ITUPublications

International Telecommunication Union

Standardization Sector

ITU Focus Group Technical Report

(12/2023)

ITU Focus Group on metaverse
(FG-MV)

FGMV-10

Cyber risks, threats, and harms in the metaverse

Working Group 6: Security, Data and Personally identifiable Information Protection

Technical Report ITU FGMV-10

Cyber risks, threats, and harms in the metaverse

Summary

This Technical Report emphasizes the importance of understanding the cybersecurity landscape in the metaverse. It provides an overview of this emerging digital realm and its potential, highlighting its transformative nature. It also analyzes and documents the specific cybersecurity risks, threats, and potential harms associated with the metaverse. This Technical Report covers areas such as identity theft, malware, data breaches, and social engineering. Moreover, it explores the background of cybersecurity risks in the metaverse. Additionally, this Technical Report examines the implications of these cybersecurity risks, including their impact on user trust, virtual economies, and assets.

Keywords

Metaverse, Cyber Risks, Cyber Threats, Harms

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Change Log

This document contains Version 1.0 of the ITU Technical Report on "Cyber risks, threats, and harms in the metaverse" approved at the 4th meeting of the ITU Focus Group on metaverse (ITU FG-MV), held on 4-7 December 2023 in Geneva, Switzerland.

Acknowledgements

This Technical Report was researched and written by Aljawharah Alsalem (National Cybersecurity Authority (NCA), Kingdom of Saudi Arabia) and Hussain Aldawood (NEOM, Kingdom of Saudi Arabia) as a contribution to the ITU Focus Group on metaverse (ITU FG-MV). The development of this document was coordinated by Vincent Affleck (DSIT, United Kingdom), as FG-MV Working Group 6 Chair, and by Christian Alvarez (UNICEF) and Hanna Linderstål (EARHART Business protection agency) as Co-Chairs of Task Group on cybersecurity.

Additional information and materials relating to this report can be found at: https://www.itu.int/go/fgmv. If you would like to provide any additional information, please contact Cristina Bueti at tsbfgmv@itu.int.

Editor:	Aljawharah Alsalem National Cybersecurity Authority (NCA) Kingdom of Saudi Arabia	E-mail: alsalem@nca.gov.sa
Editor:	Hussain Aldawood NEOM Kingdom of Saudi Arabia	E-mail: hussain.aldawood@neom.com
WG6 Chair:	Vincent Affleck DSIT United Kingdom	E-mail: Vincentaffleck2@hotmail.com
Task Group Co-Chair:	Christian Alvarez UNICEF	E-mail: calvarez@unicef.org

Task Group Co-Chair: Hanna Linderstål, EARHART Business protection agency, E-mail: hanna.linderstal@earhart.se

Table of contents

Page

Technical Report ITU FGMV-10

Cyber risks, threats, and harms in the metaverse

1 Scope

The scope of this Technical Report includes an introduction, background on cybersecurity risks and threats in the metaverse, potential harms of cybersecurity risks in the metaverse, implications of the cybersecurity risks in the metaverse, and recommendations for standardization activities.

2 References

None.

3 Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 artificial intelligence (AI) [b-ITU-T M.3080]: “Computerized system that uses cognition to understand information and solve problems.”.

3.1.2 augmented reality (AR) [b-ITU-T P.1320]: “An environment containing both real and virtual sensory components. The augmented reality continuum runs from virtual content that is clearly overlaid on a real environment (assisted reality) to virtual content that is seamlessly integrated and interacts with a real environment (mixed reality).”.

3.1.3 blockchain [b-ITU-T F.751.0]: “A type of distributed ledger that is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.”.

3.1.4 digital twin [b-ITU-T Y.4600]: “A digital representation of an object of interest.”.

3.1.5 extended reality (XR) [b-ITU-T P.1320**]:** “An environment containing real or virtual components or a combination thereof, where the variable X serves as a placeholder for any form of new environment (e.g., augmented, assisted, mixed, virtual or diminished reality).”.

3.1.6 virtual reality (VR) [b-ITU-T P.1320]: "An environment that is fully generated by digital means. To qualify as virtual reality, the virtual environment should differ from the local environment.".

3.2 Terms defined here

None.

4 Abbreviations

This Technical Report uses the following abbreviations**:**

3D	three-Dimensional
AI	Artificial Intelligence
AR	Augmented Reality
IoT	Internet of Things
MR	Mixed Reality

NFT	Non-Fungible Token
PII	Personal Identifiable Information
VR	Virtual Reality

5 Conventions

None.

6 Introduction

This introduction section provides an overview of the metaverse, highlights its potential, and establishes the purpose and significance of this report in investigating and addressing cyber risks within the metaverse.

6.1 Overview

The metaverse is an emerging network of interconnected and immersive 3D virtual worlds, powered by extended reality technology and developing digital capabilities, which is predicted to revolutionize the way in which online users work, shop, learn, and interact with each other. The economic value of the metaverse is expected to reach $5 trillion by 2030 [b-McKinsey].

At the core of creating the metaverse is the employment of extended reality (XR) systems, a catch-all term that refers to immersive technologies that create and host the 3D virtual worlds of the metaverse, including 3D modelling frameworks, virtual reality (VR), and augmented reality (AR) devices. XR products include VR headsets and AR lenses or glasses to view the virtual worlds, whilst additional wearables, such as gloves or hand-held controllers, allow users to interact with objects in these worlds [b-Council-EU]. Other fledgling technology, such as brain-computer interfaces or surgically implanted chips, are expected to be developed to replace traditional control screens and physical hardware to further enhance the experience of a fully seamless, immersive, and interactive metaverse environment [b-Threat]. In addition, it is likely that development of the metaverse will encourage investment in other supporting infrastructure, including spatial and edge computing to better mimic reality, as well as blockchain capabilities, which will likely play a role in securing digital content and avoiding delays or single points of failure. Furthermore, fully virtual workspaces will reimagine the office experience and account for 30 percent of the investment growth by enterprises in metaverse technologies [b-Shein]. Business and industry-oriented metaverses will further develop supportive technology to improve efficiency and save costs, particularly in the use of ‘digital twins’, which can create a virtual representation of an object or system, simulating how it would operate in the real world [b-IBM].

The development of the supportive technologies of the metaverse and investment in their application is expanding the potential of the platforms to revolutionize entertainment, retail, and working environments. Therefore, these technologies are also increasing risk surfaces, providing more opportunities for threat actors to exploit vulnerabilities and obtain unauthorized access to systems, for various malign purposes. Depending on the threat actor and their motivation, different metaverse platforms are at the greatest risk of being targeted. Given its hosting of hundreds of millions of people, gaming and entertainment metaverse platforms are likely to be targeted by disruptive attacks seeking to interrupt online events, ruining user experiences, and incurring likely financial costs. The retail metaverse, considering it is predicted to hold the bulk of potential value, will likely be targeted for theft of customer data and other sensitive information. For the industry-oriented metaverse, organizations are most at threat from groups seeking to conduct malicious operations, particularly those within critical industries.

6.2 Potential of the metaverse

The primary application for metaverse technologies and platforms will be through consumer-oriented offerings, such as gaming, entertainment, and retail. Online gaming and entertainment platforms have been at the forefront of metaverse development, driving the merger of 3D virtual worlds, user social interaction, and customizable avatars considered synonymous with the metaverse experience. The global metaverse gaming and entertainment market currently hosts over 400 million active users a month [b-Mileva] and is currently valued at $51 billion, with predictions it will reach $1.3 trillion by 2033 [b-Advanced-Television]. Gaming and entertainment platforms currently account for around 90 percent of VR content and hardware expenditure [b-OMDIA] and are driving new developments, including ultra-realistic 3D 'metascanning' tools to better render real life objects in the metaverse [b-Rowden] and are incorporating virtual currencies, blockchain, and non-fungible tokens (NFTs) to improve transfers of digital real estate and collectibles [b-Hickey].

Retail leaders have recognized the potential of the metaverse for e-commerce, brand visibility, and marketing purposes, using the platforms to host online events and virtual showrooms to advertise and sell both digital and physical products [b-Deloitte]. Business leaders remain confident of the metaverse's potential to enhance the retail and e-commerce industries, creating new experiences and leveraging 6G and sensory marketing techniques [b-Adcock]. By 2030, it is estimated that the e-commerce metaverse will have a value of up to $2.6 trillion [b-Cappasity].

The business-oriented metaverse also holds significant potential for changing the ways individuals work and collaborate with colleagues. This will likely be through tackling isolation, workforce disconnectedness, and 'video meeting fatigue' by developing workplace avatars and virtual experiences that operate seamlessly atop the real world so that colleagues across the world can be in the 'same place' together [b-Finnegan]. Furthering this ideal, reality technologies are being incorporated into workplaces [b-Meta] to enhance flexible and interactive collaboration within 'immersive virtual offices' that mimic 3D office-like experiences for remote workers [b-Gleason]. In addition to office-based developments, extended reality tools can be used in vocational settings and skilled trade training, replicating dangerous environments to allow for safe virtual training [b-Interplay].

Finally, in addition to consumer and business-oriented platforms, industrial workplaces are also investing in the metaverse and its supporting technologies to reduce costs, improve efficiency, and redesign factories, warehouses, and logistics systems. Typically, businesses are doing this through the use of digital twin technology, used to replicate industrial and manufacturing operations and optimize system designs around specific needs, which metaverse based versions are able to simulate with greater accuracy and sophistication [b-Carlini]. Digital twins are considered the 'cornerstone' of the industrial metaverse, allowing for replication of individual machines or pieces of equipment to allow for further investigation, redesign of an entire warehouse to improve efficiency and safety, and simulation of disaster scenarios to test system resiliency [b-MIT-Sloan]. The digital twin market, of which the industrial metaverse is just a part, is expected to grow to over $228 million by 2031 [b-Gartner].

6.3 Purpose of the report and its significance

The purpose of this report is to provide an enhanced understanding of the potential risks, and harms posed by the development, use, and implementation of the metaverse. Despite the platform and its required technology being in their early stages of development and application, it is very likely the metaverse has the capacity to dramatically alter existing ways of work, leisure, and shopping, providing a range of new online experiences and services.

Such a significant development to day-to-day lives will bring additional cybersecurity challenges, risks, and implications. The metaverse is expected to embolden established threats such as malware deployment and data theft through widened risk surfaces and extended supply chains. It is also

expected to bring a host of new challenges and enhanced risks that could have additional financial, reputational, and disruptive consequences.

The significance in understanding cybersecurity risks in the metaverse includes the implications that breaches and disruptive attacks can have, including data leaks, financial and reputational losses, and long-term damage to the metaverse's development and success. Large data breaches or extensive periods of disruption will deter large scale adoption of the metaverse, incur financial loss related to lost revenue and recovery, and cause reputational damage to metaverse providers and operators. Financial authorities also remain concerned of the impact digital assets may have in disrupting digital-to-physical exchanges and decentralized payments systems, as well as the implications of NFT theft and manipulation on user trust. Addressing these risks and their impacts to users and virtual economies is vital for the future adoption and success of the metaverse.

The final section of this report addresses standardization priorities for the metaverse, recognized as potential inhibitors to widespread adoption.

7 Background on Cybersecurity Risks and Threats in the metaverse

This section provides an overview of the cybersecurity landscape within the metaverse. It highlights different types of threats and risks in and around the metaverse. In this report we define **threat** as the threat actors and cyber activity that can intentionally take advantage of the metaverse to compromise the confidentiality, integrity, and/or availability of an asset.

Risks are defined as the combination of the likelihood that a threat exploits the metaverse, how easy the metaverse is to exploit (how vulnerable it is) and the potential impact.

7.1 Type of cybersecurity threats and their implications

The metaverse is becoming increasingly popular and has the potential to transform the way we interact with each other and with digital objects. However, by simply looking at how current technology has been exploited, for example, the use of Artificial Intelligence (AI) tools such as ChatGPT for malicious purposes, we can expect that threat actors will try to exploit the metaverse for their convenience.

This Technical Report has identified the following cybersecurity threats the metaverse and its users face.

7.1.1 Data breaches

Using the metaverse will increase the amount of personal identifiable information (PII) that is shared with immersive environments such as through cameras, microphones, and motion trackers. All this data in addition to standard PII (e.g., name, email address, financial account number, or credit card number), reveals great details about a user's location, appearance, and other private information, which is highly attractive for threat actors.

It is expected that cyber criminals will increase their efforts to breach data from the metaverse since most of data breaches are financially motivated [b-UCLA]. Cyber criminals will seek to gain access and compromise PII from applications and platforms in the metaverse to sell it in underground forums, or for conducting further fraud.

7.1.2 Supply chain attacks

The metaverse is based on emerging technologies such as AR and VR, which at the same time, rely on new technologies like AR software, sensors, or optical see-through display devices. Threat actors could access third-parties' source codes, build processes, or update mechanisms by infecting legitimate apps seeking to distribute malware. The motivation of the threat actors could be the disruption of operations across all sectors, or to access sensitive data shared between a company and its supplier.

7.1.3 Fraud

Threat actors will likely attempt to take advantage of unexperienced and unaccustomed metaverse users for monetary gain. Cyber criminals will use a vast range of methods to conduct fraud such as phishing and social engineering campaigns (e.g., business email compromise), fake giveaways, and browser wallet attacks.

Threat actors will likely attempt to impersonate a brand, encouraging users to access a website that looks legitimate, but in reality, is a phishing site designed to steal users' credentials. The metaverse could significantly augment the Business Email Compromise (BEC) threats pace. Both BEC and Vendor Email Compromise (VEC) rely heavily on social engineering, account take-overs, and fraudulent invoices or communication, which actors can amplify and augment through the metaverse.

The metaverse has also introduced '3D social engineering', in which threat actors reach out to victims via a lure that closely resembles a familiar domain, before taking the form of a 3D avatar designed to impersonate co-workers or other recognizable contacts [b-PwC]. The purpose of this operation is to get victims to share sensitive information and credentials, which could be used to access bank accounts.

7.1.4 Malware

The metaverse is predicted to heighten the risk of malware activity due to its high user connectivity, a common target for malicious threat actors [b-Vondráček-1].

Ransomware attacks remains the most feared cyber threat to entities (as reported by CISOs) [b-Accenture-1] and is one of the costliest forms of cybercrime. As the metaverse experience gains more widespread corporate adoption, it presents a new platform for ransomware groups to carry out their criminal activities.

Ransomware groups could use virtual environments within the metaverse to host ransomware, allowing better cross-teams workflows and providing a way to distribute ransomware to victims with less detection. This is especially pertinent as the current ransomware threat landscape is dominated by well-funded organized groups that are willing to invest significant resources in upgrading their capabilities and experiment with new methods and distribution tools. These groups could potentially exploit vulnerabilities in the metaverse software to gain access to corporate data and launch ransomware attacks through metaverse vulnerabilities.

7.1.5 Malicious Content

Malicious content could be embedded within the interactive elements of the metaverse, concealed in seemingly harmless objects or spaces. Users could unknowingly interact with these elements, thereby triggering the harmful content. Given the immersive and interconnected nature of the metaverse, these threats could propagate rapidly, leading to widespread damage.

7.1.6 Poor Cyber Hygiene

Poor cyber hygiene can significantly amplify the cyber threat landscape within the metaverse. Users with improper security habits, such as using weak passwords, ignoring software updates, improperly managing devices, or interacting with unknown virtual entities, can inadvertently create vulnerabilities that cybercriminals may exploit.

Considering the intertwined cyber-physical characteristics of the metaverse and the comprehensive range of sensors incorporated within the hardware, inadequate cyber hygiene can escalate the potential effects of malicious software. This escalation pertains particularly to privacy and the physical security of users.

7.2 Risks in the metaverse

This Technical Report identified the following risks that cyber threats could represent for users and organizations in and around the metaverse. The risks are dependent on the capability and intent of the threats. Intent is defined as a threat's desire and intention to target the metaverse, while capability is a measure of the threat's ability to compromise the chosen target.

7.2.1 Theft of virtual assets

Threat actors could conduct a cyber-attack in metaverse which could result in the theft of virtual assets (e.g., cryptocurrencies, NFTs). From July 2021 to July 2022, threat actors stole over $100 million in NFTs [b-Zotter].

In March 2022, when a blockchain technology company announced the launch of a new cryptocurrency, several threat actors on social media platforms tried to trick users into clicking malicious links or sending funds for fraudulent giveaways. The threat actors managed to raise around $900,000 [b-Zotter].

7.2.2 Data theft

Data theft represents one of the biggest risks for businesses and users in the metaverse. Threat actors could transfer or store personal, confidential or financial information when conducting data breaches. This information could then be used for conducting criminal activity such as identity theft and fraud.

7.2.3 Data tampering

Data tampering presents a significant cyber risk in the metaverse. data is a critical resource, driving experiences, transactions, and interactions. Cybercriminals, exploiting vulnerabilities, could alter, delete, or manipulate this data, thus distorting the truthfulness and reliability of the virtual environment. This tampering could lead to a range of adverse outcomes, from disruption of services and fraudulent transactions to misrepresentation of virtual identities and assets.

7.2.4 Misinforming

The creation of false identities through impersonated or stolen avatars increases the risk and impact of spreading false information, conducting fraudulent or other harmful activities with difficulties to identify of ownership, leading to lack of oversight and accountability.

8 Potential Harms of Cybersecurity Risks in the metaverse

8.1 Identity theft and fraud

As the Metaverse grows, avatars created using users' biometric data will become more attractive targets for threat actors, raising privacy concerns and the risk of suffering a cyberattack.

Threat actors could copy a digital avatar from one metaverse and create an identical one in another as the different virtual worlds are currently not connected. This gives a threat actor the opportunity to copy a high-profile avatar from one world and recreate it in another, in the hope of tricking people to their true identify. The fake avatar could then be used in many fraudulent ways including misinformation, phishing, and social engineering attacks.

Cybercriminals could also abuse the metaverse through the creation of illegal marketplaces, where users could buy and sell stolen data and digital identity wares. From January 2021 to January 2023, darknet discussions pertaining to the possible usage of the metaverse increased by 488 percent [b-Accenture-2]. While this rise is partially attributed to the overall focus on the metaverse, it does showcase the criminal interest in the metaverse as a focal point of criminal activity.

8.2 Malware and viruses

The metaverse faces the threat of ransomware and new types of malwares. Unlike traditional malware, which targets physical systems and networks, malware targeting the metaverse will be tailored to exploit vulnerabilities within virtual platforms, aiming for assets, data, or functionalities specific to these realms [b-Cooper].

Cybersecurity researchers have identified several new malwares targeting the metaverse, such as 'Metaverse's Immersive Virtual Reality Malware' [b-Vondráček-2], and 'Big Brother' [b-Reason-Labs].

In a 'Metaverse's Immersive Virtual Reality Malware' and Man-in-the-Room (MitR) attack, threat actors in a public or private room, convince other users to click a link that contains a malware. The malware can give threat actors complete control over one end of audio, video, and data streams, allowing threat actors to see the screens of the victim's computers and hear their audio and microphone [b-Vondráček-2].

The 'Big Brother' malware originates from a PC malware program installed and executed on a Windows computer. The malware lies dormant on the system until an Android-based VR headset with developer mode enabled connects to the PC. When the malware recognizes a VR device, it opens a TCP port. It then has the ability to record the user's headset screen remotely. [b-Reason-Labs] Threat actors can use this malware for compromising data and conduct extortion or fraud.

8.3 Data breaches and leaks

Data breaches and leaks represent a significant threat to the metaverse. There are various motivations for a threat actor to breach sensitive information and personal data. Firstly, threat actors can sell and leak the compromised information to make a profit. Secondly, threat actors might use the information compromised in the breach to access a company's networks to achieve persistence and collect intelligence or to conduct impersonation fraud.

In March 2023, a company developing the industrial metaverse was found leaking sensitive information that included office plans, IoT devices, and WordPress sets containing user credentials (including users' names and avatar pictures) belonging to a third-party, endpoints, and three sets of backend and authentication endpoint URLs on different endpoints of the affected systems [b-Secure-Blink]. Threat actors could have carried out disruptive attacks, ransomware attacks, or conducted social engineering campaigns if they had received access to the exposed data.

In July 2022, a virtual pet website suffered a data breach leading to the theft of 460MB of compressed source code and a database containing the personal information of over 69 million members. A threat actor known as 'TarTarX' claimed to be selling the source code and database for four bitcoins, worth approximately $94,000 [b-Abrams].

8.4 Social engineering attacks

In its current state, the metaverse is especially susceptible to social engineering attacks due to low user experience, new technology, and lack of prowess amongst operating entities in the space, which can seriously enhance the ability for threat actors to target entities.

Social engineering is viewed as the cheapest tool in the box and a key determinant of success and is being deployed by crude and skilled groups alike as a first line of attack and an option of last resort.

It has already been mentioned that the metaverse could increase the amount of PII collected by the immersive environments through cameras, microphones, and motion trackers. This data can reveal great details about a user's location, appearance, and other private information while also enabling attackers to carry out more sophisticated phishing and social engineering scams.

9 Implications of Cybersecurity Risks in the metaverse

9.1 Impact on platforms

As previously stated, the structure and multi-purpose nature of the metaverse means it will host a large amount of standard PII, as well as additional motion tracking data and lifelike digital avatars. It has also been recognized that this large holding of personal information will likely motivate cyber criminals and other actors to conduct data theft operations to support further social engineering efforts. The combination of these factors has the potential to increase both the likelihood of data breaches and their severity, which can in turn have significant regulatory and financial consequences. Organizations may be fined for following a data breach for non-compliance of General Data Protection Regulation (GDPR) and privacy regulations in a number of operating territories. [b-Nadeau] Additionally, these data breaches and subsequent regulatory fines can incur reputational damage, with research assessing that 46 percent of organizations suffered lasting reputational damage due to a data breach [b-EasyDMARC].

Metaverse providers are also at risk of potential spillover effects from the digital to the physical world. As the metaverse remains in its infancy, both tech giants and smaller organizations are providing services and hosting infrastructure in both the virtual and real worlds. The implication of this connection is that organizations can have their existing long-term physical presence impacted through a compromise of new metaverse services.

9.2 Impact on users and their trust in the platform

The success of the metaverse depends upon ongoing user trust in the safety and security of its platforms and services. Cybersecurity risks and incidents represent significant threats to user trust, which will impact the long-term success of the metaverse.

As the metaverse is slated to provide a holistic service across entertainment, retail, and work, it is likely that platforms will retain a comprehensive amount of standard PII, motion tracking data, and digital avatars. As a result of the extensive information collection of highly personalized data, it is likely that any future data breaches will result in significant implications to user trust. Consumers are particularly concerned over loss of personal data, with 81 percent of consumers saying they would stop engaging with a brand altogether if it suffered a data breach [b-Ping-Identity].

Illegitimate businesses that create phishing websites which mimic real metaverse platforms pose a concerted risk to widespread metaverse take up and user trust. The current decentralized nature of the metaverse largely supports these phishing websites, as the lack of a central authority or structure means there is little oversight in digital property transactions. It is estimated that, until a central authority or set of rules are implemented across the metaverse, users remain at a heightened risk of falling victim to phishing scams, which in turn can impact user trust in the validity and safety of metaverse platforms [b-CNBC].

Research has predicted that by 2026, 25 percent of people will spend at least one hour per day in the metaverse, either for work or leisure activities, and 30 percent of global organizations will have products and services in the metaverse. [b-Rimol] Given this reliance individuals will have for the service, long term outages as a result of a concerted disruptive or destructive attack will likely incur significant implications for providers, including reduced customer usage and impacted reputation. Critical industries, including healthcare, energy, and logistics, are regularly targeted with the intention of leveraging their time-sensitive criticality to amplify impacts and it is likely that the metaverse and its more core services will be targeted in a similar way.

9.3 Impact on virtual economies and assets

A fundamental aspect of the future metaverse is the use of digital assets, such as virtual land or collectible items. Digital assets are represented and secured through NFTs, which give users the ability to show ownership, transfer, or sell assets. NFT transactions are supported by decentralized

finance technologies through the use of cryptocurrencies and blockchain, which are integral to the metaverse in providing fast and secure confirmation of information, allowing for transactions to be completed on demand with minimal risk. Several companies are offering NFT management processes to facilitate interactions and developing blockchain infrastructure to support decentralized finance in the metaverse [b-Muradzikwa].

Financial authorities remain concerned about the growth of these digital assets and supporting organizations, arguing they may affect asset values in the physical world, due to digital-to-physical exchanges and disruption of decentralized payments systems. Political authorities, whilst recognizing the efficiency of virtual economies, also remain skeptical of their growth and attached risks, including stability of platforms, volatility of prices, and associated cybersecurity threats. [b-EP-News]

NFT associated compromises resulted in losses of $52 million for the first four months of 2022, compared to less than $7 million for the whole of 2021 [b-Silent-Breach]. Cybersecurity concerns include the exploitation of vulnerabilities that allow for the theft of digital assets, or their manipulation in pump-and-dump schemes [b-White-Blue-Ocean]. In addition, threat actors are likely to establish copycat NFT sites that closely resemble authentic sites, in order to sell counterfeit NFTs or conduct phishing operations [b-Morgan-Stanley]. The wider implications associated with cyber threats to NFTs, digital assets, and virtual economies includes financial authorities, political bodies, and metaverse stakeholders withholding their trust and choosing to divest from their use and application within the metaverse, which in turn will have financial implications for involved companies and long-term reputational impacts for the metaverse.

10 Recommendations for Standardization Activities

Agreements on technical standards related to data privacy and security in the metaverse is integral to its widespread adoption and success. Technical standards provide assurances and clarity on responsibilities for stakeholders and providers, reduce operational risk, and secure user trust in platforms and service providers.

The formalized agreements on information security standards for the cloud, known as ISO/IEC 27017 [b-ISO/IEC 27017], which provides best practice recommendations on information security management, offers a useful operational framework to approach metaverse standardization and information security risks. For the metaverse, stakeholders should consider:

10.1 Identity Management

Verification of user identities in the metaverse is the bedrock of user trust in the platform, as users must be confident that both their online identity and those they interact with is accurate and secure. Maintaining secure and trusted identity management is crucial to verify identities, establish relationships, and enable participation in virtual transactions and interactions. Identity management secures trust, reduces risk of security incidents such as data theft, avatar hijacking, and social engineering, and fosters a more robust and trustworthy virtual economy.

Identity security systems need evaluation, assessment, and collaboration to ensure that individual identities are properly authenticated and protected to prevent fraud and misuse, maintaining the integrity and trust of the metaverse. Effective identity management can be established through the creation of agreed standards and enforceable regulations discussed and proposed through organised forums. Existing identity management standards outside of the metaverse offer useful frameworks and clear guidance and can be used by stakeholders and providers in ongoing discussions to establish and implement identity management standards for the metaverse. The UK's National Cyber Security Centre offers guidelines which ensures new users are properly authenticated and attached to their online identity, ensuring appropriate level of access to systems and placing appropriate assertions on third parties. The guidelines also cover policies regarding monitoring of privileged user actions, activity logging, and maintenance of records [b-NCSC].

10.2 Interoperability

The need for interoperability in the metaverse is a consequence of the decentralized environment in which hardware, platforms, and services are developed and operate in silos, distinct from one another. There is widespread agreement within forum working groups that the metaverse must develop to become a frictionless space with interoperability baked in to ensure that the various interlocking technologies can interact efficiently, that platforms and services are provided with interconnected standards, systems, and applications, and that the opportunities for security incidents and data breaches are minimized.

Failure to ensure effective interoperability will slow down the progression of data exchange, hinder the frictionless user experience, and provide malicious users opportunities to exploit gaps and vulnerabilities within systems. By its nature, interoperability will require the storage and transfer of greater quantities of personal data, providing additional opportunities for threat actors to gain access to and steal data, requiring these interoperable platforms to have set agreements and certainties in place. The current immaturity of interoperability in platforms is providing opportunities for malicious users, expanding risk surfaces, and adding unnecessary complexity towards the allocation of responsibilities in the event of a compromise. Whatever the agreed standards and limits of interoperability, entities and stakeholders within the emerging metaverse ecosystem will at some point need to rely on the cyber security of others, increasing the likelihood of supply chain compromises and incidents in which a number of platforms, services, organisations, and participants are impacted.

Platform and service providers should work together to agree on technical interoperable standards for the features, interactive elements, digital items, and services across the metaverse.

Technical interoperability issues under discussion include network constraints, IP protections, secure payments, data privacy, and other security considerations. Addressing these issues requires agreements on what constitutes strong network infrastructure foundation, allowing for data interchange across hardware and platforms that enables seamless virtual experiences. Components of this agreement include scope of data, timeliness of data exchange, accepted file formats, and stylistic consensus [b-WEF].

It should be noted that, despite widespread clarity on emerging technical interoperability standards, these regulations must not be established as a single value at the expense of other concerns, and stakeholders should seek to ensure that eventual agreements reflect human-first interoperability standards that places user safety, security, and data privacy at its heart.

10.3 Asset Management

As a combination of interoperability and identity management considerations, asset management is a core factor of metaverse standardization discussions. Asset management refers to the authentication, access, and availability of digital assets, as well as the interoperability, portability, and digital rights of these assets across different metaverse platforms. Simply put, effective asset management secures digital purchases and supports the free movement of assets between virtual worlds, allowing, for example, a user who purchases a digital t-shirt from a virtual music concert in one world the ability to continue wearing this as they move to other spaces.

To ensure this seamless flow of assets and maintain accurate version control between distinct spaces in the metaverse, platform and service providers, stakeholders, and participants must agree on technical standards for operations. Currently there are a number of options for metaverse platforms to improve interoperable asset management, which require discussion and agreement. This includes cross-chain decentralized exchanges, which act as a bridge to support the communication and exchange of information, creating a cross-chain ecosystem that promotes the seamless movement of assets across different blockchain networks [b-Purushotham]. Stakeholders must also assess the role of smart contracts, which may offer additional speed and security of asset exchange. One example is

to use atomic swaps, an asset transferal solution that does not require a trusted intermediary but secures movement through hash time-locked contracts.

A further number of solutions to ensure the seamless and secure transferal of virtual assets between metaverse worlds are available for adoption or development, but it remains incumbent on metaverse providers, stakeholders, and participants to guide and design the development of asset management to ensure security and equality of use. To further support these smooth transfers, stakeholders must also agree on the role of blockchain and level of decentralization of platforms, as well as standardize minimum level requirements of persistence across virtual worlds and data movement performance. Agreements on these issues will ensure effective working of asset management, will instill user confidence in the systems and wider metaverse, and reduce instances and possibilities of security breaches, data theft, and exploitation of vulnerabilities.

10.4 Access to the metaverse

The metaverse aims to be an accessible, safe, and open space for users and organisations. Interoperability and safeguarding data are two key factors for achieving this goal since metaverse platforms have different access conditions (e.g., while VR headsets are optional for most platforms, some may only be joined using one; some platforms may require social media accounts; others have different authentication requirements) [b-Ėinorytė]. In order to guarantee the data and operability safety, organisations should limit access to information and information assets according to their business needs.

Metaverse service providers should provide access controls that allow organisations to restrict access to its metaverse services, functions, and the data maintained in the platform (e.g., segregation in networks, limitation of connection time). At the same time, organisations should ensure that access to information in the metaverse can be restricted in accordance with its access control policy and that such restrictions are realized (e.g., privilege management, review of user access rights) [b-Small].

10.5 User Awareness about Cyber Hygiene

User awareness about cyber hygiene is crucial for securely using the metaverse due to the unique and complex nature of this digital universe. Cyber hygiene refers to practices and steps that users can take to maintain system health and improve online security. These include using strong, unique passwords, regularly updating software, securely storing their devices, avoiding suspicious links or virtual entities, and being cautious about the personal information they share. In addition, cyber hygiene can help users to identify and respond to threats promptly, thereby limiting the potential damage.

Bibliography

[b-ITU-T M.3080] Recommendation ITU-T M.3080 (2021), *Framework of artificial intelligence enhanced telecom operation and management (AITOM).*

[b-ITU-T P.1320] Recommendation ITU-T P.1320 (2022), *Quality of experience assessment of extended reality meetings*.

[b-ITU-T F.751.0] Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger systems*.

[b-ITU-T Y.4600] Recommendation ITU-T Y.4600 (2022), *Requirements and capabilities of a digital twin system for smart cities*.

[b-Abrams] Abrams, Lawrence. (2022). *Neopets data breach exposes personal data of 69 million members.* Bleeping Computer. Available [viewed 2023-11-09] at: https://www.bleepingcomputer.com/news/security/neopets-data-breach-exposes-personal-data-of-69-million-members/

[b-Accenture-1] Accenture. (2021). *2021 Cyber Threat Intelligence Report.* Dublin: Accenture. 24pp. Available [viewed 2023-11-09] at: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-172/accenture-2021-cyber-threat-intelligence-report.pdf

[b-Accenture-2] Accenture. (2023). *State of Cybersecurity Resilience 2023.* Dublin: Accenture. 39pp. Available [viewed 2023-11-09] at: https://www.accenture.com/us-en/insights/security/state-cybersecurity

[b-Adcock] Adcock Solutions. (2023). *How the Metaverse Will Change Retail Experiences.* Adcock Solutions. Available [viewed 2023-11-09] at: https://www.adcocksolutions.com/post/how-the-metaverse-will-change-retail-experiences

[b-Advanced-Television] Advanced Television. (2023). *Study: Metaverse gaming redefining sector's future.* Advanced Television Ltd. Available [viewed 2023-11-09] at: https://advanced-television.com/2023/06/30/study-metaverse-gaming-redefining-sectors-future

[b-Cappasity] Cappasity Blog. (2022). *Retail trends: the value of e-commerce in the metaverse can reach $2.6T by 2030.* Meidum. Available [viewed 2023-11-09] at: https://medium.com/cappasity-blog/retail-trends-the-value-of-e-commerce-in-the-metaverse-can-reach-2-6t-by-2030-6d93d8bfece8

[b-Carlini] Carlini, Steven. (2023). *The Industrial Digital Twin Metaverse Of Today And Its Path To The Future.* Jersey City, New York: Forbes. Available [viewed 2023-11-09] at: https://www.forbes.com/sites/forbestechcouncil/2023/03/29/the-industrial-digital-twin-metaverse-of-today-and-its-path-to-the-future/

[b-CNBC] Javers, E., Zamost, S., Tortorelli, P., Maharishi, M. (2022). *Cybercriminals target metaverse investors with phishing scams.* Englewood Cliffs, New Jersey: CNBC. Available [viewed 2023-11-09] at: https://www.cnbc.com/2022/05/26/cybercriminals-target-metaverse-investors-with-phishing-scams.html

[b-Cooper] Cooper, Verena. (2023). *Metaverse Security: Identifying Threats and Safeguarding Your Digital Presence.* Splashtop. Available [viewed 2023-11-09] at: https://www.splashtop.com/blog/metaverse-security-threats#heading-3

[b-Council-EU] Council of the European Union, General Secretariat, ART analysis and research team. (2022). *Metaverse – Virtual World, Real Challenges*. Brussel: Council of the European Union. 15pp.

Available [viewed 2023-11-09] at: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf

[b-Deloitte] Deloitte. (2022). *Retail in the metaverse: Understanding opportunities.* London: Deloitte. Available [viewed 2023-11-09] at: https://www2.deloitte.com/us/en/pages/consulting/articles/metaverse-for-the-future-of-retail.html

[b-EasyDMARC] EasyDMARC. (2023). *Reputational Cost of a Data Breach*. Easydmarc. Available [viewed 2023-11-09] at: https://easydmarc.com/blog/reputational-cost-of-a-data-breach/#:~:text=A%20data%20breach%20has%20the,t%20be%20so%20trusting%20anymore

[b-Einorytė] Einorytė Aurelija. (2023). *How to join the metaverse: The complete guide*. Nord VPN. Available [viewed 2023-11-09] at: https://nordvpn.com/blog/how-to-join-the-metaverse

[b-EP-News] European Parliament News. (2016). *Virtual currencies: what are the risks and benefits?* European Parliament. Available [viewed 2023-11-09] at: https://www.europarl.europa.eu/news/en/headlines/economy/20160126STO11514/virtual-currencies-what-are-the-risks-and-benefits

[b-Finnegan] Finnegan, Matthew. (2023). *Microsoft advances mixed-reality plans with Teams avatars, Mesh update.* Computer World. Available [viewed 2023-11-09] at: https://www.computerworld.com/article/3697316/microsoft-advances-mixed-reality-plans-with-teams-avatars-mesh-update.html

[b-Gartner] Gartner Research. (2020). *Emerging Technologies: Revenue Opportunity Projection of Digital Twins.* Stamford, Connecticut: Gartner. Available [viewed 2023-11-09] at: https://www.gartner.com/en/documents/4011590

[b-Gleason] Gleason, Mike. (2021). *BlueJeans to launch a virtual workspace in 2022.* TechTarget. Available [viewed 2023-11-09] at: https://www.techtarget.com/searchunifiedcommunications/news/252507585/BlueJeans-to-launch-a-virtual-workspace-in-2022

[b-Hickey] Hickey, Seth. (2022). *Cryptovoxels vs. Decentraland.* Finder. Available [viewed 2023-11-09] at: https://www.finder.com/cryptovoxels-vs-decentraland

[b-IBM] IBM. (2023). *What is a digital twin?* Armonk, New York: IBM. Available [viewed 2023-11-09] at: https://www.ibm.com/topics/what-is-a-digital-twin

[b-Interplay] Interplay Learning. (2021). Available [viewed 2023-11-09] at: https://www.interplaylearning.com/

[b-ISO/IEC 27017] International Standard ISO/IEC 27017:2015, *Information technology – Security techniques – Code of practices for information security controls based on ISO/IEC 27002 for cloud services.*

[b-McKinsey] Elmasry, T., Hazan, E., Khan, H., Kelly, G., Srivastava, S., Yee, L., Zemmel, R.W., editors (2022). *Value creation in the metaverse: The real business of the virtual world*. New York, NY: McKinsey. 77 pp. Available [viewed 2023-07-14] at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf

[b-Meta] Meta. (2023). *Meta Horizon Workrooms.* Meta. Available [viewed 2023-11-09] at: https://forwork.meta.com/gb/horizon-workrooms/

[b-Mileva] Geri, Mileva. (2023). *48 Metaverse Statistics | Market Size & Growth (2023).* Influencer Marketing Hub. Available [viewed 2023-11-09] at: https://influencermarketinghub.com/metaverse-stats/

[b-MIT-Sloan] Purdy, M., Eitel-Porter, R., Krüger, R., Deblaere, T. (2020). *How Digital Twins Are Reinventing Innovation.* MIT Sloan. Available [viewed 2023-11-09] at: https://sloanreview.mit.edu/article/how-digital-twins-are-reinventing-innovation/

[b-Morgan-Stanley] Morgan Stanley. (2022). *Common NFT and Metaverse Scams.* New York City: Morgan Stanley. Available [viewed 2023-11-09] at: https://www.morganstanley.com/articles/nft-metaverse-scams-cybersecurity

[b-Muradzikwa] Muradzikwa, T., Kazmierczak, A., Diaz, A. (2023). *The Rise of the Virtual Economy: Exploring Finance in the Metaverse.* Plug and Play. Available [viewed 2023-11-09] at: https://www.plugandplaytechcenter.com/resources/exploring-finance-in-metaverse/

[b-Nadeau] Nadeau, Micheal. (2020). *General Data Protection Regulation (GDPR): What you need to know to stay compliant.* CSO. Available [viewed 2023-11-09] at: https://www.csoonline.com/article/562107/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

[b-NCSC] National Cyber Security Centre. (2018). *Introduction to identity and access management.* London: National Cyber Security Centre. Available [viewed 2023-11-09] at: https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management

[b-OMDIA] OMDIA. (2021). *Omdia research reveals 12.5m consumer VR headsets sold in 2021 with content spend exceeding $2bn.* London: OMDIA. Available [viewed 2023-11-09] at: https://omdia.tech.informa.com/pr/2021-dec/omdia-research-reveals-12m-consumer-vr-headsets-sold-in-2021-with-content-spend-exceeding-2bn

[b-Ping-Identity] Ping Identity. (2019). *81% of Consumers Would Stop Engaging with a Brand Online After a Data Breach, Reports Ping Identity.* Business Wire. Available [viewed 2023-11-09] at: https://www.businesswire.com/news/home/20191022005072/en/81-of-Consumers-Would-Stop-Engaging-with-a-Brand-Online-After-a-Data-Breach-Reports-Ping-Identity

[b-Purushotham] Purushotham, Abhishek. (2023). *An Overview of Cross-Chain Decentralized Exchanges*. Axelar. Available [viewed 2023-11-09] at: https://axelar.network/blog/cross-chain-dex-decentralized-exchanges

[b-PwC] PwC. (2022). *Metaverse security: Emerging scams and phishing risks.* London: PwC. Available [viewed 2023-11-09] at: https://www.pwc.com/us/en/tech-effect/cybersecurity/emerging-scams-and-phishing-risks-in-the-metaverse.html

[b-Reason-Labs] Reason Labs Research Team. (2023). *"Big Brother": A New Attack Vector Affecting Metaverse Security.* Reason Labs. Available [viewed 2023-11-09] at: https://reasonlabs.com/research/big-brother

[b-Rimol] Rimol, Meghan. (2022). *Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026.* Stamford, Connecticut: Gartner. Available [viewed 2023-11-09] at: https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026

[b-Rowden] Rowden, Seth. (2022). *What Is Metahero? How Does HERO Work?* BITKAN. Available [viewed 2023-11-09] at: https://bitkan.com/learn/what-is-metahero-how-does-hero-work-7257

[b-Secure-Blink] Secure Blink. (2023). *Siemens Metaverse Leaks Sensitive Corporate Data: Millions Exposed!* Secure Blink. Available [viewed 2023-11-09] at: https://www.secureblink.com/cyber-security-news/siemens-metaverse-leaks-sensitive-corporate-data-millions-exposed

[b-Shein] Shein, Esther. (2022). *7 top technologies for metaverse development.* TechTarget. Available [viewed 2023-11-09] at: https://www.techtarget.com/searchcio/tip/7-top-technologies-for-metaverse-development

[b-Silent-Breach] Silent Breach. (2022). *3 ways the metaverse will change cybersecurity.* Silent Breach. Available [viewed 2023-11-09] at: https://silentbreach.com/BlogArticles/3-ways-the-metaverse-will-change-cybersecurity/#:~:text=The%20Top%20Cybersecurity%20Concerns%20in%20the%20Metaverse&text=For%20example%2C%20NFT%20hacks%20resulted,the%20entire%20year%20of%202021

[b-Small] Small, Mike. (2016). *ISO/IEC 27017 was it worth the wait?* Kuppinger Cole. Available [viewed 2023-11-09] at: https://www.kuppingercole.com/blog/small/isoiec-27017-was-it-worth-the-wait

[b-Threat] Threat, L'Oreal. (2021). *The Future in the Metaverse.* Peacock Plume. Available [viewed 2023-11-09] at: https://peacockplume.fr/opinion/future-metaverse

[b-UCLA] UCLA. (2023). *Data Breaches and Data Theft.* Los Angeles, California: UCLA Office of the Chief Information Security Officer. Available [viewed 2023-11-09] at: https://ociso.ucla.edu/cybersecurity-you/protect-your-identity#:~:text=A%20data%20breach%20is%20an,step%20that%20follows%20a%20breach

[b-Vondráček-1] Vondráček, Martin., Baggili, Ibrahim., Casey, Peter. (2022). *Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses.* Computers & Security. 13pp. Available [viewed 2023-11-09] at: https://doi.org/10.1016/j.cose.2022.102923

[b-Vondráček-2] Vondráček, Martin., Baggili, Ibrahim., Casey, Peter. (2022). *Supplemental Material for Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses.* Computers & Security. 11pp. Available [viewed 2023-11-09] at: https://ars.els-cdn.com/content/image/1-s2.0-S0167404822003157-mmc1.pdf

[b-WEF] World Economic Forum, Accenture. (2023). *Interoperability in the Metaverse*. Cologny: World Economic Forum. 24 pp. Available [viewed 2023-11-09] at: https://www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf

[b-White-Blue-Ocean] White Blue Ocean. (2023). *Cyber Security Risks of the Metaverse.* London: White Blue Ocean. Available [viewed 2023-11-09] at: https://www.whiteblueocean.com/newsroom/cyber-security-risks-of-the-metaverse/

[b-Zotter] Zotter Angelika. (2022). *Financial crime in the metaverse is real – how can we fight back?* Vienna, Austria: Wolf Thesis. Available [viewed 2023-11-09] at: https://www.wolftheiss.com/insights/financial-crime-in-the-metaverse-is-real/f