Exploring Risks in the Metaverse in an Immersive Digital Economy

Victor Chang[1], Sandra Strittmatter[1], Vitor Jesus[1], Lewis Golightly[2], Pin Ni[3] and Karl Hall[2]
[1]*Aston University, Birmingham, U.K.*
[2]*Teesside University, Middlesbrough, U.K.*
[3]*University College London, London, U.K.*

Keywords: Metaverse, Immersive, Virtual Reality (VR), Augmented Reality (AR), Extended Reality (XR), Cybersecurity.

Abstract: The Metaverse is the next paradigm of computing and a combination of the words next and the universe. Immersive technology such as Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR), and Extended Reality (XR) have been emerging at a fast pace in recent years. The Metaverse aims to solve the limited social dynamic of using the internet for communications. Since the Covid-19 pandemic, the internet has been used for education, work, and gaming in a more immersive method than ever before. However, the problem the Metaverse aims to solve is the social limitations of using technology such as Microsoft teams. In this paper, we address the opportunities of the Metaverse, such as online gaming and an enhanced 3D virtual community life, alongside the potential of cyber risk and security issues, such as data privacy and information security. We complement our paper with a risk assessment of the Metaverse, particularly focusing on risks associated with cybersecurity.

1 INTRODUCTION

There isn't a consensus on the definition of the *Metaverse*, yet some argue that it entails all aspects of Augmented Reality (AR), Mixed Reality (MR), and Virtual Reality (VR), which make up the networked Extended Reality (XR) (Anderson and Rainie, 2022); others define it as the convergence of the virtual world and the real world (Deloitte, 2022). While organizations across sectors are attempting to define what the future of the Metaverse represents for them, we see initiatives to leverage the early stages of the Metaverse to extend their brand presence and customer touchpoints (Brown, 2022). AR and VR enhance the Metaverse and enable businesses to elevate their offering with a new layer of experiences and interactions (Bechtel and Launer, 2022). For example, L'Oréal and Avon allow users to try on makeup virtually using their app or website, enabling consumers to select their preferred shade. These are small steps towards transforming customer journeys into fully immersive experiences that are poised to permeate and transform retail and advertising, work, education, entertainment, and social interaction (Deloitte, 2022).

As this rise of the Metaverse is in motion, there has been an acceleration in its technological advancement brought upon by the investment of brands and new social behaviors stemming from the COVID-19 pandemic (Anderson and Rainie., 2022). It is estimated that the market value of the Metaverse could reach above 750 billion USD by 2026, thus motivating investment in devices, tools, and platforms (Elnaj, 2022). The Metaverse presents many opportunities for businesses and consumers, with brands creating content that generates value for customers and extends brand interaction (Elnaj, 2022). However, along with the rapid development and perceived opportunities and advantages, many risks and uncertainties are associated with it (Arbanas et al., 2022). Brands must integrate risk identification and mitigation within their plans to leverage the Metaverse in their marketing plans; however, it must come with an integrated exercise on the risks it poses, such as cybersecurity, brand reputation, or digital rights management (Arbanas et al., 2022).

This paper offers an analysis of risks associated with the Metaverse as well as shedding light on its scope, challenges, and opportunities. Our contributions are as follows:

Chang, V., Strittmatter, S., Jesus, V., Golightly, L., Ni, P. and Hall, K.
Exploring Risks in the Metaverse in an Immersive Digital Economy.
DOI: 10.5220/0011990900003494
In *Proceedings of the 5th International Conference on Finance, Economics, Management and IT Business (FEMIB 2023)*, pages 107-113
ISBN: 978-989-758-646-0; ISSN: 2184-5891

- a review of academic literature around immersive reality and the Metaverse;
- a conceptualization of the cyber threat landscape in the immersive technology and the Metaverse;
- an approach to a set of recommendations to integrate risk, opportunity, and business strategy.

The remainder of our paper is as follows. In Section 2, we identify existing themes and review the current literature. In Section 3, we present emerging directions and challenges. Section 4 concludes our paper.

2 BACKGROUND

In this section, we will focus on contemporary risks associated with immersive technology and the Metaverse. We will then move on to address the challenges with these risks and cybersecurity practices that can be adopted to defend against them.

2.1 Risks Associated with the Metaverse

Early opportunities for brands are being leveraged in gaming and fitness, among other industries (Elnaj., 2022). However, brands want to offer extended services and integrate virtual environments to create enhanced user experiences beyond playing games. They will likely use the Metaverse to enable their customers to communicate, shop, watch movies, and attend concerts, as well as most things they are accustomed to doing in the real world. How the Metaverse will interact with the real world in the future is still to be seen (The Economist, 2021), and so are the business and technical specifications, as they vary widely in this initial stage when brands are in a test-and-learn situation (Balis, 2022). Experts are recommending brands enter the Metaverse by selecting target audiences, focusing on their current behaviors and trends, conducting an updated competitive analysis of metaverse adoption, finding natural extensions to their current offering, and identifying the best opportunity to successfully define the brand's user interface and integrate their brand into the Metaverse (Balis, 2022). However, while most companies are focused on the potential opportunities and rewards of the Metaverse, risk should also be a focal point. To extend their brands into the Metaverse, companies need to adopt comprehensive security policies, processes, and technologies that account for safe data collection, processing, transmission, and management (Figure 1), covering the physical and digital domains, protecting customers' personal data, increasing risk detection, and ensuring compliance with new regulations (Arbanas et al., 2022).

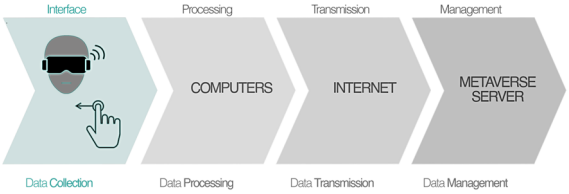

Figure 1: Physical and Digital Domains of the Metaverse.

2.2 Addressing the Metaverse Risks

The Metaverse presents new challenges to brands, and novel risks, as their likelihood and impact are challenging to quantify at this stage (Kaplan et al., 2020). However, companies must initiate and maintain constant documentation of the potential risks the Metaverse could present to be better prepared with a mitigation plan. A Risk Assessment (see Appendix A) can help record each brand's potential risks, estimate their likelihood and impact on the brand, and hence, aid in the prioritization and allocation of resources to mitigate these risks per their "total rating/score" based on the combination of each risk's likelihood and impact. Considering the risk assessment, Internal Risks (Jesus et al. 2022) could be argued to be the most prominent in the Metaverse, as most challenges could be encountered within its boundaries. Furthermore, three main metaverse risks stand out, and they center around cybersecurity involving its main components, the technology, which is new and evolving; the people using the Metaverse, which is now early adopters and learning as it evolves and processes that are not yet regulated, standardized, or advanced enough (Deloitte, 2022). Cybercriminals motivated by the potential of profit are the main actors in the most prominent risks: the potential lack of safety in Metaverse spaces, loss of personal data, and cyber-attacks.

2.3 Security Practices in the Metaverse

Even large companies in the Metaverse continue to consider safety and privacy as a compliance item or afterthought (Anderson and Rainie., 2022). Spaces providing users with the benefits of interaction with the brand and other customers will need to be safe and earn users' trust (Smaili and Rancourt-Raymond, 2022). Gaining safety and trust is imperative as the Metaverse will become an extension of the best and

the worst aspects of people's lives with more complete and immersive experiences. Experts have noted the potential threat of metaverse spaces to exacerbate the prevalence of discrimination, harassment, bullying, hate, and crime (Anderson and Rainie, 2022). Failing to provide safe virtual spaces may result in the loss of customers' adoption of brand extension spaces (Fares, 2022). In order to mitigate this risk, legislation must safeguard users by establishing strict laws that converge the real world and the Metaverse. In turn, the laws will need to protect the users' safety and the virtual avatars created by users (Sethi, 2022). Policing in the Metaverse: What Law Enforcement Needs to Know, a Europol report, focuses on future crimes fueled by new technology. It is intended to inform law enforcement agencies and policymakers on the Metaverse and the need to extend and modernize policing tactics. Enforcing entities have begun to enter the Metaverse to protect users. The INTERPOL has also acted by designing a virtual experience intended for law enforcement with hands-on training (Europol, 2022). To support law enforcement efforts, brands must integrate content moderation into their process and technology to identify and address content and user behavior that violates their user terms (Europol, 2022). Safety is a considerable risk. A Risk Matrix can be used by Cybersecurity Managers to make strategic security decisions which can be observed in Appendix A, which calls for attention and dedication of resources.

3 CYBERSECURITY STRATEGIES IN IMMERSIVE TECHNOLOGY

In this section, we address Cybersecurity considerations around immersive technology and the Metaverse, including personal data and the emerging cyber-attack landscape.

3.1 Protecting Personal Data

While the metaverse spaces pose a major risk, the personal data collected and its use carries meaningful risk as well, Appendix A. Brands can benefit from the vast data generated by the metaverse users and behaviors, as it can be utilized to enhance the development of robots and problem-solving (Sun et al., 2022), 20 minutes of a VR experience can gather 2 million distinct data elements, including the way a user breathes, walks, moves or stares, which further enables targeted marketing (Kramer, 2022). However, such extensive information raises ethical concerns surrounding the collection, management, and utilization of user data within the Metaverse (Anderson and Rainie, 2022). Developers must receive prompt guidance to develop metaverse experiences that protect user privacy. This is a difficult challenge due to the wide range of existing technical configurations of each Metaverse, the lack of unified standards (Kumar, 2022), and the increasing interest from attackers to obtain sensitive user data. Data-related attacks will increase as the Metaverse evolves and more data collection methods are developed (Sun et al., 2022). This ties into new privacy concerns that have been raised after the worrying discovery that users overwhelmingly favor mirroring their real-life selves in this virtual environment (Nair et al., 2022). Physical characteristics, such as height, eyesight and physical fitness, and personal characteristics, including gender, age, ethnicity and even disability status, have been provably inferred in such a way (Nair et al., 2022). Users are typically unaware of the true extent of the amount of personal information they are giving away by doing this and are also unaware of its value to potential attackers. For example, such information can be sold to companies employing targeted marketing and advertising. Therefore, companies utilizing this technology should take on the responsibility of communicating to their users the consequences of revealing potentially sensitive information where possible.

Legislation, industries, and brands must work together to protect metaverse user data. The vast amounts of user data and its management require methodical planning that accounts for companies' data gathering, storage, and utilization while maintaining users' confidentiality in a secure location. Data gathering must be limited to necessary data and curated to ensure accuracy (whether collected by devices or provided by users) and include parameters that comply with user data protections (Sun et al., 2022), e.g., EU'S GDPR or the California Consumer Privacy Act. Brands that collect the user data must be anonymized to ensure users cannot be identified (Smaili and Rancourt-Raymond, 2022) and store it in decentralized server structures to avoid massive data leaks or tampering from a single data repository (Sun et al., 2022).

3.2 Emerging Cyber Attack Landscape

Overlapping with the risks to metaverse space safety and the looming threats to user data is the broad subject of cyber-attacks. Much like in the evolution

of the internet, as the Metaverse continues to develop, it will create various opportunities for criminals (Europol, 2022), and the safeguards and technology architecture needed to avoid negative impact are not yet in place (Anderson and Rainie, 2022). Policing the Metaverse will be a monumental task (Europol, 2022). Like other nascent technology, the Metaverse can provide new attack vectors which criminals can exploit. Bad actors can access weaknesses in the evolving Metaverse (Europol, 2022). Users immersed in their metaverse devices will be exposed to exploits through the control of their virtual reality. An XR experience can lead to an attacker influencing users in the real world by manipulating their virtual environment. Users can be victims of several types of attacks, e.g., 'Human Joystick Attacks' by being deceived into moving to unintended physical locations, a 'Chaperone Attack' in which the users' safety boundaries are altered, or an 'Overlay Attack' giving an attacker control of the users' virtual environment. (Europol, 2022).

With threats such as these, a significant responsibility will need to be addressed by the companies building the metaverse platforms (Europol, 2022). Developers need to consider potential cyber-attacks when designing security protocols and firewalls of metaverse platforms. One of the features needed to help avoid hackers from accessing entire networks will be the isolation of incidents since the device and developers will need to leverage edge computing to distribute the processing of data across a range of data centers, servers, and devices (Sun et al., 2022). Furthermore, development for the Metaverse should include integrating antivirus software and novel machine-learning techniques to detect and prevent attacks and, more importantly, to forecast attacks by analyzing metaverse data trends based on the User Generated Content collected (Sethi, 2022). In addition, the builders of the platforms will need to establish a process to relay law enforcement organizations with prompt and accurate information to protect systems, service providers, and users (Europol, 2022). Therefore, law enforcement entities around the world should prepare to access the information needed and support the impending needs and challenges of the Metaverse.

4 EMERGING CONCEPTS IN THE METAVERSE

In this section, we explore contemporary factors and issues surrounding immersive technology and the Metaverse. We focus on how this technology impacts modern warfare, information security and privacy, economic issues, and prospects.

4.1 Cybersecurity and Privacy

The Metaverse presents a wide range of challenges; an important one is client vulnerabilities with the hardware and software associated with the VR and AR headsets which can be an attack vector for malicious hackers. The impact ranges from location spoofing to devise manipulation, which can cause identity theft and a spiral of criminal activity in the Metaverse under someone else's identity (Dunnett et al., 2022).

4.2 Modern Warfare

The Metaverse can present new horizons for Modern Warfare and how the battlefield will change and adapt to technology. There is a theory that with the wonders of the Metaverse, conflict and competition between competing countries will present themselves with future expansion and the immersive university with goals of domination for land and space (Baughman, 2022). One of the most successful use cases of the Metaverse is that it will be adopted the fastest by the military for training experiences, particularly dangerous and high intensity. This method of military training does have limitations from the traditional physical approach but does have enhanced scalability through technology (Ooi et al., 2022).

4.3 Intelligent Healthcare Systems

While the Metaverse initially emerged as an entertainment and social media platform, the extent to which it can positively affect society is far-reaching. Recent developments have suggested incorporating Metaverse into the field of medical technology alongside artificial intelligence (AI). Such an approach could facilitate improvement in many areas of AI-based healthcare, such as therapy and medical image-guided disease diagnosis, by utilizing the Metaverse to aid in the development, prototyping, evaluation, regulation, and translation of such practices (Wang et al., 2022). There is precedent for the use of virtual environments in this way. By using the Second Life platform, one of the precursors to the Metaverse, a virtual environment was developed to train users in nano-computed topography (CT) (Mishra et al., 2012). CT images can be reconstructed virtually and analyzed by using state-of-the-art AI and machine learning algorithms (Litjens et al., 2017). In this case, it is feasible for larger-scale

collaborations between developers and healthcare practitioners to drive forward advances in medical imaging and AI technology in the virtual reality space. Additionally, incorporating virtual interactions into the healthcare sector only adds to the omnichannel strategy, which is becoming increasingly popular and robust in the post-pandemic landscape. Understandably, there are reservations about the validity of such an approach. In response to these concerns, guidance has been issued to assess the credibility of computational modeling in accordance with the Food and Drug Administration in the US.

4.4 The Role of Blockchains

We can also see the introduction of the virtual world independent currency that can be spent in the Metaverse. This can integrate the cryptocurrency movement with coins such as “decentraland” (MANA), the digital property that uses the Ethereum Blockchain, where the owners can make applications and sell and purchase goods and services. The Sandbox (SAND) is a game platform that works on a play-to-earn (P2E) system utilizing Ethereum Blockchain. As a decentralized platform that allows developers to own space in the virtual gaming universe, Axie Infinity (AXS) is a P2E game that works on the Blockchain Ethereum. This game has collectible creatures that you can keep as pets. The game hosts a player's own economy (Akkus et al., 2022). There can also be many positive economic changes presented with the rise of virtual currency, such as a fairer, more transparent financial system moving away from traditional banking. This works by eliminating third-party institutions that we have to put our trust in for every transaction we make (Yu et al., 2018).

With immersive technology providing a landscape for words other than ours, opportunities are demonstrated around owning property and digital real estate inside those worlds. Despite the excitement this causes for investors and the younger generation attempting to get on the property ladder, there are legal issues to address with owning real estate in the Metaverse. These legal issues include defining and understanding property ownership, how to establish and transfer ownership rights for value (potentially resolved through Blockchain and Smart Contracts), how transparent we should be on user identities with their usage, and how will disputes over the contract be determined (Radhakrishna, 2022). The Metaverse presents the opportunity for decentralized virtual worlds in the future. This can be provided immersive 3D virtual events, conferences, and experiences from a singular room. This highlights a potential solution to the 2023 economic crisis, for example. In this housing crisis, in the innovation of this technology, the future could be people in a small property in the physical world. This means businesses do not need to invest in large corporate buildings but can host their meetings, teaching, and office work using immersive reality (George et al., 2021).

The development of the Metaverse could also greatly accelerate the process of asset tokenization. This process is achieved by securitizing non-traded or tradable assets using blockchain technology to enhance the liquidity of these physical assets, reduce transaction costs and risks, accelerate settlement, etc. (BNY Mellon, 2019). The Metaverse serves as a suitable social environment to allow asset tokenization to democratize illiquid assets and investments, which can be real-life physical assets (e.g., real estate, vehicles, commodities) or digital assets such as images, films, recordings, etc. in the virtual world. All assets are broken down into their smallest units (i.e., ownership) and these can be stored securely and circulated quickly in a metaverse using blockchain technology. Hence, the Metaverse is an ideal place to enable online and offline assets to be placed in the same place in a flexible and trusted manner, in a more diverse form for more complex financial transactions. This will undoubtedly further drive the financial industry to produce more reliable, convenient, and customized financial derivatives, financial instruments, portfolio products, etc. For example, portfolios that combine equities and NFT (non-fungible token) digital assets. This will undoubtedly completely revolutionize the order, appearance, and structure of the financial industry in terms of security, credibility, circulation capacity, cost reduction, and efficiency enhancement.

4.5 Digital Twins

In addition, the application of the Metaverse to the digital twin, for example, will also contribute significantly to the transformation of industry and society. The digital twin is essentially an equivalent mapping of the cyber world to the physical world and can be seen as a digital mapping system of one or more critical, interdependent equipment systems, thus reflecting the full lifecycle process of the corresponding physical equipment. One of the most successful applications of the Cyber-Physical System (CPS), CPS brings together computational, cyber, and physical processes. By integrating and collaborating the three technologies of Computation, Communication, and Control, the overall system can be sensed and dynamically controlled in real-time

through information transfer. The digital twin, as an important part of the CPS and even the entire industrial Metaverse, has taken society from "Data" monitoring to "Model" control and gradually to "Meta-Model" management. This has led to applications such as forecasting and automated operations based on artificial intelligence technology (Ni et al., 2021). This will undoubtedly lead to disruptive changes in many industries.

5 CONCLUSIONS

The Metaverse, as an extension of brands in advertising, has excellent potential to engage users in the future, helping users create unique experiences beyond the real world. Brands around the globe see an opportunity for the metaverse spaces to provide a fuller and more immersive brand experience that complements their real-world offering. These immersive experiences will allow customers to interact with their brands and other customers. Consumers, in turn, are eager to try new technology and marketing experiences. However, brands will be increasingly met with challenges, including cybersecurity, threats to customer trust, brand perception, and digital rights management. While newly identified metaverse risks are common across industries, brands will need to establish their priorities in assessing their unique metaverse risk-mitigation responsibility by identifying risks and assessing their importance, with special attention to security, data privacy, guidelines and monitoring, legislation, controlling, and reporting. This will need to be an ongoing process as the metaverse risks will continue to evolve and change as the technology advances, creating the need for innovative and scalable legal, regulatory, and technical solutions. Critical risks identified through the use of a Risk Assessment document indicate the critical need to address potential lack of safety in metaverse spaces, loss of personal data, and cyber-attacks. To support law enforcement efforts, brands must integrate content moderation into their process and technology to identify and address content and user behavior that violates user terms. It will require a two-fold approach to providing solutions to the metaverse risks. The legislation will need to be established with the creation of international and global authority and standards to regulate the Metaverse, in addition to companies establishing adequate programs to mitigate and respond to metaverse risks. The new legislation must safeguard users by establishing strict laws that converge the real world and the Metaverse. The laws will need to protect the users' safety and the virtual avatars created by users. Developers will need to aim at accounting for the unforeseen risks that will come with the expansion and increasing complexity of the Metaverse. This paper has also provided recommendations to address and mitigate mainstream and future challenges in the Metaverse, particularly on Cybersecurity, Modern Warfare, Economical Transformation and Cryptocurrency.

REFERENCES

Anderson, J., and Rainie, L., 2022, The Metaverse in 2040, Pew Research Center Arbanas, J., et al., 2022, The metaverse and Web3: The next internet platform, Deloitte Insights, Deloitte.

Balis, J., 2022, How Brands Can Enter the Metaverse, Brand Management, Harvard Business Review.

Bechtel, M., and Launer, N., 2022, Thinking about investing in the metaverse? Let history be your guide, Deloitte Insights, Deloitte.

Brown, S., 2022, What Second Life and Roblox can teach us about the Metaverse, Ideas Made to Matter, Technology, MIT Management Sloan School.

Deloitte, 2022, The Metaverse Overview, Deloitte, Available at: https://www2.deloitte.com/cn/en/ pages/ technology-media-and-telecommunications/articles/me taverse-report.html (Accessed 08 December 2022)

Elnaj, S., 2022, The Challenges and Opportunities with the Metaverse, Forbes Technology Council, Forbes.

Europol, 2022, Policing in the Metaverse: What Law Enforcement Needs to Know, an Observatory Report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.

Fares, O., 2022, The Metaverse Offers Challenges and Possibilities for The Future of The Retail Industry, Economy, The Conversation.

Ho, M., 2022, The Metaverse is the Marketer's Digital Playground: How Can The Play?, Leadership, Forbes

Jeong, J. and Doss, R., 2022, Just 25% of businesses are insured against cyber attacks. Here's why, Economy, The Conversation.

Kaplan, R., et al., 2020 The Risks You Can't Foresee, Risk Management, Harvard Business Review.

Kramer, S., 2022, Metaverse Privacy Concerns: Are We Thinking About Our Data? Forbes.

Kumar, N., 2022, Six Unaddressed Legal Concerns for The Metaverse, Innovation, Forbes.

Smaili, N. and Rancourt-Raymond, A., 2022, We Need to Anticipate and Address Potential Fraud in The Metaverse, Economy, The Conversation.

Sun, J., et al, 2022, Metaverse: Survey, Applications, Security, and Opportunities, ACM Comput. Surv., Vol. 1, No. 1, Article.

The Economist, 2021, What is the Metaverse?, The Economist explains, The Economist.

Radhakrishna, G., 2022, December. Legal Issues with Real Estate in the Metaverse. In International Conference on

Law and Digitalization (ICLD 2022) (pp. 74-82). Atlantis Press.
George, A.H., Fernando, M., George, A.S., Baskar, T. and Pandey, D., 2021. Metaverse: The next stage of human culture and the internet. International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), 8(12), pp.1-10.
Akkus, H.T., Gursoy, S., Dogan, M. and Demir, A.B., Metaverse and Metaverse cryptocurrencies (Meta Coins): Bubbles of Future?, Journal of Economics Finance and Accounting, 9(1), pp.22-29.
Zhang, L., Xie, Y., Zheng, Y., Xue, W., Zheng, X. and Xu, X., 2020. The challenges and countermeasures of blockchain in finance and economics. Systems Research and Behavioral Science, 37(4), pp.691-698.
Dunnett, K., Pal, S., Jadidi, Z. and Jurdak, R., 2022. The Role of Cyber Threat Intelligence Sharing in the Metaverse. IEEE Internet of Things Magazine.
Yu, T., Lin, Z. and Tang, Q., 2018. Blockchain: The introduction and its application in financial accounting. Journal of Corporate Accounting & Finance, 29(4), pp.37-47.
Baughman, J., 2022. Enter the Battleverse: China's Metaverse War. Military Cyber Affairs, 5(1), p.2.
Ooi, B.C., Tan, K.L., Tung, A., Chen, G., Shou, M.Z., Xiao, X. and Zhang, M., 2022. Sense the physical, walkthrough the virtual, manage the Metaverse: A data-centric perspective. arXiv preprint arXiv:2206.10326.
Nair, V., Garrido, G.M. and Song, D., 2022. Exploring the unprecedented privacy risks of the Metaverse. arXiv preprint arXiv:2207.13176.
Wang, G., Badal, A., Jia, X., Maltz, J.S., Mueller, K., Myers, K.J., Niu, C., Vannier, M., Yan, P., Yu, Z. and Zeng, R., 2022. Development of Metaverse for intelligent healthcare. Nature Machine Intelligence, pp.1-8.
Mishra, S., Sharma, K.S., Lee, S.J., Fox, E.A. and Wang, G., 2012. SLATE: Virtualizing multiscale CT training. Journal of X-ray Science and Technology, 20(2), pp.239-248.
Litjens, G., Kooi, T., Bejnordi, B.E., Setio, A.A.A., Ciompi, F., Ghafoorian, M., Van Der Laak, J.A., Van Ginneken, B. and Sánchez, C.I., 2017. A survey on deep learning in medical image analysis. Medical image analysis, 42, pp.60-88.
The Bank of New York Mellon Corporation (2019) Tokenization: Opening illiquid assets to investors, BNY Mellon.
Ni, P., Li, Y., Li, G. and Chang, V., 2021. A hybrid Siamese neural network for natural language inference in cyber-physical systems. ACM Transactions on Internet Technology (TOIT), 21(2), pp.1-25.

APPENDIX A

#	Risk	Likelihood	Impact	Mitigation	Total Risk Score
	Potential risks. Up to six risks per category	1 = Very unlikely 5 = Very likely	1 = Very low 5 = Very high	If substantial enough, provide mitigation details	Likelihood x Impact
1	Lack of **Safety in Spaces**	5	5	• Legislation & Law Enforcement enter the metaverse. Policing. • Brands to moderate, monitor. • Users reporting suspicious situations or behavior.	25
2	Customer Trust	2	4	• Brands to provide factual data to users. • Brands to maintain space safety.	8
3	Loss / Leak of **Personal Data**	4	5	• Legislation to protect user data. • Brands to create a plan to safely gather, process, transmit, and store user data. • Brands to collect only necessary and allowed data.	20
4	Brand Reputation	2	5	• Brands to associate with trusted partners. • Brands to maintain space safety.	10
5	**Cyber Attacks**	4	5	• Legislation to protect spaces, users and user data. • Distributed network configuration for incident isolation.	20
6	Digital Rights Management	2	2	• Legislation to protect content and data rights. • Concent from users for data collection and ownership.	4
7	Lack of Adoption / Engagement	2	4	• Brands to identify users and create engagement startegies. • Brands to create a scalable and evolving release plan. • Brands and Legislation to create inclusive devices and experiences.	8