

ผู้ประกอบการในโลกของเมตาเวิร์สและความปลอดภัยทางไซเบอร์ในยุคดิจิทัล

Entrepreneurship in Metaverse World and Cyber Security in Digital Era

ณัฐปภัศ จุ้ยเจริญ¹ สุรเดช หวังทอง² และพรณา เปี่ยมไทย³

Nhatphaphat Juicharoen¹ Suradetch Wangthong² and Pornapa Peamchai³

Received : August 24, 2023 Revised : May 16, 2024 Accepted : May 23, 2024

บทคัดย่อ

ในอดีตที่ผ่านมาภาคธุรกิจขาดการตระหนักรู้ถึงปัญหาภัยคุกคามทางไซเบอร์ จนละเลยต่อการจัดการระบบความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรให้มีประสิทธิภาพ ซึ่งเป็นเหตุให้ถูกกลุ่มอาชญากรไซเบอร์เข้าโจมตีจนสร้างความเสียหายให้กับภาคธุรกิจ บทความนี้มีวัตถุประสงค์เพื่อรับรู้และเตรียมความพร้อมรับในการป้องกันปัญหาที่เกิดขึ้นจากเมตาเวิร์ส และความปลอดภัยทางไซเบอร์ โดยใช้วิธีการวิเคราะห์เนื้อหาจากงานวิจัย วารสาร ในฐานะข้อมูลระดับชาติและนานาชาติ ดังนั้น ผู้ประกอบการในยุคปัจจุบันจำเป็นที่จะต้องมีการเร่งจัดการมาตรการความมั่นคงปลอดภัยทางไซเบอร์ภายในธุรกิจ เพื่อลดช่องโหว่ทางเทคโนโลยีคอมพิวเตอร์ และเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ที่กำลังสร้างความปั่นป่วนให้กับธุรกิจไปทั่วโลก

คำสำคัญ : เมตาเวิร์ส จักรวาลเสมือนจริง ความปลอดภัยทางไซเบอร์ ยุคดิจิทัล

¹ อาจารย์ คณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

¹ Lecturer, Faculty of Business Administration, Rajamangala University of Technology Thanyaburi

² ผู้ช่วยศาสตราจารย์ สาขาวิทยาการจัดการ มหาวิทยาลัยสุโขทัยธรรมาธิราช

² Assistant Professor, Management Science, Sukhothai Thammathirat Open University

³ ผู้ช่วยศาสตราจารย์ คณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

³ Assistant Professor, Faculty of Business Administration, Rajamangala University of Technology Thanyaburi

* Corresponding author Email: Nhatphaphat_j@rmutt.ac.th

Abstract

In the past, business sectors were not aware of cyber-threats then they failed to manage efficiency cyber security systems. Thus, they were manipulated by cybercriminal attacks. This article aims to recognize and arrange to prevent problems from arising of Metaverse and cyber security issues. Content analysis from various research and journals in national and international databases was used in this study. Therefore, entrepreneurs in present day need to organize cyber security issues within their businesses to reduce gap of computer technology and to conform cyber-treats which disrupt all businesses around the world.

Keywords: Metaverse, Virtual Universe, Cybersecurity, Digital Era

บทนำ

เนื่องจากในปัจจุบันขีดจำกัดการเป็นผู้ประกอบการเชิงนวัตกรรมกำลังถูกผลักดัน ด้วยคนรุ่นใหม่ที่จะคิดค้นซอฟต์แวร์ และฮาร์ดแวร์ ที่จะทำให้ชีวิตง่ายมากขึ้นจึงต้องให้ความสำคัญกับความจริงเกี่ยวกับโลกยุคใหม่และต้องมีการเตรียมความพร้อมหรือรองรับสถานการณ์ดังกล่าว โดยนวัตกรรมที่เรียกว่า เมตาเวิร์ส (Metaverse) หรือที่รู้จักกันว่า “จักรวาลเสมือนจริง” (Virtual Universe) ซึ่งถูกจัดให้เป็นการพัฒนาอีกก้าวหนึ่งของระบบอินเทอร์เน็ต เป็นอุปกรณ์เสมือนจริงที่ทำให้การรับรู้ความรู้สึกต่าง ๆ ได้อย่างเต็มที่โดยไม่ต้องมีการกระทำทางกายภาพใด ๆ จักรวาลเสมือนจริงดังกล่าวสามารถทำให้นutzerเข้าไปสู่สภาพแวดล้อมทางกายภาพจำลอง ดังนั้น คอมพิวเตอร์ อุปกรณ์ที่ใช้จอสัมผัส หรือ แพลตฟอร์มที่มีความสามารถต่าง ๆ ปัจจุบันหลายคนและหลายองค์กรทั่วโลกได้เข้าสู่กระบวนการ เมตาเวิร์ส (Metaverse) อย่างรวดเร็ว รวมถึงใช้ในการคาดการณ์อนาคตด้วย และ เมตาเวิร์ส (Metaverse) ดังกล่าวเป็นที่นิยมสำหรับผู้ประกอบการและรู้จักกับ อวตาร (Avatar) คือ ภาพกราฟิกที่ถูกสร้างขึ้นเพื่อใช้แทนภาพลักษณ์จริงของผู้ใช้งานบนอินเทอร์เน็ต จะสามารถเข้าประชุมโดยใช้ เมตาเวิร์ส (Metaverse) ได้โดยสามารถเลือกได้ว่าจะเป็น อวตาร (Avatar) ใด และแต่งกายแบบใด รวมถึงการเลือกเสียง และการแสดงสีหน้า เรายังสามารถไปท่องเที่ยวทั่วโลกได้และเรียนรู้สิ่งต่าง ๆ ได้จากการช้อปปิ้ง จนถึงการลงทุน ตัวอย่างเช่น ไม่ว่าจะอยู่ที่ไหนในโลก จะสามารถใช้จักรวาลเสมือนจริงได้ทุกเมื่อตามต้องการในการท่องเที่ยวหรือช้อปปิ้งที่ได้ก็ได้ เป็นต้น

ประเทศที่พัฒนาแล้วและบริษัทชั้นนำของโลกได้เริ่มปฏิบัติงานเกี่ยวกับเรื่องสารสนเทศตั้งแต่กลางยุค 1990 โดยดึงดูดกลุ่มคนรุ่นใหม่เข้าสู่สายงานนี้ด้วย โดยเปิดโอกาสในการสรรหาคณะใหม่อยู่ที่ เมตาเวิร์ส (Metaverse) แห่งโลกเสมือนจริง (VR), โลกเสมือนผสมโลกแห่งความจริง (AR) ปัญญาประดิษฐ์ (AI), เทคโนโลยีการจัดเก็บข้อมูลที่เชื่อมโยงกันเป็นเครือข่ายผ่านการเข้ารหัสทางคอมพิวเตอร์ (blockchain), เทคโนโลยีเซลลูลาร์ไร้สายยุคที่ 5 (5G), เทคโนโลยีที่สวมใส่ได้ (Wearable Tech) เป็นอุปกรณ์อัจฉริยะที่อยู่ติดตัวเสมือนเครื่องแต่งกาย เทคโนโลยีเหล่านี้มาในรูปของ นาฬิกาอัจฉริยะ (Smart watch), ป้ายอัจฉริยะ (Smart Badges) และเทคโนโลยีเซ็นเซอร์ โดยเทคโนโลยีโลกเสมือนผสมโลกแห่งความจริง (AR) นั้น ถูกพัฒนาขึ้นเพื่อแสดงสิ่งต่าง ๆ ให้เหมือนจริง และมีการพัฒนามากยิ่งขึ้น โดยผ่านภาพ 3 มิติ ซึ่งทำให้เกิดการสร้างโอกาสที่จำเป็นกับโลกธุรกิจและผู้บริโภค ได้เห็นการทำธุรกิจ นักการตลาด และทำแบรนด์จำนวนมาก ประกาศกระโดดเข้าสู่โลกของเมตาเวิร์ส ทั้งในไทยและในระดับโลก ตัวอย่างเช่น บริษัท Nike เตรียมผลิตสินค้าเสมือนจริงเพื่อขายในโลกเมตาเวิร์ส เริ่มมีการรับพนักงานสายออกแบบวัสดุเสมือนสำหรับรองเท้าและสินค้าอื่น ๆ บริษัท Microsoft สร้างแพลตฟอร์มเพื่อการประชุมในโลกเสมือนจริง 3 มิติ แบบไม่ต้องแว่น หรือการจำลองภาพให้เสมือนจริง แบบ 360

องศา (VR) บริษัท Tinder วางแผนพัฒนาแพลตฟอร์มเพื่อรองรับระบบเศรษฐกิจบนโลกเสมือน (Virtual Economy) เพื่อเตรียมสร้างฟีเจอร์ที่ทำให้ลูกค้ามีประสบการณ์ในการออกเดทในโลกเสมือนจริง และบริษัทนั้นยัง แปรนตร์รองเท้าที่อยู่คนไทยมานาน ได้ประกาศสร้าง “อาคารรองเท้าแตะ” ในรูปแบบของสินทรัพย์ดิจิทัลที่มีลักษณะเฉพาะตัว ไม่ซ้ำใคร จำต้องไม่ได้แต่สามารถซื้อขายได้เหมือนทรัพย์สินอื่น ๆ (NFT) ใน Metaverse Thailand จากข้อมูลจะเห็นได้ว่าธุรกิจบางแห่งได้ปรับตัวให้อยู่ในรูปของเมตาเวิร์ส แล้ว

จากการค้นคว้าในแหล่งข้อมูลต่างๆ เกี่ยวกับเมตาเวิร์ส (Metaverse) และความปลอดภัยทางไซเบอร์ เป็นเรื่องสำหรับผู้ประกอบการยุคดิจิทัลที่ต้องให้ความสนใจเป็นอันดับต้นๆ ที่นำเทคโนโลยีเข้ามาเกี่ยวข้องในการดำเนินธุรกิจซึ่งเกิดช่องโหว่ของความปลอดภัยทางไซเบอร์ เช่น ข้อมูลหลักทรัพ์จัดการกองทุน (บลจ.) ทิสโก้ (2564) พบว่า ประเทศที่มีจำนวนการเกิดอาชญากรรมไซเบอร์สูงสุด 3 อันดับแรก ได้แก่ สหรัฐอเมริกา ถูกโจมตีจำนวน 156 ครั้ง อังกฤษ จำนวน 47 ครั้ง และ อินเดีย จำนวน 23 ครั้ง บริษัท และเชื่อมโยงกับข้อมูลของ Canalys Special Report ได้ระบุว่าอาชญากรรมไซเบอร์ทั่วโลก มีแนวโน้มเร่งตัวขึ้น โดยเฉพาะอย่างยิ่งในช่วงที่เกิดการแพร่ระบาดของ COVID-19 ซึ่งบริษัทต่าง ๆ ได้นำเทคโนโลยีเข้ามาใช้ในการทำงาน เช่น การติดต่อประสานงาน การรับส่งข้อมูลที่เป็นความลับขององค์กร เพื่อสร้างความสะดวกสบายให้พนักงานสามารถทำงานได้จากที่บ้านได้ (Work From Home) โดยไม่ต้องเข้าออฟฟิศ ดังนั้นจะเห็นได้ว่าความเสี่ยงที่จะเกิดขึ้นที่เรียกว่าอาชญากรรมไซเบอร์เข้ามาแทรกแซงในการทำงานเกี่ยวกับระบบสารสนเทศภายในหน่วยงานมีเพิ่มมากขึ้นอย่างต่อเนื่อง บทความวิชาการนี้จึงขอเสนอในแง่มุมของการนำ เมตาเวิร์ส (Metaverse) มาใช้มีทั้งผลดีและผลเสียซึ่งอาจเพิ่มความเสี่ยงด้านความปลอดภัยในโลกไซเบอร์ และแนวทางการป้องกันการจากความเสี่ยงที่จะเกิดขึ้น จึงขยายความเข้าใจและอธิบายเนื้อหาในเชิงลึกเพื่อเตรียมพร้อมปรับตัวรับมือการเปลี่ยนแปลงซึ่งจะเกิดขึ้นอย่างแน่นอนในอนาคต

การทบทวนวรรณกรรม

เมตาเวิร์ส (Metaverse) คำว่า เมตาเวิร์ส (Metaverse) มาจากคำว่า meta ก็คือโลกเสมือนจริงที่สามารถใช้ชีวิต หรือทำกิจกรรมต่าง ๆ ได้เหมือนในโลกของความจริง โดยมีอินเทอร์เน็ตเป็นตัวกลางเชื่อมกับโลกเสมือน และใช้เทคโนโลยี VR (Virtual Reality) และ AR (Augmented Reality) จำลองสิ่งที่คิดให้เกิดขึ้นจริง ๆ โดยมีนักวิชาการหลายท่านศึกษาเกี่ยวกับเมตาเวิร์ส ดังนี้ สุรพล บุญลือ (2565) ได้ศึกษาเมตาเวิร์ส พบว่า การอวตาร ไปเป็นคนอื่นอาจจะทำให้เกิดความสนุก เกิดความแปลกใหม่ และหลีกเลี่ยงจากตัวตนที่เป็นอยู่หลีกเลี่ยงจากความจริงที่เกิดขึ้น แม้ความเสมือนจะมีการนำมาใช้กับการศึกษาทำให้เกิดประสบการณ์ ซึ่งสอดคล้องกับ สมเกียรติ วุฒิธรรมมาภิวัฒน์ (2565) Metaverse ระบุว่าเป็นการผสมผสานระหว่างองค์ประกอบต่าง ๆ ของเทคโนโลยีรวมทั้งความเป็นจริงเสมือน (VR) ความเป็นจริงเสริม (AR) และวิดีโอที่ผู้คนใช้ ชีวิตภายในโลกดิจิทัล Metaverse จึงเปรียบเสมือนสะพานเชื่อมระหว่างโลกความเป็นจริงและโลกเสมือน และธนภัทร ศรีผาน (2565) ได้กล่าวตรงกันว่า เมตาเวิร์ส (Metaverse) หรือจักรวาลนฤมิต คือเครือข่ายสามมิติบน โลกเสมือนจริง (Virtual World) ที่ถูกสร้างขึ้นเพื่อให้ผู้คนเข้ามามีปฏิสัมพันธ์ระหว่างกันได้ทุกรูปแบบ ทั้งการพูดคุย การเรียนการสอน และการทำงานร่วมกัน ผู้ใช้เมตาเวิร์สสามารถเข้าสู่โลกเสมือนจริงได้ ทุกที่ทุกเวลาผ่านร่างอวตาร (Avatar) ที่ตนเป็นผู้สร้างขึ้นตามความต้องการ เทคโนโลยีที่ใช้ในเมตาเวิร์ส ประกอบด้วย Augmented Reality (AR) ช่วยสร้างกราฟิกซ้อนทับขึ้นมามบนโลกจริง เทคโนโลยี Virtual Reality (VR) สร้างสภาพแวดล้อมเสมือนจริงสามมิติแบบ 360 องศา ซึ่งต้องอาศัยอุปกรณ์ที่ ใช้ปฏิสัมพันธ์กับโลกเสมือน เช่น แว่นตา VR ซึ่งยังมีข้อจำกัด คือ ผู้ใช้จะมองไม่เห็นสถานที่จริงและ อาจทำให้เกิดการเดินชนสิ่งของหรือผนังห้องได้ จนต่อมาได้มีการพัฒนาเทคโนโลยี Mixed Reality (MR) ที่ผสาน

AR และ VR เข้าด้วยกัน อีกทั้งยังสามารถมองเห็นภาพเสมือนซ้อนทับกับในโลกของความเป็นจริง ทำให้ผู้ใช้เมตาเวิร์สสามารถเดินทางและใช้ชีวิตในสถานที่จริงพร้อมกับมองเห็นโลกเสมือนที่เป็นโลกคู่ขนานไปพร้อมกันโดยไม่มีข้อกักรวเลื่องการเดินชนหรืออุบัติเหตุ โดยมีนักวิชาการ คือ (Zhang, 2022); (Lee & Kim, 2022); (Folger, 2022); (Akour et al., 2022 ; Enache, 2022) ได้สรุปว่า เมตาเวิร์ส (Metaverse) หรือจักรวาลอนฤมิต เป็นการผสมผสานร่างกายของมนุษย์ กับอุปกรณ์อิเล็กทรอนิกส์ให้ความรู้สึกที่เหมือนจริงแบบรอบทิศทาง ไม่ว่าจะเป็นการมองเห็น การขยับร่างกาย ให้ความรู้สึกเหมือนกันเราอยู่ในสถานที่นั้นๆจริง แต่ความเป็นเราอาจนั่งอยู่ในมุมห้อง เล็กๆ

เนื่องจาก เมตาเวิร์ส (Metaverse) เป็นเรื่องใหม่ จึงได้รับความนิยมมาต่อเนื่องเป็นเวลหลายปี และบริษัทเทคโนโลยีทั่วโลกได้ทุ่มเทพทรัพยากรจำนวนมากหรือบางส่วนในการพัฒนา เมตาเวิร์ส (Metaverse) เช่น Microsoft และบริษัทขนาดใหญ่อื่น ๆ ได้ลงทุนหลายร้อยล้านดอลลาร์ในโครงการพัฒนา เมตาเวิร์ส (Metaverse) ซึ่งแสดงให้เห็นถึงความเชื่อที่เพิ่มขึ้นว่า แนวคิด เมตาเวิร์ส (Metaverse) ซึ่งเป็นโลกเสมือนจริง จะเป็นหลักในการพัฒนาในอนาคตและก่อให้เกิดประโยชน์ได้อย่างมาก ซึ่งการเพิ่มขึ้นของโลกเสมือนบนอินเทอร์เน็ต (Second Life) เป็นสิ่งที่เพิ่มแรงจูงใจให้คนมีส่วนร่วมในโลกเสมือนจริงและทำธุรกิจได้ (Slagter et al., 2007) รวมถึงกระตุ้นให้เกิดนวัตกรรม ผู้ประกอบการ ในโลกเสมือนจริงและโลกแห่งความเป็นจริง โดย (Chandra and Leenders, 2012; Mystakidis, 2022)) กล่าวว่า ความก้าวหน้าทางเทคโนโลยี เช่น พลังการประมวลผลและอินเทอร์เน็ตเฟช รวมถึงผลประโยชน์ทางธุรกิจที่ได้รับการปรับปรุงใหม่ โดยเฉพาะอย่างยิ่งจากบริษัทเทคโนโลยีขนาดใหญ่ ตัวอย่างเช่น Facebook รีแบรนด์ตัวเองเป็น เมตาเวิร์ส (Meta, 2021) กล่าวว่า Meta จะส่งผลให้ความสนใจในโลกเสมือนจริงและ เมตาเวิร์ส (Metaverse) ได้รับความสนใจขึ้นมามากครั้ง เมตาเวิร์ส (Metaverse) ประกอบด้วยโครงสร้างพื้นฐานดิจิทัลที่กลมกลืนและต่อเนื่องกับโลกเสมือนจริงหลายแห่ง

ผู้ประกอบการดิจิทัล

การเป็นผู้ประกอบการดิจิทัลถือกำเนิดขึ้นในยุคที่มีเทคโนโลยีเข้ามามีบทบาทอย่างมากในการดำเนินธุรกิจ ซึ่ง (Le Dinh et al., 2018) กล่าวว่าผู้ประกอบการในยุคดิจิทัลต้องเผชิญกับความแตกต่างมากมายเมื่อเทียบกับผู้ประกอบการแบบดั้งเดิม ทั้งผลิตภัณฑ์ การตลาด และสถานที่ในรูปแบบเทคโนโลยีที่เป็นเกณฑ์สำคัญในการสร้างความแตกต่างระหว่างผู้ประกอบการในยุคดิจิทัลและผู้ประกอบการแบบดั้งเดิม (Kraus et al., 2019) ซึ่งเมื่อศึกษาผลการวิจัยของ นภัสพร นิยะวานนท์ (2564) พบว่า การเป็นผู้ประกอบการดิจิทัล นั้น หมายถึง ความสามารถของผู้ประกอบการในการริเริ่มค้นพบโอกาสทางธุรกิจใหม่ๆ การเปลี่ยนแปลงกลยุทธ์การดำเนินงาน ความสามารถตัดสินใจได้อย่างเป็นอิสระในการดำเนินงานให้สำเร็จ ส่วน (Niyawanont, 2021; von Briel et al., 2018) สรุปว่าองค์ประกอบของการเป็นผู้ประกอบการดิจิทัลสรุปได้ 4 องค์ประกอบหลักๆ คือ 1) การก่อตั้งหน่วยธุรกิจดิจิทัล (Digital Venturing) เป็นการปรับเปลี่ยนแนวคิดการดำเนินธุรกิจด้วยเทคโนโลยีดิจิทัล การปรับโครงสร้างองค์การ ตลอดจนการเปลี่ยนแปลงกลยุทธ์การดำเนินงาน 2) การแข่งขันเชิงรุกด้วยดิจิทัล (Digital Proactive Competition) เป็นการริเริ่มการจัดการหรือการดำเนินงานด้วยเทคโนโลยีดิจิทัลที่ทำให้องค์การนำเสนอสินค้าหรือบริการใหม่ๆ เป็นรายแรกที่เหมาะสมความสำเร็จ เข้าสู่ตลาดได้ก่อนคู่แข่งท่ามกลางสภาพแวดล้อมทางธุรกิจที่มีการแข่งขันอย่างรุนแรงด้วยเทคโนโลยีดิจิทัล 3) อิสระภาพการดำรงธุรกิจยุคดิจิทัล (Digital Existence Autonomy) เป็นการกระทำที่เป็นอิสระของแต่ละบุคคลหรือทีมด้วยเทคโนโลยีดิจิทัลที่สามารถนำเสนอแนวคิดหรือวิสัยทัศน์โดยทำหน้าที่และตัดสินใจได้อย่างเป็นอิสระในการดำเนินงานให้สำเร็จ และ 4) การวิจัยและพัฒนาด้านดิจิทัล (Digital Research and Development) เป็นการพัฒนาผลิตภัณฑ์หรือบริการตามความ

ต้องการของลูกค้านี้เกิดขึ้นจากความก้าวหน้าทางเทคโนโลยีดิจิทัล รวมถึงการสนับสนุนแนวคิด หรือผลงานวิจัยเพื่อนำมาพัฒนาต่อยอดผลิตภัณฑ์หรือบริการใหม่ด้านเทคโนโลยีดิจิทัล ตามความคิดเห็นของ

การเป็นผู้ประกอบการในยุคดิจิทัลต้องเผชิญกับระบบนิเวศทางธุรกิจที่เปลี่ยนแปลงตาม ความก้าวหน้าของเทคโนโลยีดิจิทัลที่เข้ามามีบทบาทอย่างมากในการดำเนินธุรกิจ การเกิดขึ้นของยุคดิจิทัล เป็นยุคเศรษฐกิจใหม่แห่งการแข่งขัน (The New Economic of Competition) การใช้นวัตกรรมเป็นกลยุทธ์ของบริษัทที่สำคัญแสดงถึงความสามารถในการแข่งขันระดับโลกที่ทำให้ประสบความสำเร็จในระดับสากลตามที่นักวิชาการ (Sussan and Acs, 2017) เห็นว่าด้วยการนำความก้าวหน้าของเทคโนโลยีดิจิทัลที่เกิดขึ้นอย่างรวดเร็วจากการพัฒนานวัตกรรม ทำให้ผู้ประกอบการต้องหันมาดำเนินการเชิงรุก (Proactiveness) คาดการณ์ แสวงหา และติดตามโอกาสใหม่ๆ จากเทคโนโลยีดิจิทัล วิธีที่บริษัทมองเห็นโอกาสทางการตลาดในกระบวนการเข้าสู่ตลาดใหม่ เป็นเรื่องสำคัญที่จะต้องใช้ความรวดเร็วในการสร้างสรรค์หรือแสวงหาโอกาสใหม่ ๆ ส่วน (Shan, Song, and Ju, 2016) กล่าวว่า จากข้อมูลข้างต้นจะทำให้องค์กรสร้างความได้เปรียบในการแข่งขัน

ความปลอดภัยทางไซเบอร์

ปัจจุบันผู้คนต่างพึ่งพาเครื่องมือดิจิทัลกันมากขึ้นจึงเป็นเหตุผลให้หลายบริษัทมีความเสี่ยงจากการโจมตีทางไซเบอร์ การแฮกค์ข้อมูล และการละเมิดความปลอดภัยบนระบบอินเทอร์เน็ต ดังนั้นความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์เป็นสิ่งสำคัญของผู้ประกอบการดิจิทัลที่ต้องมีความรู้เกี่ยวกับความเสี่ยงที่อาจเกิดขึ้นกับธุรกิจตนเอง อาจกล่าวได้ว่าการโจมตีดังกล่าวจะมีการพัฒนาอย่างต่อเนื่องและมีความซับซ้อนมากขึ้นโดยความเสี่ยงที่เกิดอาจจะเป็นการสูญเสียข้อมูลที่จะเสียก่อน ความสูญเสียทางการเงิน อันเป็นผลพวงมาจากการโจรกรรม ค่าใช้จ่ายที่สูงขึ้นในการกู้คืนข้อมูลที่ถูกลบไป การสูญเสียชื่อเสียงที่ดี ขาดความเชื่อมั่น และอาจต้องปิดกิจการในกรณีร้ายแรงก็เป็นไปได้ ดังนั้นความปลอดภัยทางไซเบอร์จึงเป็นสิ่งสำคัญสำหรับทั้งบุคคลและองค์กรภาครัฐและภาคเอกชน แต่การดูแลความปลอดภัยเป็นเรื่องยาก ซึ่งนักวิชาการ (de Bruijn & Janssen, 2017; Spremić & Šimunic, 2018) กล่าวว่า ความปลอดภัยทางไซเบอร์ คือ เทคโนโลยีและกระบวนการที่ออกแบบมาเพื่อป้องกัน คอมพิวเตอร์ เครือข่าย โปรแกรม และข้อมูล จากการโจมตี การได้รับความเสียหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งภัยคุกคามทางไซเบอร์ที่เห็นมากในปัจจุบัน ก็คือ 1) ซอฟต์แวร์ประเภทหนึ่งที่เป็นอันตราย หรือเรียกว่า Malware ที่สามารถนำมาใช้ทำอันตรายต่อคอมพิวเตอร์ของผู้ใช้ได้ ซึ่งอาจจะมาในรูปแบบของไฟล์หรือโปรแกรม รวมถึงไวรัส ไรต์ส ไทจัน และสไปยาแวร์ 2) การโจมตีเพื่อขัดขวางการรับส่งข้อมูลของระบบของเป้าหมาย หรือเรียกว่า Distributed denial-of-service (DDoS) attacks เช่น เซิร์ฟเวอร์ เว็บไซต์ หรือเครือข่าย โดยการส่งคำขอร้องของการเชื่อมต่อ หรือ Package เป็นจำนวนมากไปยังเป้าหมาย เพื่อให้ระบบช้าลงหรือหยุดทำงาน 3) เป็นการโจมตีอีกรูปแบบ โดยการหลอกให้ผู้ใช้ เพื่อขโมยข้อมูลที่สำคัญหรือเรียกว่า Social engineering 4) การปลอมอีเมลที่มีแหล่งที่มาที่เป็นที่รู้จักกันอย่างกว้างขวางและเชื่อถือได้ และส่งอีเมลหลอกให้เหยื่อหลงเชื่อ หรือเรียกว่า Phishing เป็นอีกรูปแบบหนึ่งของ Social Engineering เช่น การปลอมอีเมลเพื่อขโมยข้อมูลชื่อผู้ใช้และรหัสผ่านของ Facebook โดยปลอมอีเมลเป็นเจ้าหน้าที่ของ Facebook ซึ่งคล้ายกับอีเมลจริงจนแยกไม่ออก ทำให้เกิดการหลงเชื่อ เป็นต้น 5) การหลอกลวงด้วยการพุ่งเป้าเจาะจงไปที่เหยื่อกลุ่มใดกลุ่มหนึ่งชัดเจน เริ่มจากการลวงข้อมูลส่วนตัวของเหยื่อแล้วส่งอีเมลที่เนื้อหามีความเฉพาะเจาะจงและสร้างความน่าเชื่อถือมากยิ่งขึ้น หรือเรียกว่า Spear Phishing เป็นการโจมตีแบบ Phishing อีกประเภทหนึ่ง ที่มีเป้าหมายที่ชัดเจน 6) Ransomware เป็นมัลแวร์อีกประเภท ที่เกี่ยวข้องกับการโจมตีผู้ใช้ โดยผู้โจมตีจะล็อกไฟล์หรือว่าจะเป็นล็อกระบบคอมพิวเตอร์ของผู้ใช้ที่เป็นเหยื่อโดยการเข้ารหัสไว้ และเรียกเงินเพื่อได้รับ

รหัสผ่านในการปลดล็อกไฟล์หรือระบบคอมพิวเตอร์ของผู้ใช้ 7) ภัยคุกคามที่เกิดขึ้นจากภายในองค์กร อาจจะโดยตั้งใจหรือไม่ตั้งใจ หรือเรียกว่า Insider Threats เช่น พนักงานภายในองค์กร ผู้รับเหมา หรือลูกค้า 8) การโจมตีโดยปลอมเป็นคนกลาง คอยดักฟังข้อมูลของเป้าหมายและสามารถปลอมตัวเป็นเป้าหมายได้โดยการส่งข้อมูลหลอก ๆ ให้กับเป้าหมายอีกคน หรือเรียกว่า Man-in-the-middle (MitM) attacks และ 9) การโจมตีโดยที่ผู้โจมตีจะแทรกซึมเข้าไปในเครือข่ายที่เป็นเป้าหมาย และซ่อนตัวอยู่เป็นเวลานาน เพื่อขโมยข้อมูล หรือเรียกว่า Advanced persistent threats (APTs) ซึ่งมีนักวิชาการ (Okokpuije, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E., 2023; Iorackis, C., Louca, C., Michaely, R., & Weber, M., 2023) ได้ให้ความคิดเห็นจากข้อมูลเบื้องต้นตรงกัน

ดังนั้น ปัญหาการคุกคามทางไซเบอร์ จะยังเกิดขึ้นและเป็นอันตรายกับผู้ประกอบการดิจิทัลเมื่อ รู้สึกว่าการคุกคามนี้จะสร้างความเสียหายเฉพาะบุคคล กลุ่มธุรกิจหรือองค์กรต่างๆ เช่น การ Hack บัญชีธนาคาร หรือการเจาะข้อมูลเข้าไปในอีเมลเป็นรายบุคคล และยังสามารถที่เจาะระบบหรือปล่อยมัลแวร์เข้าไปโจมตีองค์กรธุรกิจทุกระดับ เช่น ปล่อยมัลแวร์เรียกค่าไถ่ในภาคธุรกิจ เจาะระบบความปลอดภัยและขโมยข้อมูลทางการค้าของบริษัทใหญ่ๆ เพื่อนำไปขายให้คู่แข่ง ไปจนกระทั่งถึงการเจาะระบบเข้าไปในหน่วยงานภาครัฐเพื่อสร้างข่าวปลอมเพื่อให้เกิดผลกระทบต่อความมั่นคงและเศรษฐกิจของประเทศได้ และนี่ก็เป็นตัวอย่างเบื้องต้นที่แสดงให้เห็นว่า อาชญากรทางไซเบอร์อันตรายและสามารถสร้างความเสียหายได้รุนแรงอย่างมากในโลกยุคปัจจุบัน

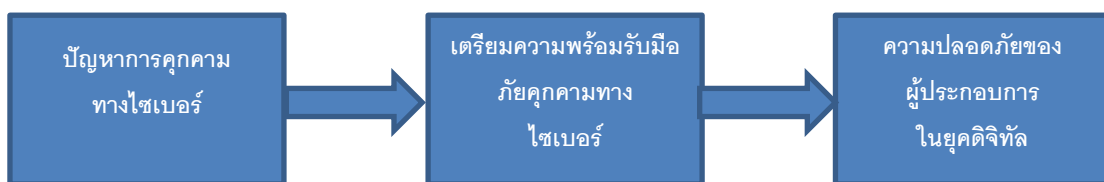
ทางออกที่ดีที่สุดในการป้องกันเรื่องเหล่านี้ไม่ให้เกิดขึ้น ผู้ประกอบการดิจิทัลหรือผู้บริหารในองค์กรต้องมองถึงความสำคัญที่จะต้องลงทุนกับระบบ Cyber Security คือ ความคุ้มค่า นั่นเอง เพราะการหาระบบมาปกป้องโครงสร้างพื้นฐานทางไอทีขององค์กร หรือทำให้ระบบข้อมูลขององค์กรมีความเป็นส่วนตัวมากขึ้นนั้น ย่อมดีกว่าการถูกเจาะระบบหากเมื่อเทียบกันแล้ว การลงทุนไปกับระบบความปลอดภัยยังถือว่าน้อยกว่าความเสียหายที่อาจเกิดขึ้นอย่างเทียบกันไม่ได้เลย ซึ่งการเร่งศึกษาและให้ความสำคัญ ก่อนที่ความเสียหายจะเกิดขึ้น เมื่อเกิดเหตุการณ์ที่องค์กรไม่สามารถรักษาข้อมูลไว้ได้ จนทำให้บุคคลภายนอกสามารถเข้าถึงหรือทำการเปิดเผยข้อมูล อาจส่งผลกระทบต่อองค์กรอย่างร้ายแรงในแง่ของการสูญเสียค่าใช้จ่ายมหาศาลเพื่อแลกกับข้อมูลที่ถูกขโมยไป และชื่อเสียงด้านความปลอดภัยขององค์กรจะติดลบทันที กลายเป็นภาพลักษณ์เชิงลบที่จะติดตัวองค์กรไป และยากที่จะแก้ไขความเชื่อมั่นของผู้ใช้บริการให้กลับมาเป็นดังเดิม ด้วยเหตุนี้ การรักษาความปลอดภัยทางไซเบอร์จึงมีความสำคัญและจำเป็นอย่างยิ่งในองค์กรทุกแห่ง เพื่อรวบรวมประมวลผล และจัดเก็บข้อมูลบนคอมพิวเตอร์ รวมถึงอุปกรณ์อื่น ๆ ที่องค์กรใช้งาน ภายใต้มาตรฐานการรักษาความปลอดภัยที่มีประสิทธิภาพและเหมาะสมอันเป็นสิ่งสำคัญอย่างยิ่งในปัจจุบัน โดยบทความนี้จะสรุปแนะนำวิธีการในการรักษาความปลอดภัยเพื่อเป็นการป้องกันปัญหาที่จะเกิดขึ้นในอนาคตได้ โดยองค์กรจะต้องเข้าใจความปลอดภัยทางไซเบอร์ที่สำคัญ คือ 1) องค์กรจะกระบวนกรปกป้องเครือข่ายจากแฮกเกอร์หรือภัยคุกคามภายนอก โดยจะมีระบบแจ้งเตือนความผิดปกติที่เกิดขึ้น 2) องค์กรจะต้องมีตัวช่วยในการรักษาความปลอดภัยทางแอปพลิเคชัน ซึ่งจะมีการอัปเดตและทดสอบอย่างต่อเนื่อง เพื่อป้องกันการโจมตีหรือการแฝงตัว 3) องค์กรต้องมีการรักษาความปลอดภัยของระบบโครงสร้างพื้นฐาน ซึ่งมีความเสี่ยงในการถูกโจมตีสูงกว่าระบบอื่น ๆ 4) องค์กรต้องมีระบบเก็บข้อมูลที่มีความปลอดภัยและประหยัดค่าใช้จ่าย ทั้งยังมีการพัฒนาและปรับปรุงระบบอยู่เสมอ ทำให้ในปัจจุบันหลายองค์กรนิยมเก็บข้อมูลในรูปแบบดิจิทัลหรือคลาวด์มากขึ้น 5) องค์กรต้องมีการรักษาความปลอดภัยบนอุปกรณ์ซึ่งมีการรับ-ส่งข้อมูลกันอย่างต่อเนื่องผ่านระบบอินเทอร์เน็ต 6) องค์กรต้องมีการจัดแบ่งระบบเครือข่ายภายในองค์กรที่เกี่ยวข้องกับงานสำคัญเท่านั้นสำหรับพนักงานในองค์กร และระบบเครือข่ายภายนอกองค์กร ที่ผู้เยี่ยมชมสามารถเข้ามาได้จากการค้นหาทางอินเทอร์เน็ต แต่ไม่สามารถเข้าถึงเครือข่ายองค์กรขององค์กรได้ โดยตั้งข้อกำหนดด้านความปลอดภัยที่ชัดเจน ยกตัวอย่าง

เช่น ไม่อนุญาตให้เว็บไซต์ฟเวอร์ดำเนินการเข้าถึงเครือข่ายภายใน แต่อาจอนุญาตให้เข้าถึงในแบบผู้เยี่ยมชม หรือพิจารณาแยกเครือข่ายตามหน้าที่ของธุรกิจต่าง ๆ (ส่วนบันทึกลูกค้า การเงิน พนักงานทั่วไป) เป็นต้น 7) องค์การต้องมีการกำหนดเอกสารนโยบายความปลอดภัยทางไซเบอร์ให้ชัดเจนและให้พนักงานรับทราบโดยทั่วกัน เช่น การใช้อุปกรณ์และการสื่อสารทางออนไลน์ หรือเก็บรักษาข้อมูลที่สำคัญธุรกิจของคุณให้ปลอดภัย เพื่อลดปัญหาการถูกคุกคามทางไซเบอร์ 8) องค์การต้องมีการจัดฝึกอบรมเรื่องความปลอดภัยทางด้านข้อมูลให้กับพนักงานทุกคนได้ทราบ เช่น ใช้อีเมลอย่างไรให้ปลอดภัย รวมถึงการใช้งานผ่านเว็บเบราว์เซอร์ เพื่อป้องกันภัยคุกคามทางคอมพิวเตอร์ เป็นต้น

จากข้อมูลโดยกล่าวสรุปได้ว่า การเป็นผู้ประกอบการในโลกเมตาเวิร์สนั้นเต็มไปด้วยความเสี่ยงต่าง ๆ ทั้งทางด้านกายภาพและเสมือนจริง จะมีความสำคัญต่อผู้บริหารที่ต้องการทำธุรกิจที่เกิดจากภัยคุกคามและการโจมตีโดยความเสี่ยงที่เกิดขึ้นจากเมตาเวิร์ส 3 ประเภทที่โจมตีธุรกิจ ดังนี้ 1) ความเสี่ยงด้านฮาร์ดแวร์ทางกายภาพ อย่างเช่น การโจมตีแบบ man-in-the-middle (MITM) ที่พบเห็นในชีวิตจริงที่ตู้ ATM และบนแอปมือถือ 2) ความเสี่ยงในสินทรัพย์คริปโตเคอร์เรนซี ขณะที่คริปโตเคอร์เรนซีเริ่มเป็นอุตสาหกรรมเฉพาะที่มีการควบคุมขับเคลื่อนโดยผู้เชี่ยวชาญที่มีความกังวลเกี่ยวกับความปลอดภัยและความเป็นส่วนตัวเป็นอย่างมาก การเติบโตของพื้นที่คริปโตได้นำพาโอกาสเสี่ยงมากขึ้นจำนวนผู้ค้าผู้บริโภค บริษัทใหม่ และแฮกเกอร์เพิ่มขึ้น ล้วนเป็นปัจจัยเสี่ยงในการทำธุรกรรมคริปโต คริปโตกลายเป็นสกุลเงินปัจจัยสำหรับแรนดอมแวร์ไปแล้ว ส่งผลให้การโจมตีทางไซเบอร์ต่อบัญชีคริปโตนั้นเพิ่มขึ้น และ 3) ความเสี่ยงในการระบุตัวตน เมตาเวิร์สขึ้นอยู่กับการไม่เปิดเผยตัวตนและลึกลับ ความเป็นจริงดิจิทัลแตกต่างจากโลกออฟไลน์ ทำให้ผู้ใช้งานสามารถปิดบังตัวตนและสร้างสรรค์ตัวละครของตนเองได้ อวตารดิจิทัลถือว่าเป็นตัวตนที่เจ้าของเลือกไว้ และข้อมูลประจำตัวเหล่านั้นไม่ได้ถูกควบคุมอย่างระมัดระวัง เนื่องจากบนอินเทอร์เน็ต นามแฝง สามารถเปลี่ยนแปลงได้ทั้งหมดนั้นจึงเป็นปัจจัยเสี่ยงที่แท้จริงเช่นเดียวกับทุก ๆ วงการธุรกิจ จำเป็นต้องมีการจัดการความเสี่ยงเชิงรุกอย่างแท้จริง

สรุป

จากการทบทวนวรรณกรรม จึงขอสรุปดังภาพต่อไปนี้



จากภาพจะกล่าวได้ว่าจากการนำ**เมตาเวิร์ส** หรือโลกเสมือนจริงที่สามารถใช้ชีวิต หรือทำกิจกรรมต่าง ๆ ได้เหมือนในโลกของความจริง โดยมีอินเทอร์เน็ตเป็นตัวกลางเชื่อมกับโลกเสมือน และใช้เทคโนโลยีจำลองสิ่งที่เกิดขึ้นจริง ๆ ที่ถูกสร้างขึ้นเพื่อให้ผู้คนเข้ามาปฏิบัติสัมพันธ์ระหว่างกันได้ทุกรูปแบบ ทั้งการพูดคุย การเรียนการสอน และการทำงานร่วมกัน จากความก้าวหน้าทางเทคโนโลยี Meta จะส่งผลให้ความสนใจในโลกเสมือนจริง ซึ่งหลายองค์กรได้มีการใช้งานที่เชื่อมต่อกับอินเทอร์เน็ต โดยมีทั้งข้อมูลสำคัญและข้อมูลละเอียดอ่อนมากมายซึ่งเป็นเป้าหมายของแฮกเกอร์ ดังนั้น ระบบความปลอดภัยทางไซเบอร์ทุกองค์กรจึงต้องมีการอัปเดตที่บ่อยขึ้น และพัฒนาฟีเจอร์อยู่เรื่อยๆ เพื่อให้สอดคล้องกับความต้องการที่หลากหลาย และเพื่อป้องกันภัยอันตรายจากการโจมตีทางไซเบอร์ และยังคงเป็นความท้าทายที่ผู้ประกอบการต้องรู้จักป้องกันเมื่อก้าวเข้าสู่โลกเมตาเวิร์ส เนื่องจากระบบที่ซับซ้อนมากขึ้นอาชญากรไซเบอร์ในพื้นที่นี้ก็มีวิธีการที่มีความซับซ้อนมากขึ้น ดังนั้นผู้ประกอบการจึงต้องหาความรู้และมีความเข้าใจว่าต้องใช้ข้อมูลใดบ้าง

เพื่อเข้าถึงเพื่อป้องกันความเสี่ยง และในส่วนของบริษัทเจ้าของ เมตาเวิร์ส ที่รวบรวมข้อมูล ก็ต้องพยายามทำทุกวิถีทางเพื่อปกป้องข้อมูลของผู้ใช้ ทั้งนี้ ในอนาคตธุรกิจต่าง ๆ ก็อาจให้ความสนใจและมีความมั่นใจในการร่วมงานกับ เมตาเวิร์ส มากขึ้น เมื่อปัญหาและความเสี่ยงทางไซเบอร์ต่าง ๆ ได้ถูกจัดการได้ดีขึ้นต่อไป

เอกสารอ้างอิง

- ทิสโก้. (2564). *เจาะอาชญากรรมในโลก Metaverse เมื่อธุรกิจตกเป็นเป้าหมายต้องลุกขึ้นสู้*. ค้นเมื่อ 21 มีนาคม 2567, จาก <https://www.tisco.co.th/th/advisory/2021-12-31-cybersecurity-in-metaverse-with-tycyber.html>
- ธนาคารกรุงเทพ. (2567). *การดูแลความมั่นคงปลอดภัยทางไซเบอร์และคุ้มครองข้อมูลของลูกค้า*. ค้นเมื่อ 21 มีนาคม 2567, จาก <https://www.bangkokbank.com/th-TH/About-Us/Sustainability/Cybersecurity-Customer-Data-Privacy-Protection>.
- ธนภัทร ศรีพาน. (2565). การพัฒนาขั้นสุดท้ายของนวัตกรรมและบทบาทของเมตาเวิร์สเพื่อการศึกษาและการฝึกอบรมในยุคเน็กซ์นอร์มอล. *วารสารนวัตกรรมและการจัดการ มหาวิทยาลัยราชภัฏสวนสุนันทา*, 7(2), 174 – 188.
- นภัสพร นิยะวานนท์. (2564). โมเดลสมการโครงสร้างของการเป็นผู้ประกอบการดิจิทัล นวัตกรรมโลจิสติกส์และการเปลี่ยนแปลงสู่ดิจิทัลที่มีอิทธิพลต่อผลการดำเนินงานโลจิสติกส์ของผู้ประกอบการโลจิสติกส์ในประเทศไทย. *บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์ เพื่อความสมบูรณ์แห่งปัญญาปรัชญาดุสิตบัณฑิต (บริหารธุรกิจ)*.
- สมเกียรติ วุฒิธรรมมาภิวัฒน์. (2565). การจัดการศึกษาวรรณคดีไทยโดยการใช้ Metavers. *วารสารวิจัยธรรมศึกษา*, 5(2), 282-303.
- สุรพล บุญลือ. (2565). อิทธิพลของการทำการตลาดแบบอาศัยบุคคลที่มีชื่อเสียงเสมือนจริงต่อความตั้งใจใช้บริการเครือข่ายโทรศัพท์มือถือเอไอเอสและทรูของผู้บริโภคในเขตกรุงเทพมหานคร.
- Akour, I. A., Al-Marouf, R. S., Alfaisal, R., & Salloum, S. A. (2022). A Conceptual Framework for Determining Metaverse (Metaverse) Adoption in Higher Institutions of Gulf Area: An Empirical Study using Hybrid SEM-ANN Approach. *Computers and Education: Artificial Intelligence*, 3, 100052. <https://doi.org/10.1016/j.caeai.2022.100052>.
- Chandra, Y., Leenders, M.A.A.M., (2012). User innovation and entrepreneurship in the virtual world: a study of Second Life residents. *Technovation*, 32(7), 464–476.
- de Bruijn, H. and Janssen, M. (2017). Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies. *Government Information Quarterly*, 34, 1-7. <https://doi.org/10.1016/j.giq.2017.02.007>
- Enache, M. C. (2022). Opportunities for Businesses. *Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics*, 28(1), 67-71.
- Folger, J. (2022). *Alternative Investments: เมตาเวิร์ส (Metaverse) Definition*. Investopedia. Retrieved March 21, 2024, from [https://www.investopedia.com/เมตาเวิร์ส \(Metaverse\)-definition-5206578](https://www.investopedia.com/เมตาเวิร์ส (Metaverse)-definition-5206578).
- Kraus et al. (2019). Digital innovation and venturing: an introduction into the digitalization of entrepreneurship. *Review of Managerial Science*, 13, 519–528. <https://doi.org/10.1007/s11846-019-00333-8>

- Le Dinh et al. (2018). Digital entrepreneurship: A research agenda on new business models for the twenty-first century. *International Journal of Entrepreneurial Behaviour & Research*, 25(2), 353-375. DOI:10.1108/IJEBr-06-2018-0425
- Iorackis, C., Louca, C., Michaely, R., & Weber, M., (2023). Cybersecurity Risk: The Data. Chicago Booth Research Paper, 23-01.
- Meta. (2021). Introducing Meta: A Social Technology Company. Retrieved March 21, 2024 from <https://about.fb.com/news/2021/10/facebook-comp>
- Mystakidis, S., (2022). Metaverse. *Encyclopedia*, 2(1), 486-497. encyclopedia201003.
- Niyawanont. (2021). Digital Entrepreneurship. Retrieved March 21, 2024 from <https://medium.com/@napatsaporn.ni/digital-entrepreneurship-4baf2be4d40c>
- Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading. *International Journal of Sustainable Development & Planning*, 8(1), 225-263.
- Shan, Peng & Song, Michael & Ju, Xiaofeng. (2016). "Entrepreneurial orientation and performance: Is innovation speed a missing link?," *Journal of Business Research, Elsevier*, 69(2), 683-690.
- Slagter, R., Fiet, E., Janssen, W., (2007). Real business in virtual worlds: first insights. In: Huizing, A., de Vries, E.J. (Eds.), *Information Management: Setting the Scene*.
- Spremić & Šimunic. (2018). An insight to cyber threats, attacks and challenges. *International Journal of Electrical Engineering & Technology*, 11(5). DOI:10.34218/IJEET.11.5.2020.010
- Sussan and Acs. (2017). The digital entrepreneurial ecosystem. *Small Bus Econ*, 49, 55-73. DOI 10.1007/s11187-017-9867-5
- von Briel et al. (2018). Not all digital venture ideas are created equal: Implications for venture creation processes. *The Journal of Strategic Information Systems*, 27(4), 278-295.
- Zhang, X. (2022). Expert consensus on the metaverse in medicine. *Clinical eHealth*, 5, 1-9. <https://doi.org/https://doi.org/10.1016/j.ceh.2022.02.001>