

Capacity and Potential Development Model of Security Companies in the Digital Era

Boonruen Thongthip^{1*}

¹ Bachelor of Arts, program in Security Management, Rattana Bundit University, Thailand

* Corresponding author. E-mail: boonruen.th@hotmail.com

ABSTRACT

This research aims to (1) study the development of capacity and Potential of security service companies in the digital era through the use of new technologies and innovations to enhance service quality and Potential, and (2) analyze the factors affecting the development of personnel capacity in security service companies in the digital era, including training and developing information technology skills for efficient job performance. This research is qualitative research, with 35 key informants, divided into three groups: experts and academics in the field of security, executives and managers in security service companies, and personnel working in security service companies. The research findings revealed that the application of new technologies such as Artificial Intelligence (AI), Big Data Analytics, and the Internet of Things (IoT) in security services significantly enhances the Potential of threat detection and prevention. These technologies enable companies to analyze complex data and quickly and accurately detect abnormal behavior. Additionally, connecting and controlling security devices through IoT allows for immediate and efficient monitoring and response to incidents. Developing personnel capacity is crucial for improving service Potential. Quality training and the creation of a learning culture within the organization help personnel be prepared to use new technologies in their work. Supporting continuous learning and knowledge sharing within the organization enables personnel to quickly adapt to technological changes. Furthermore, effective human resource management and support from executives are essential factors in developing personnel capacity. The findings from this research can be applied to enhance the quality and Potential of security service companies in the digital era.

Keywords: Capacity Development, Potential, Digital Technology, Security Companies

รูปแบบการพัฒนาศักยภาพและประสิทธิภาพของบริษัทรักษาความปลอดภัยในยุคดิจิทัล

บุญเรือน ทองทิพย์^{1*}

¹ หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาการจัดการระบบรักษาความมั่นคงปลอดภัย มหาวิทยาลัยรัตนบัณฑิต ประเทศไทย

* Corresponding author. E-mail: boonruen.th@hotmail.com

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ (1) ศึกษาการพัฒนาศักยภาพบริษัทรักษาความปลอดภัยยุคดิจิทัล ด้วยเทคโนโลยีและนวัตกรรม และ (2) ศึกษาวิเคราะห์วิธีการพัฒนาศักยภาพบุคลากรรักษาความปลอดภัยในยุคดิจิทัลและการฝึกอบรมเทคโนโลยีสารสนเทศ การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยมีผู้ให้ข้อมูลหลักจำนวน 35 ท่าน ที่อาศัยอยู่ในกรุงเทพมหานครและปริมณฑล แบ่งเป็นสามกลุ่ม ได้แก่ ผู้เชี่ยวชาญและนักวิชาการในสาขาความปลอดภัย ผู้บริหารและผู้จัดการในบริษัทที่ให้บริการรักษาความปลอดภัย และบุคลากรที่ทำงานในบริษัทที่ให้บริการรักษาความปลอดภัย วิเคราะห์ข้อมูลจะใช้วิธีการตรวจสอบแบบสามเส้า (Triangulation) ผลการวิจัยพบว่า การนำเทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ (AI), การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics), และ Internet of Things (IoT) มาใช้ในการให้บริการรักษาความปลอดภัย ช่วยเพิ่มประสิทธิภาพในการตรวจจับและป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ การใช้เทคโนโลยีเหล่านี้ช่วยให้บริษัทสามารถวิเคราะห์ข้อมูลที่ซับซ้อนและตรวจจับพฤติกรรมที่ผิดปกติได้อย่างรวดเร็วและแม่นยำ นอกจากนี้ การเชื่อมต่อและควบคุมอุปกรณ์รักษาความปลอดภัยผ่าน IoT ช่วยให้การตรวจสอบและตอบสนองต่อเหตุการณ์เป็นไปอย่างทันทีและมีประสิทธิภาพ และ การพัฒนาศักยภาพของบุคลากรเป็นปัจจัยสำคัญในการเพิ่มประสิทธิภาพในการให้บริการฝึกอบรมที่มีคุณภาพและการสร้างวัฒนธรรมการเรียนรู้ในองค์กรช่วยให้บุคลากรมีความพร้อมในการใช้เทคโนโลยีใหม่ ๆ ในการปฏิบัติงาน การสนับสนุนการเรียนรู้และการแบ่งปันความรู้ในองค์กรช่วยให้บุคลากรสามารถปรับตัวกับการเปลี่ยนแปลงทางเทคโนโลยีได้อย่างรวดเร็ว นอกจากนี้ การจัดการทรัพยากรบุคคลที่มีประสิทธิภาพและการสนับสนุนจากผู้บริหารยังเป็นปัจจัยที่สำคัญในการพัฒนาศักยภาพของบุคลากรอีกด้วย จากผลการวิจัยนี้สามารถนำไปใช้ในการพัฒนาบริษัทที่ให้บริการรักษาความปลอดภัยในยุคดิจิทัลให้มีคุณภาพและประสิทธิภาพมากยิ่งขึ้น

คำสำคัญ: การพัฒนาศักยภาพ, ประสิทธิภาพ, เทคโนโลยีดิจิทัล, บริษัทรักษาความปลอดภัย

© 2024 JSSP: Journal of Social Science Panyapat

บทนำ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศและการสื่อสารได้รับการพัฒนาอย่างรวดเร็วและต่อเนื่อง การรักษาความปลอดภัยได้กลายเป็นประเด็นที่สำคัญและมีความจำเป็นเพิ่มขึ้นเรื่อย ๆ บริษัทที่ให้บริการรักษาความปลอดภัยจำเป็นต้องปรับตัวและพัฒนาศักยภาพของตนเองให้สอดคล้องกับเทคโนโลยีใหม่ ๆ เพื่อให้สามารถให้บริการที่มีประสิทธิภาพและตอบสนองความต้องการของลูกค้าได้อย่างทันสมัย (วันเฉลิม แสงสว่าง, 2556) นอกจากนี้ การเพิ่มขึ้นของภัยคุกคามทางไซเบอร์และการโจรกรรมข้อมูลส่วนบุคคลก็เป็นปัจจัยที่ทำให้บริษัทต้องพัฒนาการดำเนินงานและนวัตกรรมใหม่ ๆ เพื่อป้องกันและตอบโต้การโจมตีที่อาจเกิดขึ้น (Hidayat, A., & Aziz, M., 2022) ในทศวรรษที่ผ่านมา ความต้องการบริการรักษาความปลอดภัยได้เพิ่มขึ้นอย่างมาก โดยเฉพาะอย่างยิ่งในองค์กรภาครัฐและเอกชนที่ต้องการความมั่นคงและปลอดภัยในการดำเนินงาน บริษัทที่ให้บริการรักษาความปลอดภัยต้องพัฒนาในด้านบุคลากร เทคโนโลยี และกระบวนการทำงานอย่างต่อเนื่อง (บุญเรือน ทองทิพย์ และวัชรบุตร กุลบุตร, 2563) โดยเฉพาะการนำเทคโนโลยีใหม่ๆ เช่น ปัญญาประดิษฐ์ (AI) และการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) มาช่วยในการตรวจจับและป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ (Hughes, Robert, Frady, & Arroyos, 2019) นอกจากนี้ การใช้ระบบสื่อสารและการจัดการข้อมูลที่มีประสิทธิภาพยังช่วยให้บริษัทสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและความมั่นคงยิ่งขึ้น การนำระบบ Internet of Things (IoT) มา

ใช้ในการเชื่อมต่อและการสื่อสารระหว่างอุปกรณ์ต่างๆ ยังช่วยให้การตรวจสอบและตอบสนองต่อเหตุการณ์เป็นไปอย่างทันทั่วทั้ง (โกสินทร์ ชำนาญพล และสุดาใจ โล่ห์วนิชชัย, 2562)

อย่างไรก็ตาม การพัฒนาศักยภาพและประสิทธิภาพของบริษัทในยุคดิจิทัลยังคงเผชิญกับความท้าทายต่างๆ เช่น ค่าใช้จ่ายที่สูงในการลงทุนในเทคโนโลยีใหม่ๆ รวมถึงความจำเป็นในการปรับตัวของบุคลากรในองค์กรให้สามารถใช้เทคโนโลยีเหล่านั้นได้อย่างมีประสิทธิภาพ (นวพล แก้วสุวรรณ, ธัญญาลักษณ์ ใจเที่ยง และสิริกร บำรุงกิจ, 2563) การฝึกอบรมและพัฒนาบุคลากรให้มีความรู้และทักษะทางด้านเทคโนโลยีสารสนเทศจึงมีความสำคัญมาก (Blume, Ford, Baldwin, & Huang, 2010) ยิ่งไปกว่านั้น การเพิ่มประสิทธิภาพในการให้บริการรักษาความปลอดภัยจำเป็นต้องคำนึงถึงความต้องการและความพึงพอใจของลูกค้า โดยเฉพาะการพัฒนากระบวนการที่ตอบสนองต่อความต้องการเฉพาะของลูกค้าแต่ละราย (พรวรรณ นันทแพทย์, 2566) การใช้เทคโนโลยี Internet of Things (IoT) ในการเชื่อมต่อและสื่อสารระหว่างอุปกรณ์รักษาความปลอดภัยต่างๆ ยังช่วยให้การตรวจสอบและการตอบโต้เหตุการณ์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ (Hajjar & Alkhanaizi, 2018) การวิจัยที่เกี่ยวข้องนี้จึงมีประโยชน์อย่างยิ่งสำหรับบริษัทที่ให้บริการรักษาความปลอดภัย ทั้งในการพัฒนาศักยภาพและประสิทธิภาพการดำเนินงานขององค์กรให้สอดคล้องกับความต้องการที่เปลี่ยนแปลงไปในยุคดิจิทัล (Birdi, Patterson, & Wood, 2007)

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาการพัฒนาศักยภาพบริษัทรักษาความปลอดภัยยุคดิจิทัล ด้วยเทคโนโลยีและนวัตกรรม
2. เพื่อศึกษาวิเคราะห์วิธีการพัฒนาศักยภาพบุคลากรรักษาความปลอดภัยในยุคดิจิทัลและการฝึกอบรมเทคโนโลยีสารสนเทศ

ระเบียบวิธีวิจัย

การวิจัยครั้งนี้เน้นการวิจัยเชิงคุณภาพ โดยใช้วิธีการสัมภาษณ์เชิงลึกแบบเจาะจง เพื่อรวบรวมข้อมูลจากผู้ให้ข้อมูลสำคัญ รวมถึงการวิเคราะห์ข้อมูลจากเอกสารเพื่อเสริมสร้างความเข้าใจในเนื้อหาของการวิจัยด้วย ดังต่อไปนี้

1. ผู้ให้ข้อมูลสำคัญ

การเลือกผู้ให้ข้อมูลสำคัญใช้วิธีการเลือกแบบเฉพาะเจาะจง โดยแบ่งเป็น 3 กลุ่ม ได้แก่ กลุ่มที่ 1 ผู้เชี่ยวชาญและนักวิชาการในสาขาความปลอดภัย จำนวน 15 ท่าน กลุ่มที่ 2 ผู้บริหารและผู้จัดการในบริษัทที่ให้บริการรักษาความปลอดภัย จำนวน 10 ท่าน และกลุ่มที่ 3 บุคลากรที่ทำงานในบริษัทที่ให้บริการรักษาความปลอดภัย จำนวน 10 ท่าน รวมทั้งหมด 35 ท่านที่อาศัยอยู่ในกรุงเทพมหานครและปริมณฑล (Miles, M. B., Huberman, A. M., & Saldaña, J., 2014)

2. เครื่องมือที่ใช้เก็บรวบรวมข้อมูล

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลในงานวิจัยนี้ ได้แก่ แบบสอบถามสำหรับการสัมภาษณ์เชิงลึกแบบเจาะจงสำหรับการสัมภาษณ์ทางไกล บันทึกเสียงและการจดบันทึกขณะสัมภาษณ์ และเอกสารและบทความวิจัยที่เกี่ยวข้อง

3. การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลจะดำเนินการในระยะเวลา 1 ปี ตั้งแต่เดือนมกราคม 2566 ถึงเดือนธันวาคม 2566 โดยใช้วิธีการสัมภาษณ์เชิงลึกแบบเจาะจง การสนทนากลุ่ม และการจดบันทึกการสังเกตทั้งแบบมีส่วนร่วมและไม่มีส่วนร่วม ผู้วิจัยและผู้ช่วยวิจัยจะลงพื้นที่เป็นครั้งคราว รวมถึงใช้การสัมภาษณ์เพื่อเข้าใจความคิดเห็นและประสบการณ์ของผู้ถูกสัมภาษณ์ รูปแบบการพัฒนาศักยภาพและประสิทธิภาพของบริษัทรักษาความปลอดภัยในยุคดิจิทัลจะศึกษาจากกลุ่มผู้ให้ข้อมูลหลักทั้ง 3 กลุ่ม

4. ขั้นตอนในการดำเนินการวิจัย

4.1 ศึกษาข้อมูลพื้นฐานเกี่ยวกับเรื่องที่ต้องการศึกษา รวมถึงการวิจัยที่เกี่ยวข้องและกรอบแนวคิดที่เหมาะสม เพื่อให้มีความเข้าใจในเรื่องที่ต้องการศึกษาอย่างชัดเจน

4.2 วิเคราะห์และตีความข้อมูลที่ได้รับ โดยให้ความสำคัญกับความถูกต้องและคุณค่าของข้อมูลเพื่อให้เข้าใจความหมายที่แท้จริงของข้อมูล

4.3 กำหนดกรอบแนวคิดและแนวคิดที่เกี่ยวข้องในการดำเนินการวิจัย โดยให้ความสำคัญกับการมองเห็นใหม่เกี่ยวกับความรับผิดชอบทางสังคมของภาคธุรกิจในการรักษาความปลอดภัย

4.4 วางแผนและเตรียมการสำหรับการสัมภาษณ์ ตระหนักถึงวัตถุประสงค์ของการวิจัยและเตรียมคำถามที่เหมาะสมเพื่อเปิดเผยความคิดเห็นและข้อมูล

4.5 ดำเนินการสัมภาษณ์เชิงลึกแบบเจาะจง การสนทนากลุ่ม การจดบันทึกการสังเกต โดยผู้วิจัยจะลงพื้นที่เป็นครั้งคราวและผู้ช่วยวิจัยจะเข้าไปตลอดเวลา ใช้วิธีการสัมภาษณ์เพื่อเข้าใจความคิดเห็นและประสบการณ์ของผู้ถูกสัมภาษณ์อย่างละเอียด

5. การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลจะใช้วิธีการตรวจสอบแบบสามเส้า (Triangulation) เพื่อค้นหาความเชื่อมโยงระหว่างข้อมูลและอธิบายความสัมพันธ์เป็นเหตุ-ผล จากนั้นจะเขียนรายงานเพื่อนำเสนอผลการวิเคราะห์ โดยใช้การพรรณนาวิเคราะห์ตามวัตถุประสงค์ของการวิจัย (Creswell, J. W., & Poth, C. N., 2017)

กรอบแนวคิดในการวิจัย

การวิจัยนี้มีความสำคัญในการทำทำความเข้าใจและพัฒนาแนวทางที่เหมาะสมสำหรับการบริหารจัดการและปรับตัวของธุรกิจที่ให้บริการรักษาความปลอดภัยในยุคที่เทคโนโลยีเปลี่ยนแปลงอย่างรวดเร็ว กรอบแนวคิดในการวิจัยนี้จะพิจารณาจากหลายแง่มุม ได้แก่ การพัฒนาศักยภาพบุคลากร การประยุกต์ใช้เทคโนโลยี และการสร้างระบบการจัดการที่มีประสิทธิภาพ

การพัฒนาศักยภาพบุคลากร การพัฒนาศักยภาพของบุคลากรเป็นปัจจัยสำคัญที่จะทำให้ธุรกิจรักษาความปลอดภัยสามารถดำเนินงานได้อย่างมีประสิทธิภาพ ในยุคดิจิทัล การเรียนรู้และพัฒนาทักษะทางด้านเทคโนโลยีสารสนเทศเป็นสิ่งจำเป็น บุคลากรต้องมีความรู้และทักษะในการใช้เครื่องมือและเทคโนโลยีใหม่ ๆ เพื่อป้องกันและตอบโต้ภัยคุกคามทางไซเบอร์ การฝึกอบรมและการพัฒนาบุคลากรจึงต้องเน้นไปที่การสร้างความรู้ความเข้าใจในเทคโนโลยีปัจจุบันและการพัฒนาทักษะในการใช้เทคโนโลยีเหล่านี้ (ฉัตรวัฒน์ ชัยชนฐาภรณ์, 2566)

การประยุกต์ใช้เทคโนโลยี การประยุกต์ใช้เทคโนโลยีเป็นหัวใจสำคัญของการพัฒนาศักยภาพและประสิทธิภาพของธุรกิจรักษาความปลอดภัย เทคโนโลยีเช่น ปัญญาประดิษฐ์ (AI) การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) และ Internet of Things (IoT) เป็นเครื่องมือที่สำคัญในการตรวจจับและป้องกันภัยคุกคาม การใช้ AI สามารถช่วยในการวิเคราะห์ข้อมูลและตรวจจับพฤติกรรมที่ผิดปกติ ซึ่งสามารถช่วยลดความเสี่ยงและป้องกันเหตุการณ์ไม่พึงประสงค์ (Hughes, C., Robert, L., Frady, K., & Arroyos, A., 2019).

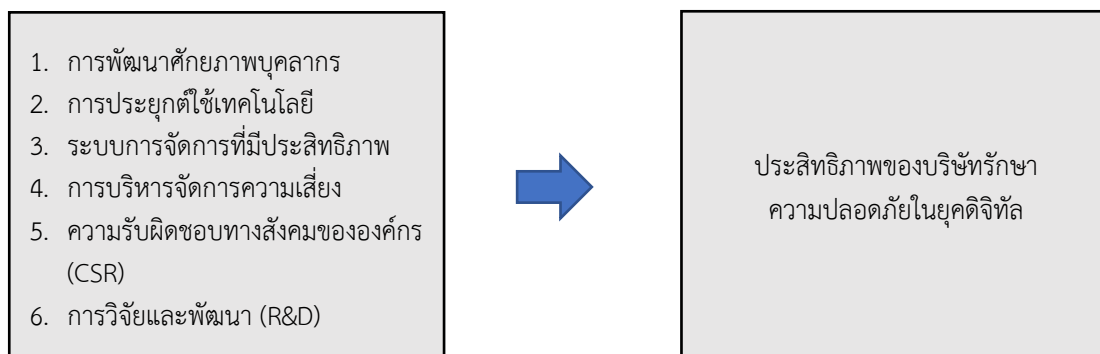
ระบบการจัดการที่มีประสิทธิภาพ ระบบการจัดการที่มีประสิทธิภาพเป็นสิ่งที่ขาดไม่ได้ในการพัฒนาธุรกิจรักษาความปลอดภัย การจัดการทรัพยากรบุคคล การวางแผนและการบริหารจัดการโครงการ การควบคุมคุณภาพ และการจัดการความเสี่ยงเป็นปัจจัยที่สำคัญ ระบบการจัดการที่ดีจะช่วยให้ธุรกิจสามารถดำเนินงานได้อย่างมีประสิทธิภาพและสามารถตอบสนองต่อความต้องการของลูกค้าได้อย่างทันท่วงที (Gupta, K., Bhaskar, P., & Singh, S., 2017)

การบริหารจัดการความเสี่ยง การบริหารจัดการความเสี่ยงเป็นองค์ประกอบสำคัญของการรักษาความปลอดภัยในยุคดิจิทัล การตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ การจัดการเหตุการณ์และการฟื้นฟูสภาพหลังจากเกิดเหตุการณ์เป็นสิ่งที่ยุทธศาสตร์ต้องมีการเตรียมการและวางแผนอย่างรอบคอบ การบริหารจัดการความเสี่ยงที่มีประสิทธิภาพจะช่วยลดความเสียหายและเพิ่มความมั่นคงในการดำเนินงานของบริษัท (Hajjar, S., & Alkhanaizi, M., 2018)

ความรับผิดชอบต่อสังคมขององค์กร (CSR) ความรับผิดชอบต่อสังคมขององค์กร (CSR) เป็นอีกแง่มุมหนึ่งที่สำคัญในการพัฒนาธุรกิจที่ให้บริการรักษาความปลอดภัย การมีส่วนร่วมในกิจกรรมที่เป็นประโยชน์ต่อสังคมและการสร้าง

ภาพลักษณ์ที่ดีจะช่วยให้บริษัทได้รับความไว้วางใจและการสนับสนุนจากลูกค้าและสังคม การมีแนวคิด CSR ที่ดีจะช่วยให้บริษัทมีความมั่นคงและสามารถดำเนินงานได้อย่างยั่งยืน (Jumanne, A., & Njoroge, J., 2019)

การวิจัยและพัฒนา (R&D) การวิจัยและพัฒนาเป็นส่วนสำคัญในการสร้างนวัตกรรมและการพัฒนาบริษัท การลงทุนใน R&D จะช่วยให้บริษัทสามารถพัฒนาเทคโนโลยีใหม่ ๆ และปรับปรุงการให้บริการได้อย่างต่อเนื่อง การวิจัยและพัฒนาจะช่วยให้บริษัทสามารถแข่งขันได้ในตลาดที่มีการแข่งขันสูงและสามารถตอบสนองต่อการเปลี่ยนแปลงของเทคโนโลยีได้อย่างทันท่วงที (Birdi, K. S., Patterson, M. G., & Wood, S. J., 2007)



ภาพที่ 1 กรอบแนวคิดในการวิจัย

ดังนั้น จากภาพที่ 1 กรอบแนวคิดในการวิจัยครั้งนี้เน้นไปที่การพัฒนาศักยภาพและประสิทธิภาพของบริษัทรักษาความปลอดภัยในยุคดิจิทัล โดยให้ความสำคัญกับการพัฒนาศักยภาพ การประยุกต์ใช้เทคโนโลยี ระบบการจัดการที่มีประสิทธิภาพ การบริหารจัดการความเสี่ยง ความรับผิดชอบต่อสังคมขององค์กร และการวิจัยและพัฒนา การวิจัยนี้จะช่วยให้บริษัทที่ให้บริการรักษาความปลอดภัยสามารถปรับตัวและพัฒนาตนเองให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีและความต้องการของลูกค้าได้อย่างมีประสิทธิภาพ (Imran, M., Maqbool, N., & Shafique, H., 2014).

ผลการวิจัย

จากการศึกษาวิจัย พบว่า

1. การพัฒนาศักยภาพบริษัทรักษาความปลอดภัยยุคดิจิทัล ด้วยเทคโนโลยีและนวัตกรรม

การวิเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกแบบเจาะจง การสนทนากลุ่ม และการจดบันทึกการสังเกตทั้งแบบมีส่วนร่วมและไม่มีส่วนร่วมที่ผู้วิจัยและผู้ช่วยวิจัยได้ลงพื้นที่เป็นครั้งคราว รวมถึงการใช้การสัมภาษณ์เพื่อเข้าใจความคิดเห็นและประสบการณ์ของผู้ให้ข้อมูลหลักในยุคดิจิทัล พบว่ามีประเด็นสำคัญ 9 ประการที่สามารถสรุปได้จากการวิจัยนี้ ประการแรก การนำเทคโนโลยีใหม่เข้ามาใช้ในการให้บริการรักษาความปลอดภัย ผู้ให้ข้อมูลเห็นพ้องกันว่าเทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ (AI) ระบบการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) และ Internet of Things (IoT) เป็นปัจจัยสำคัญที่ช่วยเพิ่มประสิทธิภาพในการตรวจจับและป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ การใช้ AI ในการวิเคราะห์ข้อมูลและคาดการณ์พฤติกรรมที่ผิดปกติ รวมถึงการใช้ Big Data Analytics ในการตรวจสอบข้อมูลจำนวนมากเพื่อหาความสัมพันธ์และรูปแบบที่บ่งบอกถึงภัยคุกคามได้ ประการที่สอง การพัฒนาศักยภาพและการฝึกอบรม ผู้ให้ข้อมูลเน้นถึงความสำคัญของการพัฒนาทักษะและความรู้ของบุคลากรในบริษัท โดยบุคลากรจำเป็นต้องได้รับการฝึกอบรมด้านเทคโนโลยีใหม่ ๆ และการใช้เครื่องมือที่ทันสมัยในการทำงาน นอกจากนี้ การสร้างวัฒนธรรมการเรียนรู้ภายในองค์กรยังเป็นสิ่งสำคัญที่ช่วยให้บุคลากรสามารถปรับตัวกับการเปลี่ยนแปลงของเทคโนโลยีได้อย่างรวดเร็ว ประการที่สาม การปรับปรุงกระบวนการทำงาน การใช้เทคโนโลยีและนวัตกรรมใหม่ ๆ ช่วยให้บริษัทสามารถปรับปรุงกระบวนการทำงานให้มีประสิทธิภาพมากขึ้น เช่น การใช้ระบบการจัดการความปลอดภัยแบบรวมศูนย์ (Integrated Security Management Systems) ที่สามารถเชื่อมต่อและควบคุมการทำงานของอุปกรณ์รักษาความปลอดภัยได้อย่างมีประสิทธิภาพ รวมถึงการใช้ระบบการรายงานและ

การติดตามผลแบบเรียลไทม์เพื่อให้ผู้บริหารสามารถตัดสินใจได้อย่างรวดเร็วและแม่นยำ ประการที่สี่ การเพิ่มความพึงพอใจของลูกค้า ผู้ให้ข้อมูลชี้ว่าการใช้เทคโนโลยีใหม่ในการให้บริการรักษาความปลอดภัยช่วยเพิ่มความพึงพอใจของลูกค้าได้ ระบบการรายงานและการติดตามผลแบบเรียลไทม์ช่วยให้ลูกค้าสามารถรับรู้สถานะและความปลอดภัยของทรัพย์สินได้ตลอดเวลา ซึ่งสร้างความมั่นใจและความเชื่อถือในบริการของบริษัท ประการที่ห้า การสร้างนวัตกรรมในการให้บริการ การวิจัยพบว่าบริษัทที่สามารถนำเทคโนโลยีใหม่ ๆ มาใช้ในการพัฒนาบริการมีความสามารถในการสร้างนวัตกรรมที่ตอบสนองต่อความต้องการของตลาดได้อย่างรวดเร็ว เช่น การพัฒนาระบบการรักษาความปลอดภัยที่สามารถปรับตัวตามสถานการณ์ได้ (Adaptive Security Systems) ที่ใช้เทคโนโลยี AI ในการปรับเปลี่ยนการทำงานของระบบตามสภาพแวดล้อมและความเสี่ยงที่เกิดขึ้น ประการที่หก การบริหารจัดการข้อมูลและความปลอดภัยทางไซเบอร์ บริษัทที่ให้บริการรักษาความปลอดภัยในยุคดิจิทัลต้องมีความสามารถในการบริหารจัดการข้อมูลที่ได้รับอย่างมีประสิทธิภาพ การใช้เทคโนโลยีการเข้ารหัสข้อมูลและการป้องกันภัยทางไซเบอร์เป็นสิ่งจำเป็นเพื่อป้องกันการโจมตีจากภายนอกและรักษาความปลอดภัยของข้อมูลลูกค้า ประการที่เจ็ด การสร้างความร่วมมือกับภาคส่วนอื่น ๆ ผู้ให้ข้อมูลระบุว่า การสร้างความร่วมมือกับภาครัฐและเอกชนเป็นสิ่งสำคัญในการพัฒนาศักยภาพของบริษัท การแลกเปลี่ยนข้อมูลและประสบการณ์การทำงานร่วมกันช่วยให้บริษัทสามารถพัฒนาการให้บริการที่มีประสิทธิภาพและตอบสนองต่อความต้องการของลูกค้าได้ดียิ่งขึ้น ประการที่แปด ความรับผิดชอบต่อสังคม บริษัทต้องคำนึงถึงผลกระทบต่อสังคมในการดำเนินธุรกิจ การใช้เทคโนโลยีใหม่ ๆ ต้องคำนึงถึงผลกระทบต่อสิ่งแวดล้อมและชุมชน โดยบริษัทสามารถมีส่วนร่วมในการพัฒนาชุมชนและปกป้องสิ่งแวดล้อมผ่านการใช้เทคโนโลยีที่ยั่งยืนและเป็นมิตรต่อสิ่งแวดล้อม และประการที่เก้า การวิจัยและพัฒนา (R&D) การวิจัยและพัฒนาเป็นปัจจัยสำคัญในการขับเคลื่อนนวัตกรรมและการพัฒนาบริการใหม่ ๆ บริษัทที่ลงทุนในการวิจัยและพัฒนาสามารถพัฒนาผลิตภัณฑ์และบริการที่มีคุณภาพสูง และสามารถตอบสนองต่อความต้องการของลูกค้าได้อย่างมีประสิทธิภาพ จากการวิเคราะห์ข้อมูลพบว่า การพัฒนาศักยภาพและประสิทธิภาพของบริษัทรักษาความปลอดภัยในยุคดิจิทัลจำเป็นต้องอาศัยหลายปัจจัย ได้แก่ การนำเทคโนโลยีใหม่ ๆ มาใช้ การยกระดับทักษะของบุคลากร การปรับปรุงกระบวนการทำงาน การจัดการข้อมูลอย่างมีประสิทธิภาพ การลงทุนในงานวิจัยและพัฒนา การสร้างความร่วมมือกับหน่วยงานต่าง ๆ และการรับผิดชอบต่อสังคม เพื่อให้สามารถให้บริการที่มีคุณภาพและมีประสิทธิภาพสูงสุด โดยผู้วิจัยได้จัดทำตารางความถี่เพื่อแสดงผลการสัมภาษณ์ ดังปรากฏในตารางที่ 1

ตารางที่ 1 ความถี่เพื่อแสดงผลการสัมภาษณ์

ประเด็นสำคัญ	จำนวนผู้ให้ข้อมูล
การนำเทคโนโลยีใหม่เข้ามาใช้ในการให้บริการรักษาความปลอดภัย	28
การพัฒนาบุคลากรและการฝึกอบรม	30
การปรับปรุงกระบวนการทำงาน	25
การเพิ่มความพึงพอใจของลูกค้า	27
การสร้างนวัตกรรมในการให้บริการ	22
การบริหารจัดการข้อมูลและความปลอดภัยทางไซเบอร์	24
การสร้างความร่วมมือกับภาคส่วนอื่น ๆ	20
ความรับผิดชอบต่อสังคม	18
การวิจัยและพัฒนา (R&D)	21

2. วิธีการพัฒนาศักยภาพบุคลากรรักษาความปลอดภัยในยุคดิจิทัลและการฝึกอบรมเทคโนโลยีสารสนเทศ

จากการวิเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกแบบเจาะจง การสนทนากลุ่ม และการจัดบันทึกการสังเกตทั้งแบบมีส่วนร่วมและไม่มีส่วนร่วม โดยผู้วิจัยและผู้ช่วยวิจัยจะลงพื้นที่เป็นครั้งคราว ใช้การสัมภาษณ์เพื่อเข้าใจความคิดเห็นและประสบการณ์ของผู้ถูกสัมภาษณ์ในยุคดิจิทัลของผู้ให้ข้อมูลหลักทั้ง 3 กลุ่ม และวิเคราะห์เอกสารที่เกี่ยวข้องประกอบ พบว่า

ประการแรก ความสำคัญของการฝึกอบรมและพัฒนาทักษะทางด้านเทคโนโลยีสารสนเทศ ผู้ให้ข้อมูลย้ำถึงความสำคัญของการฝึกอบรมบุคลากรให้มีความรู้และทักษะทางด้านเทคโนโลยีสารสนเทศ การฝึกอบรมที่มีคุณภาพจะช่วยให้บุคลากรมีความพร้อมในการใช้เทคโนโลยีใหม่ ๆ ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

ประการที่สอง การจัดการทรัพยากรบุคคลที่มีประสิทธิภาพ การจัดการทรัพยากรบุคคลที่ดีเป็นปัจจัยสำคัญในการพัฒนาศักยภาพของบุคลากร บริษัทควรมีการวางแผนการฝึกอบรมและพัฒนาบุคลากรอย่างเป็นระบบ โดยคำนึงถึงความต้องการและความสามารถของบุคลากรแต่ละคน

ประการที่สาม การสร้างวัฒนธรรมการเรียนรู้ในองค์กร การสร้างวัฒนธรรมการเรียนรู้ในองค์กรช่วยส่งเสริมให้บุคลากรมีความกระตือรือร้นในการพัฒนาตนเองและการเรียนรู้เทคโนโลยีใหม่ ๆ การสนับสนุนการเรียนรู้ต่อเนื่องและการแบ่งปันความรู้ในองค์กรช่วยให้บุคลากรมีความพร้อมในการปรับตัวกับการเปลี่ยนแปลงทางเทคโนโลยี

ประการที่สี่ การสนับสนุนจากผู้บริหาร ผู้บริหารมีบทบาทสำคัญในการสนับสนุนและส่งเสริมการพัฒนาศักยภาพของบุคลากร การจัดสรรทรัพยากรและการให้โอกาสในการฝึกอบรมเป็นสิ่งจำเป็นในการพัฒนาทักษะทางด้านเทคโนโลยีสารสนเทศของบุคลากร

ประการที่ห้า การใช้เทคโนโลยีในการฝึกอบรม การใช้เทคโนโลยีในการฝึกอบรม เช่น การเรียนรู้ออนไลน์ (e-learning) และการใช้สื่อมัลติมีเดียช่วยให้การฝึกอบรมมีประสิทธิภาพมากขึ้น บุคลากรสามารถเข้าถึงข้อมูลและการเรียนรู้ได้ตลอดเวลา และสามารถฝึกฝนทักษะทางด้านเทคโนโลยีได้อย่างต่อเนื่อง

ประการที่หก การวิเคราะห์และประเมินผลการฝึกอบรม การวิเคราะห์และประเมินผลการฝึกอบรมเป็นสิ่งสำคัญในการปรับปรุงและพัฒนากระบวนการฝึกอบรม การวัดผลความรู้และทักษะที่ได้รับจากการฝึกอบรมช่วยให้สามารถปรับปรุงการฝึกอบรมให้เหมาะสมและมีประสิทธิภาพมากขึ้น

ประการที่เจ็ด การสร้างโอกาสในการพัฒนาทักษะภายในองค์กร การสร้างโอกาสในการพัฒนาทักษะภายในองค์กร เช่น การจัดทำโครงการหรือกิจกรรมที่ส่งเสริมการใช้เทคโนโลยีใหม่ ๆ ช่วยให้บุคลากรมีโอกาสดูแลและพัฒนาทักษะอย่างต่อเนื่อง

ประการสุดท้าย การรับรองมาตรฐานและการประกอบวิชาชีพ การรับรองมาตรฐานและการประกอบวิชาชีพที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเป็นสิ่งที่ช่วยส่งเสริมให้บุคลากรมีความรู้และทักษะที่เป็นมาตรฐาน และสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

จากผลการวิเคราะห์ข้อมูล พบว่าปัจจัยที่มีผลต่อการพัฒนาศักยภาพของบุคลากรในบริษัทที่ให้บริการรักษาความปลอดภัยในยุคดิจิทัลนั้น ไม่เพียงแต่การฝึกอบรมและพัฒนาทักษะทางด้านเทคโนโลยีสารสนเทศเท่านั้น แต่ยังรวมถึงการจัดการทรัพยากรบุคคลที่มีประสิทธิภาพ การสร้างวัฒนธรรมการเรียนรู้ในองค์กร การสนับสนุนจากผู้บริหาร การใช้เทคโนโลยีในการฝึกอบรม การวิเคราะห์และประเมินผลการฝึกอบรม การสร้างโอกาสในการพัฒนาทักษะภายในองค์กร และการรับรองมาตรฐานและการประกอบวิชาชีพที่เกี่ยวข้อง การผสมผสานของปัจจัยเหล่านี้จะช่วยให้บริษัทสามารถพัฒนาศักยภาพของบุคลากรได้อย่างมีประสิทธิภาพและสอดคล้องกับความต้องการของยุคดิจิทัล

อภิปรายผล

การพัฒนาศักยภาพและประสิทธิภาพของบริษัทรักษาความปลอดภัยในยุคดิจิทัลผ่านการใช้เทคโนโลยีใหม่และนวัตกรรมต่าง ๆ มีความสำคัญอย่างยิ่งในการเพิ่มคุณภาพและประสิทธิภาพการให้บริการ ซึ่งสามารถอภิปรายผลได้ดังนี้

ประการแรก การนำเทคโนโลยีใหม่เข้ามาใช้ในการให้บริการรักษาความปลอดภัยช่วยเพิ่มประสิทธิภาพในการตรวจจับและป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ การใช้เทคโนโลยีเช่น ปัญญาประดิษฐ์ (AI), การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics), และ Internet of Things (IoT) ได้รับการยืนยันจากงานวิจัยที่ระบุว่า การใช้ AI ช่วยเพิ่มความสามารถในการคาดการณ์และตอบสนองต่อภัยคุกคามได้รวดเร็ว (Javaid et al., 2022) นอกจากนี้ การใช้ Big Data Analytics ยังช่วยให้การวิเคราะห์ข้อมูลเป็นไปอย่างละเอียดและมีประสิทธิภาพในการหาความสัมพันธ์ที่ซ่อนอยู่ในข้อมูล (Hughes et al., 2019) ประการที่สอง การพัฒนาทักษะและฝึกอบรมบุคลากรถือเป็นปัจจัยสำคัญในการปรับตัวกับเทคโนโลยีใหม่ งานวิจัยระบุว่าบุคลากรที่ได้รับการฝึกอบรมสามารถนำเทคโนโลยีมาใช้ในการทำงานได้อย่างมีประสิทธิภาพ (Jalil et al., 2019) การสร้างวัฒนธรรมการเรียนรู้ในองค์กรยังเป็นปัจจัยที่สนับสนุนการพัฒนาทักษะและความรู้ให้กับบุคลากร (Kim & Park, 2020)

ประการที่สาม การปรับปรุงกระบวนการทำงานด้วยเทคโนโลยีช่วยให้บริษัทสามารถทำงานได้มีประสิทธิภาพมากขึ้น เช่น การใช้ระบบบริหารจัดการความปลอดภัยแบบรวมศูนย์ (Integrated Security Management Systems) ช่วยลดความผิดพลาดและเพิ่มความรวดเร็วในการตัดสินใจ (Hajjar & Alkhanaizi, 2018) ประการที่สี่ การใช้เทคโนโลยีในการให้บริการรักษาความปลอดภัยช่วยเพิ่มความพึงพอใจของลูกค้า งานวิจัยชี้ให้เห็นว่าลูกค้าที่สามารถติดตามสถานะและความปลอดภัยของทรัพย์สินได้แบบเรียลไทม์มีความมั่นใจและพึงพอใจในบริการมากขึ้น (Blume et al., 2010) ประการที่ห้า การใช้เทคโนโลยีใหม่ยังช่วยให้บริษัทสามารถสร้างนวัตกรรมที่ตอบสนองต่อความต้องการของตลาดได้อย่างรวดเร็ว เช่น การนำ AI มาใช้ในระบบรักษาความปลอดภัยทำให้ระบบสามารถปรับตัวตามสถานการณ์ได้ (Birdi et al., 2007) ประการที่หก การบริหารจัดการข้อมูลและความปลอดภัยทางไซเบอร์เป็นอีกหนึ่งความท้าทายในยุคดิจิทัล การใช้เทคโนโลยีการเข้ารหัสข้อมูลช่วยป้องกันการโจมตีจากภายนอกและรักษาความปลอดภัยของข้อมูลลูกค้า (Gupta et al., 2017)

ประการที่เจ็ด การสร้างความร่วมมือระหว่างภาครัฐและเอกชนเป็นปัจจัยสำคัญในการพัฒนาศักยภาพของบริษัท การแลกเปลี่ยนข้อมูลและประสบการณ์ช่วยให้บริษัทสามารถพัฒนาบริการที่ตรงตามความต้องการของลูกค้าได้ดีขึ้น (Hughes et al., 2019) ประการที่แปด การนำเทคโนโลยีใหม่มาใช้ต้องคำนึงถึงผลกระทบต่อสิ่งแวดล้อมและชุมชน ซึ่งการพัฒนาเทคโนโลยีควรสอดคล้องกับความรับผิดชอบต่อสังคมและสิ่งแวดล้อม (Jalil et al., 2019) ประการที่เก้า การลงทุนในการวิจัยและพัฒนา (R&D) เป็นปัจจัยสำคัญในการสร้างนวัตกรรมใหม่ ๆ และพัฒนาบริการที่ตอบสนองความต้องการของลูกค้า (Blume et al., 2010)

จากการอภิปราย สามารถสรุปได้ว่าการพัฒนาศักยภาพและประสิทธิภาพของบริษัทรักษาความปลอดภัยในยุคดิจิทัลจำเป็นต้องใช้เทคโนโลยีใหม่ ๆ ร่วมกับการพัฒนาทักษะของบุคลากร การปรับปรุงกระบวนการทำงาน และการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพ ทั้งนี้เพื่อให้บริการที่มีคุณภาพและตอบสนองต่อความต้องการของลูกค้าในยุคดิจิทัลได้อย่างครบถ้วนและมีประสิทธิภาพ

การพัฒนาศักยภาพของบุคลากรในบริษัทที่ให้บริการรักษาความปลอดภัยในยุคดิจิทัลมีความหลากหลายและซับซ้อน ซึ่งปัจจัยหลักที่มีผลต่อการพัฒนาเหล่านี้สามารถอภิปรายได้ดังนี้

1) การฝึกอบรมและพัฒนาทักษะทางด้านเทคโนโลยีสารสนเทศถือเป็นปัจจัยสำคัญในการเพิ่มประสิทธิภาพการทำงานของบุคลากร บุคลากรที่ได้รับการฝึกอบรมในเทคโนโลยีใหม่ ๆ มีความสามารถในการใช้เครื่องมือและระบบได้อย่างมีประสิทธิภาพ การฝึกอบรมแบบเน้นปฏิบัติช่วยเสริมความมั่นใจและความชำนาญในการใช้งานเทคโนโลยี (นาวพล แก้วสุวรรณ, ธัญญาลักษณ์ ใจเที่ยง, สิริกร บำรุงกิจ, 2563) นอกจากนี้ โปรแกรมฝึกอบรมออนไลน์และการเรียนรู้ผ่านสื่อดิจิทัลช่วยให้บุคลากรสามารถเข้าถึงข้อมูลและการเรียนรู้ได้อย่างต่อเนื่อง (Gashi, Pugh, & Adnett, 2010)

2) การจัดการทรัพยากรบุคคลที่มีประสิทธิภาพเป็นอีกหนึ่งปัจจัยที่ช่วยเพิ่มศักยภาพให้กับบุคลากร การวางแผนการฝึกอบรมอย่างเป็นระบบและการประเมินผลอย่างต่อเนื่องทำให้สามารถระบุความต้องการในการพัฒนาและปรับปรุง

กระบวนการฝึกอบรมได้อย่างเหมาะสม การจัดการทรัพยากรบุคคลที่ดีช่วยสร้างสภาพแวดล้อมการทำงานที่ส่งเสริมการเรียนรู้และการพัฒนา (อนุชิต นาคกล่อม, เอกกมล บุญยะผลานันท์, พูลศักดิ์ โกษิยาภรณ์, 2563)

3) การสร้างวัฒนธรรมการเรียนรู้ในองค์กรช่วยกระตุ้นให้บุคลากรพัฒนาตนเองอย่างต่อเนื่อง การสนับสนุนการเรียนรู้และการแบ่งปันความรู้ภายในองค์กรช่วยให้บุคลากรมีความพร้อมในการปรับตัวกับการเปลี่ยนแปลงทางเทคโนโลยี (Hidayat & Aziz, 2022) การฝึกอบรมที่มีการต่อเนื่องและการเรียนรู้อย่างสม่ำเสมอทำให้บุคลากรมีความพร้อมในการใช้งานเทคโนโลยีที่เปลี่ยนแปลงไป

4) การสนับสนุนจากผู้บริหารมีบทบาทสำคัญในการพัฒนาบุคลากร ผู้บริหารที่ให้ความสำคัญกับการพัฒนาบุคลากร และการฝึกอบรมช่วยเสริมสร้างแรงจูงใจและความมั่นใจในบุคลากร การจัดสรรทรัพยากรเพื่อการฝึกอบรมและการให้โอกาสพัฒนาทักษะเป็นสิ่งสำคัญที่ช่วยเสริมสร้างศักยภาพในการทำงาน (บุญทัน ดอกไธสง, 2563)

5) การใช้เทคโนโลยีในการฝึกอบรมช่วยเพิ่มความน่าสนใจและความสะดวกสบายในการพัฒนาทักษะของบุคลากร โปรแกรมการเรียนรู้ออนไลน์ (e-learning) และสื่อมัลติมีเดียทำให้บุคลากรสามารถเข้าถึงเนื้อหาได้ตามความสะดวกและเรียนรู้ได้อย่างต่อเนื่อง (Hughes, Robert, Frady, & Arroyos, 2019)

6) การประเมินผลการฝึกอบรมเป็นส่วนสำคัญในการปรับปรุงกระบวนการฝึกอบรมให้มีประสิทธิภาพยิ่งขึ้น การวัดผลจากการฝึกอบรมช่วยให้สามารถระบุจุดแข็งและจุดอ่อนในกระบวนการฝึกอบรมได้อย่างแม่นยำ การใช้เครื่องมือการวัดผลที่เหมาะสมสามารถช่วยในการปรับปรุงการฝึกอบรมให้มีประสิทธิภาพมากขึ้น (ปรินทร พลรัฐธนาสิทธิ์, นิธิตา สิริพงศ์ ทักขิณ, 2563)

7) การสร้างโอกาสให้บุคลากรได้พัฒนาทักษะใหม่ ๆ ภายในองค์กร เช่น การจัดโครงการหรือกิจกรรมที่ส่งเสริมการใช้เทคโนโลยี ช่วยให้บุคลากรสามารถฝึกฝนทักษะได้อย่างต่อเนื่อง การส่งเสริมการเรียนรู้เช่นนี้ทำให้บุคลากรมีความมั่นใจในการใช้งานเทคโนโลยีและมีความพร้อมในการปฏิบัติงานในยุคดิจิทัล (Gupta, Bhaskar, & Singh, 2017)

8) การรับรองมาตรฐานและการประกอบวิชาชีพที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศช่วยเสริมสร้างความมั่นใจให้กับบุคลากรที่ปฏิบัติงาน การได้รับการรับรองจากสถาบันที่มีความน่าเชื่อถือช่วยเพิ่มคุณค่าทางวิชาชีพและส่งเสริมความเชื่อมั่นในทักษะการทำงานของบุคลากร (Birdi, Patterson, & Wood, 2007) จากผลการวิจัยพบว่า ปัจจัยที่มีผลต่อการพัฒนา ศักยภาพของบุคลากรในบริษัทที่ให้บริการรักษาความปลอดภัยในยุคดิจิทัลไม่เพียงแต่การฝึกอบรมและพัฒนาทักษะทางด้านเทคโนโลยีสารสนเทศเท่านั้น แต่ยังรวมถึงการจัดการทรัพยากรบุคคลที่มีประสิทธิภาพ การสร้างวัฒนธรรมการเรียนรู้ใน องค์กร การสนับสนุนจากผู้บริหาร การใช้เทคโนโลยีในการฝึกอบรม การวิเคราะห์และประเมินผลการฝึกอบรม การสร้าง โอกาสในการพัฒนาทักษะภายในองค์กร และการรับรองมาตรฐานและการประกอบวิชาชีพ การผสมผสานของปัจจัยเหล่านี้ จะช่วยให้บริษัทสามารถพัฒนา ศักยภาพของบุคลากรได้อย่างมีประสิทธิภาพและสอดคล้องกับความต้องการของยุคดิจิทัล

องค์ความรู้ใหม่

จากการวิจัยนี้ ได้มีการค้นพบองค์ความรู้ใหม่ที่สำคัญ ซึ่งสามารถนำไปใช้ในการพัฒนาบริษัทที่ให้บริการรักษาความปลอดภัยได้อย่างมีประสิทธิภาพในยุคดิจิทัล ดังนี้

1) การบูรณาการเทคโนโลยีใหม่เพื่อการรักษาความปลอดภัย การใช้เทคโนโลยีใหม่ ๆ เช่น ปัญญาประดิษฐ์ (AI), การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics), และ Internet of Things (IoT) ในการตรวจจับและป้องกันภัยคุกคามมีประสิทธิภาพสูง เทคโนโลยีเหล่านี้ช่วยให้สามารถวิเคราะห์ข้อมูลที่ซับซ้อนและตรวจจับพฤติกรรมที่ผิดปกติได้อย่างรวดเร็วและแม่นยำ นอกจากนี้ การเชื่อมต่อและควบคุมอุปกรณ์รักษาความปลอดภัยผ่าน IoT ช่วยให้การตรวจสอบและตอบสนองต่อเหตุการณ์เป็นไปอย่างทันทีและมีประสิทธิภาพมากขึ้น

2) การพัฒนา ศักยภาพบุคลากรผ่านการฝึกอบรมและการสร้างวัฒนธรรมการเรียนรู้ การฝึกอบรมที่มีคุณภาพ และการพัฒนาทักษะทางด้านเทคโนโลยีสารสนเทศช่วยให้บุคลากรมีความพร้อมในการใช้เทคโนโลยีใหม่ ๆ ในการปฏิบัติงาน การสร้างวัฒนธรรมการเรียนรู้ในองค์กรช่วยส่งเสริมให้บุคลากรมีความกระตือรือร้นในการพัฒนาตนเองและการ

เรียนรู้เทคโนโลยีใหม่ ๆ การสนับสนุนการเรียนรู้และการแบ่งปันความรู้ในองค์กรช่วยให้บุคลากรสามารถปรับตัวกับการเปลี่ยนแปลงทางเทคโนโลยีได้อย่างรวดเร็ว

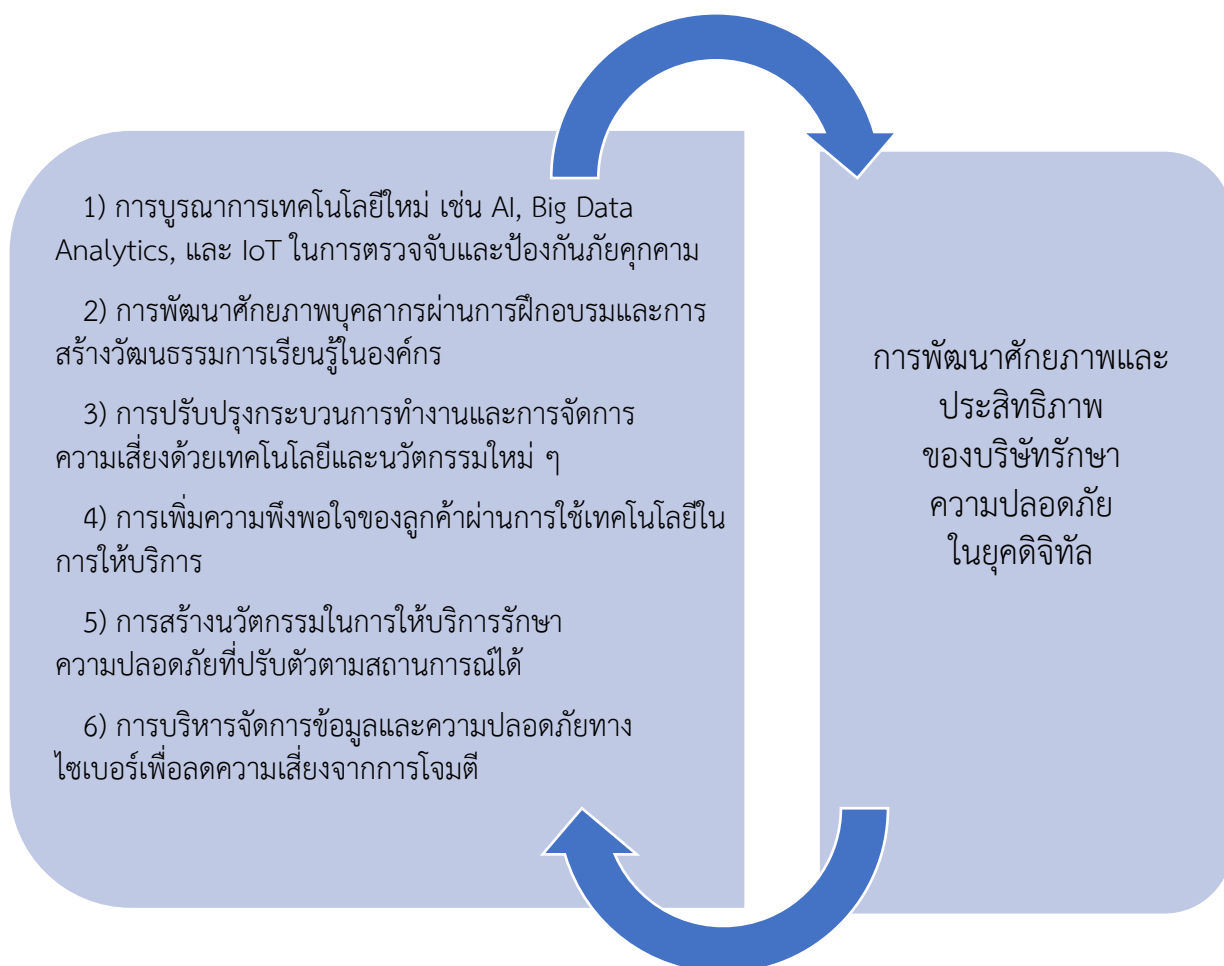
3) การปรับปรุงกระบวนการทำงานและการจัดการความเสี่ยง การปรับปรุงกระบวนการทำงานโดยใช้เทคโนโลยีและนวัตกรรมใหม่ ๆ ช่วยให้บริษัทสามารถดำเนินงานได้อย่างมีประสิทธิภาพ การใช้ระบบการจัดการความปลอดภัยแบบรวมศูนย์ (Integrated Security Management Systems) และระบบการรายงานและการติดตามผลแบบเรียลไทม์ช่วยให้ผู้บริหารสามารถตัดสินใจได้อย่างรวดเร็วและแม่นยำ นอกจากนี้ การบริหารจัดการความเสี่ยงที่มีประสิทธิภาพช่วยลดความเสียหายและเพิ่มความมั่นคงในการดำเนินงานของบริษัท

4) การสร้างความพึงพอใจของลูกค้าผ่านการใช้เทคโนโลยี การนำเทคโนโลยีใหม่มาใช้ในการให้บริการช่วยเพิ่มความพึงพอใจของลูกค้า การใช้ระบบการรายงานและการติดตามผลแบบเรียลไทม์ทำให้ลูกค้าสามารถรับรู้สถานะและความปลอดภัยของทรัพย์สินหรือสถานที่ได้ตลอดเวลา ซึ่งสร้างความมั่นใจและความเชื่อถือในบริการของบริษัท การสร้างระบบการบริการที่ตอบสนองต่อความต้องการเฉพาะของลูกค้าเป็นสิ่งสำคัญในการเพิ่มความพึงพอใจและความไว้วางใจจากลูกค้า (พรพรรณ นันทแพศย์. 2566, นน. 5-6)

5) การสร้างนวัตกรรมในการให้บริการรักษาความปลอดภัย การสร้างนวัตกรรมในการให้บริการรักษาความปลอดภัยเป็นปัจจัยที่สำคัญในการตอบสนองต่อความต้องการของตลาด การพัฒนาระบบการรักษาความปลอดภัยที่สามารถปรับตัวตามสถานการณ์ได้ (Adaptive Security Systems) ช่วยให้การบริการมีประสิทธิภาพมากขึ้น การใช้ AI ในการปรับเปลี่ยนการทำงานของระบบตามสภาพแวดล้อมและความเสี่ยงที่เกิดขึ้นเป็นตัวอย่างของนวัตกรรมที่สามารถเพิ่มประสิทธิภาพของการให้บริการได้

6) การบริหารจัดการข้อมูลและความปลอดภัยทางไซเบอร์ การบริหารจัดการข้อมูลและความปลอดภัยทางไซเบอร์เป็นสิ่งจำเป็นในการพัฒนาศักยภาพของบริษัทที่ให้บริการรักษาความปลอดภัย การใช้เทคโนโลยีการเข้ารหัสข้อมูลและการป้องกันภัยทางไซเบอร์ช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์และรักษาความปลอดภัยของข้อมูลลูกค้า การจัดการข้อมูลที่มีประสิทธิภาพช่วยให้บริษัทสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและมีความมั่นคง

จากองค์ความรู้ใหม่ที่ได้จากการวิจัยนี้สามารถนำไปใช้ในการพัฒนาบริษัทรักษาความปลอดภัยในยุคดิจิทัลได้อย่างมีประสิทธิภาพ การบูรณาการเทคโนโลยีใหม่ การพัฒนาบุคลากร การปรับปรุงกระบวนการทำงาน การสร้างความพึงพอใจของลูกค้า การสร้างนวัตกรรมในการให้บริการ และการบริหารจัดการข้อมูลและความปลอดภัยทางไซเบอร์เป็นปัจจัยที่สำคัญที่ช่วยให้บริษัทสามารถให้บริการที่มีคุณภาพและมีประสิทธิภาพในยุคดิจิทัลที่เทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็วและต่อเนื่อง ดังแสดงได้ตามภาพที่ 2



ภาพที่ 2 องค์ความรู้ใหม่

สรุปผลการวิจัย

การวิจัยนี้ได้ทำการศึกษาและวิเคราะห์ปัจจัยต่าง ๆ ที่มีผลต่อการพัฒนาบริษัทที่ให้บริการรักษาความปลอดภัยพบว่า การบูรณาการเทคโนโลยีใหม่ ๆ เช่น ปัญญาประดิษฐ์ (AI), การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics), และ Internet of Things (IoT) เป็นสิ่งสำคัญที่ช่วยเพิ่มประสิทธิภาพในการตรวจจับและป้องกันภัยคุกคาม การใช้เทคโนโลยีเหล่านี้ช่วยให้บริษัทสามารถวิเคราะห์ข้อมูลที่ซับซ้อนและตรวจจับพฤติกรรมที่ผิดปกติได้อย่างรวดเร็วและแม่นยำ การพัฒนาศักยภาพของบุคลากรเป็นปัจจัยที่มีความสำคัญอย่างยิ่ง การฝึกอบรมที่มีคุณภาพและการสร้างวัฒนธรรมการเรียนรู้ในองค์กรช่วยให้บุคลากรมีความพร้อมในการใช้เทคโนโลยีใหม่ ๆ ในการปฏิบัติงาน การสร้างสภาพแวดล้อมการทำงานที่ส่งเสริมการเรียนรู้และการพัฒนาทักษะช่วยให้บุคลากรสามารถปรับตัวกับการเปลี่ยนแปลงทางเทคโนโลยีได้อย่างรวดเร็ว

นอกจากนี้ การปรับปรุงกระบวนการทำงานโดยใช้เทคโนโลยีและนวัตกรรมใหม่ ๆ ช่วยให้บริษัทสามารถดำเนินงานได้อย่างมีประสิทธิภาพ การใช้ระบบการจัดการความปลอดภัยแบบรวมศูนย์และระบบการรายงานและการติดตามผลแบบเรียลไทม์ช่วยให้ผู้บริหารสามารถตัดสินใจได้อย่างรวดเร็วและแม่นยำ การบริหารจัดการข้อมูลและความปลอดภัยทางไซเบอร์เป็นสิ่งจำเป็นในการลดความเสี่ยงจากการโจมตีทางไซเบอร์และรักษาความปลอดภัยของข้อมูลลูกค้า การสร้างความพึงพอใจของลูกค้าเป็นอีกหนึ่งปัจจัยที่สำคัญ การใช้เทคโนโลยีใหม่ในการให้บริการช่วยเพิ่มความพึงพอใจของลูกค้า การใช้ระบบการรายงานและการติดตามผลแบบเรียลไทม์ทำให้ลูกค้าสามารถรับรู้สถานะและความปลอดภัยของทรัพย์สินหรือสถานที่ได้ตลอดเวลา ซึ่งสร้างความมั่นใจและความเชื่อถือในบริการของบริษัท

สุดท้าย การสร้างนวัตกรรมในการให้บริการรักษาความปลอดภัยช่วยให้บริษัทสามารถตอบสนองต่อความต้องการของตลาดได้อย่างมีประสิทธิภาพ การพัฒนาระบบการรักษาความปลอดภัยที่สามารถปรับตัวตามสถานการณ์ได้ช่วยให้การบริการมีประสิทธิภาพมากยิ่งขึ้น สรุปได้ว่าการพัฒนาศักยภาพและประสิทธิภาพของบริษัทรักษาความปลอดภัยในยุคดิจิทัล

จำเป็นต้องอาศัยการประยุกต์ใช้เทคโนโลยีใหม่ ๆ การพัฒนาบุคลากร การปรับปรุงกระบวนการทำงาน การสร้างความพึงพอใจของลูกค้า การสร้างนวัตกรรมในการให้บริการ และการบริหารจัดการข้อมูลและความปลอดภัยทางไซเบอร์ ปัจจัยเหล่านี้จะช่วยให้บริษัทสามารถให้บริการที่มีคุณภาพและมีประสิทธิภาพในยุคดิจิทัลที่เทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็วและต่อเนื่อง

ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงนโยบาย

1.1 หน่วยงานรัฐบาลและองค์กรที่เกี่ยวข้องควรสนับสนุนการนำเทคโนโลยีใหม่ เช่น AI, Big Data Analytics และ IoT มาใช้ในองค์กรรักษาความปลอดภัย โดยจัดทำโครงการหรือมาตรการที่ส่งเสริมการลงทุนในเทคโนโลยีเหล่านี้ รวมถึงการให้สิทธิประโยชน์ทางภาษีแก่บริษัทที่ลงทุนในเทคโนโลยีเพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน

1.2 ควรมีนโยบายในการพัฒนาบุคลากรอย่างต่อเนื่อง โดยจัดทำโปรแกรมการฝึกอบรมและพัฒนาทักษะทางด้านเทคโนโลยีสารสนเทศ ให้แก่บุคลากรในองค์กรรักษาความปลอดภัย เพื่อให้มีความพร้อมในการใช้เทคโนโลยีใหม่ ๆ ในการปฏิบัติงาน

1.3 หน่วยงานที่เกี่ยวข้องควรกำหนดมาตรฐานและแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ เพื่อให้บริษัทที่ให้บริการรักษาความปลอดภัยสามารถปฏิบัติตามมาตรฐานที่กำหนดและมีการป้องกันภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

2. ข้อเสนอแนะด้านการวิจัยครั้งต่อไป

2.1 ควรมีการวิจัยเปรียบเทียบประสิทธิภาพของเทคโนโลยีต่าง ๆ เช่น AI, Big Data Analytics, และ IoT ในการรักษาความปลอดภัย เพื่อหาข้อมูลที่เป็นประโยชน์ในการตัดสินใจเลือกใช้เทคโนโลยีที่เหมาะสมกับความต้องการและสภาพแวดล้อมของแต่ละองค์กร

2.2 ควรมีการวิจัยเพื่อศึกษาผลกระทบของการนำเทคโนโลยีใหม่มาใช้ต่อประสิทธิภาพการทำงานของบุคลากร เช่น การเปลี่ยนแปลงในกระบวนการทำงาน ความพึงพอใจในการทำงาน และการปรับตัวของบุคลากร เพื่อหาวิธีการปรับปรุงและเพิ่มประสิทธิภาพในการทำงาน

2.3 ควรมีการวิจัยเพื่อศึกษาความสำเร็จขององค์กรที่นำเทคโนโลยีใหม่มาใช้ในการรักษาความปลอดภัย โดยวิเคราะห์ปัจจัยที่นำไปสู่ความสำเร็จและแนวทางปฏิบัติที่ดี เพื่อเป็นแบบอย่างและแนวทางในการนำเทคโนโลยีมาใช้ในการองค์กรรักษาความปลอดภัยอื่น ๆ

เอกสารอ้างอิง

โกสินทร์ ชำนาญพล และ สุดาใจ โล่ห์นิชชัย. (2562). การพัฒนารูปแบบเทคโนโลยีดิจิทัลเพื่อส่งเสริมศักยภาพ

ผู้ประกอบการ. *วารสารราชพฤกษ์*, 17(2), 30-138.

ฉัฐวัฒน์ ชัชณฐาภักดิ์. (2566). *การบริหารการพัฒนาเชิงกลยุทธ์*. กรุงเทพฯ: ProTexts.

นवल แก้วสุวรรณ, ธัญญาลักษณ์ ใจเที่ยง และ สิริกร บำรุงกิจ. (2563). การจัดการความรู้ เพื่อก้าวสู่องค์กรดิจิทัลในยุคเทคโนโลยีพลิกผัน. *วารสารศิลปากร*, 40(4), 120-135.

บุญทัน ดอกไธสง. (2563). *รัฐประศาสนศาสตร์เปลี่ยนโลก*. พระนครศรีอยุธยา: โรงพิมพ์มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย.

บุญเรือน ทองทิพย์ และ วัชรบุตร กุลบุตร. (2563). การจัดการการเปลี่ยนแปลงทรัพยากรมนุษย์ของ RANGER SECURITY GUARD INVESTIGATION CO., LTD. *วารสาร มจร นาคทรรค์*, 7(11), 342-356.

ปรินทร์ พลรัฐนาสิทธิ และ นิธิตา สิริพงศ์ทักษิณ. (2563). การเมืองในการกำหนดนโยบายธุรกิจรักษาความปลอดภัย. *วารสารการวิจัยการบริหารการพัฒนา*, 10(3), 65-76.

- พรวรรณ นันทแพทย์. (2566). อิทธิพลของคุณลักษณะบุคลิกภาพ การยอมรับเทคโนโลยี พฤติกรรมการลงทุน ที่มีต่อการตัดสินใจลงทุนสกุลเงินดิจิทัล. *Procedia of Multidisciplinary Research*, 1(7), 1-9.
- วันเฉลิม แสงสว่าง. (2556). ปัจจัยที่ส่งผลต่อการบริหารความสัมพันธ์ของพนักงาน รักษาความปลอดภัยในเขตกรุงเทพมหานคร : กรณีของบริษัท มิตรสยามรักษาความปลอดภัย จำกัด. *วารสารวิชาการมหาวิทยาลัยปทุมธานี*, 5(1), 10-22.
- อนุชิต นาคกล่อม, เอกกมล บุญยะผลานันท์ และ พูลศักดิ์ โกษียาภรณ์. (2563). การพัฒนาหลักสูตรฝึกอบรมนักพัฒนาระบบด้วยเทคโนโลยีดิจิทัล โดยใช้แพลตฟอร์มการเรียนรู้ด้วยเทคโนโลยีไอโอทีอาศัยรูปแบบการเชื่อมโยงองค์ความรู้มหาวิทยาลัย และภาคอุตสาหกรรม. *วารสารศึกษาศาสตร์มหาวิทยาลัยนเรศวร*, 24(3), 303-314.
- Birdi, K. S., Patterson, M. G., & Wood, S. J. (2007). Learning to perform? A comparison of learning practices and organisational performance in profit and non-profit-making sectors in the UK. *International Journal of Training and Development*, 11(4), 265–281.
- Blume, B. D., Ford, J. K., Baldwin, T. T., & Huang, J. L. (2010). Transfer of training: A meta-analytic review. *Journal of Management*, 36(4), 1065–1105.
- Creswell, J. W., & Poth, C. N. (2017). Qualitative inquiry and research design: Choosing among five approaches. (4th ed.). California: SAGE Publications, Inc.
- Gashi, A., Pugh, G., & Adnett, N. (2010). Technological change and employer-provided training: evidence from UK workplaces. *International Journal of Manpower*, 31(4), 426-448.
- Gupta, K., Bhaskar, P., & Singh, S. (2017). Prioritization of factors influencing employee adoption of e-government using the analytic hierarchy process. *Journal of Systems and Information Technology*, 19(1/2), 116-137.
- Hajjar, S., & Alkhanaizi, M. (2018). Exploring the factors that affect employee training effectiveness: a case study in Bahrain. *SAGE Open*, 8(2), 1-10.
- Hidayat, A., & Aziz, M. (2022). The role of job training in improving employee performance. *Adpebi International Journal of Multidisciplinary Sciences*, 1(1), 21-30.
- Hughes, C., Robert, L., Frady, K., & Arroyos, A. (2019). *Managing technology and middle-and low-skilled employees: Advances for economic regeneration*. Leeds: Emerald Publishing Limited.
- Imran, M., Maqbool, N., & Shafique, H. (2014). Impact of technological advancement on employee performance in banking sector. *International Journal of Human Resource Studies*, 4(1), 57-65.
- Jalil, R., Perizade, P., & Widiyanti, H. (2019). Effect of training and work discipline on employee performance at PT PLN (Persero). *International Journal of Management and Humanities*, 3(11), 37-42.
- Javaid, M., Khan, S., Haleem, A., & Rab, S. (2022). Adoption of modern technologies for implementing industry 4.0: an integrated MCDM approach. *Benchmarking: An International Journal*, 30(10), 3753-3790.
- Jumanne, A., & Njoroge, J. (2019). Technological change management and performance of employees of the parliamentary service commission in Kenya. *American Journal of Public Policy and Administration*, 4(1), 18-30.
- Kim, J., & Park, C. Y. (2020). Education, skill training, and lifelong learning in the era of technological revolution: A review. *Asian-Pacific Economic Literature*, 34(2), 3-19.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook*. (3rd ed.). California: SAGE Publications, Inc.