BRC
BOARD RISK COMMITTEE

BOARD RISK REPORT

Deep Dive Edition - Emerging Technology

April 6, 2023

Emerging Technology from Metaverse to ChatGPT

What Board Directors Need to Know About Our Immersive Digital Future

By Lisa O'Connor

Emerging technology is the key to business value transformation and ensuring our digital futures. Companies and their directors must have their eyes on tomorrow and foster the agility to engage early with technologies that prove value in increasingly complex AI driven environments. Businesses should have a strategic approach to emerging technology that reflects an understanding of the nature and speed of the opportunity or disruption, engages early to learn and manage risks, and adopts the technology with a responsible approach.

Over the next three years, businesses will test the value propositions of the metaverse and web3 technologies and implement pilot programs to test how metaverse-fueled digital transformation could create new business value and contribute to corporate strategy. At the same time, metaverse ecosystems and technologies will transform dramatically as they become business ready, building capabilities and controls to appropriately manage sensitive business and user data.

ChatGPT, OpenAI's generative AI Large Language Model (LLM), has exposed the world to the potential and power of LLMs to transform business, allowing us to reimagine what is possible. The immediacy of Generative AI's disruption is only matched by its breadth as these foundational models will transform work in every industry and impact an estimated 40% of all working hours [1]. Work, itself, will be broadly transformed.

While the future of emerging technologies is promising, one fact is clear: success of emerging technologies will depend on trust. Establishing and maintaining trust means ensuring the security, privacy, and safety of individuals, communities, businesses, data and services of experiences enabled by emerging technology. If the trust in how businesses use emerging technologies is lost, the business strategies will fail fast.

TERMS TO KNOW

GENERATIVE AI: Generative artificial intelligence (AI) describes software that can be used to create new content, data, and information, including audio, code, images, text, simulations, and videos.

GPT: Generative Pre-trained Transformers - a machine learning model trained using internet data to generate content.

"We see the metaverse as a continuum that spans the spectrum of digitally enhanced worlds, realities and business models…The Metaverse Continuum will transform how businesses interact with customers, how work is done, what products and services companies offer, how they make and distribute them, and fundamentally how they operate their organizations. Leaders need to step back and reimagine how [they] will approach business for the next decade – which worlds [they] will define and design, starting now." - Accenture [2]

PILOTS SHOULD BE INITIATED TO EXPLORE FUTURE VALUE PROPOSITIONS

Fully realized, the metaverse is a persistent, shared, 3-dimensional space where people will be immersed (via extended reality technologies) in social, entertainment, learning, citizen, business and cultural experiences. Persistence of these environments is key to enabling the flow of individuals, data, commerce and experiences across space that is shared, collaborative, interoperable, trusted and owned by many parties.

The terms metaverse and Web 3.0 are often used interchangeably, though they refer to two different but related concepts. Web 3.0 describes the third phase or incarnation of the internet. It is an evolution focused on distributing systems to create a more secure, transparent, and open internet experience that enables direct interactions between users and their peers without intermediaries. Those direct interactions are why we often hear about the "creator" economy of Web 3.0, as they give power back to the creators, removing barriers to entry and engagement. One way to think about the vision of Web 3.0 is democratizing access, services, and experiences—shared ownership. In practice, Web 3.0's structure will likely be a combination of centralized, single business or entity ownership, and decentralized, shared ownership by stakeholders, environments that will co-exist.

The Web 3.0 vision is achieved using web3 technologies that enable decentralization, security, and transparency. These enabling technologies include Augmented Reality (AR), Mixed Reality (MR), Virtual Reality (VR)--collectively known as Extended Reality (XR)--5G, blockchain, digital twins, Artificial Intelligence (AI), smart(er) edge devices and networks, and improvements in processing and graphics. Many of these technologies existed well before the development of metaverse ecosystems. The power of metaverse is in the sum of the parts to enable new and enhanced experiences. Metaverse ecosystems are provoking us to think more broadly about how these technologies could be used for engagement across ecosystems to experience place and ownership.

The manner in which these various technologies are converging will be transformative, and businesses should be developing use cases and piloting metaverse applications. Generative AI, showcased publicly with OpenAI's ChatGPT is already demonstrating the power of disruptive emerging technologies. Generative AI will transform how we think about work, insights, software development, learning, art and more that we are just starting to imagine. Generative AI is a fast-moving technology with few barriers to entry that is allowing us to rethink enablement, efficiency, and creativity in all dimensions of our lives. Generative AI will also be important in the rapid creation of metaverse experiences because the technology can readily generate text, audio, code, images and video in the context of the business process or experience [3].

Large Language Models (LLMs) have now reached two significant milestones: (1) language mastery with the ability to understand context, intent and be creative and, (2) scale from truly massive quantities of training data which allow these models to be used, adapted, or tuned for a myriad of different tasks. With a simple conversational interface, we can receive data, insights, and responses that we can then refine through the conversation with reinforced (machine) learning.

"The ability of Large Language Models (LLMs) to process massive data sets allows them to potentially know everything an organization has ever known—the entire history, context, nuance and intent of a business, and its products, markets and customers. Anything conveyed through language (applications, systems, documents, emails, chats, video and audio recordings) can be harnessed to drive next-level innovation, optimization and reinvention" - Accenture [4]

Early engagement is critical to understanding how these emerging AI technologies can transform and disrupt businesses. Pilots will be the foundation for shaping opportunities and value propositions and should be used to provide critical feedback to technology providers and standards organizations. This critical feedback can be used to develop standardized business ready applications and an enhanced understanding of necessary controls.

Siloed development should be avoided at all costs. It's very important that cross-organization development teams be at the table and include representatives from legal, risk, IT, marketing, security, etc. Emerging technology pilots should also be prioritized relative to the nature of the emerging technology disruption – how quickly and at what scale will this technology become a strategic business opportunity or a threat to the business by a competitor? In the case of generative AI, these opportunities and disruptions may be relatively immediate. Successful innovators will have multiple emerging technology workstreams to enable rapid strategic learning.

What Boards Should Do:

- Boards should build emerging technology acumen. Engage outside experts to help the board gain contextual clarity around industry specific opportunities.
- Understand the businesses' emerging tech strategy.
  - Determine whether the leadership team is keeping pace with industry peers on innovation, or whether the business is a target for disruption by falling behind.
  - Is the strategy multithreaded? Will it allow learning across multiple disruptive technologies?
  - Does the strategy recognize the unique time to value of the different technologies?
- Understand which business units are leading the respective emerging tech efforts and shaping pilots that could lead to future value or transformations in services or customer engagement.
- Ensure that these teams include representation from Marketing, Risk, Security, IT, Line of Business Leaders and Legal. Ask whether the team includes any outside expertise or advisors.
- Understand what others are doing in their industry around the portfolio of emerging tech pilots/enablement.
- Understand how success will be measured in pilots.

TODAY'S TECH IS RAPIDLY EVOLVING, LEVERAGE IT TO LEARN AND ENSURE APPROPRIATE DATA PROTECTION

Metaverse ecosystems and technologies were initially designed for gaming, entertainment, and social networking. As a result, the expected security, privacy, and safety controls needed by the business may not be natively built into those technologies or ecosystems. As they select pilot technology, businesses must carefully navigate the selection of both ecosystems and technologies to determine whether the expected security, privacy and safety controls are present or forthcoming on product roadmaps. Navigating the rapid evolution of technologies and ecosystems is a complex task and may require external expertise.

Businesses will be expected, at a minimum, to provide the same level of protection for business and user data in Web 3.0 as Web 2.0. Compliance teams, auditors and regulators will expect to find the same standard of care and comparable controls. While ecosystem and technologies are maturing, businesses

should be identifying pilots that can be exercised within the existing controls environment. In practice, the sensitivity of business and user data should not exceed the ability of the selected technology and ecosystems to protect it. This practice may help in the prioritization and sequencing of early pilots.

While Generative AI and Large Language Models (LLMs) are here and ready to use, it's important to understand how these models work, before they are used with business data. The disciplines of Responsible and Trustworthy AI provide the guardrails and practices that help manage the risks in developing and using models [5]. It is also important to understand the appropriate uses and limitations of each model, and of the data that trained the model, in order to ensure effectiveness. One simple example of the value of this exercise is GPT's self-admission that it cannot respond about events after September 2021, as these were outside of the training data. More serious impacts of not understanding or curating the training data set are outcomes of inaccuracies, misinformation, discrimination, bias, harm, lack of fairness or adversarial actions like data poisoning. For AI at large, businesses should focus on being great stewards and custodians of their business data.

Businesses should understand the underlying data ownership, usage rights and protections when selecting ecosystem and technologies. Some technology, platforms and services may retain rights to your business and user data. VR headsets are a case in point; each vendor has unique practices with some claiming full or shared ownership of collected user sensor data. Governance, data protection and user protection should drive which ecosystems are suitable for business pilots. Businesses should also consider additional data management strategies. Supporting technologies such as mobile device management for VR headsets and privacy-preserving computing provide additional layers of data and user protection. OpenAI shares how they collect and use account information and user content in their privacy policy. For OpenAI business offerings, customer agreements cover the access and use within the business offerings. In early pilots, businesses should consider the use of business offerings which may provide additional data and privacy protections. Businesses should also explore the use of synthetic data, private instances and privacy preserving techniques as these services for business evolve.

What Boards Should Do:

- Understand how the business is monitoring emerging technology changes.
- Understand how pilot and product risks are being assessed. Understand how privacy concerns are being anticipated and addressed.
- Understand the organization's talent strategy for building skills to enable the successful application of AI related technology.

PROTECTING THE HUMAN AND DELIVERING TRUST

Adopting emerging technology comes with a responsibility to understand the new risks it may introduce.

In a virtual reality enabled metaverse, humans are fully integrated and therefore present a new attack surface to defend. In fact, during metaverse experiences, people are integrated with technology in a way that they have never been before with sensory perceptions completely immersed: vision, hearing, spatial orientation, sense of balance, depth perception, proprioception [6] and touch. Virtual reality technology provides unparalleled proximity to the human mind. A host of sensors capture eye tracking, facial expression, motion, hand tracking, voice, spatial boundaries to enable these experiences. With this sensor data, AI can readily infer age, gender, disability, ethnicity, health conditions, user attention, identity, speech content and more.

TERM TO KNOW

Proprioception (or kinesthesia) is the sense through which we perceive the position and movement of our body, including our sense of equilibrium and balance, senses that depend on the notion of force. [6]

The inferred data is a rich digital fingerprint of personal and private data that needs appropriate protections. In the wrong hands it can be used for discrimination, bias, targeting, identification, impersonation and cybercrime. VR vendors have already experienced cyber and privacy breaches on more than 14 products. Attacks on the sensors themselves could change the experience and perception of the person, leading to physical, psychological or neurological harm, misinformation, deception, surveillance or hijacking. We will see new cyber/physical/neurological attack methods as adversaries focus on the human attack surface in these experiences.

Businesses have a responsibility to protect customers' security, privacy and safety in metaverse experiences. But the duty of care is even greater: businesses will also need to ensure their corporate values and environmental, social and governance (ESG) stewardship convey to the metaverse. As companies engage in the metaverse—whether to design experiences, build platforms or leverage devices—they should be guided by a set of core principles and a deep understanding of the risks and opportunities across trust and human dimensions.

> *"**The trust dimensions**—privacy, security, resilience, and intellectual property rights—shape how technology, product policies and practices are designed and deployed. Getting these trust dimensions right is essential to creating a metaverse in which people will want to engage and return. **The human dimensions**—safety, sustainability, inclusion/diversity/accessibility, and well-being—ground the design and build of the user experience." - Accenture [7]*

Businesses must have trust as the cornerstone of their metaverse strategy. Customer expectations, corporate values, and the protection of customer interests should underly all metaverse development efforts. Customers must be able to trust their metaverse experiences and the companies behind those experiences.

There is no single recipe for trust. Businesses need to understand that customers' expectations are informed by norms, culture, geography, and context of that virtual experience. Businesses need to think forward in their strategy to accommodate a global community with many different expectations for trust.

> *"And as we evolve the Metaverse Continuum, we must seize the opportunity to ensure that it is developed with responsibility at the core. From ownership of data, to inclusion and diversity, to sustainability and through to security and personal safety, this work must begin now."- Sweet, Daugherty - Accenture [8]*

Businesses should adopt an enterprise-wide strategy for Responsible AI, at large, with specific guidance for generative AI and large language models. Organizations should ensure that risk management is a fundamental part of the emerging technology adoption. For generative AI, it will be particularly important for businesses to understand the legal, ethical, reputational risks they may be incurring.

What Boards Should Do:

- Ask leaders how they are assessing customer expectations and values. How are they ensuring diverse representation in customer surveys?
- Understand how leaders are implementing security and privacy by design in metaverse pilots.
- Understand how the organization is learning about adversarial activity, cybercrime and the human attack surface in these metaverse ecosystems.
- Many firms are designating a leader of Responsible Metaverse. Determine if such a role makes sense for your organization.
- Understand whether your organization has developed principles and guidance for responsible innovation.

- Determine if your firm is working with outside organizations or standards bodies to understand and navigate human and trust protections.
- Understand whether there is a trust and safety strategy to help navigate issues such as content moderation, brand safety, civility, and toxicity mitigation.

WORKS CITED:

[1] https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-A-New-Era-of-Generative-AI-for-Everyone.pdf#zoom=40
[2] https://www.accenture.com/us-en/insights/technology/technology-trends-2022
[3] https://openai.com/research/gpt-4
[4] https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-A-New-Era-of-Generative-AI-for-Everyone.pdf#zoom=40 page 6
[5] https://www.accenture.com/us-en/services/applied-intelligence/ai-ethics-governance
[6] https://www.sciencedirect.com/topics/neuroscience/proprioception
[7] https://www.accenture.com/us-en/insights/technology/responsible-metaverse
[8] Julie Sweet and Paul Daugherty https://www.accenture.com/us-en/insights/technology/technology-trends-2022

REFERENCE LINKS:

https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies
https://www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf
https://www.weforum.org/reports/demystifying-the-consumer-metaverse
https://www.accenture.com/content/dam/accenture/final/accenture-com/a-com-custom-component/iconic/document/Accenture-Technology-Vision-2023-Full-Report.pdf

---

ABOUT THE AUTHOR

Lisa O'Connor
Managing Director – Accenture Security, Cybersecurity R&D, Accenture Labs

Lisa is the Global Leader of Security Research and Development at Accenture, leading two Labs in Washington DC and Herzliya, Israel. Her role is to ideate, develop and co-innovate with the Global 2000 to create the future of security and cyber defense. Key to her success, she looks over the horizon at the global start-up ecosystem and emerging technologies to identify white space opportunities and develop next generation cybersecurity proof of concepts. Current research areas include Metaverse Security, Quantum Security, Cyber Digital Twins, Intelligent Data Operations and Mesh, Trustworthy Artificial and Security of Operational Technology.

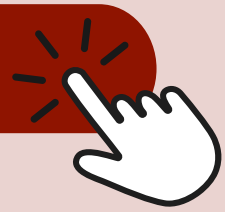
Throughout her 30-plus-year career in security, she has played many critical roles, including CISO at Fannie Mae where she served as an active member of the Financial Services Sharing and Analysis Center (FS-ISAC) and the Financial Services Sector Coordinating Council. The first nine years of her career at the National Security Agency included tours at the White House Communications Agency and the Surveys and Investigations Staff of the House Appropriations Committee. She moved to the private sector where she led national security consulting practices at several top-tier firms. Lisa has worked directly for the Board Risk Committee of a top 10 financial services company. She was recognized as one of The Top 25 Women Leaders in Cybersecurity of 2020 by The Software Report. She chairs the Accenture Cybersecurity Forum's Women's Council, a CISO council focused on professional development of Cyber leaders and bringing the next generation of rising women leaders forward.

QUICK SURVEY

What content and in-person events matter to you most?

The BRC is entering our next chapter of program delivery, and we want to know what content and events are most relevant to you. Please complete the quick survey below to help us decide where to focus our efforts and provide you with the most valuable insight into board risk oversight and enterprise risk management.

Click to Access Survey



The Board Risk Report *is the periodic publication of the BRC.* ***SUBSCRIBE NOW*** *to receive complimentary world-class risk management practices delivered directly to your inbox.*

WHO WE ARE

The Board Risk Committee (BRC) is the foremost thought leadership peer council for board risk committee members and chief risk officers. The BRC is a nonprofit, non-competitive, trusted place for the exchange of ideas, strategies, and best practices in enterprise risk oversight. We advocate for having risk committees of boards, where appropriate, and for educating board directors about enterprise risk. The BRC aims to foster more effective risk management and board oversight. The BRC works in partnership with The Santa Fe Group (SFG) and Shared Assessments (SA). SFG is a strategic advisory company providing expertise to leading corporations and other critical infrastructure organizations in the area of risk management. SA is the thought leader and provider of tools, education and certifications in the third party risk management space. *The Board Risk Report is the periodic publication of the BRC.*

BRC Contacts:
Catherine A. Allen, Founder and Chair of the Board, cathy@boardriskcommittee.org
Ellen Dube, Executive Director, ellen@boardriskcommittee.org
Susan C. Keating, Chief Partnership Officer, susan@boardriskcommittee.org