servant-oriented dimension, where leaders prioritize empathy, visibility, and accessibility. Several CEOs interviewed stressed the importance of being physically present among employees, engaging actively across levels of the organization. This “hands-on” leadership style not only strengthens decision-making but also reduces misinformation and silos—an insight rarely explored in digital-era leadership studies. Ultimately, while existing models capture fragments of these traits, they remain too abstract or generic to fully address the relational demands of managing cyber risk in the telecommunications sector.

Just as core competencies can be interpreted as responses to external threats, relational and soft skills may be seen as emerging in response to internal risks. Challenges such as low employee awareness and the lack of technical expertise within organizations act as push factors that shape the demand for communication, empathy, and delegation in leadership. These vulnerabilities demonstrate that technical measures alone are insufficient; leaders must also address the human dimension of cybersecurity. For instance, when employees are prone to errors due to limited awareness, leaders need to translate complex concepts into simple, actionable guidance and cultivate a culture of shared responsibility. Likewise, in contexts marked by skill shortages, effective delegation and trust in specialized teams become vital for maintaining resilience. In this sense, internal risks drive the development of people-centered leadership competencies, complementing the more technical and strategic capabilities that external threats necessitate.

In addition to technical competencies and relational skills, the ability to think strategically and adaptively emerges as a defining characteristic of cyber risk leadership. Unlike traditional leadership models that primarily emphasize authority, vision, or motivation, the leaders interviewed in this study revealed a nuanced perspective: cyber risk leadership requires both keeping pace with innovation and simultaneously safeguarding organizations from its unintended negative impacts. This dual responsibility underscores the importance of strategic foresight, adaptability, international exposure, and continuous learning as indispensable competencies in the telecommunications sector.

Strategic foresight was among the most emphasized attributes across interviews with CEOs, CTOs, and CISOs. Unlike mere adaptability, which implies reacting to change once it has already occurred, foresight requires anticipating emerging threats, identifying early signals of disruption, and proactively designing strategies before risks materialize. Several interviewees highlighted how anticipating regulatory shifts or predicting the geopolitical consequences of cyberattacks allowed them to prepare their organizations more effectively than competitors who responded only after crises unfolded. This finding reflects a marked departure from conventional leadership literature, where foresight is often underexplored or presented in abstract terms. In the cyber context, foresight becomes an operational necessity rather than a theoretical ideal, enabling leaders to design resilient systems, plan crisis responses, and minimize the business and societal costs of cyber disruptions.

Equally significant is the role of adaptability, which complements foresight by equipping leaders to respond effectively when events do not unfold as predicted. The cyber environment is inherently uncertain, characterized by rapid technological change, constantly evolving attack vectors, and a regulatory landscape in flux. Leaders therefore require the agility to pivot strategies in real time, mobilize resources under pressure, and reassess priorities as circumstances evolve. The impact of major breaches, for example, has shown how rigid organizational structures often fail under stress, while adaptive leaders who can reorganize teams, communicate priorities clearly, and shift focus to critical assets are far more effective in mitigating damage. Adaptability thus bridges the gap between planning and execution, reinforcing leadership as a dynamic practice rather than a static role.

Another notable finding from the interviews, not widely reflected in prior literature, is the value of international experience and cross-sector exposure. Many of the executives interviewed had worked across multiple countries or industries before joining telecommunications, and they identified this diversity of experience as a major factor in their ability to lead effectively in cyber contexts. International exposure broadens cultural competence, enhances sensitivity to global regulatory variations, and strengthens leaders' ability to navigate interconnected markets. For instance, understanding how data protection frameworks differ between the European Union and Asia was cited as essential for anticipating compliance challenges and designing consistent global strategies. Unlike earlier leadership models, which often prioritized deep expertise within a single domain, modern cyber leaders benefit from diverse professional trajectories that equip them to evaluate risks through multiple lenses and coordinate across cultural and regulatory boundaries.

The theme of continuous learning also emerged strongly across interviews, reflecting both humility and an awareness of the rapidly evolving threat landscape.[368]Leaders emphasized that cybersecurity cannot be mastered once and for all but requires ongoing engagement with new knowledge, emerging technologies, and evolving threats. This perspective challenges the "traits theory" of leadership, which often frames effectiveness as rooted in innate characteristics such as charisma or decisiveness. By contrast, interviewees stressed that while natural predispositions such as curiosity or strong communication skills provide advantages, the most critical competencies can and must be cultivated over time. Continuous learning, in this sense, is not only about personal growth but also about shaping organizational culture. Leaders are responsible for creating opportunities for employee development, investing in training programs, and fostering environments where knowledge-sharing is encouraged.[369] This participatory, knowledge-driven approach marks a significant evolution from static, hierarchical models toward leadership as an adaptive and collective practice.

These findings also bring to light the temporal dimension of leadership, which is often overlooked in classical models. Traditional frameworks tend to portray leadership as a fixed set of qualities, while the evidence from interviews points instead to an evolving capacity shaped by experience, exposure, and deliberate learning over time. Leaders in the telecommunications sector are constantly required to reassess strategies in response to technological disruptions, shifting market dynamics, and regulatory changes. Their effectiveness lies not in static authority but in agility, the willingness to revise assumptions, and the ability to learn from past events to prepare for future

[368] Eberl, J. K., Drews, P. (2021). *Digital leadership–mountain or molehill? A literature review.* Wirschaftsinformation 2021 Proceedings (pp. 223−237). doi:10.1007/978-3-030-86800-0_17.

[369] Wrede, M., et al. (2020). *Top managers in the digital age: Exploring the role and practices of top managers in rms' digital transformation.* Managerial & Decision Economics, 41(8), 1549–1567. doi:10.1002/mde.3202.

challenges. In this sense, leadership is increasingly a process of continual recalibration, where foresight, adaptability, and learning form a cycle of ongoing development. While these aspects are emphasized in the crisis leadership concept, particularly in the Leadership-As-Practice perspective, that offers valuable insights into the emergence of leadership during crises, traditional crisis leadership frameworks have not been extensively validated for cyber-related events.[370]

Importantly, these strategic and adaptive abilities do not emerge in a vacuum but can be understood as shaped by structural risks that dominate the telecommunications landscape. Regulatory compliance, breach impact, and industry competition act as powerful push factors compelling leaders to cultivate new competencies. For example, the growing complexity of regulations in the European Union requires leaders to engage in strategic foresight, anticipating future compliance obligations and aligning business models accordingly. The severe operational and reputational impacts of breaches, meanwhile, force leaders to become more adaptable, capable of making rapid adjustments in strategy and communication under pressure. Finally, intense industry competition in a globalized market highlights the value of international experience, as leaders must be able to identify opportunities, adapt strategies across borders, and respond to global trends in real time.

Overall, the findings indicate that effective leadership in the cybersecurity era cannot be fully captured by any single classical or contemporary model. While traits from transformational, servant, and participative leadership are evident, the combination of technical knowledge, specifically cybersecurity literacy, strategic foresight, cyber risk awareness, and international exposure represents a set of new characteristics not previously emphasized in leadership literature.

[370] Lehtonen, S., et al. (2025). Rethinking Crisis Leadership through Leadership-as-Practice: A Narrative Review and Future Directions. *International Journal of Disaster Risk Reduction*, 105671. Rethinking Crisis Leadership through Leadership-as-Practice

Additionally, managing cyber risk requires a deep understanding of business priorities and the ability to make informed trade-offs. This emerging model emphasizes vigilance, continuous learning, and the capacity to operate effectively under uncertainty, traits increasingly critical across sectors, particularly in telecommunications.

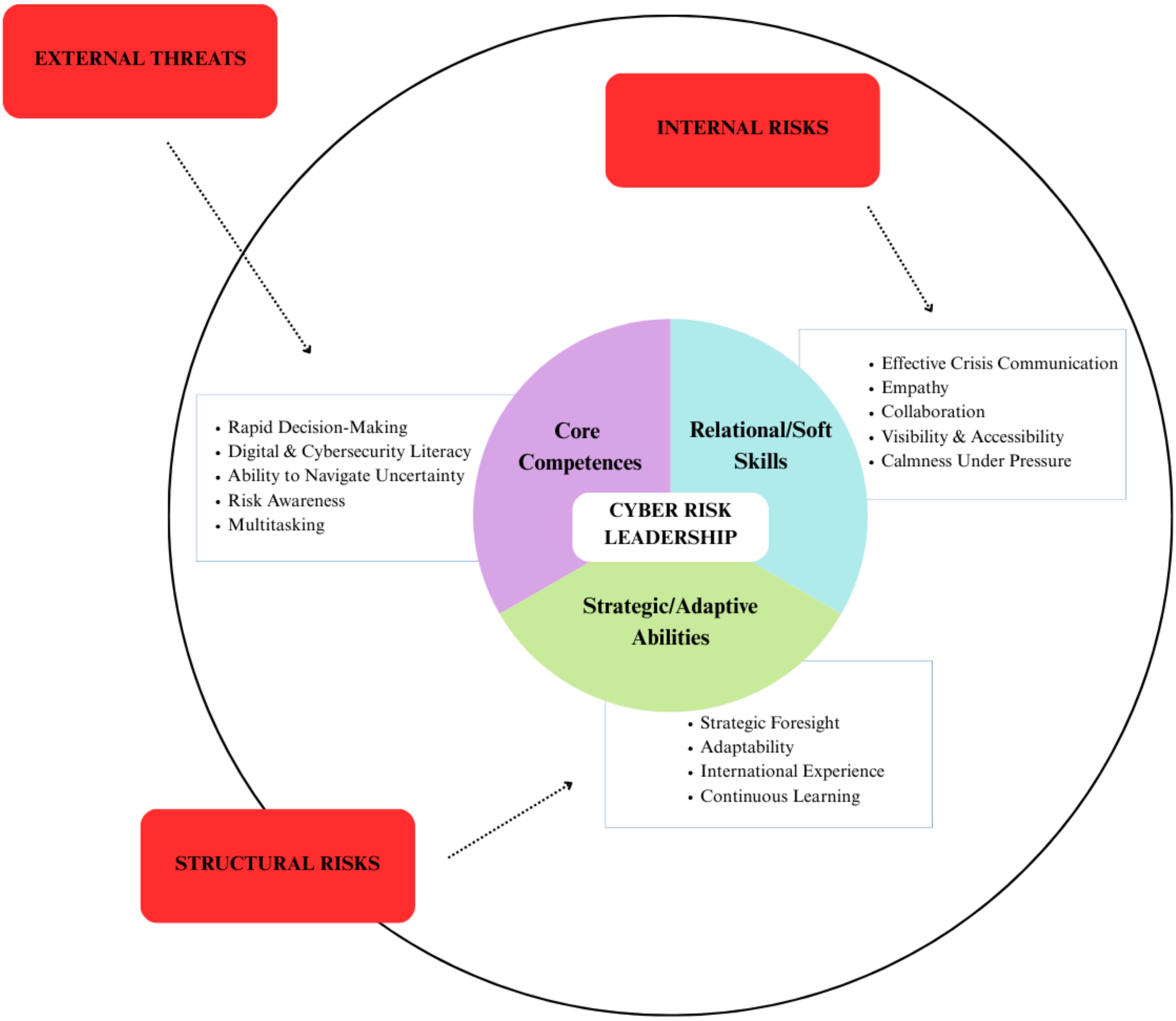
This study advances the literature by providing a systematic and empirically grounded understanding of the leadership traits essential for navigating cyber risks in the telecommunications sector. By synthesizing insights from interviews with executives and cybersecurity experts, it moves beyond generalized discussions of digital leadership or broad organizational competencies, highlighting a nuanced, multidimensional set of characteristics uniquely suited to the challenges of the cyber era. Unlike prior research, which often focuses on regulatory compliance, technical strategies, or employee training, this work emphasizes the human and strategic dimensions of leadership, demonstrating how leaders integrate technical knowledge, risk awareness, adaptability, and people-centered skills to safeguard organizations. By articulating the concept of "cyber risk leadership," the study not only fills a critical gap in scholarship but also provides a practical framework to guide leadership development, support decision-making under uncertainty, and enhance organizational resilience in the face of rapidly evolving digital threats. Its findings underscore the necessity of tailoring leadership approaches to sector-specific contexts, offering actionable insights for both theory and practice.

An important aspect of cyber risk leadership is its strong connection to the specific risks of the cyber era, categorized into external, internal, and structural dimensions.[371] By examining external

[371] This discussion does not imply direct causal links between risks, leadership characteristics, and core competencies. Rather, it highlights patterns of alignment and complementarity, suggesting that certain risks necessitate the adoption of new leadership models and the development of specific skills.

threats such as evolving cyberattacks, internal challenges like low employee awareness and skill gaps, and structural pressures including regulatory requirements and industry competition, this study illustrates how these risks act as push factors that shape the development of leaders' core, relational, and strategic competencies. This linkage, represented in the table below, highlights that effective leadership in the cybersecurity context is not only a matter of personal traits or traditional frameworks but is deeply informed by the very challenges leaders must navigate, driving the emergence of skills tailored to the dynamic, high-risk environment of the digital era.

Figure 6.3 Relationship between Risk Factors and Cyber Risk Leadership Model



6.3 Future Implications for Leadership Development

In addition to introducing a new framework, the Cyber Risk Leadership model, which contributes theoretically to the study of leadership in the cybersecurity era, the findings also carry practical relevance. By identifying key leadership characteristics, this research provides a basis for developing targeted training and capacity-building programs.

One recurring theme that emerged from the interviews was the limited availability, or in some cases the complete absence, of leadership training in the field of cyber risk management. While interviewees consistently highlighted the importance of continuous learning, most noted that their knowledge acquisition was self-directed, often through reading newspapers or independent study, rather than through structured programs. Formal training was more frequently associated with employees, particularly for raising awareness of cyber risks, rather than with leaders themselves. Only one CEO mentioned having participated in a cyberattack simulation exercise designed to reveal gaps and strengthen response strategies.

To further validate these findings, a discussion was conducted with an expert in cybersecurity and leadership development, followed by direct observation of an immersive cyberattack simulation. These experiences were instrumental in substantiating the leadership traits identified in the interviews and in providing deeper insights into the future direction of leadership training in cybersecurity. The simulation exercise brought together CEOs, CISOs, and cross-functional teams, placing them in a high-pressure scenario where each participant assumed specific roles. With limited information and evolving inputs, participants were required to react quickly, prioritize tasks, and make critical decisions under uncertainty.

This type of simulation highlighted the shortcomings in crisis management, demonstrated how different leadership styles emerge under pressure, and underscored the tools and competencies that can best support decision-making in such situations. By replicating real-world challenges in a controlled environment, these simulations serve as valuable tabletop exercises. They not only reveal how leaders interpret complex situations and allocate priorities under stress, but also provide a platform to test, refine, and develop the leadership characteristics essential for effective cyber risk management.

The experience highlighted the critical importance of cross-departmental collaboration and the ability to communicate complex information clearly, even when limited data is available, in order to make timely and effective decisions. The discussion with the cybersecurity expert further emphasized the lack of adequate preparation among today's leaders. Many operate without structured frameworks, facing difficulties in developing and implementing comprehensive cyber risk management strategies. While training initiatives often focus on employees, leadership-specific training remains insufficient and urgently needed.

These findings bring to light aspects that the existing literature has largely overlooked, opening an important discussion on the future of leadership in cybersecurity. The ultimate goal of simulation exercises is to help leaders understand what is required to manage cyber risks effectively. Participants are expected to return to their organizations equipped to design stronger strategies and to promote the creation of targeted training programs specifically tailored to leadership in cyber risk management.

The findings of this research underline the urgent need to strengthen leadership development in the context of cyber risk management. Simulation exercises and expert discussions highlighted how leaders are often required to act with limited information, make rapid decisions, and communicate effectively across departments under pressure. Yet, as several interviewees noted, today's leaders frequently lack structured frameworks for cyber risk management and rely on improvisation rather than established strategies. This gap demonstrates the necessity of targeted leadership training that integrates both technical knowledge and human-centered skills.

This has direct implications for academic institutions and their curricula. Universities and professional academies should move beyond traditional leadership courses to offer programs that actively combine cyber risk management with leadership development. Instead of limiting education to theoretical classes, universities should adopt more experiential approaches, such as workshops, immersive simulations, case studies, and problem-solving exercises. A few institutions in Italy have begun incorporating cyber risk management modules into their programs, but such initiatives remain rare. Expanding these practices, through seminars, internships, and hands-on learning, would better prepare future leaders to face the realities of the digital and cyber era.

A key challenge is balancing technical expertise with soft skills. Leaders, particularly those in future roles such as CISOs or other technical executives, must not only understand cybersecurity concepts but also possess strong communication, empathy, and decision-making abilities. The capacity to translate complex technical risks into accessible messages for diverse stakeholders is just as critical as technical literacy. Therefore, leadership development curricula should prioritize multidisciplinary approaches that integrate managerial, technical, and interpersonal dimensions.

The benefits of such an approach extend beyond individual leaders or organizations. By embedding cyber risk leadership training into academic curricula, universities contribute to building a broader culture of resilience. Future leaders equipped with these skills can reduce the impact of human error, strengthen institutional preparedness, and lower the long-term costs of employee training in cyber-safe behavior. Moreover, this contributes to societal resilience, preparing communities to adapt to an increasingly insecure and volatile digital environment.

Universities have a pivotal role to play in designing curricula that foster not only technical awareness but also strategic foresight, adaptability, and collaboration. By emphasizing continuous development alongside traditional leadership traits, academic programs can equip leaders with the tools to manage both current and future risks.

In conclusion, effective leadership in the era of cyber risk requires a multidimensional approach that integrates technical knowledge, strategic insight, adaptability, and strong interpersonal skills. By systematizing these characteristics, this study not only enriches theoretical understanding but also provides actionable guidance for universities, organizations, and policymakers to cultivate the next generation of leaders prepared for the challenges of the digital age.

6.4 Strengths of the Research

This research possesses several significant strengths that greatly enhance its value to both scholarly work and practical leadership growth. A primary advantage is its focus on identifying and organizing the specific leadership traits that are most effective for addressing cyber risk management in today's digital landscape. While previous literature has addressed leadership in the context of digital transformation or general organizational management, it often treats these characteristics in a fragmented manner, mentioning them in isolation rather than integrating them into a coherent framework. This study, by contrast, brings together diverse traits, ranging from strategic foresight, adaptability, and effective communication, to technical and cybersecurity awareness, highlighting how they collectively define a new type of leadership tailored to the complexities and challenges of the modern digital landscape.

Another strength of this research is its contextual focus on the telecommunications sector, which is particularly exposed to cyber threats due to its critical infrastructure and the sensitive data it handles. By engaging with leaders from this sector, including CEOs, CISOs, CTOs, and board members, the study provides a nuanced understanding of how leadership operates under conditions of high uncertainty, continuous technological evolution, and frequent cyber incidents. The study's methodology, based on thematic analysis of semi-structured interviews, allows for the identification of both widely recognized traits and emerging leadership dimensions that may not yet be represented in classical or contemporary literature. This approach ensures that the findings are grounded in real-world practice, reflecting the perspectives of leaders who actively navigate cyber risks on a daily basis.

A further strength is the study's emphasis on the human factor in cybersecurity. While technical defenses and organizational frameworks are important, the research highlights the critical role of leadership in shaping organizational culture, fostering cyber awareness among employees, and promoting proactive, informed decision-making. This perspective aligns with the growing recognition that human behavior is often the most significant determinant of cybersecurity outcomes, yet is frequently overlooked in both literature and practice. By capturing leaders' insights on how to integrate knowledge, communication, and strategic foresight into daily decision-making, the study contributes to a deeper understanding of leadership as a central enabler of effective cybersecurity management.

Moreover, the research emphasizes continuous learning and development as fundamental to leadership effectiveness. Leaders interviewed consistently noted that while certain traits may be innate, leadership is ultimately cultivated through experience, education, and training. This reinforces the notion that leadership is not a static quality but a dynamic capability, requiring ongoing refinement to keep pace with evolving technological, regulatory, and strategic challenges.

The study thus offers practical implications for leadership development programs, providing a foundation for targeted training initiatives that address both behavioral competencies and technical knowledge in cybersecurity.

6.5. Limits of the Research

Despite these strengths, one key limitation of this study is the relatively small sample size, which may affect the generalizability and robustness of the findings. While thematic saturation was achieved, meaning that the same concepts were repeatedly observed across interviews, a larger and more diverse pool of respondents could have revealed additional perspectives or nuanced variations in leadership characteristics. In particular, some traits or strategies mentioned only once might have emerged more prominently with a broader sample, potentially enriching the framework proposed in this study.

Another limitation concerns gender representation. Although attempts were made to include both men and women in the interview process, the majority of respondents were male. Only two female leaders, a CISO and an expert from ACN, participated, and there were no women in CEO roles interviewed. This imbalance may limit the generalizability of the findings, as female perspectives on leadership, communication styles, and approaches to cyber risk management may differ in ways that are not fully captured in this research.

Cultural representation also presents a constraint as interviewees were primarily from Italy. Leadership approaches and perceptions of cyber risk can vary significantly across cultures, influenced by factors such as uncertainty avoidance, power distance, and organizational norms. Consequently, the findings may not fully reflect leadership practices in other regions, and further research is needed to explore how cultural contexts shape the traits and behaviors necessary for effective cyber risk management.

Finally, while the research focuses on the telecommunications sector, which provides a rich context for studying cyber risk, the applicability of the findings to other industries remains to be tested. Although many of the identified leadership characteristics, such as adaptability, communication, strategic foresight, and risk awareness, are likely relevant across sectors, the specific pressures, regulatory frameworks, and technological vulnerabilities of other industries may necessitate additional or modified traits.

6.6 Implications for Further Research

These limitations suggest several avenues for future research. Expanding the number of interviewees would enhance the robustness and diversity of perspectives captured. Incorporating a more balanced gender representation would allow for a better understanding of how leadership in the cyber era may differ across genders. Including respondents from diverse cultural and regional backgrounds would provide insight into how leadership traits are shaped by broader social, economic, and regulatory contexts. Additionally, applying the framework to leaders in other industries could test the generalizability of the proposed model and identify sector-specific adaptations.

Despite these limitations, the study provides a meaningful contribution to the literature by integrating leadership traits into a comprehensive framework specifically tailored to cyber risk management. It demonstrates that leadership in the digital era is not only about personal traits or classical models but also about cultivating knowledge, strategic awareness, and continuous learning to foster organizational resilience. By capturing these insights, the research lays the groundwork for further studies on targeted leadership development, practical training programs, and the broader applicability of this emerging model across industries and cultures.

CONCLUSION

The present study set out to contribute to the growing body of literature on leadership by offering new insights into leadership development in the context of cybersecurity. The research was motivated by the recognition that cyberthreats represent one of the most significant risks confronting telecommunications companies today. These organizations operate in an environment where data has become one of the most valuable assets, frequently referred to as the “new currency, and where the consequences of cyberattacks extend far beyond financial loss to include reputational damage, erosion of public trust, and threats to national security. Realizing that human error constitutes one of the greatest vulnerabilities for companies, and that employee awareness is crucial to preventing breaches, the role of leadership in fostering a culture of cyber awareness emerged as a critical dimension of effective cyber risk management, one that extends beyond purely technical solutions. This recognition, combined with the observation that existing leadership literature had largely overlooked the intersection between leadership and cybersecurity, motivated the study to investigate this gap. Accordingly, the research was guided by the central question: *What leadership characteristics must today’s leaders in the telecommunications sector possess to effectively manage cyber risks in the context of digital transformation?*

The findings of the interviews, beyond providing a comprehensive overview of the risks and challenges faced by the telecommunications industry in the digital and cybersecurity era, ranging from external threats to internal vulnerabilities and structural and contextual pressures, also confirm the critical importance of leadership in guiding organizations toward cyber-resilient strategies. They suggest that leaders in this sector must develop a multidimensional skillset that combines technical understanding with strong interpersonal and adaptive abilities. The proposed *Cyber Risk Leadership* model reflects this reality by emphasizing the interdependence of three domains of leadership. First, leaders require core competencies, such as digital and cybersecurity literacy, heightened risk awareness, rapid decision making, ability to multitask and capacity to navigate uncertainty. Second, they must cultivate relational skills that encompass effective crisis communication, empathy, collaboration, calmness under pressure and visibility in order to foster trust and collective responsibility. Finally, leaders are expected to demonstrate strategic and adaptive abilities, particularly foresight, adaptability, international exposure and a commitment to continuous learning, enabling them to steer their organizations through an evolving and unpredictable cyber landscape. This combination equips leaders not only to interpret and respond to technical risks but also to foster a culture of awareness, accountability, and preparedness across all levels of the organization.

By identifying these characteristics, the study advances existing literature on leadership in two important ways. First, it expands leadership theory into a domain that remains underexplored: the intersection between leadership and cybersecurity. While previous research has highlighted models such as transformational and participative leadership, this study shows that cyber risk leadership not only draws on elements of these approaches but also introduces distinctive dimensions shaped by the digital era, such as cybersecurity literacy, international experience, heightened risk awareness, composure under pressure, and effective crisis communication.

Second, it recognizes that effective cyber risk management is not solely a technical challenge but also a leadership one. By framing cybersecurity as a strategic and cultural issue, the study underscores the importance of equipping leaders with the competencies, relational skills, and adaptive capacities needed to guide their organizations through an increasingly complex and hostile digital landscape. In doing so, it enriches the broader literature on leadership while also providing actionable insights for practitioners tasked with navigating the realities of cyber risk.

Beyond its theoretical contributions, this research offers several important practical implications for leadership development, organizational training, and higher education curricula. The identification of the cyber risk leadership model, combining core competencies, relational skills, and adaptive abilities, points to specific directions for strengthening leadership practices in the telecommunications sector and beyond.

First, the study underscores the need for targeted training and capacity-building programs that move beyond generic leadership development to address the specific challenges of cybersecurity. Interviews with executives and technical leaders consistently revealed that human error often arises from inadequate awareness and insufficient preparedness. Addressing this requires training strategies that do not merely impart technical knowledge but also cultivate the interpersonal and decision-making capacities essential for guiding organizations through cyber crises. For example, immersive simulations, such as the one attended, along with scenario-based exercises and cyberattack drills, can further substantiate the results by preparing leaders to make effective decisions under pressure, communicate clearly with diverse stakeholders, and align organizational responses with both technical and strategic needs. These experiential learning methods are particularly valuable for bridging the gap between technical expertise and soft skills such as empathy, collaboration, foresight, and crisis communication, which the findings identified as indispensable for cyber risk leadership.

Second, the results highlight the importance of integrating cybersecurity and leadership development in university and professional curricula. Current leadership programs in management schools or professional academies often treat cybersecurity as a purely technical field, detached from broader leadership concerns. Conversely, computer science or cybersecurity courses rarely incorporate organizational or relational dimensions of leadership. This divide limits the capacity of future leaders to manage risks holistically. Universities and training institutions should therefore design multidisciplinary programs that merge managerial and technical education, offering courses that combine cyber risk management, leadership theory, and organizational psychology. Experiential components such as workshops, case studies, internships, and collaborative projects should complement theoretical instruction. Such initiatives would better prepare graduates and professionals to operate in a digital environment where leadership must account for both technological complexity and human vulnerability.

Third, the study has practical implications for organizations in the telecommunications sector and other critical industries. By using the cyber risk leadership framework, companies can evaluate the readiness of their leadership teams and identify areas for improvement. Human resources and talent development departments can adopt the model as a reference to design leadership assessments, recruitment criteria, and professional development pathways. For example, rather than selecting leaders solely on the basis of technical expertise or past managerial performance, organizations could emphasize adaptability, communication skills, and the ability to translate technical risk into accessible language. By doing so, companies not only reduce their exposure to cyber threats but also build a more resilient organizational culture that supports long-term sustainability.

While this study has provided meaningful insights into leadership in the cybersecurity era, several limitations must be acknowledged. The first concerns the sample size and diversity. Although thematic saturation was achieved, with recurring themes consistently emerging across interviews, the relatively small number of participants restricted the breadth of perspectives. Expanding the pool to include more leaders, particularly across different roles and organizational levels, could have revealed additional nuances or reinforced characteristics that appeared only sporadically in this study. The relatively low response rate also posed a challenge, limiting the opportunity to capture the full variety of leadership experiences within the telecommunications sector.

A second limitation relates to gender representation. Only two women participated in the study, one in a CISO role and one as an expert from the ACN, while no women CEOs were included in the interviews. This imbalance reflects the broader underrepresentation of women in senior leadership positions within the telecommunications and cybersecurity sectors, but it nonetheless constrains the findings. Greater participation of women could have surfaced additional perspectives on leadership characteristics which remain underexplored in this field.

A third limitation is the cultural context of the sample. The fact that interviewees were based in Italy, which may have shaped the results in ways that reflect national or regional cultural traits. Leadership approaches and perceptions of cyber risk can be influenced by cultural factors and as such, the findings may not fully capture leadership dynamics in other European countries or in non-European contexts where telecommunications companies operate under different regulatory, cultural, and market conditions. Future studies should aim to expand the cultural and geographical scope of the sample to validate and refine the cyber risk leadership model across diverse settings.

Given these limitations, several avenues for future research emerge. First, expanding the empirical basis of the study with a larger, more diverse, and internationally representative sample would allow for more robust conclusions and increase the generalizability of the findings. Comparative studies across countries or regions could also shed light on the role of cultural differences in shaping cyber risk leadership. Second, future studies could benefit from employing mixed-method research designs that integrate qualitative interviews with quantitative surveys or experimental simulations. This approach would allow for triangulating results and provide a deeper understanding of how leadership traits practically impact organizational resilience. Third, specific attention should be given to gender dynamics in cyber risk leadership, exploring how women leaders perceive and enact their roles in cybersecurity contexts and whether their approaches differ from those of their male counterparts.

Finally, future work could investigate the longitudinal development of cyber risk leadership, analyzing how leaders acquire, refine, and adapt these skills over time. Such studies would not only enrich academic knowledge but also guide the design of leadership development programs, ensuring they remain responsive to the evolving nature of cyber threats and digital transformation.

In sum, this research has provided an initial framework for understanding the characteristics of cyber risk leadership and has identified key areas for training, curriculum development, and organizational practice. At the same time, it acknowledges the limitations of scope and representation, pointing to the need for further inquiry. By addressing these gaps, future research can build upon the foundation laid here to strengthen leadership theory, enhance organizational resilience, and prepare future generations of leaders for the challenges of the digital age.

BIBLIOGRAPHY

1. Ablon, L. (2018, March 15). *Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data.* Testimony before the Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance, United States House of Representatives. RAND Corporation.

2. Adams, H. S. (2024, June 15). *Cybersecurity budgets rise for telecommunications & tech.* Mobile Magazine. Cybersecurity budgets rise for telecommunications & tech.

3. Adewuyi, N. A., et al. (2024). The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems. World Journal of Advanced Research and Reviews, 23(1), 379–394. https://doi.org/10.30574/wjarr.2024.23.1.1993

4. Agenzia per la Cybersicurezza Nazionale. (2025). *Operational summary: First semester 2025 [Report].* https://www.acn.gov.it/portale/w/operational-summary-1-semestre-2025

5. Agrawal, Vivek. (2016) "Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard." HAISA.

6. Ahmed, S. K., et al. (2025). Using thematic analysis in qualitative research. *Journal of Medicine Surgery and Public Health*, 100198. https://doi.org/10.1016/j.glmedi.2025.100198

7. Aksoy, C. (2025b). Building Effective Cybersecurity Leadership: The Crucial Role Of Leaders In Protecting Businesses Against Cyber Threats. *Kalite Ve Strateji Yönetimi Dergisi*, *5*(1), 33–49. https://doi.org/10.56682/ksydergi.1539408

8. Albrecht, J. P. (2016). *How the GDPR will change the world.* European Data Protection Law Review (EDPL), 2(3), 287-289.

9. Aljazeera (2025, July 16). *Joint global operation takes down pro-Russian hacking group. Al Jazeera*. https://www.aljazeera.com/news/2025/7/16/joint-global-operation-takes-down-pro-russian-hacking-group

10. Almeida, F.,et al. (2020). *The challenges and opportunities in the digitalization of companies in a post-COVID-19 World.*

11. Araujo, L. M., et al. (2021). *Digital leadership in business organizations.* International Journal of Educational Administration, Management, and Leadership, 2(1), 45–56. doi:10.51629/ijeamal.v2i1.18.

12. Aruna, A. (2024, December 13). BT's Eye-Opening Data on Daily Cyber Threats and Emerging Risks. *Telecom Review Europe*. BT's Eye-Opening Data on Daily Cyber Threats and Emerging Risks

13. Azubuike, C. F. (2023). *Cyber security and international conflicts: An analysis of state-sponsored cyber attacks.* Nnamdi Azikiwe Journal of Political Science (NAJOPS), 9(1). ISSN: 2992-5924.

14. Babin, R., & Grant, K. (2019). How do CIOs become CEOs? Journal of Global Information Management, 27(4), 1–15. doi:10.4018/JGIM.2019100101; Cresnar, R., & Nedelko, Z. (2020). Understanding future leaders: How are personal values of generations Y and Z tailored to leadership in industry 4.0? Sustainability, 12(11), 4417. doi:10.3390/su12114417

15. Badman, A., Kosinski, M. *What is asymmetric encryption?* IBM Think.

16. Bakare, S. S., et al., (2024). *Data Privacy Laws And Compliance: A Comparative Review Of The EU GDPR And USA Regulations.* Computer Science & IT Research Journal.

17. Bass B.M., 2008, The Bass Handbook of Leadership: Theory, Research, and Managerial Applications, 4th ed., New York: Free Press.

18. Bass, B.M.1999, Two Decades of Research and Development in Transformational Leadership, European Journal of Work and Organizational Psychology.

19. Bass B.M., Stogdill R.M, 1990, Handbook of Leadership: Theory, Research, and Managerial Applications, 3rd ed., New York: Free Press.

20. Batko K, & Ślęzak A., (2022). *The use of Big Data Analytics in healthcare.* J Big Data. doi: 10.1186/s40537-021-00553-4. PMID: 35013701; PMCID: PMC8733917.

21. Baumann, B. (2024). The key challenges in aligning corporate culture with digital transformation. *Panorama Consulting Group*. Key Challenges in Aligning Corporate Culture with Digital Transformation

22. Bay, M. (2016). *What is cybersecurity? In search of an encompassing definition for the post-Snowden era.* French Journal for Media Research, 6, 2264-4733.

23. Bellamkonda, S. (2021). *Strengthening cybersecurity in 5G networks: Threats, challenges, and strategic solutions.* Journal of Computational Analysis and Applications, *29*(6), 1159-1173.

24. Bennett, N., & Lemoine, G. J. (2014). What a difference a word makes: Understanding threats to performance in a VUCA world. Business Horizons, 57(3), 311–317. doi:10.1016/j.bushor.2014.01.001.

25. Berman, S. (2012). Digital transformation: *Opportunities to create new business models.* Strategy & Leadership, 40(2), 16–24. doi:10.1108/10878571211209314 and Kohli, R., & Johnson, S. (2011). *Digital transformation in latecomer industries: CIO and CEO leadership lessons from Encana Oil & Gas (USA) Inc.* MIS Quarterly Executive, 10(4), 141–156.

26. Bolden R., 2004, *What is Leadership?*, Leadership South West Research Report 1, University of Exeter.

27. Boje, D. (2000). "The Isles Leadership: The Voyage of the Behaviorists". The Leadership Box. Northern Michigan State University

28. Burgelman, R. & A., Meza P., E., (2003). *AOL: The Emergence of an Internet Media Company*. Stanford Graduate School of Business. AOL: The Emergence of an Internet Media Company

29. Burton, S. L., et al. (2023). Exploring the nexus of cybersecurity leadership, human factors, emotional intelligence, innovative work behavior, and critical leadership traits. *Scientific Bulletin*, *28*(2), 162–175. https://doi.org/10.2478/bsaft-2023-0016

30. Cardenes, W. (2025, August 28). *National Critical Infrastructure*. Enea. Securing National Critical Infrastructure

31. Carlyle T.. 1841. On Heroes, Hero-Worship and The Heroic in History. London: James Fraser.

32. Carreras-Coch, A., et al. (2022). *Communication technologies in emergency situations.* Electronics, *11*(7), 1155. https://doi.org/10.3390/electronics11071155

33. Carroll B., et al. (2008). Leadership as practice: challenging the competency paradigm, Leadership 4 (4) 363–379, https://doi.org/10.1177/1742715008095186.

34. Carter, E. (2025, August 1). *5G Security Risks 2025: Mitigation Plan.* Online Hash Crack. https://www.onlinehashcrack.com/guides/cybersecurity-trends/5g-security-risks-2025-mitigation-plan.php

35. Cempaka Sari, A., et al. (2022). *Review Of Text Based Password And Other Authentication Methods For E-Commerce Data Protection.* In Bina Nusantara University, Journal Of Theoretical And Applied Information Technology (Vol. 100, Issue 6, Pp. 1604–1605) [Journal-Article]. Little Lion Scientific. https://Www.Jatit.Org

36. Charter Global (2024). *Digital transformation for SMEs: Overcoming challenges & Embracing growth*. Charter Global. Digital transformation for SMEs

37. Check Point Software Technologies Ltd. (2025, July 21). Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions. Check Point Research. Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions

38. Charles, L., et al. (2022). *Digitalization and Employment: A Review*. International Labour Office. Digitalization and Employment

39. Chebitko, R. (2024). *The first antivirus was called.* MS.Codes. he First Antivirus Was Called

40. Check Point Software. (2025, March 24). *What is spear phishing?* What is Spear Phishing?

41. Chuang, S., & Graham, C. M. (2020). Contemporary issues and performance improvement of mature workers in industry 4.0. Performance Improvement, 59(6), 21–30. doi:10.1002/p.21921.

42. Cimmarusti, I. (2025, July 8). Cybersecurity, investment in the euro area to reach EUR 75 billion. *Il Sole 24 ORE*. Cybersecurity, investment in the euro area to reach EUR 75 billion

43. *Cisco Secure Firewall: first line of defense*. (2025, February 3). Cisco. What is a Firewall?

44. CodeHunter. (2025). Cybersecurity incident response: Time is of the essence. https://codehunter.com/news-and-blog/-cybersecurity-incident-response

45. Colabianchi, S., et al. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation & Knowledge*, *10*(3), 100695. https://doi.org/10.1016/j.jik.2025.100695

46. Collin, J. (2015). *Digitalization and dualistic IT. IT Leadership in Transition - The Impact of digitalization on Finnish organizations (pp. 29−34).* Aalto University.

47. Connolly, L. Y., et al. (2020). *An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability.* Journal of Cybersecurity, *6*(1). https://doi.org/10.1093/cybsec/tyaa023

48. Covey S.R., 2009, The 8th Habit: From Effectiveness to Greatness, New York: Free Press.

49. Cox A., (2024). *Changes for 'Over The Top' communications services following their inclusion within the European Electronic Communications Code*. Arthur Cox LLP. Changes for 'Over The Top' communications services following their inclusion within the European Electronic Communications Code

50. Crevani L., Endrissat N., (2016). Mapping the leadership-as-practice terrain: comparative elements, in: J.A. Raelin (Ed.), Leadership-as-Practice: Theory and Application, Routledge, New York, pp. 21–49.

51. Cresnar, R., & Nedelko, Z. (2020). Understanding future leaders: How are personal values of generations Y and Z tailored to leadership in industry 4.0? Sustainability, 12(11), 4417. doi:10.3390/su12114417

52. *Cyberattack on Vodafone Portugal*. Vodafone Portugal. Cyberattack on Vodafone Portugal

53. Daft R.L. . 2011. *The Leadership Experience*, 5th ed. Mason, OH: Cengage Learning

54. Dahal, M. S. (2023). *Transforming Telecom Revenue- The impact of OTT Service.* Research Square. https://doi.org/10.21203/rs.3.rs-3084516/v1

55. Dennis, A.,M. (2025, February 15). *Defense Advanced Research Projects Agency (DARPA)*. Encyclopedia Britannica. https://www.britannica.com/topic/Defense-Advanced-Research-Projects-Agency

56. Derue S.L. , et al., 2011, "A Meta-Analytic Review of Leadership Behavior and Effectiveness," *Journal of Applied Psychology*, vol. 96, no. 3.

57. Desmarais, A. (2024, September 16). UK telecoms provider records 2,000 possible cyber-attacks every second. *Euronews*. UK telecoms provider records 2,000 possible cyber-attacks every second

58. Devry, J. (2024). *The state of cloud security - cybersecurity insiders*. Cybersecurity Insiders. The State of Cloud Security

59. Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (ePrivacy Directive).

60. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, 27.12.2022, pp. 80-152.

61. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

62. Eberl, J. K., & Drews, P. (2021). Digital leadership–mountain or molehill? A literature review. Wirschaftsinformation 2021 Proceedings (pp. 223−237). doi:10.1007/978-3-030-86800-0_17;

63. El Sawy, O. A., et al. (2016). *How LEGO built the foundations and enterprise capabilities for digital leadership.* MIS Quarterly Executive, 15(2), 141–166

64. Ellis, A., (2024). *Cyber chaos: Pro-Russian hackers hit Italian airports.* Euro Weekly News. Cyber chaos: Pro-Russian hackers hit Italian airports

65. Euronews. (2024, May 29). Disruptive attacks double in EU in recent months, cybersecurity chief says. *Euronews*. https://www.euronews.com/next/2024/05/29/disruptive-attacks-double-in-eu-in-recent-months-cybersecurity-chief-says

66. European Commission. (2024). *Cybersecurity and resiliency of Europe's communications infrastructures and networks: Follow-up to the Nevers Call of 9 March 2022.* NIS Cooperation Group. Cybersecurity and resiliency of Europe's communications infrastructures and networks

67. EY. (2025). Top 10 risks for telecommunications in 2025. EY. Top 10 risks for telecommunications in 2025

68. Fathauer, M. (2025). Mandatory & Discretionary access control: Which to choose? *Ping Identity*. https://www.pingidentity.com/en/resources/blog/post/access-control.html

69. Feliciano-Cestero, M. M., et al. (2022). *Is digital transformation threatened? A systematic literature review of the factors influencing firms' digital transformation and internationalization.* Journal of Business Research, *157*, 113546. https://doi.org/10.1016/j.jbusres.2022.113546

70. Fiedler F.E., "A Contingency Model of Leadership Effectiveness," in *Advances in Experimental Social Psychology*, vol. 1, ed. L. Berkowitz (New York: Academic Press, 1965), 149–190.

71. Finio, M., & Downie, A. (2024). *What is a cybersecurity risk assessment?* IBM. https://www.ibm.com/think/topics/cybersecurity-risk-assessment

72. Fortinet. (2025). 2025 Global Threat Landscape Report. Fortinet. 2025 Global Threat Landscape Report

73. Foulon, M., & Meibauer, G. (2024). *How cyberspace affects international relations: The promise of structural modifiers.* Contemporary Security Policy, *45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

74. Fransman, M. (2001). *Evolution of the telecommunications industry into the internet age.* Communications and Strategies, vol. 43, pp. 57-113.

75. Freiberger, P. A., & Swaine, M. R. (2025, January 25). *ENIAC | History, Computer, Stands For, Machine, & Facts*. Encyclopedia Britannica. ENIAC

76. Friedman, A., et al. (2020). *Cost of A Cyber Incident: Systematic Review And Cross-Validation*. Cybersecurity and Infrastructure Security Agency (CISA) | Defend Today, Secure Tomorrow.

77. Forescout Technologies, Inc. (2025, February 10). *What is Cybersecurity Risk Management?* Forescout.

78. FortiGuard Labs (2025). Fortinet Global Threat Landscape Report. Fortinet Global Threat Landscape Report.

79. Galton F., 1869, *Hereditary Genius*, London: Macmillan.

80. Gartner, Inc. (2025). Gartner Leadership Vision for 2025: Security and Risk Management by Tom Scholtz and Lisa Neubauer. Absolute Software. Key Imperatives for SRM Leader in 2025 by Gartner®

81. Gay, C. (2019). *The GDPR's effect on transatlantic relations*. University of Chicago Law School, Chicago Unbound.

82. Geers, K. (2009). *The cyber threat to national critical infrastructures: Beyond theory.* Information Security Journal: A Global Perspective, *18*(1), 1–7.

83. Gilpin D.R., Murphy P.J., (2008). Crisis Management in a Complex World, Oxford University Press, New York.

84. GLOBE Project. (2011, April 1). 2004, 2007 Studies - GLOBE Project: An overview of the 2004 study: Understanding the relationship between national culture, societal effectiveness and desirable leadership attributes. https://globeproject.com/study_2004_2007.html

85. Goddard, M. (2017). *The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact.* International Journal of Market Research, 59(6), 703-705. https://doi.org/10.2501/IJMR-2017-050

86. Grant M.J, (2024). *Concurrent data collection and analysis in grounded theory*. The Grounded Theorist. Concurrent Data Collection

87.

88. Greco, E., Marconi, F. (2024). Technological innovation and cybersecurity: The role of the G7. Istituto Affari Internazionali (IAI).

89. Guinan, P. J., Parise, S., & Langowitz, N. (2019). Creating an innovative digital project team: Levers to enable digital transformation. Digital Transformation & Disruption, 62(6), 717–727. doi:10.1016/j.bushor.2019.07.005.

90. Gupta, A., Verbree, M., Rica, F., Michaux, D., & KPMG International Cooperative. (2019). Global Perspectives on Cyber Security in Telco: A roundtable discussion on the state of cyber security management in the telco sector. Global Perspectives on Cyber Security in Telco

91. Guzman, V. E., et al. (2020). Characteristics and skills of leadership in the context of industry 4.0. Sustainable manufacturing - hand in hand to sustainability on globe. In Proceedings of the 17th Global Conference on Sustainable Manufacturing (pp. 543−550). doi:10.1016/j.promfg.2020.02.167.

92. Haleem A, et al. (2021). *Telemedicine for healthcare: Capabilities, features, barriers, and applications.* Sens Int. 2021;2:100117. doi: 10.1016/j.sintl.2021.100117. PMID: 34806053; PMCID: PMC8590973.

93. Herold, G. (2016). Leadership in the fourth industrial revolution. Stanton Chase Business Journals, 22(12), 1–15.

94. Hersey P., Blanchard K.H., "Life Cycle Theory of Leadership," *Training and Development Journal* 23, no. 5 (1969): 26–34. P. Hersey and K.H. Blanchard, Management of Organizational Behavior: Utilizing Human Resources, 5th ed. (Englewood Cliffs, NJ: Prentice Hall, 1988).

95. Hofmann, S. C., & Pawlak, P. (2023). *Governing cyberspace: policy boundary politics across organizations*. Review of International Political Economy, 30(6), 2122–2149. https://doi.org/10.1080/09692290.2023.2249002

96. Hogan, M., & Newton, E. (2015b). *Supplemental information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S.* Objectives for Cybersecurity. https://doi.org/10.6028/nist.ir.8074v2.

97. House R.J., Mitchell T.R. , "Path-Goal Theory of Leadership," *Journal of Contemporary Business* 3, no. 4 (1974): 81–97.

98. House R.J., 1988, Leadership Research and Theory: A Functional Integration, Psychological Bulletin, vol. 103, no. 3, pp. 41–47.

99. House, R. J., et al. (Eds.). (2004). Culture, leadership, and organizations: The GLOBE study of 62 societies. Sage Publications.

100. Hunder, M., et al. (2023, December 12). *Ukraine's top mobile operator hit by biggest cyberattack of war.* Reuters.

101. Hunt R. and Larson C., 1977, "Leadership as Behavior," *Journal of Applied Psychology*.

102. IBM Security. (2024). Cost of a Data Breach Report 2025. IBM. Cost of a Data Breach Report 2025

103. Imber, D. (2025, April 9). The Latest Cyber Crime Statistics (updated April 2025) | AAG IT Support. *AAG IT Services*. https://aag-it.com/the-latest-cyber-crime-statistics/

104. Imran, F., et al. (2020). Leadership competencies for digital transformation: Evidence from multiple cases. International Conference on Applied Human Factors and Ergonomics (pp. 81−87). doi:10.1007/978-3-030-50791-6_11.

105. IndustryTrends, & IndustryTrends. (2025, March 10). *Quantum Cryptography: A new era of Encryption*. Analytics Insight. Quantum Cryptography: A New Era of Encryption

106. International Telecommunication Union. Global Cybersecurity Agenda (GCA). GCA

107. International Telecommunication Union. Global Cybersecurity Index (GCI). https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

108. International Telecommunication Union. (2024). Global Cybersecurity Index 2024 (GCI 2024). https://www.coit.es/sites/default/files/uit_global_cybersecurity_index_2024.pdf

109. Iovan, S., & Iovan, A.-A. (2016). From cyber threats to cyber-crime. Journal of Information Systems & Operations Management, 10(2), 425–434 https://web.rau.ro/websites/jisom/Vol.10 No.2 - 2016/JISOM-WI16-A15.pdf

110. Ivančić, L., et al. (2019). Mastering the digital transformation process: Business transformation 4.0 as a new paradigm. Business Systems Research Journal, 10(1), 37–48.

111. Larjovuori, R.-L., et al. (2018). Leadership in the digital business transformation. In Proceedings of the 22nd International Academic Mindtrek Conference (pp. 212−221). doi:10.1145/3275116.3275122.

112. Lirosi, M. (2025, August 5). *Cybersecurity in Italy 2025, the threat grows: cyber attacks up 53%, record data breaches, and websites down - FIRSTonline*. FIRSTonline. https://www.firstonline.info/en/Cybersecurity-in-Italy-2025-the-threat-grows-cyber-attacks-with-53-records-of-data-breached-and-sites-down/

113. Judge T.A. , et al., 2002, Personality and Leadership: A Qualitative and Quantitative Review, Journal of Applied Psychology, vol. 87, no. 4, pp. 765–780.

114. Kane, G. C., et al. (2015). Strategy, not technology, drives digital transformation: 14 (pp. 1−25). MIT Sloan Management Review and Deloitte University Press.

115. Karkera, A., et al., (2022, April 1). *Data-fueled government*. Deloitte Insights. Data-fueled government Breaking down silos with turbo-charged data

116. Kazim, F. (2019). Digital transformation and leadership style: A multiple case study. The ISM Journal of International Business, 1(1), 1–12.

117. Kenton, W. (2022). *Michigan Leadership Studies: History and Criticism*. Investopedia. Michigan Leadership Studies

118. Khan, M.K. (2022) *Technology and telecommunications: a panacea in the COVID-19 crisis.* Telecommun Syst 79, 1–2. https://doi.org/10.1007/s11235-022-00880-8

119. Khanom, T. M. (2023). *Business strategies in the age of digital transformation.* Journal of Business, 08(01), 28-35. https://doi.org/10.18533/job.v8i01.296

120. Khormali, A., et al. (2021). *Domain name system security and privacy: A contemporary survey.* Computer Networks, 185, 107699.

121. Kotter, J. P. (2000). What leaders really do. Harvard Business Review, 79(11), 24–33.

122. KPMG International. (2025). Cybersecurity considerations for Technology, Media & Telecommunications (TMT) companies 2025. KPMG. Strategic Foresight / Trend Research Readiness

123. Kraus, S., et al. (2021). Digital transformation: An overview of the current state of the art of research. Sage Open, 11,(3) 21582440211047576

124. Kumar, M. J. (2023) Privacy-Preserving Technologies in Telecom Data Analytics: Implementing Privacy-Preserving Techniques Like Differential Privacy to Protect Sensitive Customer Data During Telecom Data Analytics. http://dx.doi.org/10.2139/ssrn.5136773

125. Kuzior, A., et al. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal Of International Studies, 17*(2), 220–239. Cybersecurity and Cybercrime

126. *Larjovuori, R.-L., et al. (2018). Leadership in the digital business transformation. In Proceedings of the 22nd International Academic Mindtrek Conference (pp. 212−221). doi:10.1145/3275116.3275122.*

127. Lehtonen, S., et al. (2025). Rethinking Crisis Leadership through Leadership-as-Practice: A Narrative Review and Future Directions. *International Journal of Disaster Risk Reduction*, 105671. https://doi.org/10.1016/j.ijdrr.2025.105671

128. Lemieux, R. (2025, August 12). *Leadership's role in enabling cyber operational resilience*. DVMS Institute. Leadership's Role In Enabling Cyber Operational Resilience

129. Lewis, C., (2025). *AI is the greatest threat—and defense—in cybersecurity today. Here's why*. McKinsey & Company. AI is the greatest threat—and defense—in cybersecurity today. Here's why.

130. Ling, X. & Wu, L. (2023). *Adversarial attacks against Windows PE malware detection: A survey of the state-of-the-art.* Computers & Security *128*, 103134. https://doi.org/10.1016/j.cose.2023.103134

131. Lord, R. G., & Maher, K. J. (1991). Leadership and information processing: Linking perceptions and performance. Unwin Hyman.

132. Lule, M.-L., (2024) *Telecom Security Incidents 2022. Annual Report.* European Union Agency for Cybersecurity.

133. Maglaras, L., et al. (2022). *Cybersecurity of critical Infrastructures: challenges and solutions.* Sensors, *22*(14), 5105. https://doi.org/10.3390/s22145105

134. Manukonda, K. R. R. (2019). *Cyber attack on telecommunications company*. European Journal of Advances in Engineering and Technology, *6*(12), 113-120.

135. Matt, C., et al. (2015). *Digital transformation strategies.* Business & Information Systems Engineering, 57(5), 339–343. doi:10.1007/s12599-015-0401-5.

136. McGillem, & D, C. (2025, August 23). *Telegraph | Invention, History, & Facts*. Encyclopedia Britannica. https://www.britannica.com/technology/telegraph

137. McGuire, T. (2017, December 4). *Why Big Data is the new competitive advantage - Ivey Business Journal*. Ivey Business Journal.Why Big Data is the new competitive advantage

138. McClelland D.C. , 1975, *Power: The Inner Experience*, New York: Irvington Publishers.

139. Métayer, D. L., et al. (2015). Privacy and Data Protection by Design - from policy to engineering. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1501.03726

140. Nadella, S., & Euchner, J. (2018). *Navigating digital transformation: An interview with Satya Nadella.* Research Technology Management, 61(4), 11–15. doi:10.1080/08956308.2018.1471272.

141. Nagar, G. (2024). The role of human factor in cybersecurity: Behavioral insights and training strategies. *International Research Journal of Modernization in Engineering, Technology and Science, 6*(3), 5723–5730. https://www.irjmets.com

142. Nahavandi A., 2015, *The Art and Science of Leadership*, 7th ed., Upper Saddle River, NJ: Pearson.

143. Natalucci, F., et al. (2024, April 9). *Rising cyber threats pose serious concerns for financial stability. I*nternational Monetary Fund. Rising Cyber Threats Pose Serious Concerns for Financial Stability

144. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*(Version 1.1). U.S. Department of Commerce.

145. National Institute of Standards and Technology. (2024b). The NIST Cybersecurity Framework (CSF) 2.0. In *NIST CSWP 29*[Report]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

146. Nilupul, S. A. (2024). *Evolution and Impact of Malware: A Comprehensive Analysis from the First Known Malware to Modern-Day Cyber Threats*. Cyber Security. Evolution and Impact of Malware: A Comprehensive Analysis from the First Known Malware to Modern-Day Cyber Threats

147. Noah, A., et al. (2024, December 4). *The consequences of non-compliance with data protection regulations on business analytics.* ResearchGate.

148. Nobles, C. (2018). *Botching human factors in cybersecurity in business organizations.* Holistica–Journal of Business and Public Administration, 9(3), 71-88.

149. *Nokia Threat Intelligence Report finds cybercriminal attacks on telco infrastructure are accelerating, driven by Generative AI and automation*. (2024). Nokia.com. Nokia Threat Intelligence Report finds cybercriminal attacks on telco infrastructure are accelerating, driven by Generative AI and automation.

150. Northouse P.G., 2004, *Leadership: Theory and Practice*, 3rd ed., London, Sage Publications Ltd.

151. Nyagadza, B. (2022). *Sustainable digital transformation for ambidextrous digital rms: A systematic literature review and future research directions.* Sustainable Technology and Entrepreneurship 100020.

152. Olaoluwa F. Samuel, et al. (2024). Ensuring Cybersecurity in telecommunications: Strategies to protect digital infrastructure and sensitive data. Computer Science & IT Research Journal, 5(8), 1855-1883. https://doi.org/10.51594/csitrj.v5i8.1448.

153. Packard, N. (2020). *The ARPANET into the Internet: A tale of two networks.* Studies in Media and Communication, 8(1), 37. https://doi.org/10.11114/smc.v8i1.4783

154. Pandya, D., et al. (2015). Brief history of encryption. In *International Journal of Computer Applications* (Vol. 131, Issue No.9, pp. 28–29). Brief History of Encryption

155. Peel, M. (2025, April 23). Secure 'quantum messages' sent over telecoms network in breakthrough. *Financial Times*. https://www.ft.com/content/51a65e45-302c-45fa-8bd1-c828a66b012d?

156. Pickle, C. (2024). *The changing character of cyber warfare.* Proceedings, 150(6), 1-456. U.S. Naval Institute.

157. Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.006

158. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778; Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983-988.

159. Reed, E., (2023, December 1). *The Origins of Computer Viruses: A journey back to 1949 - Eric Reed Cybersecurity training*. Eric Reed Cybersecurity Training. The Origins of Computer Viruses:

160. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). OJ L 119, 4.5.2016.

161. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification, and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union, L 151*, 7 June 2019, 15–69.

162. *Report on the EU 5G Toolbox Implementation by Member States published.* (2020) *ENISA*. Report on the EU 5G Toolbox Implementation by Member States Published

163. Reuters. *Cybercrime and sabotage cost German firms $300 bln in past year.* (2024). Reuters. Cybercrime and sabotage cost German firms $300 bln in past year

164. Ribeiro, A. (2024). *US Congressional Research Service reports on PRC state-sponsored Salt Typhoon hacks on telecoms*. Industrial Cyber. Report on the EU 5G Toolbox Implementation by Member States Published

165. Ribeiro, A. (2025a, June 6). *EU Cyber Blueprint unifies crisis management, sets joint response framework, enhances cross-border coordination*. Industrial Cyber. EU Cyber Blueprint unifies crisis management, sets joint response framework, enhances cross-border coordination

166. Ribeiro, A. (2025, June 13). *EU invests €145.5 million to strengthen cybersecurity across healthcare systems and public institutions*. Industrial Cyber. EU invests €145.5 million to strengthen cybersecurity across healthcare systems and public institutions

167. Ribeiro, A. (2025). *EU invests €145.5 million to strengthen cybersecurity across healthcare systems and public institutions*. Industrial Cyber. EU invests €145.5 million to strengthen cybersecurity across healthcare systems and public institutions

168. Ribeiro, A. (2025c). *NERC 2025 RISC report finds cybersecurity, supply chain, critical infrastructure interdependencies among top reliability risks*. Industrial Cyber. NERC 2025 RISC Report

169. Rintel S. E., et al. (2001). *First Things First: Internet Relay Chat Openings*, Journal of Computer-Mediated Communication, Volume 6, Issue 3. https://doi.org/10.1111/j.1083-6101.2001.tb00125.x

170. Rosenbach, E., Mansted, K., (2019). *The Geopolitics of Information*. Belfer Center for Science and International Affairs, Harvard Kennedy School.The Geopolitics of Information

171. Sabani, M., et al. (2022). Quantum Key Distribution: Basic Protocols and Threats. In *26th Pan-Hellenic Conference on Informatics (PCI 2022), November 25–27, 2022, Athens, Greece.* ACM, New York, NY, USA 6 Pages. https://doi.org/10.1145/3575879.3576022

172. Sadiku, M. N. O., et al. (2024). *Telecommunications industry: An overview.* International Journal of Trend in Scientific Research and Development (IJTSRD), 8(6), 503-510.

173. Saeed, S., et al. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

174. Salviotti, G., Abbatemarco, N., De Rossi, L. M., & Bjoernland, K. (2023). Understanding the role of leadership competencies in cyber crisis management: A case study. Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS).

175. SANS Institute. (2025). SANS 2025 SOC Survey. SANS Institute. SANS 2025 SOC Survey

176. Savino, S. (2002). *Digital subscriber line: leading technology revolutionizing access to the information highway.* Proceedings of the 2000 IEEE Engineering Management Society. EMS - 2000 (Cat. No.00CH37139), 453–457. https://doi.org/10.1109/ems.2000.872545

177. Schneider, J., (2023). *The history of malware: A primer on the evolution of cyber threats.* IBM blog https://www.ibm.com/think/topics/malware-history.

178. Schwab K. (2016). The Fourth Industrial Revolution: what it means, how to respond. World Economic Forum. The Fourth Industrial Revolution: what it means, how to respond

179. Schwarzmüller, T., et al. (2018). *How does the digital transformation affect organizations? key themes of change in work design and leadership.* Management Revue, 29(2), 114–138

180. Shi, X., & Wang, J. (2011). Interpreting Hofstede Model and GLOBE Model: Which way to go for Cross-Cultural research? *International Journal of Business and Management*, *6*(5). https://doi.org/10.5539/ijbm.v6n5p93

181. Shoemaker, P. (2025). *Authentication vs. Authorization: Key Roles in Access Control.* Identity. Authentication vs. Authorization

182. Singh, P. (2021). *Impact of digital platforms on traditional businesses*. Impact of Digital Platforms on Traditional Businesses

183. Smith, J. (2016). *The TalkTalk Data Breach: Lessons Learned*. Journal of Cybersecurity, 3(2), 87-102. See previous paragraphs on regulatory fines imposed on companies processing EU citizens' data.

184. Smith, K. (2024). *A History of Cybersecurity and cyber threats.* Coro Cybersecurity. A History of Cybersecurity and Cyber Threats

185. Steinberg, S., Adam, Neary, K., & Picker Center Digital Education Group. (2021). *Target cyber attack: A Columbia University case study.* In G. Rattray & J. Healey (Eds.), *SIPA* [Case study].

186. Stogdill R.M., 1948, Personal Factors Associated with Leadership: A Survey of the Literature, Journal of Psychology, vol. 25, pp. 35–71. D. Mann, 1959, A Review of the Relationship Between Personality and Performance in Small Groups, Psychological Bulletin, vol. 56, no. 4, pp. 241–270.

187. Sujan. (2025, April 13). The Ohio State Leadership Studies - TheMBAins. *TheMBAins*. https://thembains.com/the-ohio-state-leadership-studies/

188. Susnjara, S., & Smalley, I. (2024). *What is a mainframe?* IBM. https://www.ibm.com/think/topics/mainframe

189. *Telecoms and banks connect to create mobile financial services*. IBM. Telecoms and banks connect to create mobile financial services.

190. The Business Research Company. (2025). *Telecom Cyber Security Solution Global Market Report 2025.* The Business Research Company. Telecom Cyber Security Solution Global Market Report 2025

191. Tran, D. (2018). *The law of attribution: Rules for attributing the source of a cyber-attack.* Yale Journal of Law & Technology, 20(1), 376. Interesting for the problem of attribution.

192. Triplett, W. J. (2022). *Addressing human factors in cybersecurity leadership*. Journal of Cybersecurity and Privacy, 2(3), 573–586.

193. Udeh, N. E. O., et al. (2024). *The role of big data in detecting and preventing financial fraud in digital transactions.* World Journal of Advanced Research and Reviews, 22(2), 1746–1760. https://doi.org/10.30574/wjarr.2024.22.2.1575

194. Ukwandu E, Hewage C, Hindy H. Editorial: Cyber security in the wake of fourth industrial revolution: opportunities and challenges. Front Big Data. 2024 Feb 21;7:1369159. doi: 10.3389/fdata.2024.1369159. PMID: 38449565; PMCID: PMC10915258.

195. UNIDIR. *Open-Ended Working Group on security of and in the use of ICTs and UNIDIR side events. Building a More Secure World.* Open-Ended Working Group on security of and in the use of ICTs and UNIDIR side events

196. United Nations General Assembly. (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). https://undocs.org/A/70/174

197. United Nations General Assembly. (2021). Final substantive report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (A/75/816). https://docs.un.org/en/A/75/816

198. *United Nations Convention against Cybercrime*. (2024). United Nations : Office on Drugs and Crime. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

199. United Nations. (2024). Global Digital Compact. Global Digital Compact.

200. U.S. Department of Commerce, Raimondo, G. M., et al. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. In *NIST Trustworthy and Responsible AI*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

201. Vaidya, T. (2015). *2001-2013: Survey and analysis of major cyberattacks.* arXiv (Cornell University). https://doi.org/10.48550/arxiv.1507.06673

202. Verbruggen, Y. (2024). *Cyberattacks as war crimes.* International Bar Association.Cyberattacks as War Crimes

203. Vroom, V.H. (1964). *Work and Motivation,* New York: Wiley

204. Wang, P., e al. (2019). *Economic costs and impacts of business data breaches.* Issues in Information Systems, 20(2), 162-171.

205. Weigand, S. (2025, January 2). *2025 Forecast: AI to supercharge attacks, quantum threats grow, SaaS security woes*. SC Media. 2025 Forecast: AI to supercharge attacks, quantum threats grow, SaaS security woes

206. Westerman, G., Bonnet, D., & McAfee, A. (2014b). The nine elements of digital transformation. MIT Sloan Management Review, 55(3), 1–6.

207. Williams, B. (2024). *Summative content analysis in qualitative research*. Insight7 - AI Tool for Call Analytics & Evaluation. Summative content analysis in qualitative research

208. Wrede, M., et al. (2020). *Top managers in the digital age: Exploring the role and practices of top managers in rms' digital transformation.* Managerial & Decision Economics, 41(8), 1549–1567. doi:10.1002/mde.3202.

209. Yoo, Y., et al. (2012). *Organizing for innovation in the digitized world.* Organization Science, 23, 1398–1408. doi:10.1287/orsc.1120.0771.

210. Yukl G.A., 2002, *Leadership in Organizations*, 5th ed., Upper Saddle River, NJ, Prentice-Hall.

211. Zaccaro, M. 2017, Trait-Based Leadership: Early Theories and Recent Advances, Journal of Leadership Studies.

212. Zeijlemaker, S., Pal, R., & Siegel, M. (2025). *Perusing Watermelon Risks to Strengthen Cyber Resilience: Combatting the illusion of control that fosters unintended lapses of control*. Massachusetts Institute of Technology, CAMS

213. World Economic Forum. (2024). *Strategic Cybersecurity Talent Framework. World Economic Forum.* Strategic Cybersecurity Talent Framework

214. World Economic Forum. (2025). *Global cybersecurity outlook 2025 (in collaboration with Accenture).*Global Cybersecurity Outlook 2025