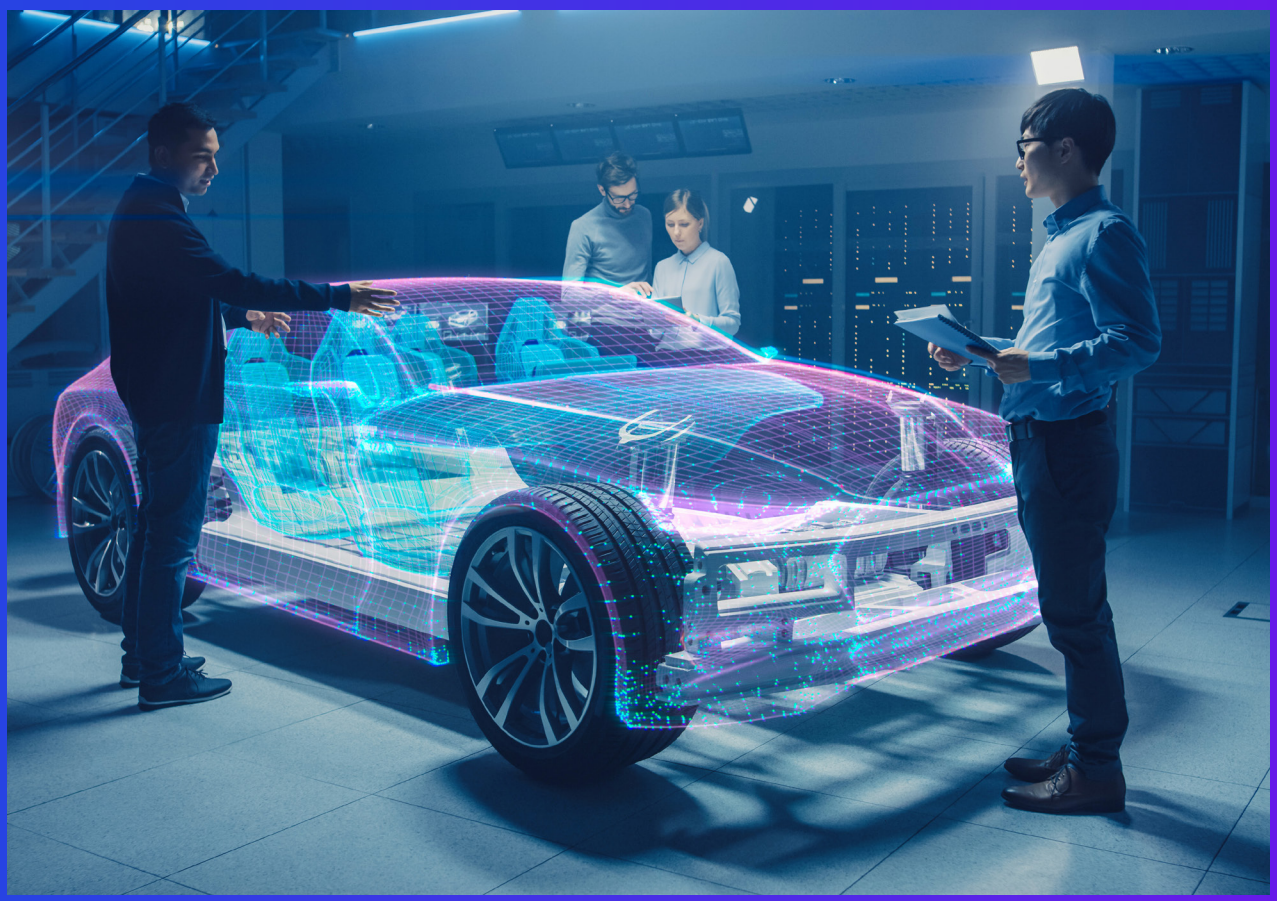
KPMG

Cyber considerations for the Metaverse



kpmg.com

Four cyber considerations for security leaders

1. Digital impersonation
2. Interoperability
3. Account takeover risk—credential replay attack
4. Data protection/Misuse

The next evolution of the internet is occurring right now, and it's called the metaverse. As the scope of the internet expands, user experiences are getting more immersive through virtual reality, while augmented reality enhances physical spaces through virtual details and embellishments. The metaverse enables millions to digitally recreate more realistic interactions as well as design entirely new ones.

From an organization's perspective, the metaverse allows businesses to unlock new paths towards growth, enhance customer relationships, and transform cost structures. Growth opportunities will continue to emerge as digital interactions get more immersive and contextual.

However, looking through the lens of cyber security, this trend raises significant risks that organizations need to consider. With the expanding boundaries of the internet, cybercriminals have an increasing attack surface to exploit. Moreover, the increasing realism of these experiences introduces additional safety and security concerns, as what users see, hear, and feel becomes more lifelike.

Security leaders are one of the most valuable participants in any organization's metaverse ambitions. By actively engaging in bringing metaverse initiatives to markets, security leaders help safeguard customers and protect their enterprises' investments. They are critical to establishing the trust required for these emerging opportunities to be realized. When you earn the trust of all your stakeholders, you create a platform for responsible growth, confident decision-making, bolder innovation, and sustainable advances in performance and efficiency.

So, what are some important risk considerations that security leaders and metaverse innovators need to consider?

1 Digital impersonation

- Identity has been the cornerstone of security capabilities, as it is the central element to building trust. Decisions to grant access to resources or authorize actions—such as transferring funds or signing a lease—are made based on how we verify and establish confidence in "who you are."
- While phishing and social-engineering attacks continue to be a top threat vector in our current digital ecosystem, the risk of bad actors impersonating your personal virtual banker/adviser or your boss/colleague and giving you directions to execute malicious tasks in a virtual room only gets compounded in the virtual world.
- Deepfakes are also on the rise, and in a virtual space with the use of voice-modulator software, it becomes increasingly easier to emulate a different person and spear phish the victims.
- Moreover, virtual experiences offer many new opportunities for malicious actors to commit fraud in increasingly creative ways. For example, imagine you attend a virtual concert, and you pay extra money for a virtual backstage pass to meet your idol and ask questions and exchange impressions. A malicious organizer could have regular people pretend to be the singer, creating several phony backstage events. So instead of selling a dozen or so backstage passes, they could sell thousands and reap big profits. In addition to cheating the buyers of the experience, the scam could cast a shadow over businesses that organize legitimate backstage events. An extreme example would be a whole concert played by an impersonator, with fraudsters charging fans to simply hear a deepfake.

Considerations

For metaverse platform providers: Establishing trust in consumer identity must become a key priority. Consumers should be able to interact with their preferred creators and enable exchange of digital assets using identity verification and proofing similar to financial institutions' norms around know your customer. Consider leveraging innovations and integrations with passwordless authentication protocols, e.g., FIDO credentials or verifiable credentials (VCs) which will allow for stronger authentication and reduce the risk of phishing and social-engineering attacks.

For consumers: Consider platforms and ecosystem partners that offer multifactor authentication and identify-verification protocols, especially for higher-risk transactions or interactions, like money movement. Additionally, understand in advance how to spot potentially fraudulent, nonvalidated identities. Just as a verified Twitter account for a celebrity has a tick box or interacting with someone on Facebook who is a friend can be spotted from someone who is just using the same name and picture, similar concepts will be adopted in the metaverse platform of choice. If the platform doesn't offer the right level of safeguards, then you are at a high risk of being targeted by fraudsters and ill-intended people.

Dependency

While there are hundreds of metaverses, interoperability and cocreation will be critical for consumers to take their avatars and broader digital identities into multiple metaverse environments with trust established. Industry stakeholders and the security community must work together to establish interoperability protocols and govern them. Cloud providers, security researchers, tech giants, ISPs, etc., play a fundamental role in enabling a secure environment that's interoperable between metaverses.

2 Interoperability

Many metaverse luminaries have stated that the metaverse can only hit critical mass once interoperability and portability is solved. Some criticize large tech companies trying to solve this problem by centralizing identities as counter to core principles of Web3. (Web3 is the third generation of the internet, which is based on the idea that the internet should be run on a decentralized computer network instead of a centralized one.) Regardless of who is connecting various metaverses (centralized or decentralized), the ability to bring your avatar, your digital identity, and your assets (NFTs, crypto, etc.) creates key security and fraud risks to the broader ecosystem.

As seen with the high-profile hacks on crypto "bridges," building secure and resilient connections must be solved to maintain trust. There is also a need for self-regulation and setting up security baseline standards to enable interoperability in a safe environment.

Having a defined set of principles to prevent certain types of attacks in various metaverses will be a critical step requiring companies to work together. Paying a certain amount of money for an exclusive asset in one metaverse that is tied to your identity and getting that stolen in a different environment with lower security and weaker fraud-prevention mechanisms would create fundamental ruptures in how interoperability would be maintained and erode trust in the broader ecosystem.

> "The value of being a trusted enterprise to customers, business partners, and regulators is especially important in this world of mixed reality and disruptive technologies."

3 Account takeover risk—credential replay attack

Development and integration of bots in the metaverse, as well as an increased attack surface, can lead to new ways of capturing or stealing user credentials and secrets. As the metaverse economy blooms, people will invest their hard-earned money into the metaverse either to purchase or sell their products. Since there will be a financial incentive, account takeover and transfer of assets to rogue accounts could become the norm. Losing access to your digital identity in an interconnected metaverse will have a similar impact to losing access today to your Google account. Bad actors will gain immediate access to your search history, location history, and emails and do further damage by taking over social media accounts or banking details. However, in the future, they could get access to exclusive assets and crypto wallets to transfer money and valuable assets while you lose control over your digital identity. Restoring a stolen account could take a significant amount of time, and damage can often be irreversible. So preventing account takeover by building a secure mechanism to prevent identity theft, detecting potential fraudulent connections in case credentials have been stolen, and creating mechanisms in place for legitimate users to recover their accounts is going to be paramount.

4 Data protection/Misuse

In the digital era, data is, at times, more valuable than money and will become even more important as the metaverse becomes mainstream. Immersive technologies, such as virtual reality and augmented reality, offer the opportunity to collect a lot more information than mobile devices can generate. The increased number of sensors in such technologies allows them to correlate many signals and offers the potential to solve problems that remain difficult to resolve today. For example, immersive technologies could help with the early detection of diseases, enhance performance of sports players, and even navigate a busy street in a foreign country to find a nearby restaurant.

But protecting all this data will be critical. Misuse of data captured by bad actors from within the metaverse can lead to real harm to the victims. For example, body movement and the way a person speaks could, in some cases, be collected and analyzed to build data points and predict certain preferences or decisions they may likely make. At the same time, this information can be misused to label the victim's sexual orientation or political affiliation in a negative manner. As more developers build their own experience on top of the metaverse platforms, granting access to the right level of data within that platform has to be highly vetted and actively monitored to avoid the illegal collection or misuse of such data.

As the evolution of the metaverse rapidly continues, security leaders need to remain vigilant and work with their business stakeholders to build a holistic cybersecurity program. By doing so, they will inspire the trust of all their stakeholders as well as create the space and permission to grow, innovate, and succeed.

> "As the boundaries of the internet expand, so does the attack surface for cybercrime."

Contact us

Vijay Jajoo
Principal
Cyber Security Services
E: vjajoo@kpmg.com

Max Hanson
Managing Director
Lighthouse
E: mahanson@kpmg.com

Cliff Justice
Principal
National Leader
Enterprise Innovation
E: cjustice@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia