บทความทางวิชาการ

เรื่อง

การรักษาความมั่นคงปลอดภัยไซเบอร์ : การทำงานแบบ Work From Home

Cyber Security : Work From Home Model

โดย

ผู้ช่วยศาสตราจารย์ (พิเศษ) ดร. ธนบวร สิริคุณากรกุล

หมายเลข ๓๗๓๒ หมู่เสือ

นักศึกษาวิทยาลัยเสนาธิการทหาร รุ่นที่ ๖๑

วิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ

ปีการศึกษา ๒๕๖๓

เอกสารนี้เป็นส่วนหนึ่งของหมวดวิชาที่ ๑ การบริหารทางการทหาร

หลักสูตรวิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ

การรักษาความมั่นคงปลอดภัยไซเบอร์ : การทำงานแบบ Work From Home

Cyber Security : Work From Home Model

ผู้ช่วยศาสตราจารย์ (พิเศษ) ดร. ธนบวร สิริคุณากรกุล*

ASST. PROF. DR. TANABOWORN SIRIKUNAKRONKUN*

บทคัดย่อ

ปัจจุบันสังคมไทยได้เข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบ มีความเจริญก้าวหน้าทางด้านเทคโนโลยีสื่อสารโทรคมนาคม จึงปฏิเสธไม่ได้ว่ามีระดับความเสี่ยงสูงที่ระบบไซเบอร์ของประเทศจะถูกโจมตีและคุกคามจนเกิดความเสียหายต่อความมั่นคงทางเศรษฐกิจและสังคมของประเทศ การสร้างความพร้อมในการรับมือกับภัยคุกคามด้านไซเบอร์จึงเป็นสิ่งสำคัญ ที่ผ่านมาหน่วยงานที่เกี่ยวข้องได้ให้ความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีนโยบายที่ชัดเจนเพื่อนำไปปฏิบัติอย่างมีเป้าหมายและมีกลไกในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เข้มแข็งยิ่งขึ้น อย่างไรก็ตามการสร้างความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์มีความจำเป็นต้องใช้งบประมาณ ขีดความสามารถของบุคลากร และค่านิยมขององค์กรในการแลกเปลี่ยนข้อมูล ดังนั้นหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์จึงควรบูรณาการความร่วมมือในการทำงานร่วมกัน พร้อมทั้งพัฒนาปรับปรุงความร่วมมือในระดับนโยบายและระดับปฏิบัติการให้มีความเหมาะสมเพื่อประโยชน์สูงสุด คือ ความมั่นคงของประเทศชาติ

ณ สถานการณ์ปัจจุบันการแพร่เชื้อไวรัสสายพันธุ์ใหม่ โรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID-19) ที่กำลังแพร่ระบาดอยู่ในขณะนี้ การปรับตัวให้การทำงานมาอยู่ในรูปแบบของ Work From Home ถือเป็นกลยุทธ์สำคัญของการทำงานแบบสถานที่ทำงานดิจิทัล (Digital Workplace) อีกรูปแบบหนึ่ง แม้จะทำให้บุคลากรมีอิสระในการทำงาน แต่การทำงานนอกสถานที่ก็มีความเสี่ยงที่อาจจะเกิดขึ้นได้เช่นกัน โดยเฉพาะความเสี่ยงในด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หลาย ๆ หน่วยงานเริ่มหาแนวทางการป้องกันในรูปแบบต่าง ๆ เพื่อมาช่วยป้องกันข้อมูลซึ่งถือว่าเป็นทรัพยากรอันมีค่าในหน่วยงาน นอกจากนี้ยังเป็นการสนับสนุนให้การทำงานแบบ Work From Home มีความมั่นคงปลอดภัยทางไซเบอร์

คำสำคัญ : ความมั่นคงปลอดภัยไซเบอร์, ขีดความสามารถของบุคลากร, ค่านิยมขององค์กรในการแลกเปลี่ยนข้อมูล, การทำงานแบบ Work From Home

---

* ผู้ช่วยเลขานุการรองประธานสภาผู้แทนราษฎร

Assistant Secretary to the Deputy Speaker of The House of Representatives

E-mail : s.tanaboworn@gmail.com

Abstract

Nowadays, Thai society has fully entered the digital age. With the civilization in telecommunications technology. Therefore, it cannot be denied that there is a high risk level that the country's cyber systems will be attacked and threatened causing damaged of country's economic and social security. It is important to be ready to deal with the cyber threats. In the past, relevant agencies have given priority to cyber security and have a clear policies for implementation with goals and have strengthened mechanisms for managing cyber security. However, the budget is important to be used for creating a cooperation in cyber security, capabilities of personnel and organizational value in exchanging the information. Thus, the agencies involved in cyber security should integrate a cooperation in working together as well as developing the cooperation at the policy level and operational level for the most suitable highest benefit which is the stability of the nation.

The current situation, the spread of new virus strains Coronavirus infection in 2019 (COVID-19) that is spreading currently. The adaption of working in the form Work From Home is considered as another important strategy of working digital workplace style. Even the personnel are free to work, but working off-site has a risk that may occur as well. Especially the risks from cyber security. Many organizations have started to find a various forms of protection in order to help protect the data which is considered as a valuable resource in the department. In addition, it also supports work from home to secure in cyber security.

Keywords: Cyber security, Capabilities of personnel, Organizational value in exchanging the information, Work From Home

บทนำ

ปัญหาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) กำลังเป็นเรื่องท้าทายของทุกประเทศ เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ทุกรูปแบบเพื่อการประกอบอาชีพและการดำรงชีวิตเกิดความเสียหายมหาศาลจากอาชญากรรมไซเบอร์ ซึ่งมีตัวเลขประมาณการจาก Forbes (นิตยสารเกี่ยวกับธุรกิจและการเงินในสหรัฐอเมริกา) ว่าแนวโน้มความเสี่ยงด้านภัยคุกคามไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่องทำให้การจ้างงานทั่วโลกในด้าน Cyber Security จะทะยานถึง ๓.๕ ล้านตำแหน่งงานในปี ๒๕๖๔

หลักการพื้นฐานที่ผู้บริหารองค์กรต้องคำนึงถึงในการจัดตั้งทีมผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (Computer Security Incident Response Team : CSIRT) ต้องมีการคัดสรรเลือกทรัพยากรบุคคลที่มีทักษะเหมาะสม ตลอดจนบุคคลที่ได้รับคัดเลือกเหล่านั้นต้องมีความเป็นผู้นำและได้รับอำนาจหน้าที่อย่างเป็นทางการในการรายงาน แนะนำ รวมถึงสั่งการส่วนงานต่าง ๆ ในองค์กร (รวมถึงในระดับผู้บริหารที่อยู่เหนือตนขึ้นไป) ที่จำเป็นต้องรับทราบและเกี่ยวข้องเมื่อเกิดเหตุการณ์ด้านความปลอดภัยทางข้อมูลขึ้น นอกจากนี้สิ่งจำเป็นอีกประการ คือ การเพิ่มขีดความสามารถขององค์กรในการรับมือเหตุการณ์ด้านความปลอดภัยทางข้อมูลให้สูงขึ้น โดยการจัดทำกระบวนการและคู่มือในการรับมือกับภัยคุกคามทางด้านนี้ให้ชัดเจน เพื่อเป็นหลักในการปฏิบัติ และมีการฝึกซ้อมการรับมือภัยคุกคามตามกระบวนการดังกล่าวอยู่เป็นประจำ จากกรณีศึกษาในประเทศญี่ปุ่นเกี่ยวกับการเตรียมความพร้อมในการรับมือภัยคุกคามนั้น จะเห็นได้ว่ามีความร่วมมือระหว่างหลายภาคส่วน ทั้งภาครัฐ ภาคเอกชน รวมถึงสถาบันการศึกษาหรือสถาบันวิจัย เพื่อยกระดับขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ดังกล่าวให้กับองค์กรทุกภาคส่วน โดยไม่ปล่อยให้แต่ละองค์กรรับผิดชอบหรือดำเนินการเอง ซึ่งในความเป็นจริงแล้วอาจเกินขีดความสามารถที่แต่ละองค์กรจะสามารถทำได้เนื่องจากการขาดแคลนบุคลากรด้านนี้ อีกทั้งจำนวนงบประมาณที่แต่ละองค์กรจะสามารถลงทุนเกี่ยวกับความปลอดภัยมีอยู่จำกัดในระดับหนึ่ง (ต้องยอมรับความจริงว่า ที่ผ่านมานั้น ถึงแม้ผู้บริหารองค์กรอาจจะทราบความสำคัญของความปลอดภัยทางไซเบอร์ แต่งบประมาณขององค์กรก็จำเป็นต้องนำไปลงทุนในส่วนที่เกี่ยวกับการดำเนินธุรกิจหลักขององค์กรก่อน ยกเว้นในกรณีที่มีความจำเป็นเร่งด่วน เช่น พบว่ามีความเสี่ยงในการถูกโจมตีหรือถูกโจมตีแล้ว ซึ่งในแง่มุมหนึ่งก็จะกลายเป็นการตามแก้ไขปัญหาที่เกิดขึ้นเสียเป็นส่วนใหญ่มากกว่า)[๑]

๑. ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) คืออะไร

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) ได้ให้ความหมายของคำว่า ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ว่าคือภาพรวมของเครื่องมือ (Tools), นโยบาย (Policies), แนวคิดการรักษาความปลอดภัย (Security Concepts), การรักษาความปลอดภัย (Security Safeguards), แนวทาง (Guidelines), วิธีการบริหารความเสี่ยง (Risk Management Approaches), การปฏิบัติ (Actions), การอบรม (Training), วิธีปฏิบัติที่เป็นเลิศ (Best Practices), การรับประกัน (Assurance) และเทคโนโลยี (Technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับเชื่อมต่อคอมพิวเตอร์, ข้อมูลส่วนตัว, โครงสร้างพื้นฐาน, แอปพลิเคชัน, บริการ,

[๑] ไพโรจน์ ธรรมศีลสุวรรร, (๒๕๖๐). ICT Trend Watch (ตอนที่ ๕๗) ความร่วมมือระหว่างภาคส่วนองค์กร เพื่อรับมือการโจมตีทางไซเบอร์. สืบค้น ๑๐ พฤษภาคม ๒๔๖๓ จาก http://www.cioworldmagazine.com/dr-pairoj-dhamsinsuwan-ict-trend-watch-57-csirt/

ระบบสารสนเทศ และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์[๒]

๒. การโจมตีทางไซเบอร์ (Cyber Attack)

การโจมตีทางไซเบอร์ คือ การกระทำใด ๆ ที่ใช้คอมพิวเตอร์, เครือข่าย หรือระบบ รวมทั้งอุปกรณ์ที่เกี่ยวข้อง โดยตั้งใจเพื่อให้เกิดภัยคุกคาม ขัดขวาง หรือทำลายระบบ ทรัพยากร และการทำงานของระบบไซเบอร์ที่สำคัญต่อเป้าหมาย ผลกระทบของการโจมตีทางไซเบอร์ไม่จำเป็นต้องจำกัดเพียงระบบคอมพิวเตอร์ และข้อมูลที่เป็นเป้าหมาย ตัวอย่างเช่น การโจมตีต่อระบบคอมพิวเตอร์ที่ต้องการลิดรอน หรือทำลายโครงสร้างพื้นฐานสาธารณูปโภค หรือขีดความสามารถของระบบบัญชาการและควบคุม (C2) การโจมตีทางไซเบอร์อาจจะต้องใช้อุปกรณ์ตัวกลางในการดำเนินการ รวมทั้ง อุปกรณ์ต่อเชื่อมต่าง ๆ (Peripheral Devices), เครื่องส่งสัญญาณอิเล็กทรอนิกส์ (Electronic Transmitters), การเข้ารหัส (Embedded Code), หรือเจ้าหน้าที่ปฏิบัติงาน (Operators) กิจกรรมหรือผลกระทบของการโจมตีอาจจะเกิดขึ้นอย่างกระจัดกระจายเป็นวงกว้าง หรือเป็นเฉพาะพื้นที่ที่เป็นเป้าหมาย

การโจมตีทางไซเบอร์ (Cyber Attack) ถูกใช้แทนที่คำว่า การโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack : CNA) เนื่องจากการโจมตีทางไซเบอร์นั้นเชื่อมโยงกับกระบวนทัศน์หรือหลักนิยมของการปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations : CNO) ที่ใหญ่กว่า ซึ่งมีความแตกต่างกันจากวิธีการในความหมายของคำว่าการโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack : CNA)

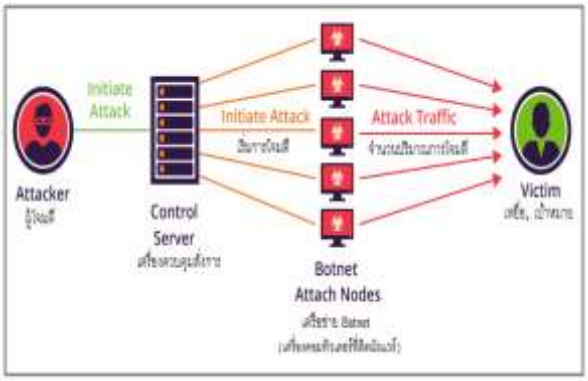
"การโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack : CNA) – [กห.สหรัฐ] คือประเภทหนึ่งของอำนาจการยิงที่ถูกใช้สำหรับวัตถุประสงค์การรุกซึ่งต้องปฏิบัติจากการใช้เครือข่ายคอมพิวเตอร์เพื่อที่จะรบกวน ลิดรอน ทำให้เสื่อมลง ทำให้เสียหาย หรือทำลายข้อมูลที่อยู่ในระบบข้อมูลข่าวสารเป้าหมาย หรือเครือข่ายคอมพิวเตอร์ หรือระบบ/เครือข่ายของอุปกรณ์ที่เกี่ยวข้อง ผลกระทบที่ต้องการอย่างยิ่งยวดอาจไม่ใช่ระบบที่เป็นเป้าหมายเพียงอย่างเดียว แต่อาจเป็นการปฏิบัติเพื่อสนับสนุนความพยายามที่สำคัญกว่านั้น เช่น การปฏิบัติการข้อมูลข่าวสาร หรือการต่อต้านการก่อการร้ายโดยใช้การเปลี่ยนแปลง (Altering) หรือการปลอมตัว (Spoofing) ต่อระบบการติดต่อสื่อสารต่าง ๆ หรือการลิดรอน (Denying) การเข้าถึงการติดต่อสื่อสารหรือช่องทางการส่งกำลังบำรุงของศัตรู"

๓. การป้องกันทางไซเบอร์ (Cyber Defense)

การป้องกันทางไซเบอร์ (Cyber Defense) เป็นการประยุกต์รวมขีดความสามารถและกระบวนการในระบบไซเบอร์ของหน่วยงานที่เกี่ยวข้อง การดำรงขีดความสามารถด้านการตรวจจับ, วิเคราะห์และลดภัยคุกคาม/จุดเสี่ยงต่าง ๆ, และดำเนินกลยุทธ์ในการเอาชนะศัตรู เพื่อป้องกันเครือข่ายที่กำหนด ปกป้องภารกิจที่สำคัญ และทำให้เกิดอิสระในการปฏิบัติของฝ่ายเรา การป้องกันทางไซเบอร์ รวมถึง การปฏิบัติการเครือข่ายเชิงรุก (Proactive NetOps) : การปฏิบัติการเครือข่าย (NetOps) ถูกกำหนดโดย กห. สหรัฐในการปฏิบัติการ การจัดโครงสร้าง และขีดความสามารถทางเทคนิคสำหรับการปฏิบัติการ และการป้องกันโครงข่ายข้อมูลข่าวสารโลก (Global Information Grid : GIG) การปฏิบัติการเครือข่าย (NetOps) รวมถึงการบริหารจัดการองค์กร (Enterprise Management), การรับรองการทำงานหรือการป้องกันของเครือข่าย (Net Assurance หรือ Net Defense), และการบริหาร

[๒] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.), (๒๕๕๙). **ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)**.

ข่าวสาร (Content Management) การปฏิบัติการเครือข่าย (NetOps) สามารถสนองตอบความต้องการของผู้บังคับบัญชาในการหยั่งรู้สถานการณ์ของ GIG เพื่อนำไปสู่การตัดสินตกลงใจในรูปแบบของการบัญชาการและควบคุม ทั้งนี้ การหยั่งรู้สถานการณ์ของ GIG ทำได้โดยการบูรณาการทั้งทางเทคนิคและการปฏิบัติการของการบริหารจัดการองค์กร การป้องกัน และกิจกรรมตลอดทุกระดับการบังคับบัญชา (ยุทธศาสตร์, ยุทธการ และยุทธวิธี)[๓]



ภาพที่ ๑ *การโจมตีทางไซเบอร์*[๔]

๔. พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒[๕]

เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่ในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม มีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องตราพระราชบัญญัตินี้

คณะกรรมการที่มีส่วนเกี่ยวข้องกับ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรียกย่อ ๆ ว่า กมช. และให้ใช้ชื่อเป็นภาษาอังกฤษว่า National Cybersecurity Committee เรียกโดยย่อว่า NCSC มีหน้าที่กำหนด เสนอ จัดทำแผนปฏิบัติ กำหนดมาตรการและแนวทางต่าง ๆ ที่มีส่วนเกี่ยวข้องกับ พ.ร.บ.

๒. คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกย่อ ๆ ว่า กกม. มีหน้าที่กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์ รวมถึงกำหนด

---

[๓] **Department of Defense NetOps Strategic Vision**, December 2008 : Department of Defense Chief Information Officer The Pentagon – Washington. D.C..

[๔] สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย, **เมื่อเครื่องคอมพิวเตอร์ติดมัลแวร์ (Malware) และมีการติดต่อไปยัง C&C เซิร์ฟเวอร์**. สืบค้น ๔ พฤษภาคม ๒๕๖๓ จาก https://www.it.chula.ac.th/th/node/4722

[๕] **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒**, ราชกิจจานุเบกษา, เล่ม ๑๓๖ ตอนที่ ๖๙ ก, ๒๗ พฤษภาคม ๒๕๖๒. หน้า ๕๑.

ระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน

โดยการรับมือกับภัยคุกคามทางไซเบอร์จะมีการพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ ทางคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์จะเป็นผู้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ดังต่อไปนี้

๒.๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลง

๒.๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่มีการโจมตีระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตี และการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศเสียหายจนไม่สามารถทำงานหรือให้บริการได้

๒.๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่มีลักษณะ ล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานจากส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน

การรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ ไม่ว่าจะเป็นการตรวจสอบคอมพิวเตอร์และประเมินผลกระทบ การรักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์ ส่วนด้านการป้องกันและรับมือ พนักงานเจ้าหน้าที่สามารถเข้าตรวจสอบสถานที่โดยมีหนังสือแจ้งถึงเหตุอันสมควรเข้าถึงข้อมูลระบบคอมพิวเตอร์ไปจนถึงยึดหรืออายัดคอมพิวเตอร์

โดยสรุปแล้วเหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ ในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ซึ่งอาจกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ดังนั้นเพื่อให้สามารถป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ทั้งหน่วยงานของรัฐและหน่วยงานเอกชนจะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ไม่ให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรงก็ตาม

๕. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวกและรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้[๖]

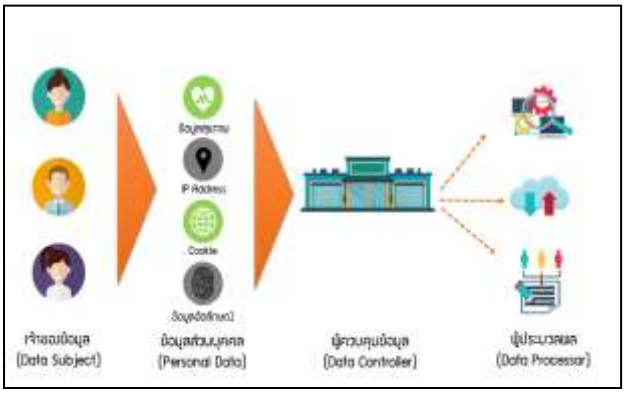
---

[๖] **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒**, ราชกิจจานุเบกษา, เล่ม ๑๓๖ ตอนที่ ๖๙ ก, ๒๗ พฤษภาคม ๒๕๖๒. หน้า ๙๕.

"ข้อมูลส่วนบุคคล" ที่ถูกบันทึกได้ง่ายบนโลกดิจิทัล ทำให้ผู้ใช้หลายคนอาจมีความกังวลถึงความปลอดภัยของข้อมูลตนเองว่าจะหลุดไปสู่ภายนอก หรือถูกนำไปใช้กรณีอื่น เพื่อยกระดับการปกป้องข้อมูลดังกล่าวทำให้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือ พ.ร.บ. ข้อมูลส่วนบุคคลฯ ผ่านการพิจารณาและมีผลบังคับใช้ในเดือนพฤษภาคม พ.ศ. ๒๕๖๓

ภาพที่ ๒ *สิทธิของเจ้าของข้อมูลส่วนบุคคล*[๗]

ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โดยเฉพาะ ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ฯลฯ



ภาพที่ ๓ *การคุ้มครองข้อมูลส่วนบุคคล*[๘]

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) คือ ข้อมูลที่ต้องระมัดระวังเป็นพิเศษในการเก็บรวบรวม หรือประมวลผล เช่น เชื้อชาติ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา รสนิยมทางเพศ ข้อมูลทางชีวภาพ ทั้งนี้กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลธรรมดา

สรุปประเด็นสำคัญ (เบื้องต้น) ๘ ประเด็นดังนี้[๙]

๑) กฎหมายคุ้มครองข้อมูลส่วนบุคคลของบุคคลธรรมดาเท่านั้น ข้อมูลบุคคลเป็นข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โดยเฉพาะ ดังนั้นจึงหมายถึงข้อมูลชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ หมายเลขบัตรประชาชน อีเมล์ ลายนิ้วมือ IP address Cookie ฯลฯ ของบุคคลทั่วไป และไม่คุ้มครองถึงข้อมูลของนิติบุคคล

๒) เจ้าของข้อมูลส่วนบุคคลต้องยินยอมก่อนการที่เก็บข้อมูลส่วนตัวต่าง ๆ เพื่อนำไปรวบรวม ใช้หรือเปิดเผยข้อมูลต่อไปนั้น ต้องเก็บจากเจ้าของข้อมูลโดยตรง และได้รับการยินยอมโดยตรงจากเจ้าของข้อมูลเป็นลายลักษณ์อักษรหรือผ่านระบบออนไลน์ตามรูปแบบที่กำหนด ดังนั้นก่อนที่จะยินยอมเจ้าของข้อมูลต้องอ่านรายละเอียดให้ดีก่อน รวมถึงเก็บข้อมูลว่าได้ยินยอมให้เก็บ ใช้ เปิดเผยข้อมูล ไปกับหน่วยงานใดบ้าง

๓) แจ้งรายละเอียดชัดเจนครบถ้วน ผู้เก็บข้อมูลต้องแจ้งวัตถุประสงค์ของการเก็บข้อมูล การใช้ข้อมูล

---

[๗] Nattapon Muangtum, **สรุป PDPA พ.ร.บ. ข้อมูลส่วนบุคคล กับ ๗ เรื่อง ที่ผู้ประกอบการต้องให้ความสำคัญ**. ๒๗ เมษายน ๒๕๖๒, สืบค้น ๒๐ พฤษภาคม ๒๕๖๓ จาก https://www.everydaymarketing.co/update-news/7

[๘] วิทวัส มงคลนวเสถียร, **การคุ้มครองข้อมูลส่วนบุคคล**. ๑๐ พฤษภาคม ๒๕๖๒. สืบค้น ๒๐ พฤษภาคม ๒๕๖๓ จาก https://www.gotoknow.org/posts/661602

[๙] ธรรมนิติ DHARMNITI, **๘ ประเด็นสำคัญจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล**. สืบค้น ๑๗ พฤษภาคม ๒๕๖๓ จาก https://www.dharmniti.co.th/law-digital-personaldataprotectionlaw/

การเปิดเผยข้อมูล ระยะเวลาที่เก็บเงื่อนไขต่าง ๆ ให้เจ้าของข้อมูลอย่างชัดเจน ที่สำคัญข้อมูลรายละเอียดในการขอความยินยอมจากเจ้าของข้อมูลต้องแยกส่วนออกมาจากข้อความอื่นอย่างชัดเจน อ่านเข้าใจง่าย เพื่อให้เจ้าของข้อมูลอ่านและทำความเข้าใจก่อนที่จะยินยอมให้เก็บข้อมูล

๔) ผู้มีสิทธิ์เด็ดขาดคือเจ้าของข้อมูล ข้อมูลส่วนบุคคลที่ให้ไว้นั้น เจ้าของข้อมูลสามารถยกเลิกการเก็บข้อมูล การนำไปใช้ แก้ไขและลบข้อมูลออกจากระบบได้ โดยที่ผู้เก็บข้อมูลไม่สามารถปฏิเสธได้ ดังนั้นผู้เก็บข้อมูลต้องเตรียมการให้การยกเลิกทำได้สะดวกเช่นเดียวกับการยอมรับ ซึ่งการคุ้มครองนี้รวมถึงข้อมูลส่วนตัวที่ส่งไปเพื่อสมัครงาน ผู้สมัครสามารถแจ้งให้ทางบริษัทส่งข้อมูลกลับหรือทำลายข้อมูลส่วนตัว เช่น สำเนาบัตรประชาชน สำเนาทะเบียนบ้าน รูปถ่าย เอกสารการศึกษา ฯลฯ หลังจากการสมัคร เพื่อป้องกันไม่ให้ข้อมูลส่วนตัวสำคัญเหล่านี้รั่วไหลออกไป

๕) ผู้เก็บต้องรักษาข้อมูลให้ปลอดภัยเป็นความลับ ผู้เก็บรวบรวมข้อมูลส่วนบุคคลจะต้องมีหน้าที่รักษาความมั่นคงปลอดภัยของข้อมูล มิให้มีการแก้ไขเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่ใช่เจ้าของข้อมูล หรือเข้าถึงข้อมูลโดยมิชอบ และดูแลไม่ให้เกิดการสูญหาย ซึ่งเรื่องนี้ทางผู้ประกอบการหรือองค์กรที่เก็บข้อมูลต้องมีการวางระบบ วิธีการ คณะทำงาน ทีมงานที่รับผิดชอบ ฯลฯ ในการดูแลข้อมูลให้ปลอดภัยมากที่สุด แต่หากข้อมูลเกิดรั่วไหลหรือถูกขโมยไป ผู้เก็บข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบใน ๗๒ ชั่วโมงนับแต่ทราบเหตุ

๖) ครอบคลุมผู้เก็บ ใช้ เปิดเผยข้อมูลทั้งในและนอกประเทศ พระราชบัญญัติข้อมูลส่วนบุคคลใช้บังคับกับการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยองค์กรหรือผู้ประกอบการในประเทศ ไม่ว่าการเก็บ การใช้หรือการเปิดเผยข้อมูล จะเกิดขึ้นในประเทศหรือนอกประเทศ หากผู้เก็บ ใช้หรือการเปิดเผยข้อมูลอยู่นอกประเทศจะควบคุมเมื่อมีการเสนอสินค้าหรือบริการและการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนตัวที่อยู่ในประเทศไทย

๗) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ใช้การจ้างบุคคลภายนอก (Outsource) ได้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งมีหน้าที่ให้คำแนะนำในการปฏิบัติ ตรวจสอบการดำเนินการให้ถูกต้อง ประสานงานเมื่อมีปัญหา และรักษาความลับ อาจเป็นพนักงานขององค์กรหรือเป็นผู้รับจ้างให้บริการตามสัญญาก็ได้

๘) ฝ่าฝืนมีโทษปรับและจำคุก ปรับเงินสูงสุด ๕ ล้านบาท หากฝ่าฝืนมีโทษทั้งทางอาญา ทางแพ่ง และทางปกครอง สำหรับโทษทางอาญาหากมีการฝ่าฝืนมีโทษจำคุกไม่เกิน ๖ เดือนถึง ๑ ปีหรือปรับไม่เกิน ๕๐๐,๐๐๐ ถึง ๑,๐๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ ส่วนระวางโทษปรับทางปกครองไม่เกิน ๕๐๐,๐๐๐ ถึง ๕,๐๐๐,๐๐๐ บาท

๖. การทำงานแบบ Work From Home

การทำงานที่บ้านเป็นหนึ่งในมาตรการเว้นระยะห่างทางสังคม (Social Distancing) ในช่วงการแพร่ระบาดของโควิด-๑๙ เนื่องจากเป็นการจำกัดการติดต่อและการสัมผัสระหว่างคน ซึ่งช่วยลดอัตราการแพร่เชื้อโรคได้อย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งในช่วงที่ยังไม่มีวัคซีนและยารักษาโรค

จากงานวิจัยเรื่อง ทัศนคติและพฤติกรรมการทำงานที่บ้านของพนักงานบริษัท[๑๐] มีวัตถุประสงค์เพื่อนำเสนอการประยุกต์ใช้เทคโนโลยีเพื่ออำนวยความสะดวกในการปฏิบัติงาน โดยการเก็บรวบรวมข้อมูลซึ่งใช้แบบสอบถามเป็นเครื่องมือในการเก็บข้อมูลจากตัวอย่างจำนวน ๔๐๐ คน ซึ่งได้แก่พนักงานบริษัทที่ต้องทำงานในสำนักงานที่อยู่ในเขตกรุงเทพมหานครและปริมณฑล ด้วยวิธีการเลือกตัวอย่างตามวิจารณญาณ โดยพิจารณา

[๑๐] โสภิต บวรไชยชาญ, (๒๕๕๕). **ปัจจัยและทัศนคติของพนักงานบริษัทต่อพฤติกรรมการทำงานที่บ้าน**. จุฬาลงกรณ์มหาวิทยาลัย. สืบค้น ๕ พฤษภาคม ๒๕๖๓ จาก https://www.car.chula.ac.th/display7.php?bib=b2124747

ให้มีการกระจายตามลักษณะงานและประสบการณ์การทำงาน สถิติที่ใช้ในการวิเคราะห์ข้อมูล คือ สถิติทดสอบค่าเฉลี่ยของข้อมูล ๒ กลุ่มที่เป็นอิสระต่อกัน การวิเคราะห์ความแปรปรวนแบบทางเดียว สถิติทดสอบไคสแควร์ และเทคนิคการวิเคราะห์ความถดถอยโลจิสติกส์ ผลการศึกษาพบว่า ลักษณะทางประชากรศาสตร์ที่มีผลต่อทัศนคติในการทำงานที่บ้าน ประกอบไปด้วยเพศ อายุ ลักษณะงาน และสถานภาพสมรส แต่ลักษณะทางประชากรศาสตร์ไม่มีผลต่อพฤติกรรมการทำงานที่บ้าน นอกจากนี้ ยังพบว่าทัศนคติในการทำงานที่บ้านด้านการบริหารชีวิตส่วนตัว และทัศนคติในการทำงานที่บ้านด้านการบริหารการทำงาน อิทธิพลต่อการเลือกบริษัทที่ทำงาน และความต้องการทำงานที่บ้านอย่างมีนัยสำคัญทางสถิติ การทำงานที่บ้านเป็นอีกทางเลือกหนึ่งขององค์กรในการลดค่าใช้จ่ายและประหยัดพลังงาน รวมถึงสร้างคุณภาพชีวิตที่ดีให้แก่พนักงาน อย่างไรก็ตาม ยังต้องอาศัยเวลาในการปรับกระบวนการของแนวคิดก่อนการนำไปใช้ในองค์กร เนื่องจากยังมีปัญหาหรือข้อจำกัดอีกมาก อย่างไรก็ดีธุรกิจต่าง ๆ ที่จำหน่ายสินค้าหรือบริการที่สนับสนุนการทำงานที่บ้านอาจใช้โอกาสนี้ในการทำการตลาดสินค้าหรือบริการของตนเองให้กับองค์กรที่มีการนำเอาการทำงานที่บ้านไปประยุกต์ใช้ได้

จากประสบการณ์ Work From Home มา ๑๐ ปี ของหัวหน้าฝ่ายการตลาดของ Google ประเทศไทย ในปัจจุบันกระแสของการทำงานที่บ้าน (Work From Home) กำลังเป็นที่นิยม เพราะการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา ๒๐๑๙ (COVID-19) ที่มีความน่ากังวลมากขึ้นเรื่อย ๆ หลายบริษัทกำลังพิจารณาให้พนักงานทำงานที่บ้านเพื่อลดความเสี่ยงที่พนักงานจะติดโรคจากการเดินทางมาทำงานที่สำนักงาน[๑๑]

ปัญหาสำคัญ คือ หลายบริษัทยังไม่เคยทดลองให้พนักงานทำงานที่บ้านมาก่อน เมื่อถึงคราวจำเป็นที่สถานการณ์บีบบังคับ จึงต้องมีการปรับการทำงานใหม่ในระยะเวลาอันสั้นซึ่งเป็นเรื่องที่ไม่ง่าย ย้อนกลับไปเมื่อ ๑๐ ปีที่แล้ว การทำงานที่บ้านยังมีข้อจำกัดมาก โดยเฉพาะการประชุมทางไกล ซึ่ง Google ใช้การประชุมผ่านทางโทรศัพท์ (Conference Call) ยังไม่มีแอปพลิเคชันที่จะใช้คุยงานกันโดยตรง ข้อเสียคือ เป็นการทำงานแบบไม่เห็นหน้ากัน ทำให้บางครั้งการประชุมกับชาวต่างชาติหลากหลายสำเนียงอาจเผชิญกับความยากลำบากบ้างเพราะไม่ได้เห็นหน้า ต้องอาศัยการอ่านปากช่วย ในยุคต่อมาเมื่อเทคโนโลยีดีขึ้น Google จึงนำระบบ VDO Conference เข้ามาใช้ผ่านทางแอปพลิเคชัน Google Hangout แต่ความเร็วอินเทอร์เน็ตยังไม่ได้รวดเร็วเหมือนในปัจจุบัน จึงพบปัญหาภาพไม่ชัดเสียงหายบ้าง ซึ่งการประชุมทางไกลของ Google จะต้องมีการสลับเวลาการประชุมตาม Time Zone ของพนักงานแต่ละคน ไม่ใช่ประชุมที่เวลาเดิมตลอด เป็นการหาจุดลงตัวให้กับพนักงาน

อุปสรรคต่อหน่วยงานในสถานการณ์ที่ต้องทำงานในรูปแบบ Work From Home[๑๒]

๑) การเผยแพร่ข้อมูลโดยไม่ได้ตั้งใจ

แม้หลาย ๆ กรณีการโจรกรรมข้อมูลส่วนใหญ่อาชญากรไซเบอร์อาจเป็นสาเหตุหลัก แต่จากข่าวที่เกี่ยวกับข้อมูลรั่วไหลหลาย ๆ ครั้งเกิดจากความประมาทเลินเล่อของบุคลากรในหน่วยงานเองที่ส่งข้อมูลออกไปภายนอกโดยไม่ได้ตั้งใจ

---

[๑๑] Pran Suwannatat, (๒๕๖๓). **ถอดประสบการณ์ Work From Home ของผู้บริหาร Jitta ทำมา ๑๐ ปี ตั้งแต่ยังไม่มีวิกฤต**. สืบค้น ๑๐ พฤษภาคม ๒๕๖๓ จาก https://brandinside.asia/entrepreneur-tell-how-work-from-home-look-like/

[๑๒] CIS Professional Center Co., Ltd., (๒๕๖๓). **ยกระดับการทำงานแบบ Work From Home ให้มั่นคงปลอดภัยด้วย CYBER SECURITY PROTECTION INSURANCE**. สืบค้น ๑๓ พฤษภาคม ๒๕๖๓ จาก https://www.techtalkthai.com/cybersecurity-protection-insurance-by-acis/

๒) Ransomware (หรืออีกชื่อเรียก WannaCrypt เป็นมัลแวร์ที่ทำการฝังตัวเข้ามาจากเว็บไซต์หรือไฟล์แนบที่มากับอีเมลที่ไม่มีการระบุตัวตนที่ชัดเจน)

การโจมตีเหล่านี้ยังคงอยู่และมีแนวโน้มเพิ่มขึ้นเรื่อย ๆ หน่วยงานต่าง ๆ มักตกเป็นเหยื่อของการเรียกค่าไถ่ข้อมูลที่มักเป็นข้อมูลสำคัญขององค์กร ส่วนใหญ่มักเกิดจากการถูกหลอกลวงแบบฟิชชิ่ง (Phishing เป็นรูปแบบหนึ่งของการทำ Social Engineering ซึ่งเป็นเทคนิคการหลอกลวงโดยใช้จิตวิทยาผ่านระบบคอมพิวเตอร์ มักมาในรูปของอีเมลหรือเว็บไซต์เพื่อหลอกให้เหยื่อเผยข้อมูลความลับต่าง ๆ เช่น รหัสผ่านหรือหมายเลขบัตรเครดิต เป็นต้น)

๓) การตั้งรหัสผ่านไม่ปลอดภัยพอ

จากการศึกษาเกี่ยวกับข้อมูลการล็อกอิน พบว่าการตั้งรหัสผ่านมักเป็นจุดอ่อนที่จะนำไปสู่การขโมยข้อมูลในหน่วยงาน เนื่องจากหลาย ๆ คนมักใช้รหัสผ่านที่คาดเดาได้ง่ายและมักใช้รหัสผ่านชุดเดียวกันนี้มาใช้ในการเข้าถึงข้อมูลส่วนตัวและข้อมูลในที่ทำงาน

๔) การไม่จำกัดช่องทางการเข้าถึงข้อมูล

หลายๆ หน่วยงานมักไม่ได้จำกัดสิทธิ์ในการเข้าถึงข้อมูล ควรมีการกำหนดสิทธิ์การเข้าใช้งาน หรือกำหนดนโยบายการเข้าถึงข้อมูลที่รัดกุมมากขึ้น

๕) Phishing Email

ในปีที่ผ่านมาพบว่าการโจมตีแบบใช้ Phishing Email (คำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น) เพิ่มสูงขึ้นอย่างต่อเนื่องจากการคิดค้นหาหนทางใหม่ ๆ ของเหล่าแฮกเกอร์เพื่อหลบเลี่ยงการตรวจจับ การแทรกซึมเข้าสู่ระบบผ่านทางผู้ใช้งานที่ไม่ระมัดระวังและขาดความตระหนักรู้

วิธีทำงานจากที่บ้าน Work From Home ซึ่งปฏิเสธไม่ได้ที่หลายบริษัท สถานศึกษา รวมถึงหน่วยงานภาครัฐบางแห่งเริ่มปรับตัวให้ใช้วิธีทำงานที่บ้าน Work From Home เพื่อลดความเสี่ยงจากการติดไวรัส COVID-19 แต่ใช่ว่าจะทำงานได้อย่างราบรื่น ยังต้องรู้และรับมือภัยไซเบอร์ด้วย ทาง ThaiCERT ได้แปลบทความจากทางสถาบัน SANS มีข้อแนะนำ ๕ ข้อในการรับมือภัยขณะทำงาน Work From Home ดังนี้[๑๓]

๑) ระวังไม่ให้ตกเป็นเหยื่อการโจมตีแบบวิศวกรรมสังคม (Social Engineering) การทำงานออนไลน์จากบ้าน จำเป็นต้องมีการติดต่อสื่อสารหรือรับส่งไฟล์กับบุคคลอื่นมากกว่าการทำงานตามปกติ ผู้ประสงค์ร้ายอาจฉวยโอกาสนี้ในการส่งอีเมลหลอกลวง แนบไฟล์มัลแวร์ หรือแนบลิงก์ที่พาไปยังเว็บไซต์ฟิชชิ่งเพื่อหลอกขโมยรหัสผ่านได้ ทั้งนี้ควรทบทวนกระบวนการสั่งงานและการอนุมัติสั่งงาน เนื่องจากการโจมตีประเภท Business Email Compromise (การหลอกให้โอนเงินผ่านทางอีเมล) หรือ CEO Fraud (การแอบอ้างทางอีเมล) ซึ่งเป็นการแฮกอีเมลของผู้บริหารแล้วสั่งให้ส่งข้อมูลหรือสั่งให้โอนเงินนั้นอาจก่อให้เกิดความเสียหายต่อองค์กรได้

๒) รักษาความมั่นคงปลอดภัยของรหัสผ่าน ควรตั้งรหัสผ่านที่เราจำได้แม่น ไม่ลืม และคาดเดาได้ยาก และไม่ซ้ำกับรหัสผ่านที่เคยใช้ในบริการอื่น หากเป็นไปได้ควรเปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัยเพื่อลดผลกระทบหากเกิดเหตุการณ์รหัสผ่านหลุด รวมถึงพิจารณาใช้โปรแกรมช่วยบริหารจัดการรหัสผ่านร่วมด้วย ทั้งนี้ รวมถึงการตั้งรหัสผ่าน Wi-Fi เพื่อป้องกันไม่ให้

---

[๑๓] iT24Hrs-s, **วิธีทำงานจากที่บ้าน work from home ให้ปลอดภัยจากภัยไซเบอร์.** ๑๘ มีนาคม ๒๕๖๐. สืบค้น ๑๓ พฤษภาคม ๒๕๖๓ จาก https://www.it24hrs.com/2020/warning-work-from-home/

ผู้ไม่ได้รับอนุญาตแอบเชื่อมต่อ Wi-Fi แล้วแพร่กระจายมัลแวร์หรือดักขโมยข้อมูล

๓) การทำงานจากที่บ้านอาจไม่ได้หมายความว่าต้องอยู่แค่ในบ้านเสมอไป หากจำเป็นต้องทำงานนอกบ้าน เช่น ตามร้านกาแฟหรือศูนย์การค้า หรือตาม Co-working space หากเป็นไปได้ควรเชื่อมต่อ Wi-Fi จากโทรศัพท์มือถือ หากจำเป็นต้องเชื่อมต่อ Wi-Fi สาธารณะควรใช้ VPN ทั้งนี้ควรอัปเดตระบบปฏิบัติการ ซอฟต์แวร์ที่ใช้งานให้ใหม่อยู่เสมอ และฐานข้อมูลของโปรแกรมแอนติไวรัสควรได้รับการอัปเดตและสแกนอย่างสม่ำเสมอเช่นกัน

๔) ทำความเข้าใจกับคนอื่นเรื่องอุปกรณ์ส่วนตัวที่มีข้อมูลเกี่ยวข้องกับงาน สงวนไว้เฉพาะกับเรื่องงานเท่านั้น ไม่ควรให้ผู้อื่นที่ไม่เกี่ยวข้องมาใช้งานอุปกรณ์ดังกล่าว เพราะอาจเสี่ยงติดมัลแวร์หรือข้อมูลรั่วไหลได้

๕) เตรียมพร้อมการแจ้งเหตุและประสานงานกับทีมไอทีขององค์กรเนื่องจากการทำงานนอกสำนักงานนั้นอาจมีข้อจำกัดบางอย่างที่ทำให้ระบบการรักษาความมั่นคงปลอดภัยขององค์กรไม่อาจป้องกันได้ หากพบเหตุการณ์ผิดปกติ ควรประสานกับผู้ที่เกี่ยวข้องให้ทราบโดยเร็วที่สุด

บทสรุป : แนวทางป้องกันการรักษาความมั่นคงปลอดภัยไซเบอร์ในการทำงานแบบ Work From Home

๑) ตรวจสอบและยืนยันสิทธิ์การเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นในการเข้าถึงระบบและข้อมูล

๒) เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบการป้องกันการโจมตี เช่น Web Application Firewall หรือ DDoS

๓) แจ้งเจ้าหน้าที่ของหน่วยงานและบุคลากรให้เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่เปิดไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับจดหมาย (Mail) แนบจากคนที่ไม่รู้จัก ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมต่าง ๆ หรือช่องทางการสื่อสารออนไลน์ (Social Network) ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์

๔) หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบข้อมูลการเข้าถึงระบบที่สำคัญ เช่น ข้อมูล Log ย้อนหลัง ๓๐ วัน เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล

๕) ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ (Log) การเข้าใช้งานระบบไม่ต่ำกว่า ๙๐ วัน หรือตามที่กฎหมายกำหนด

๖) หากเป็นไปได้ให้หน่วยงานส่งรายชื่อผู้ติดต่อ (Contact Point) กรณีเกิดเหตุภัยคุกคามไซเบอร์มายังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT)

๗) ไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบในการใช้บริการอินเทอร์เน็ต เพราะหากโดนแฮกเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่น ๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

๘) ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และอ่านพิจารณาข้อมูลก่อนการแชร์ต่อตลอดจนไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

อย่างไรก็ตาม การรักษาความมั่นคงปลอดภัยไซเบอร์ในการทำงานแบบ Work From Home จำเป็นต้องใช้เทคโนโลยี และที่สำคัญคือ ความรู้ความสามารถ ความตระหนักในการใช้งานระบบอินเทอร์เน็ตของบุคลากรแต่ละคน การคำนึงถึงความสอดคล้องกับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ของหน่วยงานนั้น ๆ มีการนำนโยบายมาเป็นแนวทางในการปฏิบัติและพัฒนาตนเองและหน่วยงาน โดยเฉพาะในเรื่องของการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อรับมือกับภัยคุกคามรูปแบบใหม่ อีกทั้งยังเป็นการยกระดับการทำงานให้มีความเป็นมาตรฐานเทียบเท่าระดับสากล

เอกสารการอ้างอิง

ธรรมนิติ DHARMNITI, **๘ ประเด็นสำคัญจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล**. สืบค้น ๑๗ พฤษภาคม ๒๕๖๓ จาก https://www.dharmniti.co.th/law-digital-personaldataprotectionlaw/

บริษัท TOT (ดิจิทัลทิปส์), **รู้ให้ชัด กับ พ.ร.บ. การรักษาความปลอดภัยมั่นคงไซเบอร์ พ.ศ. ๒๕๖๒**. สืบค้น ๔ พฤษภาคม ๒๕๖๓ จาก tot.co.th/blogs/ดิจิทัลทิปส์/now-trending/ดิจิทัลทิปส์/2019/07/01/รู้ให้ชัด-กับ-พ.ร.บ.-การรักษาความปลอดภัยมั่นคงไซเบอร์-พ.ศ.-2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, ราชกิจจานุเบกษา, เล่ม ๑๓๖ ตอนที่ ๖๙ ก, ๒๗ พฤษภาคม ๒๕๖๒.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, ราชกิจจานุเบกษา, เล่ม ๑๓๖ ตอนที่ ๖๙ ก, ๒๗ พฤษภาคม ๒๕๖๒.

ไพโรจน์ ธรรมศีลสุวรรร, (๒๕๖๐). ICT Trend Watch (ตอนที่ ๕๗) ความร่วมมือระหว่างภาคส่วนองค์กร เพื่อรับมือการโจมตีทางไซเบอร์. สืบค้น ๑๐ พฤษภาคม ๒๕๖๓ จาก http://www.cioworldmagazine.com/dr-pairoj-dhamsinsuwan-ict-trend-watch-57-csirt/

วิทวัส มงคลนวเสถียร, **การคุ้มครองข้อมูลส่วนบุคคล**. ๑๐ พฤษภาคม ๒๕๖๒. สืบค้น ๒๐ พฤษภาคม ๒๕๖๓ จาก https://www.gotoknow.org/posts/661602

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.), (๒๕๕๙). **ความมั่นคงปลอดภัยทาง ไซเบอร์ (Cyber Security)**.

สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย, **เมื่อเครื่องคอมพิวเตอร์ติดมัลแวร์ (Malware) และมีการติดต่อไปยัง C&C เซิร์ฟเวอร์**. สืบค้น ๔ พฤษภาคม ๒๕๖๓ จาก https://www.it.chula.ac.th/th/node/4722

โสภิต บวรไชยชาญ, (๒๕๕๕). **ปัจจัยและทัศนคติของพนักงานบริษัทต่อพฤติกรรมการทำงานที่บ้าน**. จุฬาลงกรณ์มหาวิทยาลัย. สืบค้น ๕ พฤษภาคม ๒๕๖๓ จาก https://www.car.chula.ac.th/display7.php?bib=b2124747

CIS Professional Center Co., Ltd., (๒๕๖๓). **ยกระดับการทำงานแบบ Work From Home ให้มั่นคงปลอดภัยด้วย CYBER SECURITY PROTECTION INSURANCE**. สืบค้น ๑๓ พฤษภาคม ๒๕๖๓ จาก https://www.techtalkthai.com/cybersecurity-protection-insurance-by-acis/

Department of Defense NetOps Strategic Vision, December 2008 : Department of Defense Chief Information Officer The Pentagon – Washington. D.C..

iT24Hrs-s, **วิธีทำงานจากที่บ้าน work from home ให้ปลอดภัยจากภัยไซเบอร์.** ๑๘ มีนาคม ๒๕๖๐. สืบค้น ๑๓ พฤษภาคม ๒๕๖๓ จาก https://www.it24hrs.com/2020/warning-work-from-home/

Mariam IbrahimEmail authorAhmad AlsheikhQays Al-Hindawi, (2019). **Automatic Attack Graph Generation for Industrial Controlled Systems**.

Nattapon Muangtum, **สรุป PDPA พ.ร.บ. ข้อมูลส่วนบุคคล กับ ๗ เรื่อง ที่ผู้ประกอบการต้องให้ความสำคัญ**. ๒๗ เมษายน ๒๕๖๒. สืบค้น ๒๐ พฤษภาคม ๒๕๖๓ จาก https://www.everydaymarketing.co/update-news/7

Pran Suwannatat, (๒๕๖๓). **ถอดประสบการณ์ Work From Home ของผู้บริหาร Jitta ทำมา ๑๐ ปี ตั้งแต่ยังไม่มีวิกฤต**. สืบค้น ๑๐ พฤษภาคม ๒๕๖๓ จาก https://brandinside.asia/entrepreneur-tell-how-work-from-home-look-like/