Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application

Halis Kıral
Gökhan Yılmaz *Editors*

Futurisks: Risk Management in the Digital Age

Springer

Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application

Series Editor

Kıymet Tunca Çalıyurt, Centre for Forensic Accounting Research and Enterprise, School of Finance and Management, SOAS University of London, London, Türkiye

This Scopus indexed series acts as a forum for book publications on current research arising from debates about key topics that have emerged from global economic crises during the past several years. The importance of governance and the will to deal with corruption, fraud, and bad practice, are themes featured in volumes published in the series. These topics are not only of concern to businesses and their investors, but also to governments and supranational organizations, such as the United Nations and the European Union. Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application takes on a distinctive perspective to explore crucial issues that currently have little or no coverage. Thus the series integrates both theoretical developments and practical experiences to feature themes that are topical, or are deemed to become topical within a short time. The series welcomes interdisciplinary research covering the topics of accounting, auditing, governance, and fraud.

Halis Kıral • Gökhan Yılmaz
Editors

Futurisks: Risk Management in the Digital Age

Springer

Editors
Halis Kıral
Social Sciences University of Ankara
Ankara, Türkiye

Gökhan Yılmaz
PwC Türkiye
Advisory Services
Istanbul, Türkiye

ISSN 2509-7873 ISSN 2509-7881 (electronic)
Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application
ISBN 978-981-96-6447-4 ISBN 978-981-96-6448-1 (eBook)
https://doi.org/10.1007/978-981-96-6448-1

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Acknowledgment

This book series is a formal series of International Group on Governance Fraud Ethics and CSR Founded by Prof Dr Kıymet Tunca Çalıyurt on 2009.

Contents

List of Figures

List of Tables

List of Charts

Part I
Introduction

Chapter 1
The Impact of Emerging Technologies and the Future of Risk Management: A Strategic Perspective

Halis Kiral and Gökhan Yılmaz

Abstract This study explores the profound impact of digital transformation on enterprise risk management. It highlights the shifting dynamics of supply and demand influenced by technological advancements, evolving customer preferences, geopolitical tensions, and regulatory developments. Beyond building digital infrastructure, digital transformation requires organizations to rethink strategic decisions, business processes, and the legal and ethical frameworks governing operations. The paper identifies critical risk areas amplified by digital transformation, including cybersecurity, data privacy, compliance, labor, third-party dependencies, business continuity, environmental sustainability, and regulatory challenges. These risks are notable not for their novelty but for their far-reaching impact and rapid propagation, exemplified by significant global IT outages caused by seemingly minor technical issues. The article underscores the need for organizations to move beyond superficial digital updates and adopt transformative approaches to business models, processes, and structures. It offers actionable strategies for leaders to navigate the complexities of rapid technological change and turn emerging risks into opportunities.

Keywords Digital transformation · Risk management · Sustainability · Cybersecurity · Data privacy · Artificial intelligence

H. Kiral
Social Sciences University of Ankara, Ankara, Türkiye
e-mail: halis.kiral@asbu.edu.tr

G. Yılmaz (✉)
PwC Türkiye, Advisory Services, İstanbul, Türkiye
e-mail: gokhan.yilmaz@pwc.com

H. Kıral, G. Yılmaz (eds.), *Futurisks: Risk Management in the Digital Age*, Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application, https://doi.org/10.1007/978-981-96-6448-1_1

1.1 Introduction

Throughout history, the risks faced by companies have varied depending on political, social, economic, and technological developments. For example, a company operating in the nineteenth century had to keep pace with the profound technological and industrial changes brought about by the Industrial Revolution. Some of the major risks that a company operating in this era had to consider were inadequate transport infrastructure, an underdeveloped banking system and limited access to financial resources. Managers who managed these risks effectively and took their companies into the twentieth century faced completely different risks this time. World Wars I and II, and the Great Depression of 1929 in the intervening years, left companies with the uphill struggle of adapting their production capacities to the war economy while at the same time managing the risk of bankruptcy. After the wars and crises, companies had to cope with the risk of adapting to the advances in electronic and computer technologies that began in the second half of the twentieth century and whose effects were felt well into the early twenty-first century. In the 2000s, international trade, complex supply chains, and advances in information technologies had a profound impact on the risks that companies had to manage to survive in intense global competition. After the second half of the 2010s, artificial intelligence (AI), the Internet of Things (IoT), autonomous robots, big data, cloud technology, blockchain, virtual and augmented reality, drones and unmanned aerial vehicles led to digital transformation. This transformation has had a profound impact on almost every sector, causing the bankruptcy of many retail giants such as Kodak, Blockbuster, Toys 'R'Us and Polaroid, while on the other hand enabling new giants such as Alibaba, Amazon, Uber, Spotify, Netflix, and Booking.com to emerge in a relatively short period of time.

1.2 Forward-Thinking Industries

Several industries are undergoing major changes as we navigate the rapidly evolving technological landscape. Traditional business structures are being transformed by innovation, creating new opportunities, and challenges for manufacturing, finance, healthcare, renewable energy, and agriculture. It is essential to take a deliberate and planned strategy that exploits the promise of new technologies while also taking risks and regulatory obligations into account to navigate this dynamic terrain.

The rapid advancement of 5G technology and its successors is poised to transform global business operations, emphasizing the need for fast and highly secure communication networks. However, this progress is accompanied by significant challenges, including cybersecurity risks and legal complexities surrounding data privacy and sovereignty in the telecommunications industry (Radu and Amon 2021). Meanwhile, breakthroughs in biotechnology are driving a transformative shift in the healthcare sector. These innovations are paving the way for personalized treatments

tailored to individual patient needs. Substantial investments in biotechnology aim not only to enhance overall human health but also to develop targeted therapies for various illnesses. Advanced approaches to treating previously incurable diseases have been made possible by advances in genetic engineering, personalized medicine, and biopharmaceuticals such as CRISPR and gene therapy (Doudna and Sternberg 2017). The establishment of smart factories is a result of the integration of IoT and AI into production processes. Advanced manufacturing is predicted to rise as a result of the predicted productivity gains, cost savings, and product quality improvements that automation will bring. However, this change also highlights the need for worker retraining initiatives and raises concerns about job displacement (Brynjolfsson and McAfee 2014).

As companies invest in solar, wind, and other green technologies, the renewable energy industry will expand and lead the transition to a low-carbon economy. However, there are significant legislative and regulatory risks associated with this shift due to changes in government climate policies (Carney 2015). The integration of blockchain and the increasing use of digital currencies in finance have the potential to completely transform the industry. Traditional banking and financial services will change as a result of fintech developments, which will improve efficiency and accessibility. Yet the industry will need to address regulatory oversight and cybersecurity deficiencies, especially regarding virtual currencies (Catalini and Gans 2016).

Agriculture is on the verge of a major transformation, thanks to the developments in precision farming, vertical farming, and lab-grown crops. These innovations can solve food safety issues, reduce negative environmental impacts, and boost crop yields (Despommier 2011). Consumer preferences are changing, with a growing trend towards plant-based and lab-grown meat products. Concerned about sustainability, animal welfare, and health, companies such as Beyond Meat and Impossible Foods are leading the way in this shift (Szejda and Urbanovich 2019). Food companies may find it advantageous to use alternative proteins, but they may encounter difficulties in gaining both market acceptance and regulatory approval (Tubb and Seba 2020). Global e-commerce sales are expected to reach $7.39 trillion by 2024, indicating the sector's tremendous expansion (eMarketer 2021). Traditional bricks-and-mortar stores have responded to this shift in consumer expectations by adopting omnichannel strategies that seamlessly integrate online and physical experiences. Furthermore, the gig economy is transforming the labor market by offering flexible work schedules, but also raising concerns about employee rights and job security (Katz and Krueger 2023).

The global business environment is undergoing fundamental transformation across various industries as a result of rapid and sustained advances in technology. In order for industries to fully benefit from these technological advances, they must successfully address the associated security, ethical, and regulatory challenges. Proactively addressing these issues, companies may realize the full potential of emerging technologies, drive growth and contribute to a sustainable and inclusive future.

1.3 Technological Advancements as a Leading Factor in Strategy

Organizations need to consider numerous elements while formulating their future plans. Imagine the early days of internet when the world was on the verge of a major digital revolution. Forward-thinking businesses that anticipated the potential of this growing technology adapted and thrived, while others fell behind, unable to fully grasp the profound consequences of the ongoing changes. Jumping ahead to the present, we are experiencing a comparable period of significant change. Fluctuating variables pose significant challenges for forecasting and preparing for the future. Particularly in light of the vibrant debate around the environment and technology, it is vital that we delve deeper into technological principles to navigate this complex terrain (WEF 2023). Just as companies in the past had to diligently observe market trends and consumer behavior, today's organizations need to proactively monitor and assess advancements in their respective industries. Constant vigilance is necessary to monitor emerging concepts, potential threats, shifts in the competitive landscape, and changes in customer preferences. Furthermore, it is crucial to consider many factors such as political conflicts, regulatory changes, macroeconomic stability, and revolutionary technological advancements that have the potential to influence global trade (Rodrik 2018). In a complicated world with many different factors, it becomes increasingly difficult to thrive and survive.

Technology has been instrumental in the growth and progress of organizations, revolutionizing operational practices. The introduction of mobile technology and cloud computing has significantly transformed businesses, converting data into an asset that influences decision-making and strategic planning. According to Reinsel et al. (2018), the amount of global data is expected to exceed 175 zettabytes by 2025, indicating a significant growth in digital information. Currently, at the brink of another significant advancement in technology, the fusion of AI and machine learning (ML) has the potential to transform various industries, ranging from customer service to supply chain management. PwC (2017) estimates that AI has the potential to make a significant contribution of $15.7 trillion to the global economy by 2030. In order to maintain their competitive edge and foster the creation of new ideas, companies need to allocate resources towards the cultivation of AI skills. Nevertheless, this incorporation also poses substantial dangers, such as potential corporate decline and ethical concerns regarding the openness of decision-making processes (Brynjolfsson and McAfee 2014). The pervasive use of IoT devices represents a substantial and revolutionary shift. Imagine a world in which everyday objects are all connected, constantly generating data, and strengthening connections. According to TechInsights' (2024) forecast, the number of connected devices was 32 billion at the end of 2023 and is projected to reach 46 billion by 2028, growing at 8% per year.

The interconnection of these networks will lead to new economic theories and increased opportunities for innovation. However, it also raises questions about the management and security of these broad networks. The integration of the IoT with

AI has the potential to create intelligent environments. However, it is crucial not to overlook the associated concerns regarding the protection of data privacy and security (Roman et al. 2013). Looking further ahead, augmented reality (AR) and virtual reality (VR) technologies are on the verge of revolutionizing many industries, such as retail, real estate, and education. While they offer new opportunities for marketing and education, they also pose significant threats in terms of user privacy and content control (Roesner et al. 2024).

Quantum computing is becoming increasingly important because of its ability to solve sophisticated problems that are currently beyond the capabilities of traditional computers. This technology has the potential to completely transform industries such as pharmaceuticals, finance, and logistics by offering unmatched computational power and optimization skills (Arute et al. 2023). Pioneering quantum technology developed by leading companies such as IBM and Google has the potential to outperform standard encryption methods, hence requiring the implementation of new cybersecurity strategies. The race for quantum supremacy also shows how dangerous it can be for geopolitics when countries compete to be the best in science (Castelvecchi 2024). Often hailed as the next revolutionary technology, blockchain has the potential to increase transparency, security, and efficiency in transactions and data management. Industries such as finance, supply chain, and healthcare are increasingly seeking to enhance trust and traceability. For instance, Walmart is using blockchain to monitor its product supply chain, ensuring food safety and reducing waste (Kamath 2023). Despite the promise of blockchain, legal uncertainties, and scaling issues make it difficult to use (Catalini and Gans 2016).

Companies in many different sectors are facing major opportunities and problems as a result of these technological advances. Not only do companies have to spend money on these technologies, but they also have to deal with the moral, legal, and security issues that come along with them. This will help them get the most out of these new technologies and make the future more connected, efficient, and environmentally friendly.

1.4 Changes on the Way

Technological advancements, changing consumer preferences, and global economic conditions will have a substantial impact on future changes in supply and demand dynamics. But technology is not the only driver of future change. Other key issues, such as changing consumer behavior, geopolitical tensions, and regulatory frameworks, also have a significant impact on shaping the overall situation.

On the demand side, consumer preferences are changing with an increasing trend towards customized, green and premium items. Businesses are being forced to adopt sustainable practices, while investors are looking for inventive solutions to meet these demands. An example of this is the emergence of the circular economy, which is the recycling-based practice of repurposing and reusing materials. This phenomenon is causing substantial transformations in various businesses and

supply chains by promoting sustainability and reducing waste. To capitalize on these opportunities, organizations need to be adept at managing the risks associated with evolving customer expectations and regulatory standards (Boudet and Vollhardt 2018; WEF 2023).

Globalization has resulted in an interconnected and interdependent business environment. Nevertheless, geopolitical conflicts and trade wars have the potential to disrupt supply chains and affect business operations. Companies need to formulate tactics to minimize the potential dangers associated with global instability and ensure the ability to withstand and recover from disruptions in their supply networks (Rodrik 2018). For example, the trade tensions between the US and China in recent years prompted many companies to re-evaluate their supply chains and explore alternative manufacturing locations to mitigate risks. This transformation requires skill and the ability to adapt quickly to changing geopolitical landscapes. The rise of protectionist measures, including tariffs and trade barriers, complicates international trade. Companies need to manage these complications by expanding their supply chains and exploring new markets.

The regulatory environment will continue to evolve as countries enact new laws and regulations to address growing concerns. Organizations will need to prioritize compliance and adapt to evolving regulatory frameworks in order to address data protection, cybersecurity, and environmental concerns. Failure to comply with regulations can result in substantial fines and reputational damage (Bamberger and Mulligan 2015). The General Data Protection Regulation (GDPR) in Europe is an example of rigorous data protection legislation that the organizations must traverse. These requirements require organizations to collect, store, and manage personal data in a way that emphasizes the importance of strong data governance processes. As data localization laws become more prevalent, organizations must rethink their data management practices to comply with local legislation (Chander and Lê 2015). The Paris Agreement remains a driving force in the environmental sphere, driving global efforts to reduce carbon emissions. Companies are increasingly required to take responsibility for their environmental footprint, which requires them to implement sustainable practices and reporting systems, such as the Task Force on Climate-related Financial Disclosures (TCFD) (Carney 2015). ESG (Environmental, Social, and Governance) investing is the practice of forcing companies to prioritize sustainability by considering environmental, social, and governance factors. Investors are increasingly taking ESG factors into account when making decisions that affect corporate behavior and strategy. Companies that prioritize to ESG factors are often seen as more responsible and forward-thinking. This perception can enhance their reputation and make them more attractive to a wider range of stakeholders. For instance, a study by Eccles et al. (2014) found that organizations with robust sustainability strategies had better operational performance and were more attractive to investors. This trend is compelling organizations to incorporate sustainable practices into their fundamental plans and operations, ensuring their long-term sustainability and competitiveness.

1.5 Challenges in Risk Management in the Digital Age

With digital transformation, risks in the areas of cyber security, data privacy, compliance, labor, third parties, business continuity, environment, and sustainability have become critical risks that need to be managed for the long-term sustainability and competitiveness of companies. The reason why these risks are considered critical risks is not because they are mostly emerging in the digital age and are new risks for businesses, but because of their impact and the speed with which they are spreading. For example, on July 19, 2024, more than 8.5 million computers worldwide experienced a blue screen error. This event, which was actually caused by a simple update, was considered the largest IT outage in history. After CrowdStrike, which provides cybersecurity software to Microsoft, distributed a faulty software update to computers, CrowdStrike CEO George Kurtz said the problem was caused by "a flaw in a single content update for Windows hosts." The "single content" update bug caused thousands of flights to be grounded, hospitals to be disrupted, banks to go offline, payment systems to crash and media outlets to go off the air around the world, from the US to India, Europe to Australia and New Zealand. It is estimated to have cost US Fortune 500 companies alone $5.4 billion. The fact that a situation caused by a software update could have such a global impact at the same time is an important indication of the scale and the speed of risk propagation in the digital age.

The incredible advances in how risks affect and propagate have created a significant challenge for managing them. By definition, risk is the possibility of a future event affecting the things we value (Luhmann 1991; Beck 1992; Aven and Renn 2009; Rosa 2010). According to Ewald (1991), calculating risk means mastering time and disciplining the future. In this respect, the time dimension of risk is extremely important. When we calculate risks, we classify them into short, medium and long-term risks according to their probability of occurrence in the near or distant future. However, with digital transformation, the rapid changes in technology, business processes and organizational structure are significantly reducing the clarity between the concepts of near and far future. A nineteenth century shoemaker, tailor, miller or baker will obviously have a very different time frame in mind when referring to the near and far future than a CEO of a global company operating in the digital age. For the former, the far future may be a century, while for the latter it may be only 15–20 years. This uncertainty between the near and far future makes it difficult to predict the risks that companies will face in the future. In 20 years' time, it is not easy to predict the technological, health, environmental, and corporate governance developments and the risks that these developments will bring with them.

As the pace of change increases, companies need to be more careful against risks. At this pace of change, the consequences of company management "falling asleep at the wheel" can be severe for the company. For those in executive positions, the concept of digitalization is no longer a technical issue that can be delegated to IT experts alone. Given the disruptive effects of digital technologies, it is difficult for organizations to survive in the digital age by simply adding a digital touch to certain processes and products (Steiber et al. 2021). In order to realize the full

potential of digital transformation, it seems inevitable that companies will have to radically change their approach to business, processes and organizational structures (Nadkarni and Prügl 2021).

1.6 The Focus of This Book

Imagine you are on the brink of an industrial revolution; the steam engine is transforming industries and communities. Those who embraced this technological leap changed their destinies; those who lagged behind were struggling to catch up. Today, we are in a similar phase of transformation. Artificial intelligence, blockchain, distributed finance, and the metaverse are among the technologies that will completely transform our interactions with the planet and our way of life.

In the fast-paced digital age, it is vital for business leaders to be aware of the changes brought about by the digital age and to consider developments in a broader context. With the advent of the digital age, there has been a surge in the publication of technical books on new technologies, and this trend is likely to continue. These books undoubtedly play a crucial role in addressing the technical aspects of the digital age. However, it is also important to recognize the need for books that address the strategic, organizational, and cultural changes that the digital age require of companies. Such books are invaluable as they provide guidance to leaders on how to navigate the transformation processes. They help leaders understand how digital technologies are impacting business models, operational processes, and customer interactions, enabling more informed and strategic decision-making. This book aims to comprehensively address the challenges and opportunities faced by companies during their digital transformation journeys and to provide guidance to executives throughout these transformation processes.

Digital transformation is about more than just building a digital infrastructure to collect and process large amounts of data. It is also about understanding how digital technologies impact organizations' strategic decisions, the way they do business, the legal and ethical environment, and the creation of innovative services and products. This book is particularly aimed at those who are leading digital transformation initiatives in their organizations or who want to develop their strategic thinking skills in the context of the digital age. Given the speed and complexity of the digital age, we have tried to give you as complete a picture as possible. The value of the book lies in the thorough analysis of these crucial matters and the extensive research offered in many chapters. Each chapter focuses on clarifying the complexities of the current business landscape and offering helpful perspectives and tactics.

The objective of this book is to motivate readers to adopt a proactive stance and to enhance their awareness of the latest technological innovations. This will facilitate the creation of a more connected, efficient, and environmentally friendly business. Futurisks provides recommendations for navigating an environment of

ongoing transformation, transforming potential threats into opportunities for success. Additionally, the book seeks to equip readers with the confidence to navigate the complexities of a rapidly changing global stage and to seize the opportunities that lie ahead.

References

Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R et al (2023) Quantum supremacy using a programmable superconducting processor. Nature 574(7779):505–510. https://doi.org/10.1038/s41586-019-1666-5

Aven T, Renn O (2009) On risk defined as an event where the outcome is uncertain. J Risk Res 12(1):1–11. https://doi.org/10.1080/13669870802488883

Bamberger KA, Mulligan DK (2015) Privacy on the ground: driving corporate behavior in the United States and Europe. MIT Press. Retrieved from https://mitpress.mit.edu/9780262029988/privacy-on-the-ground/

Beck U (1992) Risk society: towards a new modernity. SAGE Publications, London

Boudet J, Vollhardt K (2018) Personalization at scale: first steps in a profitable journey to growth. McKinsey & Company. Retrieved from https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/personalization-at-scale-first-steps. Accessed 15 Mar 2024

Brynjolfsson E, McAfee A (2014) The second machine age: work, progress, and prosperity in a time of brilliant technologies. W. W. Norton & Company

Carney M (2015) Breaking the tragedy of the horizon—climate change and financial stability. Bank of England. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/speech/2015/breaking-the-tragedy-of-the-horizon-climate-change-and-financial-stability. Accessed 15 Mar 2024

Castelvecchi D (2024) The AI–quantum computing mash-up: will it revolutionize science? Nature. https://doi.org/10.1038/d41586-023-04007-0

Catalini C, Gans JS (2016) Some simple economics of the blockchain. SSRN https://doi.org/10.2139/ssrn.2874598

Chander A, Lê UP (2015) Data nationalism. Emory Law J 64(3):677–739. Retrieved from https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/

Despommier D (2011) The vertical farm: feeding the world in the 21st century. Thomas Dunne Books/St. Martin's Press

Doudna JA, Sternberg SH (2017) A crack in creation: gene editing and the unthinkable power to control evolution. Houghton Mifflin Harcourt

Eccles RG, Ioannou I, Serafeim G (2014) The impact of corporate sustainability on organizational processes and performance. Manag Sci 60(11):2835–2857. http://www.jstor.org/stable/24550546

eMarketer (2021) Global e-commerce forecast 2021. Retrieved from https://www.emarketer.com/content/global-ecommerce-forecast-2021

Ewald F (1991) Insurance and risk. In: Burchell G, Gordon C, Miller P (eds) The Foucault effect: studies in Governmentality. Harvester Wheatsheaf, London

WEF. (World Economic Forum) (2023) Global risks report 2023. World Economic Forum. https://www.weforum.org/publications/global-risks-report-2023/. Accessed 4 Jan 2024

Kamath R (2023) Food traceability on blockchain: Walmart's pork and mango pilots with IBM. J Br Blockchain Assoc 1(1):1–12. https://doi.org/10.31585/jbba-1-1-(10)2018

Katz LF, Krueger AB (2023) The rise and nature of alternative work arrangements in the United States, 1995-2022. ILR Rev 72(2):382–416. https://doi.org/10.1177/00197939188200008
Luhmann N (1991) Soziologie Des Risikos. W. de Gruyter, Berlin
Nadkarni S, Prügl R (2021) Digital transformation: a review, synthesis and opportunities for future research. Manag Rev Q 71:233–341. https://doi.org/10.1007/s11301-020-00185-7
PwC (2017) Sizing the prize: What's the real value of AI for your business and how can you capitalise? PwC. https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf. Accessed 22 Mar 2024
Radu R, Amon C (2021) The governance of 5G infrastructure: between path dependency and risk-based approaches. J Cybersecurity 7(1) article tyab017. https://doi.org/10.1093/cybsec/tyab017
Reinsel D, Gantz J, Rydning J (2018) The digitization of the world from edge to core. IDC. Retrieved from https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. Accessed 22 Mar 2024
Rodrik D (2018) Straight talk on trade: ideas for a sane world economy. Princeton University Press
Roesner F, Kohno T, Molnar D (2024) Security and privacy for augmented reality systems. Commun ACM 57(4):88–96. https://doi.org/10.1145/2580723.2580730
Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. Comp Networks 57(10):2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018. ISSN 1389-1286, Accessed 22 Mar 2024
Rosa EA (2010) The logical status of risk—to burnish or to dull. J Risk Res 13(3):239–253. https://doi.org/10.1080/13669870903484351
Steiber A, Alänge S, Ghosh S, Goncalves D (2021) Digital transformation of industrial firms: an innovation diffusion perspective. Eur J Innov Manag 24(3):799–819. https://doi.org/10.1108/EJIM-01-2020-0018
Szejda K, Urbanovich T (2019) Plant-based and cultivated meat diffusion of innovation: profiles of U.S. early adopter consumer segments. Research Report. The Good Food Institute, Washington, DC. http://go.gfi.org/alternative-protein-early-adopter-US. Accessed 22 Mar 2024
TechInsights (2024) Global connected device forecast: growth trends and projections ethrough 2028. Retrieved from https://www.techinsights.com/blog/global-connected-and-iot-device-installed-base-forecast-2018-2028. Accessed 22 Mar 2024
Tubb C, Seba T (2020) Rethinking food and agriculture 2020–2030: the second domestication of plants and animals, the disruption of the cow, and the collapse of industrial livestock farming. RethinkX. Retrieved from https://www.rethinkx.com/food-and-agriculture. Accessed 22 Mar 2024

Halis Kiral is an associate professor at the Social Sciences University of Ankara in Türkiye. He is also Head of Audit and Risk Management Department and Director of Center for Audit and Risk Management (ASBÜDRM) at the ASBU. He was a visiting scholar in the Duke Center for International Development (DCID) for the 2017-2018 academic year. He has also worked in the Ministry of Finance of Türkiye as a state budget expert, public finance expert, head of Central Harmonization for Internal Audit, and head of the Budget Policy Department. He wrote a number of articles, books, and book chapters on topics such as public finance, public financial management and control, specifically internal audit and risk management, public budgeting, and applied economics.

Gökhan Yılmaz is a Partner at PwC Türkiye and currently leads the firm's Forensic, Financial Crime, and Compliance services. With more than 25 years of experience across global banks and consulting environments, he specializes in ethics, compliance, fraud investigations, internal audit, data analytics, and risk management. He holds a Bachelor's degree in Business Administration

from Marmara University, where he also earned a PhD in Accounting and Finance, focusing his doctoral research on the detection and prevention of fraud using big data analytics. In addition, he completed a master's thesis on computer-assisted audit techniques and holds a second master's degree in Forensic Sciences from Üsküdar University. Dr. Yılmaz is an active board member of the Association of Certified Fraud Examiners (ACFE) Turkey Chapter and the Ethics and Reputation Society. As a recognized professional and educator, he frequently delivers training and contributes to academic and industry research. He holds several prominent certifications including CFE, CIA, CISA, CPA, CCSA, and CRMA, reflecting his multidisciplinary expertise and commitment to the profession.

Part II
Futurisk in Digitalization, ESG, Finance and Supply Chain

Chapter 2
Unveiling the Shadows: Anticipating Future Cyber Risks and Their Impacts on Businesses

Çetin Karahan, Hakan Velioğlu, and Yenal Arslan

Abstract In 2023, more than five billion people in the world are using the internet and they spend about seven hours on the internet every day. Such increased dependence on Information and Communication Technologies (ICT) requires individuals and businesses to approach cyber risks and emerging technologies with greater caution. If we do not count the reputation and moral damages of the business, cyber risks cost 8.4 trillion dollars in the world in 2022. Studies on the impact of cyber risks on organizations generally consider organizations as a whole and evaluate the impact of risk from this perspective. While the impact of a risk affecting one department can affect other departments, the impact of certain risks on some departments is much more direct. Our research covers a wide range of cyber security topics, including emerging technologies, legal implications, employee training, and the interconnectedness of cyber risks within an organization and also diverges from existing studies that primarily examine businesses as a whole and evaluate the overall impact of cyber risks from that view. By delving into the future cyber risks that potentially affect departments within organizations, our study offers a more granular and comprehensive understanding of the intricate dynamics between cyber risks and departmental operations. This approach allows for a more nuanced analysis of the specific implications and tailored strategies for assessing and mitigating cyber risks at the departmental level, providing valuable insights for practitioners and decision-makers seeking to enhance their organization's cyber security posture and for academics working on cyber security.

Ç. Karahan
Secretariat of Defence Industries, Defence Industry Agency of Türkiye, Ankara, Türkiye
e-mail: ckarahan@ssb.gov.tr

H. Velioğlu
Ministry of Agriculture and Forestry, Ankara, Türkiye
e-mail: hakan.velioglu@tarimorman.gov.tr

Y. Arslan (✉)
Ankara Yildirim Beyazit University, Ankara, Türkiye
e-mail: yenalarslan@aybu.edu.tr

H. Kıral, G. Yılmaz (eds.), *Futurisks: Risk Management in the Digital Age*, Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application, https://doi.org/10.1007/978-981-96-6448-1_2

Keywords Cyber security · Future risks · Information technology management · Emerging technologies · Department-based cyber risks

2.1 Introduction

Cybersecurity is a vital issue for individuals, institutions, and companies in today's world. Cybersecurity can be defined as a set of measures taken to prevent, detect, and intervene in risks arising from the use of Information and Communication Technologies (ICT) (Ghelani 2022). ICT plays an indispensable role in the functioning of modern society, in economic development, and in social welfare. However, ICT is also susceptible to new types of cyber risks. Cyber risks refer to intentional or unintentional harmful actions directed at ICT systems, such as cyberattacks, cybercrimes, cyber espionage, cyber terrorism, cyber warfare, and cyber sabotage. Cybersecurity is an ongoing and perpetual struggle. Although the fundamental characteristics of IT, the intricate nature of information technology systems, and human imperfections are the underlying factors contributing to numerous cybersecurity vulnerabilities, the quest for a definitive and enduring solution remains elusive and is unlikely to be achieved in the immediate future (Rahaman 2022).

The magnitude and impact of cyber risks have been increasing in recent years. Particularly due to the Covid-19 pandemic, the acceleration of digitalization and the proliferation of remote activities such as work, education, health, and shopping have brought cyber risks even more to the forefront. By 2022, 4.95 billion people in the world are using the internet. This corresponds to 62.5% of the total world population. People spend almost 7 h on the internet every day (Datareportal 2022) There are 5.18 billion Internet users worldwide in 2023. It is predicted that there will be more than 7.5 billion internet users by 2030 (Stackscale 2021; Mattioli et al. 2023). Furthermore, the number of devices linked to IP networks will exceed three times the world's population. The number of networked devices is also expected to reach 29.42 billion, 14.7 billion Machine-to-Machine (M2M) connections will have been established (Statista 2023a; Safaei Pour et al. 2023).

In 2022, cybercrime collectively cost US businesses $10.2 billion, according to the FBI's annual Internet Crime Report (Internet Crime Complaint Center 2022). The surge in cyberattacks targeting organizations has prompted a significant rise in cybersecurity expenditures. According to industry reports, it was projected that firms would allocate over $169 billion in 2022 to fortify their technological defenses against cyber threats (Gartner 2021; Kumar and Mallipeddi 2022). According to Vasiloiu (2023), a study conducted by Statista (Fig. 2.1), the damage caused by cyberattacks to the global economy will reach 23.84 trillion dollars by 2027. The global cost of cybercrime was estimated at some 8.4 trillion U.S. dollars in 2022. The cost of incidents is 11 trillion U.S. dollar mark in 2023. By 2026, annual cybercrime costs exceed 20 trillion, an increase of nearly 150 percent compared to 2022.

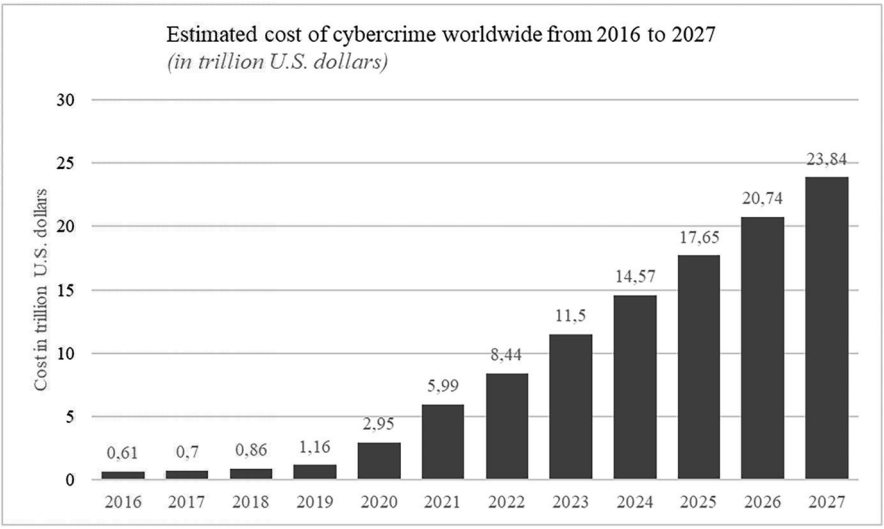

Fig. 2.1 Estimated cost of cybercrime worldwide from 2016 to 2027 (Vasiloiu 2023)

In this study, after a general literature review on cybersecurity, the threats that companies and their departments may face in the near future will be discussed. This chapter aims to provide an overview of the current state of cyber security and assess future risks that businesses may encounter. The introduction highlights the importance of cyber security for businesses and sets the stage for the rest of the paper. Along with the cyberattacks, emerging technologies and their potential impact on cyber security, insider threats and the role of employees in cyber security, AI-augmented cyber warfare and its implications, the talent gap and the need for skilled cyber security professionals, and the increased use of cyber insurance were also examined. The departmental analysis of cyber risks explores the impact of cyber risks and emerging technologies on different departments within an organization and the interconnectedness of cyber risks and reliance on the IT department. The conclusion summarizes the key findings and provides recommendations for businesses to prepare for future cyber security risks.

2.2 Cyber Security Risks

In today's digital age, businesses face an array of ever-evolving risks that threaten their operations, assets, and reputation. Among these risks, cyber security takes center stage as a critical concern for organizations worldwide. The interconnected nature of modern businesses, coupled with the growing reliance on technology, has exposed them to a multitude of vulnerabilities. From sophisticated supply chain attacks to emerging threats like quantum computing, businesses must navigate a

complex landscape of potential hazards. This chapter explores various sub-topics encompassing the future risks to businesses in the realm of cyber security, shedding light on the challenges posed by data breaches, social engineering, insider threats, and more. Furthermore, it delves into the potential dangers posed by advanced technologies such as the Internet of Things (IoT), advanced robotics, and 3D & 4D printing. Additionally, it highlights the scarcity of skilled cybersecurity professionals and the escalating adoption of cyber insurance. Lastly, it examines the role of blockchain technology as both a solution and a potential risk factor in the quest for securing business operations. By understanding these sub-topics and their implications, businesses can proactively address the ever-changing cybersecurity landscape and safeguard their interests.

2.2.1 Supply Chain Attacks

Supply chain attacks are a type of cyberattack on the rise. According to Statista, around 11 million customers were affected in supply chain cyber-attacks worldwide (Statista 2023b). In the first quarter of 2023, over 60 thousand customers were reported to be impacted by supply chain attacks. Common customer attacks in supply chain cyberattacks included counterfeiting, drive-by compromise, and malware infections. Supply chains have experienced the staggering economic cost of data breaches. For instance, cyber-attacks caused a component supplier of Boeing and Airbus to lose around $54 million (Sadeghi et al. 2023). In these attacks, malicious actors target a company's vendors and suppliers to gain access to their systems, and this type of attack is particularly challenging to defend against because it can be hard to know which vendors to trust. Additionally, these attacks can be difficult to detect because they may not cause any immediate disruption. However, the long-term impact of a successful supply chain attack can be significant, as it can give the attacker access to a company's most sensitive data.

2.2.2 Cloud Security Risks

Cloud computing has emerged as an accessible and cost-effective solution for delivering on-demand services to users. It has become particularly popular among individuals and organizations that lack the resources to invest in extensive hardware, software, and security maintenance expenses. The pay-per-use model, a fundamental aspect of cloud computing, has not only attracted individuals but also businesses seeking to maximize their profits. However, the complexity of the cloud computing model and the shared technologies it relies on have raised concerns regarding security. Virtualization, multitenancy, data security, and general vulnerabilities have been extensively discussed in the literature as key areas of focus (Ali et al. 2023; Khoda et al. 2022).

Many SMEs use cloud-based services, such as data storage or software-as-a-service (SaaS) applications, to reduce costs and improve efficiency. However, these services can create additional security risks if they are not adequately secured. As organizations increasingly rely on cloud services, there could be new cloud security risks, such as data breaches, cyberattacks, or service disruptions. 45% of breaches are cloud-based. According to a recent survey, 80% of companies have experienced at least one cloud security incident in the last year (Cloud Security Alliance 2022).

Another major risk associated with cloud security is the reliance on third-party service providers, who may not have the same security standards as the company using their services, leaving the data stored on their servers vulnerable to attack. Furthermore, interconnectedness means that a security breach at one provider could potentially impact other companies using their services, as demonstrated in 2018 when a malicious actor gained access to a cloud service provider and used it to launch attacks on other companies, including Facebook and Amazon (CBS News 2019).

2.2.3 Quantum Computing Threats

Quantum computing, rooted in the principles of quantum mechanics, explores the computational capabilities of computers and finds applications in various domains such as communications, imaging, information science, electronics, and cryptography. The emergence of practical quantum algorithms, facilitated by the increasing availability of quantum computers, has further enhanced the potential of this technology. The unique features of superposition and entanglement of states make quantum computers highly advantageous (Rasool et al. 2021). According to current projections, there is a 15% likelihood of quantum computers becoming practically available by 2026. Furthermore, these chances are expected to rise to 50% by the year 2031 (Sun et al. 2019). However, the rapid advancement of quantum computing also raises concerns in the field of cybersecurity. Classical cryptographic methods used in modern internet communications and e-commerce may become vulnerable to quantum attacks, posing a threat to encryption technology (Kumar et al. 2022; Raya et al. 2023; Chen et al. 2016).

2.2.4 Data Breaches, Compliance Violation

The prevalence of data breaches is increasing as individuals' lives become more intertwined with online activity. According to IBM average total cost of a data breach reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022 (IBM 2022). Protecting such data from cyber threats has become more challenging due to the sheer volume of information that is being stored online. In

response, regulatory compliance is gaining importance as stricter rules are implemented to safeguard data. The General Data Protection Regulation (GDPR) is an example of such regulations that mandate companies to take specific steps to protect individuals' data and be transparent about their data handling practices. The implementation of the GDPR in May 2018 has instigated a transformative change in the realm of data protection. Organizations now encounter substantial hurdles, including the need to showcase compliance (or auditability) and establish automated mechanisms for compliance verification. These challenges arise from the intricate and ever-evolving nature of consent, as well as the vast scale at which compliance verification must be executed (Chhetri et al. 2022). Looking ahead, the future of cybersecurity involves more robust measures to safeguard data, not just through investment in better security measures, but also by increasing transparency in data handling practices. Furthermore, compliance will be increasingly important as more stringent regulations are introduced. Ultimately, the protection of individuals' data will be the focal point of cybersecurity in the future, necessitating proper data encryption and storage as well as promoting individuals' awareness about how their data is being used (Qiu et al. 2020).

The interconnected and decentralized nature of contemporary digital systems and services enables the gathering of personal data from individuals across the globe, as well as its transfer between different countries (Razaghpanah et al. 2018). This introduces potential privacy risks, as organizations involved in the transmission of personal data may be subject to varying data protection laws and may not provide an equivalent level of safeguarding (Guamán et al. 2023). The International Association of Privacy Professionals (IAPP) annual privacy governance report (2020) reveals that only 47% of European companies are fully or very compliant with privacy regulations, highlighting the need for automated solutions to verify compliance with the General Data Protection Regulation (GDPR) (Chhetri et al. 2022). Noncompliance with the GDPR can lead to substantial fines, emphasizing the importance of implementing mechanisms to ensure adherence (Chhetri et al. 2022).

In addition to the GDPR, there are a number of other data protection regulations in place around the world. Figure 2.2 illustrates the global landscape of data protection regulations, highlighting some countries and their corresponding data protection laws.

2.2.5 Social Engineering and Phishing

Within the realm of cyber-attacks, the susceptibility of individuals presents a significant challenge in business communities, as hackers can easily exploit insider risks and threats (Alsharif et al. 2022). Despite the implementation of multiple layers of security measures and employee education on phishing risks, malicious actors employ sophisticated tactics to exploit the vulnerabilities of the human