

การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
The Cybersecurity Skills Development of National Cyber Security Agency

วารภรณ์ เพลิดเพลิน
Waraporn Plerdplern
6314832029@rumail.ru.ac.th

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร รวมถึงศึกษาปัญหาและอุปสรรค และแนวทางการแก้ไขปัญหาหรืออุปสรรค และข้อเสนอแนะ การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ใช้วิธีวิจัยจากเอกสารและใช้วิธีการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญ จำนวน 7 คน ผลการศึกษาพบว่า แนวทางการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบไปด้วย 3 ด้าน ได้แก่ 1. ด้านการศึกษา 2. ด้านการฝึกอบรม และ 3. ด้านการพัฒนา โดยมีปัญหาและอุปสรรคในการพัฒนาทักษะบุคลากร ดังนี้ 1. ปัญหาด้านงบประมาณ ได้รับการจัดสรรไม่เพียงพอ 2. หลักสูตรการศึกษาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีจำนวนน้อย ส่งผลให้มีผู้เชี่ยวชาญด้านไซเบอร์น้อย 3. บุคลากรของสำนักงานมีจำนวนน้อย ส่งผลให้บุคลากรไม่มีเวลาในการพัฒนาตนเอง 4. บุคลากรของสำนักงานขาดความรู้ความเข้าใจและอุปกรณ์ที่ใช้ในการปฏิบัติงาน ส่วนแนวทางการแก้ไขปัญหา คือ การสร้างความร่วมมือกับหน่วยงานทั้งภายในและต่างประเทศให้เห็นถึงความสำคัญของภัยคุกคามทางไซเบอร์ เพื่อแลกเปลี่ยนบุคลากรและสนับสนุนงบประมาณ ข้อเสนอแนะของงานวิจัย คือ การวางแผนเป้าหมายและวิสัยทัศน์ให้ชัดเจนในการพัฒนาบุคลากร โดยบุคลากรควรจัดสรรเวลาการทำงานให้ดีเพื่อหาเวลาไปพัฒนาตนเอง และควรเพิ่มโอกาสบุคลากรและประชาชนทั่วไปให้เข้าถึงความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทางสื่อสังคมออนไลน์

คำสำคัญ: การพัฒนาทักษะ, การรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร, สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Keywords: Skills Development, Cyber security, National Cyber Security Agency

* บทความนี้เรียบเรียงจากการค้นคว้าอิสระเรื่องการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

** นักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต มหาวิทยาลัยรามคำแหง

บทนำ

ปัจจุบันสังคมโลกเผชิญกับภัยคุกคามทางไซเบอร์หรือการโจมตีทางคอมพิวเตอร์ที่ส่งผลกระทบต่อดำเนินชีวิตของประชาชนและความมั่นคงของประเทศ รัฐบาลจึงมีนโยบายในการรักษาความมั่นคงปลอดภัยของประเทศ โดยเฉพาะการเพิ่มขีดความสามารถในการบริหารจัดการภัยคุกคามทางไซเบอร์ การบูรณาการความร่วมมือจากทุกภาคส่วนทั้งภายในและต่างประเทศ เพื่อให้เป็นเครือข่ายในการป้องกัน การคุกคามทางไซเบอร์และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยมียุทธศาสตร์ชาติด้านความมั่นคงแผนการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560-2564) แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ. 2560-2564) เพื่อเป็นการป้องกันภัยคุกคามทางไซเบอร์ จึงได้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่ในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure : CII) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ การประสานความร่วมมือระหว่างภาครัฐและเอกชน และระหว่างหน่วยงานด้านไซเบอร์ทั้งภายในและต่างประเทศ สร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจจะกระทบต่อการดำเนินชีวิตของประชาชนไปจนถึงความมั่นคงของรัฐที่มีสถานะเสี่ยงถูกโจมตี เนื่องจากภาครัฐหรือภาคเอกชนยังมีบุคลากรที่ขาดความรู้และเครื่องมือทางด้านไซเบอร์ รวมทั้งประเทศไทยกำลังขาดแคลนบุคลากรที่มีความรู้ความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทำให้อาชญากรรมทางไซเบอร์ใช้ช่องโหว่ของระบบในการโจมตีข้อมูลหรือเครือข่ายทางสารสนเทศ สำนักงานจึงจำเป็นต้องพัฒนาขีดความสามารถของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการให้ความรู้และความเข้าใจของบุคลากรที่ปฏิบัติหน้าที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน

จากความเป็นมาดังกล่าว ผู้วิจัยจึงมีความสนใจที่จะศึกษาการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมทั้งศึกษาถึงปัญหาและอุปสรรค และแนวทางการแก้ไขปัญหาหรืออุปสรรค ตลอดจนข้อเสนอแนะการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งผลที่ได้จากการวิจัยจะเป็นแนวทางในการพัฒนาสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต่อไป

วิธีดำเนินการวิจัย

งานวิจัยนี้เป็นงานวิจัยเชิงคุณภาพ มีวิธีเก็บรวบรวมข้อมูลจากการวิจัยเอกสาร (Documentary research) และผู้วิจัยใช้วิธีการสัมภาษณ์ โดยการสัมภาษณ์แบบมีโครงสร้างหรือการสัมภาษณ์แบบเป็นทางการ (Structured interview or formal interview) เก็บข้อมูลจากผู้ให้ข้อมูลสำคัญ (Key informants) จำนวน 7 คน โดยพิจารณาจากคุณสมบัติผู้ที่เกี่ยวข้องกับการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร

สำนักงานคณะกรรมการการรักษามันคงปลอดภัยไซเบอร์แห่งชาติ โดยใช้การนำเสนอผลการวิจัยในรูปแบบ
พรรณนา

ผลการวิจัยและการอภิปรายผล

ผลการวิจัย

ผลการวิจัยสรุปได้ดังนี้

แนวทางการพัฒนาทักษะด้านการรักษามันคงปลอดภัยไซเบอร์ของบุคลากร สำนักงาน

คณะกรรมการการรักษามันคงปลอดภัยไซเบอร์แห่งชาติ ประกอบด้วย

1) ด้านการศึกษา คือ การปลูกฝังความรู้ทางด้านการรักษามันคงปลอดภัยไซเบอร์ตั้งแต่ระดับวัย
อุดมศึกษาจนถึงระดับมหาวิทยาลัย ต้องมีความรู้ทางด้านการรักษามันคงปลอดภัยไซเบอร์หรือด้าน IT เพราะ
การศึกษาคือหัวใจถึงหลักแนวคิดทฤษฎี และเทคนิคที่ใช้ในการรักษามันคงปลอดภัยไซเบอร์ เป็นการ
เตรียมความพร้อมที่สำคัญในการพัฒนาบุคลากรในด้านหลักสูตรต่าง ๆ ที่จำเป็นต่อการทำงานหรือตามความสนใจ
ของผู้ศึกษา ดังนั้น การศึกษาจึงเป็นการวางแผนแนวทางการพัฒนาทักษะของบุคลากรทางด้านการรักษามัน
คงปลอดภัยไซเบอร์ที่จำเป็นในอนาคต เพื่อที่สำนักงานคณะกรรมการการรักษามันคงปลอดภัยไซเบอร์
แห่งชาติจะได้พัฒนาบุคลากรให้มีจำนวนที่ตอบสนองต่อความต้องการและเท่าทันต่อภัยคุกคามที่เกิดขึ้น แต่ระดับ
การศึกษาของบุคลากรนั้นอาจแตกต่างกันไปตามภารกิจและหน้าที่ความรับผิดชอบของแต่ละสายงาน บุคลากรใน
สายงานสนับสนุนทั่วไปอาจไม่ต้องลงลึกไปในทางด้านเทคนิคมากนัก แต่เป็นความรู้พื้นฐานที่ใช้ในการป้องกันภัย
คุกคามทางไซเบอร์ ส่วนบุคลากรในสายงานทางไซเบอร์จะต้องได้รับการศึกษาให้เกิดความทักษะและเชี่ยวชาญ
ทางด้านการรักษามันคงปลอดภัยไซเบอร์ ซึ่งเป็นหน้าที่และภารกิจหลักของสำนักงานในการดำเนินการให้
เป็นไปตามยุทธศาสตร์ชาติ 20 ปี ของประเทศ

2) ด้านการฝึกอบรม คือ ภาคปฏิบัติที่ให้ผู้บุคลากรได้ฝึกปฏิบัติในสถานการณ์จำลองเสมือนจริง และได้รับ
ฟังความรู้จากผู้เชี่ยวชาญทางด้านการรักษามันคงปลอดภัยไซเบอร์ที่มีประสบการณ์โดยตรง ทำให้บุคลากรได้รับความ
รู้และประสบการณ์เกิดความเข้าใจและเชี่ยวชาญในเรื่องการรักษามันคงปลอดภัยไซเบอร์มากยิ่งขึ้น
การฝึกอบรมจะช่วยเสริมในเนื้อหาของศึกษาระดับพื้นฐานให้ชัดเจนและเฉพาะทางมากยิ่งขึ้น ซึ่งเป็นวิธีการ
ปฏิบัติ การนำความรู้ที่ได้รับจากการศึกษามาต่อยอดหรือประยุกต์ใช้ในสถานการณ์จริง เพื่อให้ผู้เข้ารับการฝึกอบรม
ได้ซักซ้อมทั้งวิธีการและแนวคิดมาปรับใช้กับภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นในอนาคต ซึ่งเป็นการเพิ่มเติมความรู้
จากด้านการศึกษาอีกระดับหนึ่ง และยังช่วยให้เกิดการแลกเปลี่ยนบุคลากรที่มีความเชี่ยวชาญทางด้านการรักษา
ความมันคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ เพื่อแลกเปลี่ยนเรียนรู้ประสบการณ์ทางด้านการรักษา
ความมันคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น ซึ่งสำนักงานได้มีการจัดฝึกอบรมให้กับบุคลากรทั้งภายใน
และภายนอกสำนักงาน ดังนี้

ลำดับ	หลักสูตร/กิจกรรม/โครงการ/สัมมนา	จำนวน (วัน/ชั่วโมง/ครั้ง)
1.	Briefing – Hive Ransomware	2 ชม.
2.	NCSA Cyber Clinic 2022	9 ครั้ง
3.	Blockchain กับการรับมือภัยคุกคามทางไซเบอร์	2 ชม.
4.	Data layer Protection: Let's data protect themselves จะดีกว่าไหมถ้าข้อมูลของคุณป้องกันตัวเองได้	2 ชม.
5.	Cybersecurity ที่เกี่ยวกับ Infrastructure ในรูปแบบ Multi-Cloud	2 ชม.
6.	การรักษาความมั่นคงปลอดภัย OT System	2 ชม.
7.	Cyber Security กับการศึกษา	2 ชม.
8.	Personal Data Protection Act: PDPA	2 ชม.
9.	รู้เท่าทันภัยคุกคามทางไซเบอร์ฉบับพนักงานมืออาชีพ (Cybersecurity for professional employees)	2 ชม.
10.	Build Strong Security Awareness Program	3 ชม.
11.	Next Gen Information Security Leader	3 ชม.
12.	Cyber Security Capability Skill Building	5 วัน
13.	การยกระดับมาตรฐาน CII ตาม พ.ร.บ.ไซเบอร์	2.30 ชม.
14.	Thailand National Cyber Week 2021	3 วัน
15.	รายงานสถานการณ์ แนวโน้มและทักษะของภัยคุกคามทางไซเบอร์	4.30 ชม.
16.	Two sides of Same Coin: Investigating Critical Penetration Testing and Security Analytic Skills	3 ชม.
17.	Microsoft Women@Cybersecurity	4 ชม.
18.	ความล้มคอมพิวเตอร์ ประโยชน์ ภัยคุกคาม และการรับมือ	2 ชม.
19.	Stop Bullying จะดีกว่าไหมถ้าเราให้เกียรติกัน	2 ชม.
20.	Thailand Cybersecurity Excellent Award 2022	1 ครั้ง
21.	โครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์	2 ครั้ง

ลำดับ	หลักสูตร/กิจกรรม/โครงการ/สัมมนา	จำนวน (วัน/ชั่วโมง/ครั้ง)
	Intensive Cybersecurity Capacity Building Program	
22.	อบรมด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน/ระดับเชี่ยวชาญ	4 ครั้ง 45 รุ่น
23.	Cybersecurity Risk Management	3 ชม.
24.	หลักสูตร ECSS	-
25.	หลักสูตร CISSP: Certified Information System Security Professional	22 วัน
26.	National and CII Attack Surface Thailand Case Study	2.30 ชม.
27.	ภัยไซเบอร์จากระบบ Remote Working	1.30 ชม.
28.	Lessons in Incident Responding and Digital Forensic	1.30 ชม.
29.	The inspiration to be Malware Analyst	1.30 ชม.
30.	Focusing on Professional Pen Tester	1.30 ชม.
31.	Road to Capture the flag capture the future in 2021	1.30 ชม.
32.	วันเกษียณยุคใหม่ท่ามกลางภัยไซเบอร์	1.30 ชม.
33.	การป้องกันภัยไซเบอร์สำหรับผู้สูงอายุ	1.30 ชม.
34.	เลี้ยงลูกให้ห่างไกลภัยไซเบอร์	1.30 ชม.
35.	เสริมสร้าง Cybersecurity Awareness ให้พนักงาน	1.30 ชม.
36.	Cybersecurity และ PDPA	1.30 ชม.
37.	CISO – Talk บทเรียนภาคสนาม (รบ)	2.30 ชม.
38.	แลกเปลี่ยนความรู้ด้านการพัฒนาตนเองเพื่อโอกาสทางสายอาชีพในสายงานไซเบอร์	1 ชม.

3) ด้านการพัฒนา คือ การต่อยอดทักษะความรู้จากสิ่งที่ได้ศึกษาอบรมมาอย่างต่อเนื่องให้มีการพัฒนา มากขึ้นกว่าเดิม การพัฒนาจะดูแนวโน้มของอนาคตและสถานการณ์ของโลกที่เปลี่ยนแปลงไปเพื่อที่จะพัฒนา บุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ตรงต่อการเปลี่ยนแปลงและเป้าประสงค์ของประเทศ เช่น การพัฒนาทักษะทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่นอกเหนือจากการป้องกัน รับมือ และตอบสนอง

ต่อภัยคุกคามเพียงอย่าง อาจเพิ่มการพัฒนาทักษะทางด้านอื่น ๆ หรือทักษะจำเป็นในการปฏิบัติงาน และการพัฒนา เพื่อส่งเสริมความรู้ทางด้านต่าง ๆ ก็สามารถหาความรู้เพิ่มเติมได้เพื่อพัฒนาตนเองให้มีทักษะความรู้ทางด้านอื่น ๆ ที่ จำเป็นมากยิ่งขึ้น เนื่องจากบุคลากรจะต้องได้รับการพัฒนาเพิ่มทักษะความรู้อย่างต่อเนื่อง การพัฒนาทักษะด้านการ รักษาความมั่นคงปลอดภัยไซเบอร์อย่างเดียวยังไม่เพียงพอต่อการป้องกันภัยคุกคามที่เกิดขึ้น

ปัญหาและอุปสรรค การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกอบไปด้วย

1) ปัญหาด้านงบประมาณ เนื่องจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ ได้รับการสนับสนุนงบประมาณอย่างจำกัด ประกอบกับหน่วยงานที่สนับสนุนงบประมาณหรือรัฐบาลยังไม่ เห็นความสำคัญกับภัยคุกคามทางไซเบอร์ ทำให้ได้งบประมาณอย่างจำกัด ไม่สามารถดำเนินการพัฒนาทักษะด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์ได้เต็มที่ ทำให้สำนักงานไม่มีทุนในการดำเนินการให้พนักงานเข้ารับการศึกษ หรือฝึกอบรมได้อย่างทั่วถึง และสำนักงานจะต้องยึดติดกับกรอบเวลาของทางราชการในการดำเนินการ ส่งผลให้การ พัฒนาหลักสูตรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรไม่สอดคล้องกับสถานการณ์ที่เกิดขึ้นใน ปัจจุบัน

2) หลักสูตรการศึกษาทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ยังมีอยู่จำนวนน้อย ทำให้มีจำนวน บุคลากรที่มีความเชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์น้อย ส่งผลให้การหาผู้เชี่ยวชาญหรือ วิทยากรอบรมให้ความรู้กับบุคลากรนั้นค่อนข้างจำกัด และต้องใช้งบประมาณจำนวนมาก เพราะผู้เชี่ยวชาญส่วนใหญ่จะอยู่ในหน่วยงานเอกชนหรือหน่วยงานทางกองทัพ เนื่องจากมีค่าตอบแทนความรู้ความสามารถที่สูง

3) บุคลากรของสำนักงานมีจำนวนน้อยอันเนื่องมาจากการถูกตัดงบประมาณในการบรรจุบุคลากร ซึ่งไม่ สอดคล้องกับภาระงานที่ได้รับในปัจจุบัน ทำให้บุคลากรไม่มีเวลาในการพัฒนาตนเองทางด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ได้อย่างเต็มที่ และบุคลากรที่มีความรู้ความเชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีจำนวนน้อย ทำให้ไม่สอดคล้องกับจำนวนคนและภาระงาน หากสำนักงานจัดสรรงบประมาณที่ได้รับกับบุคลากรเน้นใน เรื่องการพัฒนาทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเดียวยังจะทำให้บุคลากรของสำนักงานไม่มีเวลาใน การทำงานให้บรรลุตามเป้าหมายของสำนักงานได้

4) ปัญหาในเรื่องของความรู้ความเข้าใจในภาระงานของแต่ละบุคคล เนื่องจากสำนักงานคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นสำนักงานที่จัดตั้งขึ้นมาใหม่ ทำให้ยังมีจำนวนบุคลากรน้อย และ บุคลากรของสำนักงานยังขาดความรู้ความเข้าใจและอุปกรณ์ที่ใช้ในการทำงาน ซึ่งอาจส่งผลต่อการพัฒนาทักษะด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์ได้เช่นเดียวกัน

แนวทางและการแก้ไขปัญหาหรืออุปสรรค และข้อเสนอแนะ การพัฒนาทักษะด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกอบไปด้วย

1) สร้างความร่วมมือกับหน่วยงานภายในประเทศและต่างประเทศให้เห็นถึงความสำคัญของภัยคุกคาม ทางไซเบอร์ เพื่อแลกเปลี่ยนบุคลากรที่มีความเชี่ยวชาญและสนับสนุนงบประมาณระหว่างกัน

2) สำนักงานมีจำนวนบุคลากรน้อยและมีภารกิจการปฏิบัติจำนวนมาก ดังนั้น จะต้องจัดสรรเวลาการทำงาน ให้ดีและคุ้มค่า และหาเวลาว่างเพื่อพัฒนาตนเองให้มีทักษะความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นประโยชน์ต่อตนเองและสำนักงาน

3) การดำเนินการทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ เพื่อให้ทุกหน่วยงาน เห็นถึงความสำคัญของภัยคุกคามทางไซเบอร์ ซึ่งอาจจะได้รับการสนับสนุนงบประมาณในการพัฒนาทักษะทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพิ่มมากยิ่งขึ้น

4) การวิธีการเผยแพร่อบรมให้ความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทางออนไลน์ จะช่วยให้ประหยัดงบประมาณในการดำเนินการ และเพิ่มโอกาสบุคลากรและประชาชนทั่วไปสามารถเข้าถึงความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ง่ายมากยิ่งขึ้น โดยไม่เสียค่าใช้จ่าย

5) สนับสนุนส่งเสริมให้เกิดการศึกษา ฝึกอบรม หรือพัฒนาทักษะของบุคลากรตามความสะดวกและความสนใจของบุคลากรแต่ละคน เพื่อที่บุคลากรจะได้พัฒนาทักษะตามความต้องการของตนเอง

6) หน่วยงานตามโครงสร้างของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ต้องมีการดำเนินการวางแผนกำหนดเป้าหมายและวิสัยทัศน์ให้ชัดเจนในการพัฒนาทักษะของบุคลากร เพื่อให้สอดคล้องกับเป้าหมายและวิสัยทัศน์ของหน่วยงาน

อภิปรายผล

การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีประเด็นที่นำมาอภิปรายดังนี้

การศึกษาแนวทางการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร ผู้วิจัยได้นำแนวคิดของ เลียนวาร์ด แนด์เลอร์ (Leonard Nadler) และการ์แลนด์ ดีวิกส์ (Garland D. Wiggs) (1989:3 อ้างใน วิธนา พิงวิวัฒน์นิกุล, 2549, หน้า 33) มาเป็นแนวทางในการศึกษาวิจัยในครั้งนี้ Nadler and Wiggs ได้อธิบายว่า การพัฒนาทรัพยากรมนุษย์ในองค์กรจะครอบคลุมองค์ประกอบทั้ง 3 ด้าน คือ การฝึกอบรม การศึกษา และการพัฒนา แต่ในทางปฏิบัติแล้วจะพบว่ากิจกรรมส่วนใหญ่ที่จัดขึ้น ในองค์กรต่าง ๆ จะเน้นกิจกรรมด้านการฝึกอบรม ซึ่งเป็นวิธีการที่องค์การใช้มากที่สุดในการพัฒนาทรัพยากรมนุษย์ สอดคล้องกับงานวิจัยของ เนตรชนก ดวนใหญ่ (2562) ได้ศึกษา การพัฒนาศักยภาพของบุคลากรในศาลอาญา ยุคดิจิทัล ประจำปี 2562 ผลการศึกษาพบว่า การดำเนินการพัฒนาศักยภาพบุคลากรของศาลอาญาในยุคดิจิทัล ประจำปี 2562 มีดังนี้ 1) การฝึกอบรม มีการจัดฝึกอบรมให้บุคลากร การส่งบุคลากรเข้ารับการอบรมกับหน่วยงานภายนอกกับสถาบันที่ได้มาตรฐาน รวมถึงการสนับสนุนให้บุคลากรที่มีความสามารถสอบชิงทุนสำนักงานศาลยุติธรรมไปอบรมที่ต่างประเทศในหลักสูตรระยะสั้น 2) การศึกษา มีการส่งเสริมให้บุคลากรมีการศึกษาในระดับที่สูงขึ้นและสนับสนุนให้ขอรับทุนสนับสนุนจากสำนักงานศาลยุติธรรมที่มีหน่วยในการดำเนินการเรื่องทุนเพื่อเป็นการพัฒนาศักยภาพในองค์ความรู้ที่สูงขึ้นหรือเพิ่มมากขึ้น 3) การพัฒนา ส่งเสริมให้บุคลากรมีการพัฒนาด้วยวิธีการต่าง ๆ เช่น การไปศึกษาดูงาน การเรียนรู้ด้วยตนเองผ่านสื่อทางเพจศาล ระบบทางเทคโนโลยีต่าง ๆ คือ ผ่านทางระบบ E – book E-learning Streaming VDO Conference รวมถึงการเป็นพี่เลี้ยง และการเป็นวิทยากร เป็นต้น

จากการศึกษาวิจัยพบว่า แนวทางการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีดังนี้

1) ด้านการศึกษา คือ การปลูกฝังความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตั้งแต่ระดับวัยอุดมศึกษาจนถึงระดับมหาวิทยาลัย เพราะการศึกษาจะช่วยให้เข้าใจถึงหลักแนวคิดทฤษฎี และเทคนิคที่ใช้ใน

การรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นการเตรียมความพร้อมที่สำคัญในการพัฒนาบุคลากรในด้านหลักสูตรต่าง ๆ ที่จำเป็นต่อการทำงานหรือตามความสนใจของผู้ศึกษา สอดคล้องกับงานวิจัยของ ธนพร นิธิพฤทธิ (2556) ได้ศึกษา การพัฒนาบุคลากรของสำนักงานคุมประพฤติประจำศาลแขวงพระนครใต้ กรมคุมประพฤติ ผลการศึกษาพบว่า แนวทางการพัฒนาบุคลากรของสำนักงานคุมประพฤติ ประจำศาลแขวงพระนครใต้ในปัจจุบัน ที่มีความสัมพันธ์กับการพัฒนาบุคลากรของสำนักงานคุมประพฤติ ประกอบด้วย การศึกษาที่เป็นทางการ (Formal Education) การประเมิน (Assessment) ประสบการณ์การทำงาน (Job Experience) ความสัมพันธ์ระหว่างบุคคล (Interpersonal Relationship) และการเรียนรู้ผ่านสื่ออิเล็กทรอนิกส์ (E-Learning) การพัฒนานั้นขึ้นอยู่กับระดับความรู้ ทักษะ และสมรรถนะที่จำเป็นสำหรับการปฏิบัติงานด้านคุมประพฤติกับผลการประเมินการพัฒนาบุคลากรของตนเองมีความแตกต่างกัน และการศึกษายังเป็นการวางแผนแนวทางการพัฒนาทักษะของบุคลากรที่จำเป็นในอนาคต เพื่อที่สำนักงานจะได้พัฒนาบุคลากรให้มีจำนวนที่ตอบสนองต่อความต้องการและเท่าทันต่อภัยคุกคามที่เกิดขึ้น ตามยุทธศาสตร์ชาติ 20 ปี สอดคล้องกับงานวิจัยของ ปรัชญา เฉลิมวัฒน์ (2561) ได้ศึกษา แนวทางการพัฒนากำลังพลด้านไซเบอร์ เพื่อพร้อมรับภัยคุกคามระดับชาติ ผลการศึกษาพบว่า แนวทางการพัฒนาบุคลากรด้านไซเบอร์ของประเทศที่ต้องมีการบูรณาการทรัพยากรบุคคลจากทุกภาคส่วน มีการวางแผนเพื่อให้สามารถบรรลุวัตถุประสงค์ของการพัฒนาบุคลากร มีการกำหนดยุทธศาสตร์ไซเบอร์ขึ้นมาเป็นส่วนประกอบของยุทธศาสตร์ความมั่นคงของชาติ

2) ด้านการฝึกอบรม คือ ภาคปฏิบัติที่บุคลากรได้ฝึกปฏิบัติในสถานการณ์จำลองเสมือนจริง และได้รับฟังความรู้จากผู้เชี่ยวชาญที่มีประสบการณ์โดยตรง การฝึกอบรมจะช่วยเสริมในเนื้อหาของการศึกษาระดับพื้นฐานให้ชัดเจนและเฉพาะทางมากยิ่งขึ้น ซึ่งเป็นวิธีการปฏิบัติ การนำความรู้ที่ได้รับจากการศึกษามาต่อยอดหรือประยุกต์ใช้ในสถานการณ์จริง สอดคล้องกับงานวิจัยของ จันทรัตน์ แทนหลาบ (2563) ได้ศึกษา การพัฒนาทักษะด้านเทคโนโลยีดิจิทัลเพื่อการปรับเปลี่ยนสู่การเป็นองค์กรดิจิทัลของบุคลากรสำนักงานเลขาธิการ สำนักงานการระบายนํ้า กรุงเทพมหานคร ผลการศึกษาพบว่า ผู้บริหารได้ทราบและให้ความสำคัญการพัฒนาทักษะด้านเทคโนโลยีดิจิทัลเพื่อการปรับเปลี่ยนสู่การเป็นองค์กรดิจิทัล พร้อมกระตุ้นให้บุคลากรเห็นถึงความสำคัญและประโยชน์ของการเปลี่ยนแปลงด้านดิจิทัล โดยการพัฒนาและสร้างนวัตกรรมขององค์กรผ่านการพัฒนาทักษะของบุคลากรให้เป็นไปในทิศทางเดียวกัน สอดคล้องกับงานวิจัยของ วิจิตา จันทรวารีเลขา (2563) ได้ศึกษา แนวทางการสนับสนุนการพัฒนาทักษะบุคลากรในการประยุกต์ใช้เทคโนโลยีดิจิทัล (Digital Savvy) ตามแผนงาน Digital Competency: กรณีศึกษา การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) ผลการศึกษาพบว่า บุคลากรทุกระดับเห็นความสำคัญของการมีทักษะทางด้านการประยุกต์ใช้เทคโนโลยีดิจิทัล (Digital savvy) ในการทำงานของตนเอง รวมทั้งส่งผลถึงประสิทธิภาพโดยรวมขององค์กร บุคลากรเห็นความสำคัญของการนำเทคโนโลยีดิจิทัลมาใช้งานเช่นเดียวกับการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับงานวิจัยของ ญัฐกานต์ ปังศรีวงศ์ (2563) ได้ศึกษา การพัฒนาทักษะด้านการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อการจัดการเรียนรู้ ในศตวรรษที่ 21 ของครูโรงเรียนตลาดหนองหวาย สังกัดสำนักงานเขตพื้นที่ การศึกษาประถมศึกษาสุราษฎร์ธานี เขต 2 ผลการศึกษาพบว่า ครูมีการใช้คอมพิวเตอร์จัดทำประมวลรายวิชา แผนการจัดการเรียนรู้ใบความรู้ใบงาน และใช้ Google Site ในการจัดการเรียนการสอน สามารถรวบรวมข้อมูลที่หลากหลายไว้ในที่เดียวได้อย่างรวดเร็ว รวมทั้งยังเป็นเว็บไซต์ของครูที่เป็นส่วนตัวหรือสาธารณะตามที่ครูต้องการ

3) ด้านการพัฒนา คือ การต่อยอดทักษะความรู้จากสิ่งที่ได้ศึกษาอบรมมาอย่างต่อเนื่องให้มีการพัฒนา มากขึ้นกว่าเดิม การพัฒนาจะดูแนวโน้มของอนาคตและสถานการณ์ของโลกที่เปลี่ยนแปลงไปเพื่อที่จะพัฒนา

บุคลากรทางด้านการศึกษาความมั่นคงปลอดภัยไซเบอร์ให้ตรงต่อการเปลี่ยนแปลงและเป้าประสงค์ของประเทศ สอดคล้องกับงานวิจัยของ ณภัทฐนันท์ ศักดิ์เจริญกุล (2562) ได้ศึกษา การเตรียมความพร้อมของบุคลากรภาครัฐไทยสู่การเป็นรัฐบาลดิจิทัล ผลการศึกษาพบว่ากระบวนการพัฒนาทักษะด้านเทคโนโลยีของบุคลากรภาครัฐมีกลไกในการพัฒนา 3 กลไก คือ การฝึกอบรมแบบเข้มข้นเรียน การเรียนรู้ด้วยตนเอง และการปรับโครงสร้างหน่วยงาน การพัฒนาบุคลากรควรเริ่มตั้งแต่การประเมินตนเองจากสมรรถนะในการปฏิบัติงาน ทักษะ ความรู้ ความสามารถ และประสบการณ์ อันเป็น 4 องค์ประกอบที่มีอิทธิพลต่อการปฏิบัติมีเพียงพอต่อภาระหน้าที่ความรับผิดชอบตามตำแหน่งหรือไม่ ซึ่งเมื่อหากพบว่า ตนเองยังขาดส่วนใด ให้ศึกษาด้วยตนเองหรือเสนอต่อผู้บังคับบัญชาเพื่อพัฒนา เป็นต้น

ปัญหาและอุปสรรค การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีประเด็นที่นำมาอภิปราย ดังนี้

1) ปัญหาด้านงบประมาณ เนื่องจากได้รับการสนับสนุนงบประมาณอย่างจำกัด ทำให้ไม่สามารถดำเนินการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้เต็มที่ สอดคล้องกับงานวิจัยของ จันทารัตน์ แทนหลาบ (2563) กล่าวว่า ปัญหาและอุปสรรคในงบประมาณทำให้ไม่มีการจัดอบรมทักษะด้านเทคโนโลยีดิจิทัลของบุคลากรภายในหน่วยงานมีเพียงส่งบุคลากรไปเข้ารับการอบรมตามหน่วยงานต่าง ๆ อุปกรณ์ด้านเทคโนโลยีดิจิทัลไม่เพียงพอ ไม่มีการจัดทำแผนพัฒนาบุคลากรที่ชัดเจน ขาดความต่อเนื่องในการพัฒนาบุคลากร และบุคลากรบางส่วนขาดความกระตือรือร้นในการพัฒนาทักษะของตนเอง และสอดคล้องกับงานวิจัยของ เนตรชนก ดวนใหญ่ (2562) กล่าวว่า งบประมาณที่ได้รับจัดสรรสำหรับการพัฒนาศักยภาพบุคลากรยังไม่เพียงพอ อุปกรณ์ เครื่องมือที่ใช้ในการปฏิบัติงานบางส่วนไม่ทันสมัยในการรองรับระบบเทคโนโลยี บุคลากรขาดการมีส่วนร่วมในแผนพัฒนาศักยภาพบุคลากร และบุคลากรในหน่วยงานมีไม่เพียงพอสำหรับการปฏิบัติงาน

2) หลักสูตรการศึกษาทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ยังมีจำนวนน้อย ทำให้มีผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์น้อย การหาผู้เชี่ยวชาญหรือวิทยากรมาอบรมให้ความรู้กับบุคลากรนั้นค่อนข้างจำกัด สอดคล้องกับงานวิจัยของ ปรัชญา เฉลิมวัฒน์ (2561) กล่าวว่า การขาดแคลนบุคลากรด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์นั้นเป็นปัญหาเร่งด่วนที่ต้องมีการแก้ไขทั้งระดับแผนและระดับปฏิบัติการ เนื่องจากบุคลากรที่มีอยู่มีขีดความสามารถในระดับผู้ฝึกสอนและไม่มีแผนแม่บทระดับชาติที่จะฝึกสอนส่งผลให้ระยะเวลาในการพัฒนาบุคลากรต้องใช้เวลาานกว่าการมีจำนวนผู้ฝึกสอนเป็นจำนวนมาก

3) บุคลากรของสำนักงานมีจำนวนน้อย ไม่สอดคล้องกับภาระงานที่ได้รับ ส่งผลให้บุคลากรไม่มีเวลาในการพัฒนาตนเอง สอดคล้องกับงานวิจัยของ เอมิกา นัดกระโทก (2564) ได้ศึกษา การพัฒนาทักษะดิจิทัลของบุคลากรในการปฏิบัติงานเพื่อรองรับการเปลี่ยนแปลงสู่องค์กรดิจิทัลของสำนักงานอัยการภาค 3 ผลการศึกษาพบว่า บุคลากรมีทัศนคติไม่ยอมรับการเปลี่ยนแปลงทางด้านดิจิทัล ขาดแรงจูงใจ ขาดการส่งเสริมในการพัฒนาทักษะดิจิทัลของตนเอง และไม่มีแนวทางในการพัฒนาทรัพยากรมนุษย์ชัดเจน

4) ปัญหาในเรื่องของความรู้ความเข้าใจในภาระงานของแต่ละบุคคล บุคลากรขาดความรู้ความเข้าใจและอุปกรณ์ที่ใช้ในการปฏิบัติงาน สอดคล้องกับงานวิจัยของ รุ่งนภา จันทร์อ่อน (2562) ได้ศึกษา การพัฒนาทักษะด้านดิจิทัลของบุคลากรกรมประชาสัมพันธ์ สู่การเปลี่ยนเป็นหน่วยงานดิจิทัล กล่าวว่า บุคลากรของกรมประชาสัมพันธ์ต้องปรับตัวให้ทันต่อการเปลี่ยนแปลงองค์กรให้เป็นดิจิทัล และช่วงอายุของบุคลากรมีผลต่อการพัฒนาทักษะด้านดิจิทัล สอดคล้องกับงานวิจัยของ โสภี วิวัฒน์ชาญกิจ (2564) ได้ศึกษา การพัฒนาทักษะการใช้เทคโนโลยีสารสนเทศของบุคลากรทางการศึกษา เพื่อการบริหารงาน โรงเรียนกีฬานครนนท์วิทยา 6 จังหวัดนนทบุรีผลการศึกษาพบว่า

ระดับความต้องการในการพัฒนาทักษะการใช้เทคโนโลยีสารสนเทศของบุคลากรอยู่ในระดับปานกลาง ทั้งด้านคอมพิวเตอร์ ด้านระบบสื่อสาร และด้านเทคโนโลยีเครือข่าย

แนวทางและการแก้ไขปัญหาหรืออุปสรรค และข้อเสนอแนะ การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีประเด็นที่นำมาอภิปราย ดังนี้

1) สร้างความร่วมมือกับหน่วยงานทั้งภายในและต่างประเทศให้เห็นถึงความสำคัญของภัยคุกคามทางไซเบอร์ เพื่อแลกเปลี่ยนบุคลากรที่มีความเชี่ยวชาญและสนับสนุนงบประมาณระหว่างกัน สอดคล้องกับงานวิจัยของ ธนพร นิธิฤทธิ์ (2556) กล่าวว่า การเตรียมความพร้อมที่จำเป็นในการปฏิบัติงานให้สอดคล้องกับประชาคมอาเซียนทั้ง 3 เสาหลัก คือ 1.ประชาคมการเมืองและความมั่นคงอาเซียน 2.ประชาคมเศรษฐกิจอาเซียน 3.ประชาคมสังคมและวัฒนธรรม สูงกว่าผลการประเมินการพัฒนาบุคลากรของตนเอง

2) สำนักงานมีจำนวนบุคลากรน้อยและมีภารกิจปฏิบัติจำนวนมาก ดังนั้น จะต้องจัดสรรเวลาการทำงานให้ดีและคุ้มค่า และหาเวลาเพื่อพัฒนาตนเองให้มีทักษะความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นประโยชน์ต่อตนเองและสำนักงาน สอดคล้องกับงานวิจัยของ ปรัชญา เฉลิมวัฒน์ (2561) กล่าวว่า การขาดแคลนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นั้นต้องมีการวางแผนระยะยาว กำหนดเป้าหมายการเรียนรู้ที่สามารถปรับให้เข้ากับสภาพของภัยคุกคามที่เปลี่ยนไป และสนับสนุนทรัพยากรต่าง ๆ ที่เกี่ยวข้องกับการพัฒนาบุคลากรให้มีศักยภาพเป็นที่ยอมรับได้ในระดับสากล

3) การดำเนินการทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ เพื่อให้ทุกหน่วยงานเห็นถึงความสำคัญของภัยคุกคามทางไซเบอร์ ซึ่งอาจจะได้รับการสนับสนุนงบประมาณในการพัฒนาทักษะทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพิ่มมากยิ่งขึ้น สอดคล้องกับงานวิจัยของ เนตรชนก ดวนใหญ่ (2562) กล่าวว่า เมื่อมีงบประมาณไม่พอเพียง ดังนั้น ควรเน้นให้เห็นถึงความสำคัญในการพัฒนาศักยภาพตนเองของบุคลากร เพื่อให้บุคลากรเกิดการเรียนรู้เพื่อพัฒนาตนเองมากขึ้น

4) เผยแพร่อบรมความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทางออนไลน์ จะช่วยให้ประหยัดงบประมาณ และเพิ่มโอกาสบุคลากรและประชาชนทั่วไปสามารถเข้าถึงความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ง่ายมากยิ่งขึ้น โดยไม่เสียค่าใช้จ่าย สอดคล้องกับงานวิจัยของ ฐิติกันต์ ปังศรีวงศ์ (2563) กล่าวว่า การนำเทคโนโลยีทางสารสนเทศเข้ามาใช้ในการเรียนการสอน เช่น Google Site ทำให้มีความพึงพอใจต่อการใช้งานในการประชุมเชิงปฏิบัติการและตรงต่อความต้องการมากยิ่งขึ้น

5) สนับสนุนส่งเสริมให้เกิดการศึกษา ฝึกอบรม หรือพัฒนาทักษะของบุคลากรตามความสะดวกและความสนใจของบุคลากรแต่ละคน เพื่อที่บุคลากรจะได้พัฒนาทักษะตามความต้องการของตนเอง สอดคล้องกับงานวิจัยของ ณภัทฐ์ธรรณ ศักดิ์เจริญกุล (2562) กล่าวว่า ผู้บังคับบัญชาต้องมีมุมมองที่เปิดกว้าง มีวิสัยทัศน์ก้าวไกล เปิดโอกาสให้ผู้ใต้บังคับบัญชายื่นข้อเสนอและพร้อมยอมรับความคิดเห็นจากผู้ใต้บังคับบัญชา และส่งเสริมให้เกิดพัฒนาตนเอง

6) หน่วยงานตามโครงสร้างของสำนักงานต้องมีการดำเนินการวางแผนกำหนดเป้าหมายและวิสัยทัศน์ให้ชัดเจนในการพัฒนาทักษะของบุคลากร เพื่อให้สอดคล้องกับเป้าหมายและวิสัยทัศน์ของหน่วยงาน สอดคล้องกับงานวิจัยของ จันทรัตน์ แทนหลาบ (2563) กล่าวว่า ควรสำรวจความต้องการของบุคลากรที่จะพัฒนาทักษะด้านดิจิทัลและให้มีส่วนร่วมในการจัดทำแผนพัฒนา และควรชี้ให้บุคลากรเห็นถึงความสำคัญในการพัฒนาทักษะของ

ตนเอง พร้อมกระตุ้นให้บุคลากรเห็นถึงความสำคัญและประโยชน์ของการเปลี่ยนแปลงด้านดิจิทัล โดยการพัฒนา และสร้างนวัตกรรมขององค์กรผ่านการพัฒนาทักษะของบุคลากรให้เป็นไปในทิศทางเดียวกัน

ข้อเสนอแนะ

ผลการวิจัยครั้งนี้สรุปได้ว่า

1. ควรขอรับการสนับสนุนงบประมาณเพิ่มเติมเพื่อให้เพียงพอสำหรับการบรรจุบุคลากรและปรับโครงสร้างและอัตรากำลังของสำนักงานให้เพียงพอต่อการปฏิบัติงาน
2. ควรร่วมมือกับหน่วยงานอื่น ๆ เพื่อขอรับการสนับสนุนงบประมาณและการสนับสนุนผู้เชี่ยวชาญ ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้มีงบประมาณในการดำเนินการสำหรับใช้จัดหาเครื่องมือและ อุปกรณ์ที่ทันสมัยเพื่อใช้ในการปฏิบัติงานและการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ บุคลากรให้มีประสิทธิภาพมากยิ่งขึ้น
3. ควรเพิ่มหลักสูตรการเรียนการสอนทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับอุดมศึกษา และระดับมหาวิทยาลัย
4. ควรมีการเน้นให้เห็นถึงความสำคัญในการพัฒนาทักษะของตนเอง เพื่อให้บุคลากรเกิดการเรียนรู้เพื่อ พัฒนาตนเองมากขึ้น รวมถึงการสำรวจความต้องการพัฒนาทักษะของบุคลากรเพื่อนำมาใช้ในแผนการพัฒนา บุคลากรตามปีงบประมาณ ซึ่งจะส่งผลให้การพัฒนาทักษะบุคลากรมีประสิทธิภาพและเป็นประโยชน์แก่หน่วยงาน
5. ควรมีการวางแผนการดำเนินงานตามภารกิจที่ชัดเจนในขอบเขตความรับผิดชอบ เพื่อให้บุคลากรได้ จัดสรรเวลาในการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
6. ควรเปิดกว้างทางโลกทัศน์ ไม่ว่าจะเป็นทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือทักษะ ความรู้ทางด้าน ๆ ที่นอกเหนือจากภารกิจที่ได้รับก็จะทำให้บุคลากรมีความรู้และทักษะที่หลากหลายมากยิ่งขึ้น

เอกสารอ้างอิง

- จันทร์รัตน์ แทนหลาบ. (2564). *การพัฒนาทักษะด้านเทคโนโลยีดิจิทัลเพื่อการปรับเปลี่ยนสู่การเป็นองค์กรดิจิทัล ของบุคลากรสำนักงานเลขาธิการ สำนักการระบายน้ำ กรุงเทพมหานคร.*
การค้นคว้าอิสระหลักสูตรประศาสนศาสตรมหาบัณฑิต, มหาวิทยาลัยรามคำแหง.
- ณภัทช์ฐันันต์ ศักดิ์เจริญกุล. (2562). *การเตรียมความพร้อมของบุคลากรภาครัฐไทยสู่การเป็นรัฐบาลดิจิทัล.*
วิทยานิพนธ์รัฐประศาสนศาสตรมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย.
- ณัฐกานต์ ปังศรีวงศ์. (2563). *การพัฒนาทักษะด้านการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อการจัดการ เรียนรู้ ในศตวรรษที่ 21 ของครูโรงเรียนตลาดหนองหวาย สังกัดสำนักงานเขตพื้นที่ การศึกษาประถมศึกษา สุราษฎร์ธานี เขต 2.* งานวิจัยการบริหารการศึกษา คณะครุศาสตร์. มหาวิทยาลัยราชภัฏสุราษฎร์ธานี.
- ธนพร นิธิฤทธิ. (2556). *การพัฒนาบุคลากรของสำนักงานคุมประพฤติประจำศาลแขวงพระนครใต้ กรมคุมประพฤติ.*
วิทยานิพนธ์รัฐประศาสนศาสตรมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย.
- เนตรชนก ดวนใหญ่. (2562). *การพัฒนาศักยภาพของบุคลากรในศาลอาญา ยุคดิจิทัล ประจำปี 2562.* การค้นคว้า อิสระหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต, มหาวิทยาลัยรามคำแหง.
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, พฤษภาคม 27). *ราชกิจจานุเบกษา,* 136(69ก), 28-30.

- ปรัชญา เฉลิมวัฒน์. (2561). *แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ*. วิทยานิพนธ์การป้องกันราชอาณาจักร, วิทยาลัยป้องกันราชอาณาจักร.
- วิฑิตา จันทรวารีเลขา. (2563). *แนวทางในการสนับสนุนการพัฒนาทักษะบุคลากรในการประยุกต์ใช้เทคโนโลยีดิจิทัล (Digital Savvy) ตามแผนงาน Digital Competency: กรณีศึกษา การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.)*. สารนิพนธ์หลักสูตรประกาศนียบัตรศาสตรมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย.
- วีณา พิงวิวัฒน์นิกุล. (2549). *เอกสารหมายเลข 239 ประกอบการบรรยาย วิชา สัมมนาปัญหาการบริหารทรัพยากรมนุษย์ในภาครัฐ (PA 449)*. กรุงเทพมหานคร: มหาวิทยาลัยรามคำแหง.
- โสภี วิวัฒน์ชาญกิจ. (2564). *การพัฒนาทักษะการใช้เทคโนโลยีสารสนเทศของบุคลากรทางการศึกษาเพื่อการบริหารงาน โรงเรียนกีฬานครนนท์วิทยา 6 จังหวัดนนทบุรี*. วารสารพุทธมัตต์ ศูนย์วิจัยธรรมศึกษา, ฉบับที่ 1 (มกราคม - มิถุนายน 2564), วิทยาลัยทองสุข, 190-200.
- สำนักงานคณะกรรมการการรักษาคความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2564). *เกี่ยวกับ สกมช.* ค้นเมื่อ 25 พฤษภาคม 2565, จาก <https://www.ncsa.or.th/about.html#about>
- สำนักงานคณะกรรมการการรักษาคความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2564). *รายงานประจำปี 2564* (พิมพ์ครั้งที่ 1). กรุงเทพมหานคร: สำนักพิมพ์สุขุมวิทการพิมพ์.
- สำนักงานคณะกรรมการพัฒนาเศรษฐกิจและสังคม, สำนักนายกรัฐมนตรี. (2559). *แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ. 2560-2564)*. ค้นเมื่อ 25 พฤษภาคม 2565, จาก https://www.nesdc.go.th/ewt_dl_link.php?nid=6422
- สำนักงานสภาพความมั่นคงแห่งชาติ. (2560). *ผลการดำเนินงานของสำนักงานสภาพความมั่นคงแห่งชาติ ประจำปีงบประมาณ 2562 และไตรมาสที่ 1 ประจำปีงบประมาณ 2563*. ค้นเมื่อ 25 พฤษภาคม 2565, จาก https://www.nsc.go.th/wp-content/uploads/2020/04/Performance62-and-Quarter1_63.pdf
- เอมิกา นัตกระโทก. (2564). *การพัฒนาทักษะดิจิทัลของบุคลากรในการปฏิบัติงานเพื่อรองรับการเปลี่ยนแปลงสู่องค์กรดิจิทัลของสำนักงานอัยการ ภาค 3*. การค้นคว้าอิสระหลักสูตรประกาศนียบัตรศาสตรมหาบัณฑิต, มหาวิทยาลัยรามคำแหง.