of C-suite respondents believe that security and privacy are the primary risks from adopting virtual environments.¹

Will blended worlds encourage deception?

Imagine that a fake, yet realistic, AI-generated video of a CEO spreading disinformation goes viral and the damage it could inflict on a company.

Unintended consequences

With virtual interactions becoming more sophisticated, they rely on more data and more complex partner ecosystems. This creates potential risks that organizations must prepare for.

Leaders must be transparent about how customer information is being used, while protecting their organizations against hackers. Leaders must also ensure that ethical safeguards are designed into the real virtualities they create.

Detecting deepfakes

Virtualization brings another unintended consequence. Beyond the benefits of realistic virtual worlds lurks a risk in the form of digital deception through “deepfakes.”

One energy firm executive thought he was speaking with his CEO, but was tricked into transferring US$243,000 to a scammer who used AI-based software to mimic the CEO’s voice.²

How can organizations defeat deepfakes?

A race is unfolding where “counterfeit realities” are looking to outpace detection capabilities. To win this race, organizations can deploy combinations of AI and quantum computing to create “truth filters,” protecting their corporate brands.

¹ Accenture Business Futures study (2021).

Copyright © 2021 Accenture. All rights reserved. Accenture and its logo are trademarks of Accenture.