รายงานฉบับย่อ

โครงการขอรับการส่งเสริมและสนับสนุนจากเงินกองทุนวิจัยและพัฒนา
กิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ

(โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชน)

(นายสมทบ แก้วเชื้อ)

ได้รับทุนอุดหนุนจาก
กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ
(สำนักงาน กสทช.)

๒.๑ ชื่อ-สกุลผู้เขียนบทความ๑ นายสมทบ แก้วเชื้อ
หน่วยงานสังกัด มหาวิทยาลัยราชภัฏสวนสุนันทา
หมายเลขโทรศัพท์ ๐๒-๑๖๐-๑๐๙๐
Email:
ที่อยู่ปัจจุบัน
ชื่อ-สกุลผู้เขียนบทความ๒ นายสมิทธินันท์ ไทยรุ่งโรจน์
หน่วยงานสังกัด มหาวิทยาลัยราชภัฏสวนสุนันทา
หมายเลขโทรศัพท์ ๐๒-๑๖๐-๑๐๙๐
Email:
ที่อยู่ปัจจุบัน

บทคัดย่อ

ชื่อรายงานการวิจัย : โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความ มั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชน

ปีที่ทำการวิจัย : 2560

.....

รายงานวิจัยฉบับนี้ผู้วิจัยมีวัตถุประสงค์ในการวิจัยส่งเสริมบุคลากรในองค์กรขนาดเล็กหรือในระดับท้องถิ่น ชุมชน ประชาชนที่มีส่วนร่วมกับองค์กรให้มีตระหนักรู้ ความรู้ ความเข้าใจพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ศึกษารวบรวมปัญหาวิเคราะห์ความเสี่ยง ผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรขนาดเล็กหรือระดับท้องถิ่น ชุมชนและจัดทำข้อเสนอแนะเชิงนโยบายและตัวแบบจำลองสำหรับองค์กรขนาดเล็กหรือระดับท้องถิ่น ชุมชนในการผลักดันให้เกิดการป้องกันภัยคุกคามทางไซเบอร์อย่างเป็นระบบอย่างบูรณการ

กลุ่มประชากรที่ใช้ศึกษาครั้งนี้ คือ องค์การปกครองส่วนท้องถิ่น 7,835 แห่งโดยเป็นกลุ่มตัวอย่าง 1,500 ตัวอย่าง รวบรวมข้อมูลด้วยแบบสอบถามและสัมภาษณ์เชิงลึก 50 ตัวอย่าง

ผลการวิจัยพบว่ากลุ่มตัวอย่างขาดองค์ความรู้ ความเข้าใจถึงภัยคุกคามทางไซเบอร์ อาจทำให้เกิดการถูกโจมตีเป็นจำนวนมากและยากต่อการป้องกัน รวมทั้งการขาดแคลนเทคโนโลยีและความรู้ในการเฝ้าระวังภัยป้องกันและกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จากเป็นประเด็นสำคัญดังกล่าวทำให้จำเป็นต้องมีกิจกรรมแลกเปลี่ยนเรียนรู้ เผยแพร่และสร้างความตระหนักให้รู้เท่าทันภัยคุกคามทางไซเบอร์บุคลากรท้องถิ่น ประชาคม ประชาชนทั่วไปในชุมชน

การออกแบบระบบป้องกันภัยทางไซเบอร์ให้เหมาะสมกับการใช้งานและคำนึงถึงแนวคิดในการแบ่งกลุ่มตัวอย่างในแบบคลัสเตอร์ของหน่วยงานท้องถิ่นมาพิจารณาในการออกแบบระบบป้องกันภัยทางไซเบอร์

คำสำคัญ : ไซเบอร์,ความปลอดภัยไซเบอร์,องค์กรปกครองส่วนท้องถิ่น

Abstract

This research study aims to research. Extension personnel in smaller organizations or individuals in the local community who are involved with the organization to be aware of the basic knowledge and understanding of cyber security. Study the problems and risk analysis The impact of cyber security for small organizations or local level. Community and make recommendations about policy and a model for small organizations or local level. Communities to advocate for the prevention of cyber threats such as system integration.
This is a population-based study of local authorities by 7835 of a sample of 1,500 samples collected by questionnaire and interviewing 50 samples.

The study found that lack of knowledge. A better understanding of cyber threats. Can cause an attack are many and difficult to prevent. Including a lack of knowledge and technologies in the surveillance, prevention and legislation related to the Computer Crime.
The key is to make learning activities. Dissemination and awareness to intentionally cyber threats personnel, local communities, the general public in the community.

The Cyber defense systems designed to suit the user and taking into account the concept of dividing the sample in a cluster of local authorities into account in the design of cyber defense.

Keywords : Cyber,Cyber Security,Department of Local Adminstration

ความสำคัญของปัญหา

ความเจริญก้าวหน้าด้านเทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทในวิถีชีวิตของคนในยุคปัจจุบันเป็นอย่างยิ่ง ในขณะเดียวกันพบว่าปัญหาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ได้ทวีความเข้มข้นและมีความรุนแรงมากขึ้นตามลำดับ ซึ่งภัยคุกคามไซเบอร์มีทั้งในด้านความมั่นคงของประเทศ ด้านอาชญากรรมคอมพิวเตอร์ และด้านการละเมิดสิทธิส่วนบุคคล โดยมีแนวโน้มที่จะมีการขยายตัวเพิ่มขึ้นทุกระดับทั้งระดับชาติลงไปถึงระดับชุมชนทั่วประเทศ ส่งผลกระทบสร้างความเสียหายร้ายแรงต่อประเทศชาติทั้งในระดับองค์กร และระดับบุคคล ทั้งภาครัฐและภาคเอกชน ในส่วนของภาครัฐเอง ยังขาดความพร้อมในด้านรักษาความมั่นคงปลอดภัยทางไซเบอร์หลายด้าน ทั้งด้านโครงสร้างพื้นฐานและไม่มีหน่วยงานสนับสนุนการเฝ้าระวัง พร้อมเสนอแนะวิธีการป้องกันหรือแก้ปัญหาภัยคุกคามทางไซเบอร์

ด้วยความก้าวหน้าด้านทางเทคโนโลยีสารสนเทศและการสื่อสารช่วงระยะเวลา 10 ปีที่ผ่านมา เป็นแรงผลักให้ทุกหน่วยย่อยของสังคมไทยทั้งองค์กรภาครัฐ ผู้ประกอบการเอกชนตั้งแต่ระดับเล็ก ระดับกลางและระดับใหญ่ รวมไปจนถึงระดับประชาชนทั่วไป ให้ความสำคัญและพยายามเข้าถึงการใช้งานสารสนเทศ (Information) และใช้งานระบบการสื่อสารข้อมูล (Data Communication) ในรูปแบบต่าง ๆ ดังปรากฏในข้อมูลรายงานจำนวนปริมาณการใช้แบนด์วิดท์ (Internet Bandwidth) รวมทั้งประเทศ เปรียบเทียบตั้งแต่ปี 2543 ถึง ปี 2559 พบว่ามีการใช้อินเทอร์เน็ตที่มีปริมาณมากขึ้น 20,216 เท่า และอินเทอร์เน็ตระหว่างประเทศ 9,612 เท่า

ตารางเปรียบเทียบ การเติบโตของการใช้งานอินเทอร์เน็ตในประเทศไทย

ปี- เดือน	Total International Bandwidth(Mbps) แบนด์วิดท์ ไปต่างประเทศ	Total Domestic Bandwidth(Mbps) แบนด์วิดท์ในประเทศ
มค. 2543	115	360
มค. 2559	2,324,888	3,460,395

ข้อมูลจาก : **ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center)**

<u>บทบาทภาครัฐในการผลักดันให้เกิดการขยายตัวการใช้งานอินเทอร์เน็ต</u>

ตามที่นโยบายของภาครัฐบาลที่ต้องการผลักดันให้ประเทศไทยเข้าสู่สังคม ที่สร้างพลวัตรบนพื้นฐานเทคโนโลยดิจิทัลทุกๆด้านอย่างเต็มรูปแบบ ดังจะเห็นได้จากนโยบายดิจิทัลไทยแลนด์ 4.0 ด้วยนโยบายดังกล่าวทำให้ภาคเอกชน ประชาชน โดยเฉพาะหน่วยงานของภาครัฐเองเร่งดำเนินการเตรียมการเข้าสู่การเป็นรัฐบาลดิจิทัลเต็มรูปแบบ

จากความสำคัญดังกล่าวนี้ภาครัฐจึงได้ศึกษาแนวทางและได้กำหนดเป็นแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด ฉบับนำเสนอคณะรัฐมนตรี 5 เมษายน 2559 (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมปศุสัตว์, 2559) เพื่อใช้เป็น กรอบในการผลักดันให้เทคโนโลยีดิจิทัลเป็นกลไกสำคัญในการพัฒนาเศรษฐกิจและสังคมของประเทศ ซึ่งรวมถึงการปรับเปลี่ยนกระบวนทัศน์ทางความคิดใน ทุกภาคส่วนเพราะเทคโนโลยีดิจิทัลจะไม่ได้เป็นเพียง เครื่องมือสนับสนุนการทำงานเฉกเช่นที่ผ่านมาอีก ต่อไป จากนโยบายการผลักดันของรัฐบาลทำให้หน่วยงานของภาครัฐเองได้เริ่มดำเนินการเตรียมการเข้าสู่การเป็นรัฐบาลดิจิทัล โดยเฉพาะอย่างยิ่งหน่วยงานของภาครัฐระดับองค์กรขนาดเล็ก เช่น องค์กรปกครองส่วนท้องถิ่นได้มีการจัดทำ

แผนพัฒนาท้องถิ่น(กระทรวงมหาดไทย, 2559) การบริหารงานบุคคล การเงินการคลัง และการบริหารจัดการ เพื่อให้องค์กรปกครองส่วนท้องถิ่นมีความเข้มแข็งและมีศักยภาพในการให้บริการสาธารณะโดยการนำเทคโนโลยีดิจิทัลเข้ามาสนับสนุนมากยิ่งขึ้น อาทิเช่น ระบบแผนที่ภาษีและทะเบียนทรัพย์สิน (LTAX GIS และ LTAX 3000) ระบบบัญชีคอมพิวเตอร์ของกรมส่งเสริมการปกครองส่วนท้องถิ่น (Electronic Administration Accounting System)และระบบโครงข่ายพื้นฐานเพื่อชุมชน เป็นต้น ซึ่งขณะที่เร่งขับเคลื่อนเพื่อเข้าสู่การเป็นรัฐบาลดิจิทัลแต่กลับต้องเผชิญกับปัญหาความปลอดภัยของระบบสารสนเทศหรือปัญหาภัยคุกคามทางไซเบอร์ (ACIS Professional Center, 2559)รุนแรงมากขึ้นทุก ๆ ปี เริ่มตั้งแต่การถูกบุกรุกเข้าสู่ระบบคอมพิวเตอร์ในรูปแบบต่าง ๆ อาทิเช่น ไวรัสคอมพิวเตอร์ มัลแวร์ สปายแวร์ หนอนคอมพิวเตอร์ การแฮ็กเข้าสู่ระบบคอมพิวเตอร์ซึ่งเป็นปัญหาที่กระทบต่อระบบการสื่อสารและทำลายระบบฐานข้อมูล ซึ่งภัยคุกคามรูปแบบนี้มีมาเป็นระยะเวลานาน แต่ในระดับองค์กรขนาดเล็กหรือระดับท้องถิ่นยังไม่ได้ถูกแก้ไขอย่างมีระบบ ประกอบกับในช่วงระยะ 2 ปีที่ผ่านมา ปัญหาการกระทำความผิดในการนำเข้าข้อมูลที่ผิดกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ซึ่งกระทบต่อความมั่นคงของประเทศที่ปรากฏขึ้นเป็นจำนวนมาก

(ธวัชชัย ชมศิริ, 2553)ปัจจุบันการป้องกันภัยคุกคามยังต้องอาศัย Hardware และ software ของต่างประเทศ ซึ่งยังมีราคาค่อนข้างสูง การใช้งานค่อนข้างยาก แต่การป้องกันการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พบว่า Hardware และ software ของต่างประเทศมิได้รองรับในส่วนนี้ ถึงแม้ว่าในประเทศไทยเอง ได้เริ่มมีการพัฒนา Hardware และ software สำหรับการป้องกันภัยคุกคามทางไซเบอร์มาระยะหนึ่งแล้ว แต่ยังไม่ค่อยได้รับความนิยมมากนัก

สำหรับหน่วยงานของรัฐระดับองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน นั้น พบว่ายังขาดความพร้อมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในด้านความรู้ความเข้าใจ ด้านบุคลากร และด้านการพัฒนาเครื่องมือเพื่อป้องกันภัยคุกคามอย่างเป็นระบบ ดังนั้น มหาวิทยาลัยราชภัฏสวนสุนันทา จึงเล็งเห็นความสำคัญในการดำเนิน “โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชน” เพื่อการศึกษาวิจัย เพื่อวิเคราะห์ความเสี่ยง เพื่อพัฒนาเครื่องมือสารสนเทศสำหรับการป้องกันภัยคุกคามทางไซเบอร์ พร้อมทั้งสร้างความรู้ความเข้าใจให้แก่บุคลากรในองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน ซึ่งองค์กรปกครองส่วนท้องถิ่นน่าจะเป็นแบบอย่างหรือเป็นต้นแบบให้กับหน่วยงานหรือองค์กรขนาดเล็กในระดับชุมชนได้เป็นอย่างดี

โดยที่ผ่านมาทางมหาวิทยาลัยได้มีการวิจัยเรื่องรูปแบบและมาตรการแก้ไขปัญหาทางไซเบอร์ **(Model and measure of Solving Problem Cyber Crime)** (ณรงค์ กุลนิเทศและณิช, 2557) ซึ่งได้รับรางวัลวิจัยดีเด่นด้านวิทยาศาสตร์และเทคโนโลยี ในงานวิจัยมีแนวทางหลักที่สำคัญเพื่อป้องกันภัยคุกคามทางไซเบอร์และอาชญากรรมทางไซเบอร์ โดยสำหรับการพัฒนาเครื่องมือที่มีประสิทธิภาพนั้น ประกอบด้วยการค้นหา (Detection) การป้องกัน (Protection) การเตือนภัย (Response) การบันทึกข้อมูลจราจรคอมพิวเตอร์ (Record) โดยเฉพาะอย่างยิ่งสถิติจากงานวิจัยสำหรับองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน มีอาชญากรรมทางไซเบอร์สูงและมีการป้องกันภัยคุกคามไซเบอร์ที่ค่อนข้างต่ำกว่าองค์กรขนาดใหญ่หรือองค์กรในระดับประเทศ/ชุมชนเมือง ทั้งนี้ องค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชนนั้นยังขาดความพร้อมด้านบุคลากรและการพัฒนาเครื่องมือสำหรับป้องกันภัยคุมคามจึงควรต้องมีกระบวนการใช้งานและคู่มือที่ใช้งานได้ง่าย สะดวก เหมาะสม และมีประสิทธิภาพสูงสุด ซึ่งองค์กรปกครองส่วนท้องถิ่นน่าจะเป็นแบบอย่างหรือเป็นต้นแบบให้กับหน่วยงานหรือองค์กรขนาดเล็กในระดับชุมชนได้เป็นอย่างดี

คณะผู้วิจัย โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชน มีความสนใจในการศึกษาถึง

ปัญหาสำคัญที่มาจากการขับเคลื่อนนโยบายดิจิทัล ไทยแลนด์ 4.0 ใน 2 มิติด้วยกันคือ 1. การขับเคลื่อนของเทคโนโลยีดิจิทัลอาศัยการเชื่อมโยงข้อมูล (Data) ด้วยอินเทอร์เน็ต ซึ่งอยู่บนพื้นฐานความเสี่ยงต่อภัยคุกคามทางไซเบอร์ 2. มีความสนใจ ศึกษาความพร้อมขององค์กร หน่วยงานท้องถิ่นต่อปัญหาการถูกภัยคุกคามทางไซเบอร์เนื่องจาก เป็นหน่วยงานที่มีมากกว่า7,853 หน่วยงาน ครอบคลุมพื้นที่ภูมิภาคทั่วประเทศ เป็นหน่วยงานที่มีการบูรณาการ ส่วนราชการหลากหลายสายงานเข้าไปรวมอยู่ด้วยกัน เช่น มหาดไทย การศึกษา สาธารณสุข เกษตรฯ รวมถึง ภาคประชาชน อาทิกลุ่มอาชีพ ประชาชน

นอกจากนี้ยังสนใจศึกษาเจาะลึกไปถึงลักษณะการใช้เทคโนโลยีดิจิทัล ทั้ง การใช้งานอุปกรณ์คอมพิวเตอร์ ลักษณะการสื่อสารข้อมูล(Data) การรับส่งข้อมูลสำคัญระหว่างหน่วยงานกลางและ หน่วยงานท้องถิ่น การพัฒนาโปรแกรมสำเร็จรูปเพื่องานประเภทต่างๆ อาทิ งานระบบการเงินบัญชี งานด้านแผนที่ภาษีที่ต้องสัมพันธ์เชื่อมโยงกับราชการส่วนกลาง ไปจนถึงการเตรียมความพร้อมในการป้องกันภัยคุกคามทางไซเบอร์ ทั้งความพร้อมด้าน ฮาร์ดแวร์ ซอฟแวร์ และการวางระบบเครือข่ายภายในรูปแบบต่างๆ ของหน่วยงานท้องถิ่น

เพื่อนำลักษณะการใช้เทคโนโลยีดิจิทัลในชุมชนไปสู่การวิเคราะห์ความเหมาะสมในการพัฒนาเครื่องมือการป้องกันภัยคุกคามทางไซเบอร์ พร้อมทั้งสร้างความรู้ความเข้าใจให้แก่บุคลากรในองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน ซึ่งองค์กรปกครองส่วนท้องถิ่นน่าจะเป็นแบบอย่างหรือเป็นต้นแบบให้กับหน่วยงานหรือองค์กรขนาดเล็กในระดับชุมชนโดยคณะผู้วิจัยฯได้กำหนดไว้ในวัตถุประสงค์ของโครงการฯดังนี้

1.เพื่อส่งเสริมบุคลากรในองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชนรวมถึงประชาชนทั่วไปที่มีส่วนร่วมกับองค์กรให้มีความตระหนักรู้ ความรู้ ความเข้าใจพื้นฐานทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2.เพื่อศึกษาและรวบรวมปัญหาวิเคราะห์ความเสี่ยงและผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน

3.เพื่อจัดทำข้อเสนอแนะเชิงนโยบายและตัวแบบจำลองสำหรับองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชนในการผลักดันให้เกิดการป้องกันภัยคุกคามทางไซเบอร์อย่างเป็นระบบอย่างบูรณาการ

วิธีการศึกษา

ในขั้นแรก คณะผู้วิจัย โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชน ดำเนินการดังนี้

1. กระบวนการในการวิจัย (Methodology) โดยคณะผู้วิจัย รวบรวมข้อมูลทั้งประเภทเอกสารและข้อมูลจากการสื่อสารผ่านบุคคลต่างๆเพิ่มเติมจากหน่วยงานราชการส่วนกลางพร้อมทำบันทึกความร่วมมือกับหน่วยงานท้องถิ่นเพื่อเตรียมลงพื้นที่สำรวจข้อมูล และ ทบทวนความถูกต้องของข้อสันนิษฐานที่ตั้งไว้ก่อนปฏิบัติงานจริง

การวิจัยในโครงการนี้ เนื่องจากเป็นการวิจัยที่มุ่งเน้นศึกษา องค์กรขนาดเล็กในระดับชุมชน เป็นการวิจัยที่ให้ความสำคัญกับ การศึกษา พฤติกรรมของ ชุมชน องค์กร การใช้เทคโนโลยี จึงเป็นการ**วิจัยทางสังคมศาสตร์ (Social research)** ที่อาศัยเนื้อความรู้ด้านเทคโนโลยีเป็นส่วนประกอบและสนับสนุนผลการวิจัยในตอนท้ายโดยวิธีการรวบรวมข้อมูลการวิจัยจากสำรวจจากตัวอย่าง (Sample survey research) ประกอบกการสังเกต (Observation research)

2. สร้างแผนปฏิบัติงาน (Action Plan) กำหนดแผนการระยะเวลาในการดำเนินการวิจัย ซึ่งคณะผู้วิจัยกำหนดกรอบการดำเนินการวิจัยออกเป็น 2 ด้านด้วยกันคือ

2.1 แผนการปฏิบัติงานโครงการตามกรอบการรายงานของ กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ ซึ่งกำหนดเป้าหมายไว้ 5 ประการด้วยกัน คือ 1.นำเสนอรายงานแผนการดำเนินงาน 2.สำรวจการใช้งานระบบเทคโนโลยีสารสนเทศของท้องถิ่น 3.การศึกษาวิเคราะห์ผลการสำรวจ พร้อมแนวทางการวิจัยพัฒนาระบบเครือข่ายความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน/รายงานผลพร้อมตัวแบบจำลอง 4.จัดเสวนาแลกเปลี่ยนเรียนรู้ เผยแพร่ และสร้างความตระหนักให้รู้เท่าทันภัยคุกคามทางไซเบอร์ 5.จัดทำข้อเสนอแนะเชิงนโยบาย และเอกสารแนวทางในการพัฒนาอุปกรณ์ป้องกันภัยคุกคามข้อมูลสารสนเทศที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน/นำเสนอผลการดำเนินงานโครงการ

2.2 กระบวนการปฏิบัติงานด้านต่างๆอย่างละเอียด โดยหัวหน้าคณะวิจัยฯประชุมหารือคณะผู้วิจัยถึงรายละเอียดเกี่ยวกับงานต่างๆ เพื่อให้คณะผู้วิจัย และ บุคคลที่เกี่ยวข้อง สามารถนำไปปฏิบัติงานส่วนต่างๆ ได้อย่างมีประสิทธิภาพจริง

3. ขั้นตอนของการลงพื้นที่สำรวจ คณะผู้วิจัยได้ดำเนินการได้ดำเนินการสำรวจการใช้งานระบบเทคโนโลยีสารสนเทศของท้องถิ่นในด้านต่างๆทั้งปัญหาภัยคุกคามทางไซเบอร์ของท้องถิ่น วิธีการแก้ไขปัญหา รวมถึงอุปสรรค์และข้อจำกัดต่างๆขององค์กรขนาดเล็กจำนวน 1,000 กลุ่มตัวอย่างโดยคณะดำเนินการได้ทำการเก็บรวบรวมข้อมูลได้จากกลุ่มตัวอย่างทั่วประเทศได้ทั้งสิ้น 1,500 กลุ่มอย่าง และได้ทำการคัดเลือกตัวแทนเพื่อทำการสัมภาษณ์เชิงลึกกับผู้เกี่ยวข้องลงโดยการลงพื้นที่ทั้งวิธีการสนทนาซักถามประเด็นที่เกี่ยวข้องและตอบแบบสัมภาษณ์และคัดเลือกกลุ่มตัวอย่างในการดำเนินการพัฒนาเครื่องมือและระบบในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรปกครองส่วนท้องถิ่น จำนวน 50 แห่งโดยการสอบถามมุ่งประเด็นหลักๆ ดังนี้ 3.1 ข้อมูลทั่วไปเกี่ยวกับการใช้คอมพิวเตอร์และระบบอินเทอร์เน็ต 3.2 สรุปข้อมูลการใช้งานระบบเทคโนโลยีระบบสารสนเทศภายในองค์กร 3.3 แบบทดสอบความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ4.4สถานภาพด้านการรักษาความมั่นคงปลอดภัยสารสนเทศภายในองค์กร 3.5แบบทดสอบความรู้เกี่ยวกับด้านกฎหมาย ว่าด้วยการกระทำผิด พรบ. เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

4. การศึกษาวิเคราะห์ผลการสำรวจ เป็นขั้นตอนของการสรุปและวิเคราะห์ผลที่ได้จาก การสำรวจจากกลุ่มตัวอย่าง และ การสัมภาษณ์เชิงเลิก รวมถึงคณะผู้วิจัย ลงพื้นที่ในหลายๆแห่ง เพื่อ หาข้อมูลจากการสังเกต (Observation research)

ภาพการลงพื้นที่ เพื่อเก็บรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกและรวบรวมข้อมูลการใช้เทคโนโลยีดิจิทัลชุมชน

5.จัดเสวนาแลกเปลี่ยนเรียนรู้ เผยแพร่ และสร้างความตระหนักรู้ โดยออกแบบในรูปแบบกิจกรรมการรับฟังความคิดเห็นจากการเสวนาแลกเปลี่ยนเรียนรู้ เผยแพร่ และสร้างความตระหนักให้รู้เท่าทันภัยคุกคามทางไซเบอร์บุคลากรท้องถิ่น / ประชาคม /ประชาชนทั่วไป ที่เกี่ยวข้องในชุมชน เพื่อการเผยแพร่ให้ความรู้เบื้องต้น โดยแบ่งได้เป็น 2 ประเด็นหลัก คือ (1) การเผยแพร่ความรู้มุ่งเน้นการจัดเก็บข้อมูลการจราจรทางอินเทอร์เน็ต 90 วัน ตาม พรบ. เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ถึงความจำเป็นในการปฏิบัติตาม

พรบ. ดังกล่าว หากไม่ดำเนินการมีบทลงโทษระบุไว้ตาม พรบ. และ (2) การรับฟังความคิดเห็นต่อร่างต้น

การจัดเสวนา ในโครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชน จัดขึ้นโดยกำหนดชื่อโครงการ เสวนา “โครงการเผยแพร่ความรู้และสร้างความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์สำหรับองค์กรขนาดเล็กระดับชุมชนและประชาชนทั่วไป

6.จัดทำข้อเสนอแนะเชิงนโยบาย และเอกสารแนวทางในการพัฒนาอุปกรณ์ป้องกันภัยคุกคามข้อมูลสารสนเทศที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชนเพื่อนำไปสู่การเสนอผลการดำเนินงานโครงการซึ่งคณะผู้วิจัยฯ เสนอแนวทางการศึกษาและพัฒนาระบบป้องกันความปลอดภัยทางไซเบอร์ในอนาคต ควรมุ่งให้ความสำคัญกับการพัฒนาวิธีวิทยา (Methodology) บนข้อจำกัดของพื้นที่ทางวัฒนธรรมที่มีความแตกต่างหลากหลายความไม่เท่าเทียมกันของหน่วยงานท้องถิ่น ให้ความสำคัญกับการศึกษาโดยการแบ่งการศึกษาเป็นรายคลัสเตอร์ เพื่อเฉพาะเจาะจงให้เกิดรูปธรรมที่มีความชัดเจนโดยเสนอกรอบแนวคิด การพัฒนาเครื่องมือเฝ้าระวังความปลอดภัยทางไซเบอร์โดยให้กำหนดพื้นที่ตามลักษณะภูมิศาสตร์(Geography)ประกอบภูมิรัฐศาสตร์(GeoPolitics) และลักษณะพื้นที่ทางวัฒนธรรม(Cultural heritage area) ที่มีความแตกต่างและหลากหลาย เช่นวัฒนธรรมประมง วัฒนธรรมนาข้าวภาคอีสาน หรือพื้นที่ทางศาสนา โดยทั้งประเทศอาจแบ่งได้ประมาณ 30 คลัสเตอร์

ผลการศึกษา

วิเคราะห์ความเสี่ยงและผลกระทบจากแบบสอบถามของกลุ่มตัวอย่าง 1,500 คนสะท้อนถึงปัญหาจำนวน 4 ประเด็นได้ดังนี้

<u>ประเด็นที่ 1 การให้องค์ความรู้เกี่ยวกับ Cyber Security</u>

ผลการสำรวจพบว่าบุคลากรขาดองค์ความรู้ ขาดความเข้าใจเป็นสำคัญ ส่งผลกระทบให้ไม่ทราบถึงภัยคุกคามทางไซเบอร์ที่มีอยู่ภายในองค์กร อาจส่งผลกระทบถึงระดับประเทศได้ เนื่องจากองค์กรระดับท้องถิ่นมีช่องโหว่ในการถูกโจมตีได้ง่าย และมีเป็นจำนวนมากยากต่อการป้องกันทั้งหมด

<u>ประเด็นที่ 2 การขาดแคลนทรัพยากรและงบประมาณ</u>

การขาดแคลนเทคโนโลยี อาทิ เช่น ระบบ antivirus รวมไปถึงการอัพเดทโปรแกรม antivirus อย่างสม่ำเสมอ ระบบบริหารจัดการการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ระบบ Firewall เป็นต้น โดยระบบต่างๆ จึงมีความจำเป็นต้องกระทำควบคู่ไปกับการเสริมสร้างองค์ความรู้ เพื่อเป็นการป้องกันอย่างรวดเร็ว เพื่อไม่ให้ส่งผลกระทบในวงกว้าง

<u>ประเด็นที่ 3 พฤติกรรมการใช้งานคอมพิวเตอร์</u>

การใช้งานคอมพิวเตอร์ของบุคลากรมีความเสี่ยง เนื่องจากขาดความเข้าใจในการเข้ารหัสข้อมูลองค์กร การบริหารจัดการข้อมูลองค์กรอย่างมีประสิทธิภาพ การป้องกันข้อมูลรั่วไหลสู่มิจชีพหรือผู้ไม่ประสงค์ดีก็ตาม โดยในส่วนนี้ ควรกระทำควบคู่ไปกับการเสริมสร้างองค์ความรู้

<u>ประเด็นที่ 4 พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐</u>

บุคลากรยังขาดความรู้ความเข้าใจใน พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งรวมไปถึงประชาชนในท้องถิ่นด้วย จึงอาจมีความเสี่ยงในกระทำความผิดต่อ พ.ร.บ. ดังกล่าวเนื่องจากขาดความรู้ความเข้าใจในการเฝ้าระวังเรื่องดังกล่าว รวมไปถึงการหาวิธีป้องกัน/เครื่องมือและบริหารจัดการการใช้งานคอมพิวเตอร์ผ่านอินเทอร์เน็ต

ผลการสัมภาษณ์โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชนคณะผู้วิจัยฯ ได้รับทราบข้อมูลเชิงลึกเกี่ยวกับปัญหาอุปสรรค์ ต่างๆของท้องถิ่นดังนี้

ระบบสารสนเทศขององค์กรปกครองส่วนท้องถิ่นในปัจจุบัน

1. ระบบสารสนเทศที่มีอยู่ในปัจจุบัน อาทิเช่น โปรแกรมและระบบต่างๆหน่วยงานมีอุปกรณ์หรือเครื่องมือสนับสนุนการปฏิบัติงาน แต่บุคลากรยังขาดองค์ความรู้ ขาดความเชี่ยวชาญเฉพาะด้าน ทำให้การใช้ระบบสารสนเทศไม่มีประสิทธิภาพ นอกจากนี้ยังพบว่าหน่วยงานไม่มีระบบ ในการป้องกันภัยคุกคามทางไซเบอร์ มีเพียงระบบสารสนเทศเพื่อการปฏิบัติงานเท่านั้น

2. ปัญหา อุปสรรคจากการที่บุคลากรขาดความชำนาญในการใช้เครื่องมือ ประกอบกับการใช้งานของระบบสารสนเทศต่างๆ มีความยุ่งยากซับซ้อนจนเกินไป เครือข่ายอินเทอร์เน็ตไม่เสถียรหรือไม่เพียงพอต่อการใช้งาน จากปัจจัยสะท้อนให้เห็นถึงปัญหาอุปสรรคหลักๆ 3 ปัจจัย ได้แก่ บุคลากร (Human) องค์ความรู้ (Knowledge) โครงข่าย (Infra Structure) และยังพบความต้องการของผู้ใช้งาน (User) ในระดับองค์กรท้องถิ่นขนาดเล็ก มีความต้องการใช้งานเครื่องมือหรือระบบสารสนเทศที่ไม่มียุ่งยากซับซ้อนจนเกินไปเน้นการใช้งานที่ง่ายและรวดเร็ว ทั้งนี้ต้องมีความปลอดภัยสำหรับผู้ใช้งานและข้อมูลที่ใช้รับ-ส่งในการใช้งาน รวมไปถึงความต้องการบุคลากรผู้เชี่ยวชาญในแต่ละด้าน ได้แก่ ด้านสารสนเทศ ด้านความปลอดภัยข้อมูลสารสนเทศ

จากการสำรวจ องค์กรปกครองส่วนท้องถิ่น พบว่า ปัจจุบันมีการใช้งาน ระบบเครือข่ายคอมพิวเตอร์หลักๆ 4 รูปแบบด้วยกันคือ

1. ใช้ในการพิมพ์เอกสารและจัดเก็บข้อมูล เช่น เอกสารการเบิกจ่ายและฎีกาต่างๆ ซึ่ง จัดเก็บทั้งในรูปแบบ กระดาษ และ สแกนเป็นไฟล์ภาพ ไว้ใน คอมพิวเตอร์สำนักงาน ประจำตัวเจ้าหน้าที่ การคลัง พัสดุ นอกจากนี้ ในส่วนของแบบ แปลน ขออนุญาต ก่อสร้างต่างๆของ ฝ่ายช่าง ปัจจุบัน ส่วนใหญ่ยังคงเก็บในรูปของ กระดาษ เป็นหลัก

2. ใช้ในการสื่อสารข้อมูลกับส่วนงานที่เกี่ยวข้อง เช่น การรับส่ง อีเมล์ หรือสอบถาม ปัญหาการทำงาน ในกรณีที่ ท้องถิ่น ไม่สามารถคลี่คลายปัญหาต่างๆได้ด้วยตนเอง เช่น ปัญหาการลงบันทึก ภาษีในระบบแผนที่ภาษี ฝ่ายการคลัง ของหน่วยงาน จำเป็นต้อง สอบถามข้อมูล เชิงลึกกับ เจ้าหน้าที่ที่เกี่ยวข้องของกรมส่งเสริมการปกครองส่วนท้องถิ่นโดยตรง

3. การส่งรายงานกับหน่วยงานต้นสังกัดผ่านโปรแกรมสำเร็จรูป ครอบคลุมส่วนงาน 6 ฝ่ายด้วยกัน คือ 1.สำนักงานปลัด 2.ส่วนการคลัง 3.ส่วนโยธา 4.ส่วนการศึกษาและวัฒนธรรม 5.ส่วนสวัสดิการสังคม 6.ส่วนสาธารณสุขและสิ่งแวดล้อม โดยภายในองค์กรปกครองส่วนท้องถิ่นมีการจัดองค์กรตามแบบ แผนกงานตามหน้าที่ (Departmentation by Function) ซึ่งได้แบ่งหน้าที่หลักๆ ออกจากกันชัดเจน แต่รับผิดชอบต่อเป้าหมายที่ควบคุมโดยผู้นำสูงสุดอันได้แก่นายกฯขณะเดียวกัน ส่วนงานทั้ง 6 ด้าน ในฐานะเป็นข้าราชการประจำถูกกำหนด หน้าที่ ในการ รายงานความคืบหน้าของการปฏิบัติงานในตำแหน่งของตนเอง ไปยัง ส่วนงานต่างๆ ของกรมส่งเสริมการปกครองส่วนท้องถิ่น ส่วนกลาง ซึ่งเป็นรูปแบบ **การจัดองค์กรแบบแมทริกซ์ (Matrix organization)** โดยข้าราชการท้องถิ่น ขึ้นตรงและรายงานสายการบังคับบัญชา **2** สาย

การรายงานความคืบหน้าและผลปฏิบัติงานในท้องถิ่นสู่ส่วนกลางปัจจุบัน ทำผ่านโปรแกรมสำเร็จรูป

ได้แก่

1 โปรแกรม ระบบบัญชีคอมพิวเตอร์ของกรมส่งเสริมการปกครองท้องถิ่น (Electronic Administration Accounting System : e-LAAS) ซึ่งเจ้าหน้าที่คลัง มีหน้าที่ต้องส่งรายงานผ่านอินเทอร์เน็ตเพื่อสรุปรายงานงบประมาณทั้ง รายวัน รายเดือน และ รอบปีงบประมาณ โดยปัจจุบัน ระบบเสร็จสมบูรณ์องค์กรปกครองส่วนท้องถิ่นทุกแห่ง ใช้ระบบนี้เสร็จสมบูรณ์แล้ว

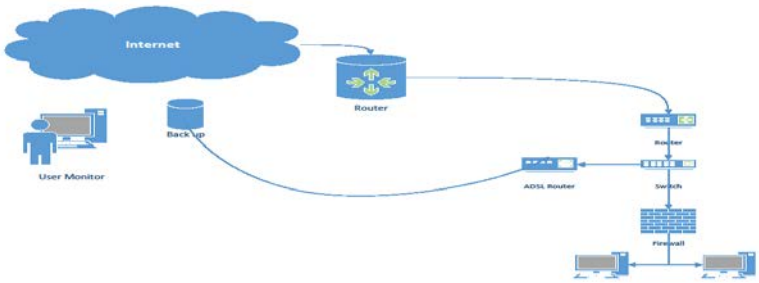
2 โปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สินและโปรแกรมประยุกต์ระบบสารสนเทศภูมิศาสตร์ (LTAX 3000 และLTAX GIS) เป็นโปรแกรมบันทึก และวิเคราะห์ข้อมูล ที่เกี่ยวข้องกับภาษีท้องถิ่นประเภทต่างๆ เช่น ป้าย โรงเรือน ที่ดิน และการคำนวณภาษีตามกฎหมาย

3. การให้บริการ อินเทอร์เน็ตแก่ประชาชน ซึ่ง ผู้ให้บริการอินเทอร์เน็ต(ISP)ส่วนใหญ่จะเชื่อมโยงระบบเครือข่ายไปถึงหน่วยงานองค์กรปกครองส่วนท้องถิ่นยังไม่ขยายบริการไปยังโรงเรียนหรือบ้านเรือนของประชาชนทั่วไปหน่วยงานท้องถิ่นในหลายพื้นที่ จึงจำเป็นต้องแบ่งปันการใช้งานอินเทอร์เน็ต เพื่อให้บริการแก่ประชาชนในพื้นที่อย่างหลีกเลี่ยงไม่ได้ซึ่งการให้บริการอินเทอร์เน็ตแก่ประชาชนภายนอก ทางองค์กรปกครองส่วนท้องถิ่นจะไม่ได้ติดตั้งระบบรักษาความปลอดภัยใดๆ

รูปแบบการเชื่อมต่อเครือข่ายอินเทอร์เน็ตภายในหน่วยงานท้องถิ่น

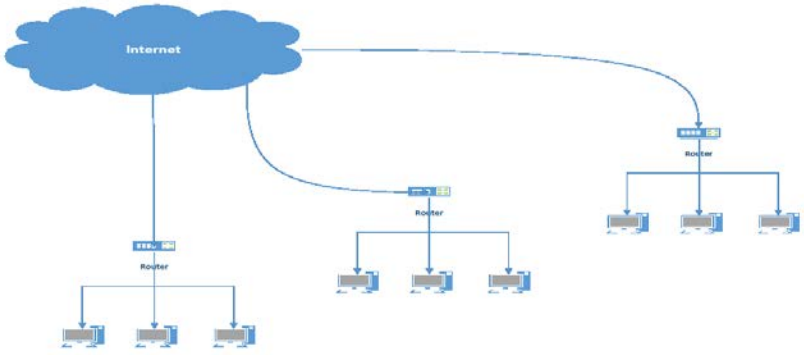
จากการลงพื้นที่สำรวจและสอบถาม อบต./เทศบาล จำนวน 30 แห่ง โดยคณะทำงานคัดเลือกกลุ่ม อบต./เทศบาลขนาดเล็กเป็นส่วนใหญ่ เพื่อให้ทราบถึงปัจจัยแวดล้อมต่างๆ รวมไปถึงการใช้งานอินเทอร์เน็ตและการวางระบบโครงข่ายขององค์กรขนาดเล็กในท้องถิ่น โดยคำนึงถึงด้านการใช้งานเทคโนโลยีสารสนเทศและการใช้งานอินเทอร์เน็ตที่มีความเสี่ยงสูงต่อภัยคุกคามทางไซเบอร์ ด้านบุคลากรที่ยังขาดความพร้อมสำหรับการป้องกันภัยคุกคามทางไซเบอร์เป็นหลัก ซึ่งการวางระบบโครงข่ายขององค์กรขนาดเล็กในท้องถิ่น อาจจะแบ่งได้หลักๆ 2 รูปแบบ

1) อบต./เทศบาล ขนาดเล็กที่อยู่ในพื้นที่เขตเมืองหรือมีประชาชนในพื้นที่ค่อนข้างสูง จะมีการวางระบบโครงข่ายขององค์กรที่มีการป้องกันระดับนึง โดยมีการติดตั้ง firewall แต่ยังพบว่าการอัพเดท software ไม่ได้ดำเนินการยังสม่ำเสมอ



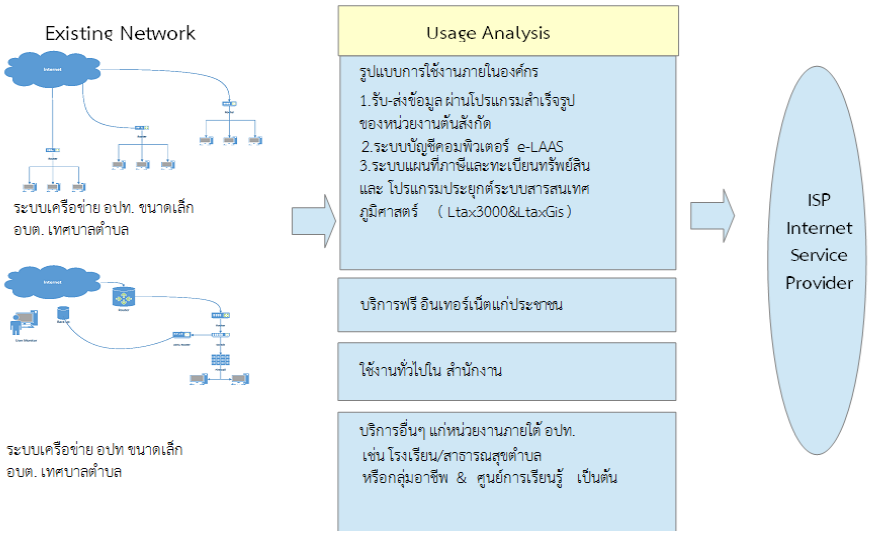
ภาพตัวอย่างการวางระบบโครงข่ายขององค์กรขนาดเล็กที่อยู่ในพื้นที่เขตเมือง

2) อบต./เทศบาล ขนาดเล็กที่อยู่ในพื้นที่เขตชานเมือง ระบบเครือข่ายมีเพียงการติดตั้ง Router แบบ 4 port ที่ติดตั้งโดยผู้ให้บริการอินเทอร์เน็ต(ISP)โดยเชื่อมต่อตรงกับคอมพิวเตอร์ภายในหน่วยงานได้



ภาพตัวอย่างการวางระบบโครงข่ายขององค์กรขนาดเล็กที่อยู่ในพื้นที่ชานเมือง

ดังนั้นโดยภาพรวม หน่วยงานท้องถิ่นโดยส่วนใหญ่ ปัจจุบันใช้อินเทอร์เน็ตในการรับส่งข้อมูลสำคัญ ทั้ง โปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สิน(LTAX3000 &LTAXGIS)และโปรแกรมระบบบัญชีคอมพิวเตอร์ (e-laas)พร้อมๆกับการใช้งานด้านอื่นๆ รวม การให้บริการแก่ประชาชนที่มีความจำเป็น ในพื้นที่ โดยยังขาดระบบป้องกันความปลอดภัยทางไซเบอร์ดัง แผนที่ แสดงพันธกิจของหน่วยงานท้องถิ่น กับระบบเครือข่ายปัจจุบัน



ภาพรวมข้อมูลการใช้งานระบบเครือข่ายและการป้องกันความปลอดภัยทางไซเบอร์

จากภาพการใช้ระบบสารสนเทศ และปัญหาด้านความปลอดภัย ของหน่วยงานท้องถิ่นสามารถสรุปได้แต่ละประเด็นดังนี้

1.การให้บริการอินเทอร์เน็ตในระดับท้องถิ่น ไม่ครอบคลุม ทำให้หน่วยงานท้องถิ่นจำเป็นต้องเป็นจุดให้บริการ แก่ ประชาชน

2. การเชื่อมต่อระบบอินเทอร์เน็ต ในหน่วยงานท้องถิ่น เป็นบริการ อินเทอร์เน็ตพื้นฐานโดยทั่วไปจากผู้ให้บริการ (ISP) ไม่ได้มีการติดตั้งอุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์

3. การให้บริการอินเทอร์เน็ต แก่ บุคคลภายนอก ของหน่วยงานท้องถิ่นไม่ได้ติดตั้งระบบการพิสูจน์ตัวตน (Authentication)

4. หน่วยงานท้องถิ่นมีพันธกิจ เชื่อมโยงกับ กรมส่งเสริมฯซึ่งเป็นต้นสังกัดในการ รายงานข้อมูลผ่านโปรแกรมสำเร็จรูปที่พัฒนาขึ้นมาโดยเฉพาะในงานแต่ละด้าน เช่น ระบบบัญชีคอมพิวเตอร์ และ ระบบแผนที่ภาษีและทะเบียนทรัพย์สิน และโปรแกรมประยุกต์ระบบสารสนเทศภูมิศาสตร์

5. การรับส่งข้อมูล สำคัญ ระหว่าง หน่วยงานกลางกับ ท้องถิ่นด้วยโปรแกรมสำเร็จรูปที่พัฒนาขึ้นผ่านเครือข่ายอินเทอร์เน็ตไม่ได้ ติดตั้งระบบความปลอดภัยรูปแบบต่างๆเพื่อใช้ระหว่างการรับส่งเช่น การติดตั้ง Private Network

6.หน่วยงานต้นสังกัด ขาดการสนับสนุนด้านเทคโนโลยีเพื่อการป้องกันภัยทางไซเบอร์

7. ขาดแคลน งบประมาณ ที่มุ่งเป้าหมายมาที่ ระบบป้องกัน

8. ขาดแคลนบุคลากรด้านเทคโนโลยีสารสนเทศ

9.ขาดความรู้ ความเข้าใจ ความตระหนัก ในภัยคุกคามทางไซเบอร์

จากประเด็นการใช้ระบบสารสนเทศ และปัญหาด้านความปลอดภัย ของหน่วยงานท้องถิ่นสามารถชี้บ่งกระบวนการด้านการจัดการความมั่นคงปลอดภัยทางไซเบอร์(Broderick J.S., 2006)ที่สำคัญที่ไว้ ๔ ประเด็น ได้แก่

1. สถานการณ์ความเสี่ยง(Risk Assessment)
2. ผลกระทบต่อท้องถิ่น(Threat&Vulnerability Analysis)
3. ความต้องการของท้องถิ่น(User Requirements)
4. แนวทางการพัฒนาระบบ(Security Policy Design)

ซึ่งเป็นแนวทางในการการวิเคราะห์กลไกด้านความปลอดภัย(Security Mechanism Ananlysis) จนพัฒนาเป็นกลไกด้านความปลอดภัย(Security Mechanism Design) ซึ่งสรุปได้ดังนี้

<u>ด้านบุคลากร(Man Power)</u>

หน่วยงานท้องถิ่นขาดบุคลากรที่มีความรู้และความชำนาญในการใช้งาน อุปกรณ์ป้องกันภัยคกคามทางไซเบอร์ ระบบสารสนเทศต่างๆ มีความยุ่งยากซับซ้อนต้องอาศัยคณะทำงานที่มีความชำนาญเฉพาะทางสนับสนุนให้เกิดเป็นรูปธรรมปัญหาด้านบุคลากรส่งผลโดยภาพรวมให้หน่วยงานท้องถิ่นขาดความตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ไปด้วยเป็นความเสี่ยงที่ส่งผลกระทบทำให้ขาดความตระหนักถึงการให้ความสำคัญกับนโยบายการรักษาความปลอดภัยทางไซเบอร์ ทำให้เกิดช่องว่างในการถูกโจมตีได้ง่ายรวมทั้งไม่ทราบถึงภัยคุกคามที่มีอยู่ภายในองค์กร อาจส่งผลกระทบถึงระดับประเทศได้ เนื่องจากองค์กรระดับท้องถิ่นมีช่องโหว่ในการถูกโจมตีได้ง่ายทำให้เข้าใจถึงที่มาปัญหาและสามารถนำไปปรับปรุงเพิ่มพัฒนาระบบการรักษาความปลอดภัยที่เหมาะสมกับ หน่วยงานท้องถิ่นซึ่งหน่วยงานท้องถิ่นมีความต้องการที่จะเพิ่มศักยภาพบุคลากรให้มีความรู้ด้านสารสนเทศและความปลอดภัยทางไซเบอร์เพื่อสนับสนุนให้การใช้เทคโนโลยีสารสนเทศในท้องถิ่นมีประสิทธิภาพมากยิ่งขึ้นและมีคณะดำเนินงานในการให้คำปรึกษา ด้านระบบสารสนเทศ และความปลอดภัยทางไซเบอร์เนื่องจากปัจจุบัน หน่วยงานต้นสังกัดสนับสนุนเพียงการพัฒนาและฝึกอบรมการใช้โปรแกรมสำเร็จรูปเฉพาะทางแต่ยังไม่มี ทีมงานดูแลระบบสารสนเทศให้ท้องถิ่น

ดังนั้นคณะผู้วิจัยจึงเห็นว่าควรพัฒนาศักยภาพด้านการการใช้เครื่องมือสารสนเทศ ทั้งความรู้ด้านการป้องกันภัยคุกคามทางไซเบอร์ การดูแลรักษาอุปกรณ์ และความรู้เบื้องต้นเกี่ยวกับระบบเครือข่ายรวมทั้ง

ปลูกฝังความตระหนักต่อมาตรการณ์รักษาความปลอดภัยของระบบคอมพิวเตอร์ซึ่งเป็นการพัฒนาบุคลากรสู่ความเป็นเลิศด้านความมั่นคงปลอดภัยทางไซเบอร์และพัฒนาองค์กรตามแนวทางมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศโดยอยู่ภายใต้แนวทางปฏิบัติของกรมส่งเสริมการปกครองส่วนท้องถิ่น

<u>ด้านการจัดการ</u>(Management)

การขาดการจัดทำข้อมูลพื้นฐานที่มีความสำคัญต่อระบบความปลอดภัยทางไซเบอร์ ได้แก่ แผนผังเชื่อมโยงระบบเครือข่ายของหน่วยงานท้องถิ่น(Network Diagram)ทำให้หน่วยงานท้องถิ่นไม่สามารถวิเคราะห์และแก้ไขปัญหาที่เกิดขึ้น ในกรณีที่ ระบบเครือข่ายคอมพิวเตอร์ในหน่วยงานมีปัญหาจึงมีความต้องการให้จัดทำแบบแผนผังการเชื่อมโยงเครือข่าย(Network Diagram) ที่เหมาะสมเพื่อพร้อมในการพัฒนาไปสู่การติดตั้งอุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์ ดังนั้นคณะดำเนินงานจึงจัดทำแผนผังการเชื่อมโยงเครือข่ายการใช้งานพร้อมทั้งเสนอแนะแนวทางปรับปรุงแก้ไข ระบบเครือข่ายให้มีความเหมาะสมเพื่อรองรับการติดตั้งอุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์ โดยสามารถวิเคราะห์เกี่ยวกับเครื่องมือที่เกี่ยวข้องในการเชื่อมต่อระบบเครือข่ายทั้งหมด/เครือข่ายการรับส่งข้อมูลทั้งภายในและภายนอกแสดง Internet Address สำหรับอุปกรณ์ที่มีการต่อเชื่อมทั้งหมดในองค์กรออกมาเป็นแผนผังการเชื่อมต่อและระบบเครือข่ายในการใช้งาน

<u>ด้านงบประมาณและเครื่องมือ(Money&Material)</u>

การขาดงบประมาณในการมุ่งเป้าไปที่ระบบความปลอดภัยทางไซเบอร์ ส่งผลกระทบต่อ การส่งเสริมการใช้อุปกรณ์ระบบความปลอดภัยทางไซเบอร์ อันได้แก่

๑.ไม่มีระบบบริหารจัดการการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

๒.ขาดการติดตั้งระบบป้องกันการบุกรุกระหว่างเครือข่ายภายในและภายนอกเช่น ระบบป้องกันไวรัส (antivirus) รวมไปถึงการอัพเดทโปรแกรมป้องกันไวรัส (antivirus) อย่างสม่ำเสมอ ระบบ Firewall เป็นต้น ทำให้เกิดการหยุดชะงักของระบบสารสนเทศภายในหน่วยงานท้องถิ่น ที่เกิดจากระบบทำงานผิดพลาด อาจมีการรั่วไหลของข้อมูลสู่มิจฉาชีพหรือผู้ไม่สงค์ดี อันเป็นการส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล ซึ่งที่มาสำคัญของปัญหาส่วนหนึ่งมาจากการที่หน่วยงานท้องถิ่นขาดแคลนงบประมาณในการจัดหาและฝึกอบรมบุคลากรเกี่ยวกับระบบความปลอดภัยทางไซเบอร์ โดยเฉพาะระบบที่เหมาะสมไม่มีความยุ่งยากซับซ้อนจนเกินไปเน้นสามารถใช้งานได้ง่ายรวดเร็วพร้อมทั้งมีการใช้ข้อมูลสารสนเทศเพื่อการสืบค้นและการสื่อสารที่สะดวกและรวดเร็วยิ่งขึ้น

ระบบที่ควรนำมาใช้ในหน่วยงานท้องถิ่น ควรเป็นระบบที่ใช้ในการบริหารจัดการเครือข่ายภายในองค์กรที่มีประสิทธิภาพและสามารถคัดกรองเนื้อหาไม่เหมาะสมที่เผยแพร่ทางอินเทอร์เน็ตซึ่งคณะผู้ดำเนินโครงการฯมีแนวทางในพัฒนาอุปกรณ์ป้องกันภัยทางไซเบอร์ในรูปแบบ Appliances สามารถเก็บ Log File ตาม พรบ.คอมฯ คัดกรองเนื้อหาที่ไม่เหมาะสม วิเคราะห์ภัยคุกคามและมีระบบแจ้งเตือนภัย โดยอุปกรณ์สามารถเชื่อมต่อฐานข้อมูลร่วมกันได้ เพื่อการบรูณาการข้อมูล สามารถเก็บรวบรวมเหตุการณ์(logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliancesเช่นFirewall,Network Devices ต่างๆ รวมทั้งระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้แ โดยระบบควรมีคุณสมบัติอย่างน้อยดังนี้

- สามารถนำเข้าฐานข้อมูลเว็บไซต์หรือโดเมนที่ไม่เหมาะสมและป้องกันข้อมูลเว็บไซต์หรือโดเมนที่ไม่เหมาะสม

- สามารถตรวจสอบกลุ่มเนื้อหาที่กระทบต่อความมั่นคงต่อประเทศ

- สามารถตรวจสอบกลุ่มเนื้อหาลามกอนาจารทั้งที่มีเนื้อหาภาษาไทยและเนื้อหาภาษาอังกฤษ

- สามารถตรวจสอบกลุ่มเว็บไซต์หรือโดเมนที่มีมีการโฆษณาชวนเชื่อ กลุ่มเนื้อหาที่ผิดกฎหมาย (การพนัน ยาเสพติด เป็นต้น) ทั้งที่มีเนื้อหาภาษาไทยและเนื้อหาภาษาอังกฤษ

- สามารถแสดงการรายงานผลผ่าน Web Base GUI

- สามารถแสดงการรายงานผลและสรุปสถิติจำนวนการใช้งานอินเทอร์เน็ตหรือการใช้งานแบนด์วิดธ์ที่เกิดขึ้น

- สามารถแสดงการรายงานผลและสรุปสถิติจำนวนการปิดกั้น (Internet Blocked) แบบภาพรวม

- สามารถแสดงผลรายงานการบันทึก Log files จากการใช้งานอินเทอร์เน็ตเพื่อเก็บบันทึกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้อย่างน้อย 90 วัน

- มีการเข้ารหัสผ่าน (HTTPS) และการบริหารจัดการระบบผ่าน SSH รวมถึงปิด Port Services ที่ไม่ได้ใช้ออกเพื่อความมั่นคงปลอดภัย

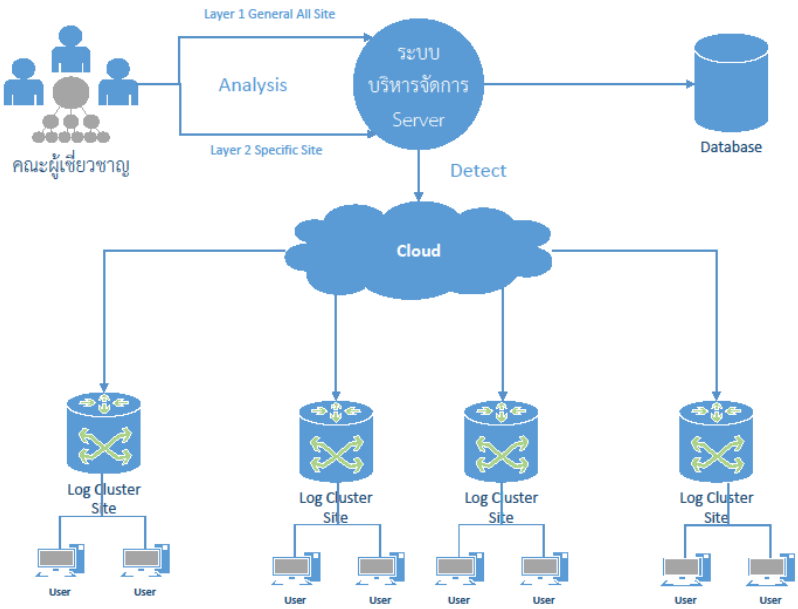
- รองรับการใช้งาน window os, mac os, android และ ios ด้วย Cloud Server ซึ่งมีค่าใช้จ่ายต่ำกว่าการลงทุนเป็น Hardware หรือServer ขนาดใหญ่ ซึ่งการกำหนดข้อมูลในการกรองข้อมูลในเบื้องต้นควรใช้คณะทำงานผู้เชี่ยวชาญด้าน Cyber Security เป็นผู้คัดกรองข้อมูล แล้วจัดเก็บฐานข้อมูลเข้าสู่ระบบตัวอย่างตามภาพได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฉบับที่มีผลบังคับใช้โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐาน เช่น ต้องผ่านการรับรองมาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ(มศอ.4003.1–2552)เป็นต้น เพื่อความแม่นยำถูกต้อง สามารถใช้ยืนยันได้ในชั้นศาล

อีกประเด็นที่สำคัญคือการขาดการติดตั้งระบบการพิสูจน์ตัวตน(Authentication)ทำให้เสี่ยงต่อการใช้เป็นช่องทางกระทำความผิด ตาม พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ หรือ การกระทำผิดทางกฎหมายด้านอื่นๆ ซึ่งทางหน่วยงานท้องถิ่นเองมีความต้องการให้สนับสนุนการติดตั้งระบบแสดงตัวตน (Authentication) เพื่อแสดงตัวตนการใช้งานอินเทอร์เน็ต

ใช้งานง่าย ไม่ซับซ้อน บุคลากรที่ใช้งานมีพื้นฐานการใช้งานคอมพิวเตอร์ทั่วไปสามารถเป็นAdminเองได้ คณะผู้ดำเนินโครงการฯจึงวางแนวทางให้ระสามารถแสดงตัวตน (Authentication) แสดงตัวตนการใช้งานอินเทอร์เน็ต กำหนดสิทธิในการใช้งานอินเทอร์เน็ตจาก Adminของหน่วยงาน กำหนดนโยบายระยะเวลาการใช้ User และ Password พัฒนาขึ้นมาเป็นส่วนหนึ่งของระบบป้องกันภัยคุกคามทางไซเบอร์ สอดคล้อง ตาม พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ฯ โดยนำมาวิเคราะห์เป็นกลไกด้านความปลอดภัยให้สามารถตรวจสอบการเข้าใช้งานอินเทอร์เน็ตของหน่วยงานท้องถิ่น มีระบบจัดการสมาชิกและสามารถสร้างรหัสผ่านให้ผู้ใช้งานได้ สามารถจัดการสมาชิกแบบรายบุคคลหรือรายกลุ่มรวมทั้งจัดการและจัดรูปแบบกลุ่มสมาชิกเช่น ความเร็ว ระยะเวลา เป็นต้น และออกแบบมาเป็นระบบพิสูจน์ตัวตนทำหน้าในการตรวจสอบ และอนุญาตให้ผู้ใช้บริการเข้าสู่การใช้งานอินเทอร์เน็ต โดยประกอบไปด้วย ส่วนการจำกัดการเข้าใช้บริการ/ส่วนพิสูจน์ตัวตนและระบบฐานข้อมูลผู้ใช้บริการ

บทสรุปและข้อเสนอแนะ

การออกแบบระบบป้องกันภัยทางไซเบอร์นอกจากจะออกแบบให้ เหมาะสมด้านการใช้งานในหน่วยงานท้องถิ่นขนาดเล็กแล้ว ยังคำนึงถึง นำแนวคิดเรื่อง คลัสเตอร์ ของหน่วยงานท้องถิ่นมาพิจารณาในการออกแบบด้วยดังนี้



ภาพต้นแบบจำลองระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์
เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น

โดยคณะผู้วิจัยได้สรุปกรอบแนวทางการศึกษาและพัฒนาระบบเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ เสำหรับองค์กรขนาดเล็กในระดับชุมชนเพื่อเป็นแนวทางการศึกษาให้เกิดผลสัมฤทธิ์ด้านการปฏิบัติที่เป็นรูปธรรมได้จริง ตามแผนภาพ

แผนภาพแนวทางการศึกษาการพัฒนาระบบเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์

การป้องกันภัยคุกคามทางไซเบอร์ควรดำเนินการในลักษณะ sector-based คือ การเฝ้าระวัง แจ้งเตือนภัย และการดูแลความปลอดภัย ซึ่งสามารถแบ่งการพัฒนาได้เป็น 3 ด้าน ได้แก่

1. พัฒนาระบบเฝ้าระวังภัยคุกคามทางไซเบอร์สำหรับองค์กรปกครองส่วนท้องถิ่น โดยเน้นให้ความสำคัญที่ หน่วยงานที่มีขนาดเล็กเพื่อสร้างความพร้อมด้านการป้องกันภัยคุกคามทางไซเบอร์ให้เกิดผลแท้จริง

2. ด้านการพัฒนาบุคลากรสู่ความเป็นเลิศด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นการพัฒนาความรู้และทักษะที่จำเป็นในการดำเนินงานด้านการรักษาความปลอดภัยไซเบอร์โดยอาจจัดทำความร่วมมือร่วมกับองค์กรที่เกี่ยวข้อง เช่นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team) ฯลฯ ในการฝึกอบรมสัมมนาเพื่อพัฒนาบุคลากร

3. ด้านการพัฒนาองค์กรสู่มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

กำหนดให้ต้องมีการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐานสากล ISO/IEC 27001 ให้มีประสิทธิภาพควรอยู่บนพื้นฐานของการประเมินความเสี่ยงและจัดการความเสี่ยงในด้านต่างๆ ควบคู่กันไป ได้แก่ (1) การรักษาความลับของข้อมูล (confidentiality) โดยการกำหนดสิทธิ์การเข้าถึงข้อมูล (2) ความถูกต้องครบถ้วนของข้อมูล (integrity) เป็นการกำหนดมาตรการ หรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล เพื่อป้องกันความผิดพลาดหรือการเข้าแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต และ (3) ความพร้อมใช้ (availability) ผู้มีสิทธิ์ในการเข้าถึงข้อมูลในระบบต่างๆ ของหน่วยงานต้องสามารถเข้าใช้ข้อมูลได้ในกรอบเวลาที่ต้องการ

การประยุกต์ใช้หลักการ Plan-Do-Check-Act : PDCA ในกระบวนการตรวจประเมินซึ่งการรับรองมาตรฐาน ISO/IEC 27001 ได้ ดังนี้

1. การตรวจประเมินจะทำการทบทวนและตรวจสอบระบบ ISMS อย่างไม่เป็นทางการ การทบทวนตรวจสอบนี้ จะหมายรวมถึงการดำเนินการต่างๆ เช่น การตรวจสอบการมีอยู่ของเอกสารที่สำคัญในระบบ ISMS และตรวจสอบระบบ ISMS โดยภาพรวม เป้าหมายของการตรวจประเมินระยะที่ 1 คือ เพื่อให้ผู้ตรวจประเมินรู้จักและคุ้นเคยกับองค์กร รวมถึงเพื่อให้องค์กรได้ทำความรู้จักกับผู้ตรวจประเมิน

2. การตรวจประเมินติดตามผล–ระยะสุดท้ายของการรับรองมาตรฐานระบบ ISO/IEC ๒๗๐๐๑ คือ การตรวจประเมินเพื่อทำให้มั่นใจว่าระบบ ISMS ของท่านได้รับการประเมินและปรับปรุงอย่างต่อเนื่อง การตรวจประเมินติดตามผลจะถูกดำเนินการอย่างน้อยที่สุดปีละหนึ่งครั้ง โดยมีจุดประสงค์เพื่อเป็นการยืนยันว่าองค์กรยังคงมีความลอดคล้องกับมาตรฐาน การตรวจประเมินติดตามผลนี้อาจถูกดำเนินการบ่อยครั้งกว่าในช่วงเริ่มต้นของการนำระบบไปปฏิบัติ

บรรณานุกรม

กระทรวงมหาดไทย. (2559). แผนพัฒนาขององค์กรปกครองส่วนท้องถิ่น (ฉบับที่ 2). http://www.thongthinlaws.com/2016/10/081035797-10-2559-2561-2564-2-2559.html

พล.ต.ท.ณรงค์ กุลนิเทศ, ณิช วงศ์ส่องจ้า (2557) *รูปแบบและมาตรการแก้ปัญหาอาชญากรรมไซเบอร์ Model and measure of Solving Problem Cyber Crime*

ธวัชชัย ชมศิริ. (2553). ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์. กรุงเทพฯ : โปรวิชั่น.

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมปศุสัตว์. (2559). สาระสาคัญ แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ฉบับนำเสนอคณะรัฐมนตรี 5 เมษายน 2559, 27 พฤษภาคม 2559. http://ict.dld.go.th/th2/images/stories/procure/2559/2-590613_1DE_27-5-59-Drkasititorn.pdf

ACIS Professional Center. (2559). บทวิเคราะห์แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ปี พ.ศ. 2559, 7 มิถุนายน 2559. https://www.acisonline.net/?p=5040&lang=th

Broderick J.S., (2006). “ISMS, security standards and security regulations”. Science Direct., 26-31