howto

หนังสือที่ทุกคนต้องมี
เพื่อรู้วิธีป้องกันตัวเอง
จากภัยร้อยพัน
ของอาชญากรรมออนไลน์

CYBER SECURITY

อย่าปล่อยให้ใคร มาใช้ข้อมูลคุณ

- รหัสรั่วจากมือถือ โดนล้วงเงินหมดบัญชี
- อีเมลลวงดูดความลับจากคอมพ์
- ลิงก์เว็บไซต์ปลอมหลอกปล้นข้อมูล

รศ. ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ
เกียรติศักดิ์ จันทร์ลอย
สมชิต กิจทองพูล
เขียน

howto

CYBER SECURITY

อย่าปล่อยให้ใครมาใช้ข้อมูลคุณ

รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ
เกียรติศักดิ์ จันทร์ลอย
สมชิต กิจทองพูล
เขียน

การอ่านคือรากฐานที่สำคัญ

ความรู้มีอยู่ทั่วไป การเก็บเกี่ยวที่ดีคือการอ่านและนำไปใช้
–คณะผู้เขียน

หนังสือคุณภาพ
โดยอมรินทร์กรุ๊ป

Cyber Security
อย่าปล่อยให้ใครมาใช้ข้อมูลคุณ

howto

ในเครือบริษัทอมรินทร์พริ้นติ้ง แอนด์ พับลิชชิ่ง จำกัด (มหาชน)
378 ถนนชัยพฤกษ์ (บรมราชชนนี) เขตตลิ่งชัน กรุงเทพฯ 10170
โทรศัพท์ 0-2422-9999 ต่อ 4964, 4969 E-mail: info@amarin.co.th
www.amarinbooks.com amarinbooks Amarin How-To

พิมพ์ครั้งแรก เมษายน 2564

ข้อมูลทางบรรณานุกรมของศูนย์ข้อมูลอมรินทร์

พงษ์พิสิฐ วุฒิดิษฐโชติ.
Cyber Security : อย่าปล่อยให้ใครมาใช้ข้อมูลคุณ / รศ. ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ, เกียรติศักดิ์ จันทร์ลอย และสมชิต กิจทองพูล. เขียน.— กรุงเทพฯ: อมรินทร์ฮาวทู อมรินทร์พริ้นติ้ง แอนด์ พับลิชชิ่ง, 2564.
(20), 184 หน้า: ภาพประกอบ (สี).

1. ความปลอดภัยของข้อมูล. 2. การควบคุมการเข้าถึงข้อมูล. I. เกียรติศักดิ์ จันทร์ลอย, ผู้แต่งร่วม. II. สมชิต กิจทองพูล, ผู้แต่งร่วม. III. ชื่อเรื่อง.

005.8 พ2ช9 DDC 005.8
ISBN 978-616-18-4214-7

คำนิยม

ปัจจุบันอุปกรณ์คอมพิวเตอร์และอิเล็กทรอนิกส์ต่าง ๆ ได้กลายเป็นสิ่งที่ขาดไม่ได้ในการใช้ชีวิต ทั้งด้านส่วนตัวและด้านการทำงาน ในขณะเดียวกันโลกได้เปลี่ยนแปลงไปอย่างมาก โดยเฉพาะภัยที่มากับเทคโนโลยีคอมพิวเตอร์ที่เราคาดไม่ถึงที่ทำความเสียหายให้กับบุคคลและองค์กรในรูปแบบต่าง ๆ ซึ่งมีคำเฉพาะเรียกว่า "ภัยคุกคามทางไซเบอร์" ประเทศต่าง ๆ รวมทั้งประเทศไทยได้นำเรื่องนี้ขึ้นเป็นวาระแห่งชาติ มีการจัดทำกฎหมายขึ้นเฉพาะเพื่อบังคับใช้ให้เกิดความปลอดภัยและลดความเสี่ยงที่อาจมี ซึ่งเป็นเรื่องใกล้ตัวมากกว่าที่หลายคนเคยคิด

หนังสือเล่มนี้เป็นหนังสือที่เขียนเรื่องยากให้เข้าใจง่าย แต่ยังคงความกว้างและลึกของเนื้อหาที่เป็น "แก่น" ของภัยคุกคามทางไซเบอร์ ทั้งข้อมูลส่วนบุคคลและความเป็นส่วนตัว เล่าถึงที่มาที่ไปของเรื่องราวต่าง ๆ ช่วยส่งเสริมความเข้าใจได้อย่างดีเยี่ยม รวมถึงกรณีตัวอย่างต่าง ๆ ที่เกิดขึ้น หนังสือเล่มนี้เขียนด้วยภาษาที่ง่ายเหมาะสมกับผู้อ่านทั่วไป สามารถอ่านเพื่อเพิ่มความรู้รอบตัวได้อย่างดี และยังเป็นพื้นฐานสำหรับการเรียนรู้ในขั้นสูงต่อไปด้วย

การเข้าสู่สังคมยุคดิจิทัลที่สมบูรณ์จำเป็นอย่างมากสำหรับการขับเคลื่อนเศรษฐกิจและสังคมในโลกสมัยใหม่และในอนาคต ต้องขอขอบพระคุณคณะผู้เขียนทั้ง 3 ท่าน คือ รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ คุณเกียรติศักดิ์ จันทร์ลอย และคุณสมชิต กิจทองพูล ที่ได้ตั้งใจรวบรวมเนื้อหาและประพันธ์ขึ้นมา สมดังเจตนารมณ์ "ความรู้มีอยู่

ทั่วไป การเก็บเกี่ยวที่ดีคือการอ่านและนำไปใช้" ผมเชื่อมั่นว่าท่านผู้อ่านจะได้รับประโยชน์จากหนังสือเล่มนี้อย่างมาก เกิดความตระหนักว่า "ภัยไซเบอร์ใกล้ตัวกว่าที่คิด" และช่วยกันเผยแพร่ในวงกว้างต่อไป

ดร. นพ.บดินทร์ ทรัพย์สมบูรณ์
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ด้านสาธารณสุข

คำนิยม

จากคำถามที่ว่า "ประเทศไทยพร้อมหรือไม่กับการรับมือการโจมตีทางไซเบอร์และการรักษาอธิปไตยไซเบอร์ของชาติ" เป็นคำถามที่คนไทยหลายท่านคงอยากทราบคำตอบ ปัญหาอาชญากรรมไซเบอร์ ภัยคุกคามไซเบอร์ การโจมตีทางไซเบอร์ต่อภาครัฐ ภาคเอกชน และประชาชนทั่วไป (Rising of Cyber Crime at National Level) ประชาชนส่วนใหญ่ ตลอดจนองค์กรทั้งภาครัฐและเอกชน ล้วนถูกโจมตีทางไซเบอร์รายวัน ส่งผลต่อเศรษฐกิจและสังคม รวมทั้งความเชื่อมั่นในระดับชาติ

การสร้างความตระหนักรู้ถึงความสำคัญเรื่องการใช้ชีวิตอย่างมั่นคงปลอดภัยในโลกไซเบอร์จึงเป็นเรื่องสำคัญ และจำเป็นที่ประชาชนชาวไทยต้องรู้เท่าทันเพื่อเป็นส่วนหนึ่งในการแก้ปัญหาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ และจากกระแส "Digital Disruption" ทั่วโลก ทำให้เราปฏิเสธไม่ได้ว่าการเปลี่ยนแปลงทางดิจิทัลของโลกมีผลต่อการดำเนินชีวิตประจำวันของมนุษย์ทุกคนบนโลกใบนี้อย่างหลีกเลี่ยงไม่ได้ คำว่า "Digital Transformation" หรือ "Digital Disruption" เป็นสิ่งที่เราได้ยินได้ฟังกันบ่อย ๆ ปัจจัยทั้งสี่ที่มีผลต่อการเปลี่ยนแปลงทางดิจิทัลดังกล่าว (The Four IT Mega Trends in S-M-C-I Era) ได้แก่ S หมายถึง Social Media M หมายถึง Mobile Computing C หมายถึง Cloud Computing และ I หมายถึง Information หรือ Big Data เทคโนโลยีการวิเคราะห์ข้อมูลขนาดใหญ่ ตลอดจนการเปลี่ยนแปลงของโลกจากเทคโนโลยี ปัญญาประดิษฐ์ (Artificial Intelligence) และอินเทอร์เน็ตในทุกสิ่ง (Internet of Things) กำลังมีการพัฒนาและประยุกต์ใช้อย่างแพร่หลายทั่วโลก โดย

การเปลี่ยนแปลงครั้งใหญ่จากปัจจัยทั้งสี่ดังกล่าวมีผลกระทบเกิดขึ้นใน 3 ระดับ ได้แก่ ระดับบุคคลและครอบครัว ระดับองค์กร และในระดับประเทศ

ผมขอชื่นชม รศ. ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ และทีมงาน ที่มีความวิริยอุตสาหะในการประพันธ์หนังสือเล่มนี้ ซึ่งเป็นหนังสือเกี่ยวกับ Cyber Security และ Privacy สำหรับให้ความรู้กับประชาชน ออกแบบเนื้อหามาให้อ่านและทำความเข้าใจได้โดยง่าย จึงขออวยพรให้อาจารย์และทีมงานประสบความสำเร็จในการให้ความรู้ประชาชนชาวไทยสมดังที่ได้ตั้งใจ ขอให้หนังสือเล่มนี้มีส่วนร่วมในการช่วยแก้ปัญหาความมั่นคงปลอดภัยไซเบอร์ระดับชาติในระยะยาวต่อไป

ปริญญา หอมเอนก

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

คำนิยม

ตั้งแต่ประเทศไทยเริ่มมีอินเทอร์เน็ต ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ก็เป็นหัวข้อที่คุยกันไม่จบทั้งในวงการวิชาการ เทคโนโลยี ธุรกิจ และประชาชนทั่วไป ในยุคดิจิทัลที่เทคโนโลยีอย่างอินเทอร์เน็ตออฟธิงส์ (Internet of Things : IoT) บิ๊กดาต้า (Big Data) และปัญญาประดิษฐ์ (AI) ส่งเสริมให้เกิดความสะดวกสบายที่เราเข้าถึงได้ด้วยปลายนิ้ว สิ่งเหล่านี้คงไม่ได้มาฟรี แต่ต้องแลกกับความเสี่ยงหลายประการที่ครอบคลุมตั้งแต่เบาๆ เช่น การละเมิดสิทธิส่วนบุคคล ไปจนถึงความรุนแรงอย่างอาชญากรรมไซเบอร์ ในฐานะของนักเทคโนโลยี ผมเป็นคนหนึ่งที่ไม่ค่อยหลงเชื่อการหลอกลวงทางไซเบอร์ จนเมื่อเร็วๆ นี้ได้รับอีเมลแจ้งเรื่องไปรษณีย์ส่งไม่ถึงบ้าน จนเกือบพลาดคลิกลิงก์ที่อยู่ในอีเมล ก่อนจะฉุกคิดได้ว่าเป็นสิ่งที่ไม่ควร สิ่งเหล่านี้เข้ามาใกล้ชีวิตพวกเรามากขึ้นจนไม่ควรละเลยที่จะศึกษาเรียนรู้เพื่อให้เท่าทันก่อนที่จะเกิดความเสียหายรุนแรง

ในประเทศไทยมีผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศเชิงลึกจำนวนไม่มาก และยิ่งจำกัดเมื่อเจาะจงลงไปในด้านความมั่นคงปลอดภัยไซเบอร์ เมื่อผู้เชี่ยวชาญด้านนี้ลุกขึ้นมาศึกษากฎหมายที่เกี่ยวข้อง ตั้งแต่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ และอื่นๆ กลายเป็นทรัพยากรบุคคลที่สำคัญอย่างยิ่งในยุคดิจิทัล และการที่ผู้เชี่ยวชาญซึ่งมีอยู่เพียงน้อยนิดนี้ได้ทุ่มเทศึกษาและนำความรู้มาตีแผ่ไว้ในหนังสือเล่มนี้ ถือเป็นเล่มแรกๆ ที่ผมเห็นในประเทศไทย เนื้อหาของหนังสือครอบคลุมความรู้พื้นฐานสำคัญและเชื่อมโยงมายังสิ่งที่พบเจอในชีวิตประจำวัน ครอบคลุมทั้งผลกระทบต่อบุคคล บริษัท และองค์กร

หน่วยงาน ความน่าสนใจของหนังสือเล่มนี้ นอกจากการเล่าจากความรู้เชิงลึกแล้ว ผู้เขียนยังกล้าตีแผ่ด้วยตัวอย่างจริงทั้งที่เป็นข่าวโด่งดังเสียหายรุนแรงในต่างประเทศ จนถึงเหตุการณ์ที่เกิดขึ้นใกล้ตัวในประเทศ ที่สำคัญเล่าด้วยภาษาที่คนทั่วไปเข้าใจได้ง่ายและด้วยความเป็นกลาง เต็มไปด้วยคติเตือนใจให้เราฉุกคิดเหมือนกับที่ผมพบเจอในกรณีอีเมลหลอกลวง

สองในสามของผู้แต่งเป็นบุคคลที่ผมมีโอกาสร่วมงานด้วย ท่านหนึ่งเป็นอาจารย์สอนปริญญาเอกโดยตรงด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนอีกท่านเป็นเพื่อนสมัยมัธยมซึ่งจบทั้งด้านกฎหมายและเทคโนโลยีสารสนเทศ จึงมีความมั่นใจอย่างมากทั้งมุมมองด้านวิชาการ ความรู้ประสบการณ์และความมุ่งมั่นตั้งใจในการผลิตหนังสือเล่มนี้ ผมเชื่อว่าผู้อ่านจะได้ประโยชน์จากเนื้อหา และช่วยส่งเสริมให้ใช้ชีวิตในโลกดิจิทัลปัจจุบันได้อย่างสนุกและปลอดภัย

ดร.ชัย วุฒิวิวัฒน์ชัย

ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์

และคอมพิวเตอร์แห่งชาติ (เนคเทค - สวทช.)

คำนิยม

คุณคงไม่อยากเป็นพระเอกในหนังชีวิต (ออนไลน์) ที่ต้องแสดงบทบาทตามที่ Hacker เขียนบทให้คุณเล่นและรับผิดชอบความเสียหาย

หนังสือเล่มนี้มีประโยชน์ต่อทุกคน ทุกเพศ ทุกวัย ทั้งตัวบุคคลหรือองค์กรธุรกิจ เพราะเป็นการ "สรุปของสรุป" เคสเรื่องราวภัยไซเบอร์ที่คุณไม่จำเป็นต้องเจ็บเอง แต่สามารถเรียนรู้ที่จะมี "สติ" และ "รู้เท่าทัน" ในการป้องกันตนเองและคนที่คุณรักได้

โลกอินเทอร์เน็ตเปิดกว้างให้ทุกคนได้เชื่อมต่อและเข้าถึงข้อมูลข่าวสารได้อย่างเสรีทั้งคนดีและคนไม่ดี ทำให้เป็นทั้งโอกาสและความเสี่ยงซึ่งอาจสร้างความเสียหายต่อทรัพย์สิน หน้าที่การงาน ชื่อเสียง หรือถึงขั้นติดคุก เพราะคุณอาจถูกสวมรอยตัวตน ถูกดักฟัง ถูกแอบอ่านแชต หรือถึงขั้นแอบอ้างเป็นตัวคุณโดยที่คุณไม่ทันรู้ตัว หรือรู้เมื่อสายเสียแล้วและตกเป็นแพะรับบาปในคดีความต่างๆ

ผู้เขียนเป็นทั้งอาจารย์และผู้เชี่ยวชาญโดยตรงเรื่องไซเบอร์ระดับประเทศและสากล ทำให้ประชาชนวงกว้างได้รับประโยชน์จากการอ่านและทำตามจากรูปภาพประกอบในการชี้แนะวิธีแต่ละขั้นตอน เพื่อให้ท่านรอดปลอดภัยจากการเป็นเหยื่อของคนที่จ้องเอาเปรียบท่านในทุกวินาที

หนังสือเล่มนี้เปรียบเสมือนอริยทรัพย์ที่ต้องอ่านและแชร์บอกต่อให้คนที่เรารัก "รีบทำความเข้าใจและทำทันที" เปรียบเสมือนเข็มทิศนำทางสู่ "นิสัยความมั่นคงปลอดภัยไซเบอร์ที่ยั่งยืน" เพราะช่วยให้คุณลดความเสี่ยงและโอกาสถูก Hack ได้ โดยไม่ต้องอาศัยโชคใดๆ

ยิ่งตอนนี้เป็นสังคมไร้เงินสด (Cashless Society) ทำให้คุณยิ่งต้องระมัดระวังและรู้เท่าทันในการใช้ Mobile Banking หรือการสแกน QR Code จ่ายเงินเป็นอย่างยิ่ง เพราะบางท่านผูกบัญชีออมทรัพย์หรือบัญชีเงินเดือนเงินเก็บไว้ ทำให้มีความเสี่ยงสูงและเป็นเป้าหมายปองของเหล่า Hacker ที่จ้องฮุบเงินทั้งหมดของคุณ

ขอย้ำว่าหนังสือเล่มนี้มีคำตอบให้คุณรอดปลอดภัยด้วยวิธีป้องกันที่ทำได้ง่ายๆ และทันที อีกทั้งฝึกให้คุณเป็นคนช่างสังเกตสิ่งแปลกปลอมล่อลวงจากโจรไซเบอร์ทั้งมือสมัครเล่นและมืออาชีพ

สุรชัย ฉัตรเฉลิมพันธุ์
ผู้อำนวยการฝ่ายกลยุทธ์และการบริหารจัดการควบคุมดูแล
ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
ธนาคารกรุงไทย จำกัด (มหาชน)

คำนิยม

เทคโนโลยีช่วยเชื่อมคนในทุกมุมโลกให้เป็นหนึ่งเดียวกันจนพัฒนากลายเป็นสังคมแห่งการติดต่อสื่อสาร ข้อมูลข่าวสารสามารถจัดเก็บและถ่ายโอนได้โดยง่ายในรูปแบบดิจิทัล คงไม่มีใครปฏิเสธว่าทุกวันนี้ข้อมูลข่าวสารกลายเป็นสิ่งที่มีมูลค่าและมีความสำคัญมากในทุกๆด้าน ไม่ว่าจะเป็นในด้านการลงทุน การแข่งขันทางธุรกิจ รวมทั้งการค้นพบ การศึกษาและพัฒนาองค์ความรู้ในด้านต่างๆ จึงไม่น่าแปลกใจที่หน่วยงานทั้งในระดับชาติและระหว่างประเทศไม่ว่าจะเป็นภาครัฐหรือเอกชน ต่างให้ความสำคัญกับข้อมูลข่าวสารในยุคปัจจุบัน มีการเก็บรวบรวมและประเมินผลในลักษณะต่างๆเพื่อประโยชน์ในการวางแผนระบบการทำงานและการบริหารจัดการ หรือการดำเนินกิจการต่างๆของตน แต่ความก้าวหน้าทางเทคโนโลยีในการเก็บข้อมูลดังกล่าวอาจทำให้เกิดการใช้หรือเปิดเผยข้อมูลส่วนบุคคล อันเป็นการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล ทำให้เกิดความเดือดร้อน รำคาญ และความเสียหาย อันถือเป็นการกระทำที่ผิดกฎหมายและละเมิดสิทธิส่วนบุคคลได้

หนังสือเล่มนี้ช่วยจุดประกายในการสร้างความตระหนักรู้ถึงความสำคัญของข้อมูลส่วนบุคคล ภัยคุกคามทางไซเบอร์ในยุคดิจิทัลที่อาจเกิดขึ้นได้ในชีวิตประจำวัน รวมทั้งให้ความรู้เบื้องต้นเกี่ยวกับกฎหมายข้อมูลส่วนบุคคลซึ่งเป็นประโยชน์อย่างยิ่งแก่ผู้สนใจที่จะได้ทราบถึงสิทธิและป้องกันตนเองจากภัยคุกคามดังกล่าว เพื่อความปลอดภัยในยุคดิจิทัล

ดร.สุธาทิพ ยุทธโยธิน
ผู้พิพากษาศาลชั้นต้นประจำสำนักประธานศาลฎีกา

คำนำสำนักพิมพ์

จะเกิดอะไรขึ้น ถ้า...

- **คุณต้องติดคุก 1 ปี 7 เดือน 13 วัน เพื่อสู้คดีเพราะมีคนสวมรอยเอาบัตรประชาชนไปส่งยาเสพติด**
- **ร้านค้าออนไลน์ทำเลขบัตรเครดิตของคุณหลุดสู่สาธารณะ**
- **เงินในบัญชีหายเกลี้ยงเพราะถูกแฮ็กรหัสผ่านที่คุณเซฟไว้ในโทรศัพท์มือถือ**
- **มีคนส่งอีเมลหรือลิงก์เว็บไซต์ปลอมให้คุณกรอกข้อมูลส่วนตัว**
- **มีมิจฉาชีพออนไลน์หลอกให้รักแล้วโอนเงิน**

เรื่องเหล่านี้ต้องบอกว่า “ไม่เกิดกับตัวเองคงไม่รู้!” เพราะในโลกไซเบอร์ ข้อมูลส่วนบุคคลเป็นสินทรัพย์ที่จับต้องไม่ได้ แต่มีมูลค่ามหาศาลกว่าที่คนทั่วไปอย่างเราจะเข้าใจมาก และหากมันรั่วไหลก็สร้างความเสียหายได้มากกว่าที่คิด ตั้งแต่การนำไปหาประโยชน์ส่วนตัว จนถึงเปลี่ยนผลการเลือกตั้งผู้นำประเทศ และนำไปสู่การใส่ความผู้บริสุทธิ์ในคดีอาญา เพราะจากผลการสำรวจพบว่า มิจฉาชีพกว่า 75% หาเหยื่อผ่านทางโซเชียลมีเดียช่องทางต่าง ๆ

ปัจจุบันเราเชื่อมต่อกันทางไซเบอร์มากขึ้นจนกลายเป็นภัยคุกคามจากตัวอย่างข้างต้นเป็นเพียงภัยคุกคามระดับบุคคลที่เป็นเรื่องใกล้ตัวคุณเท่านั้น แต่ทุกวันนี้ภัยคุกคามทางไซเบอร์ได้ขยายวงกว้างและน่ากลัวเกินกว่าจะคาดเดาได้ แม้แต่หน่วยงานหรือองค์กรระดับโลกก็พลาดท่าตกเป็นเหยื่อของภัยคุกคามทางไซเบอร์กันมาแล้ว

หนังสือเล่มนี้เล่าถึงหายนะทางไซเบอร์ที่เกิดขึ้นหลากหลายรูปแบบทั่วโลก และวิธีระวังตัวง่าย ๆ สำหรับผู้อ่านทุกระดับ รวมทั้งความรู้เบื้องต้นเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) หากคุณเคยกรอกข้อมูลส่วนตัวไม่ว่าจะเล็กน้อยแค่ไหนเข้าไปในโลกออนไลน์ ตั้งแต่ซื้อสินค้าบริการ โหลดแอปพลิเคชันต่าง ๆ หรืออนุญาตให้เข้าถึงข้อมูลของตน ไปจนถึงผู้ประกอบการที่ต้องเก็บรักษาข้อมูลผู้คนจำนวนมาก คุณล้วนมีโอกาสตกเป็นเหยื่อและต้องรับผิดชอบต่อความปลอดภัยของข้อมูลในโลกไซเบอร์ทั้งสิ้น

เพราะภัยไซเบอร์ใกล้ตัวกว่าที่คิด อย่าปล่อยให้ใครขโมยข้อมูลของคุณไปใช้ได้ตามใจ

howto

คำนำผู้เขียน

เราอยู่ในยุคดิจิทัลที่การใช้ชีวิตประจำวันล้วนเกี่ยวข้องกับเทคโนโลยีและข้อมูลข่าวสารในโลกไซเบอร์ ซึ่งช่วยอำนวยความสะดวกสบายในการใช้ชีวิต แต่ก็มีภัยแอบแฝงด้วยเช่นกัน โดยที่เราอาจไม่เคยรู้หรือตระหนักเลยจนกว่าจะเกิดผลกระทบขึ้น ไม่ว่าจะเป็นเสียทรัพย์สิน ชื่อเสียง หน้าที่การงาน และบางครั้งอาจถึงขั้นสูญเสียชีวิต เรื่องเหล่านี้เป็นเรื่องจริงที่เกิดขึ้น หนังสือเล่มนี้จึงตั้งใจที่จะพาผู้อ่านท่องไปในโลกไซเบอร์ที่นอกจากมีประโยชน์แล้ว ยังมีภัยคุกคาม มีความเสี่ยง และสร้างความเสียหายแก่เราด้วย เมื่อเกิดขึ้นแล้วมันส่งผลกระทบต่อชีวิตเราอย่างไร มีแนวทางการป้องกันแก้ไขหรือไม่ รวมทั้งยกตัวอย่างกรณีศึกษาที่เกิดขึ้นทั้งในประเทศและต่างประเทศ พร้อมแนะนำวิธีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย (Security Awareness) การใช้ชีวิตในโลกไซเบอร์ให้ปลอดภัย รวมถึงการใช้รหัสผ่าน (Password) ที่ปฏิบัติได้จริง หากท่านไม่อยากตกเป็นข่าวดัง ไม่อยากโดนแฮ็กเฟซบุ๊ก หรือเป็นผู้ต้องหาจากสิ่งที่ไม่ได้กระทำ หนังสือเล่มนี้จะช่วยให้ห่างไกลจากเหตุการณ์เหล่านี้

หลักการบริการแบบบูรณาการทั้งคน กระบวนการ และเทคโนโลยีจะช่วยให้เราและองค์กรบรรลุเป้าหมายในเรื่องของความปลอดภัยและธุรกิจ อีกสิ่งหนึ่งที่สำคัญคือ การรู้จักและเข้าใจกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งน่าจะเป็นสิ่งที่หลายคนรู้สึกว่าเข้าใจยาก รู้ไปทำไม แต่เพื่อรักษาสิทธิของตนเอง คนที่เรารัก และธุรกิจ เราจำเป็นต้องรู้และเข้าใจ แต่ไม่ต้องกังวล ในเล่มได้อธิบายกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลให้เข้าใจแบบง่าย ๆ ในภาษาชาวบ้าน พร้อมทั้งยกตัวอย่างที่มาที่ไปเพื่อให้เข้าใจและนำไปปฏิบัติได้ โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีผลบังคับใช้ซึ่งกระทบกับทุกคนและ

ทุกภาคส่วนธุรกิจอย่างแน่นอน ถ้าท่านอยากมีความปลอดภัย ความเป็นส่วนตัว และไม่อยากเสียเปรียบใคร ต้องอ่านหนังสือเล่มนี้

คณะผู้เขียนได้ผสานศาสตร์และศิลป์ทางด้านเทคโนโลยี ความมั่นคงปลอดภัย ความเป็นส่วนตัว ข้อมูลส่วนบุคคล และกฎหมาย ให้ร้อยเรียงกันเป็นเรื่องราวด้วยภาษาที่เข้าใจง่ายสำหรับประชาชนทั่วไป จนถึงใช้ประกอบการเรียนการสอนได้ถึงระดับบัณฑิตศึกษา ซึ่งมีเป้าหมายมุ่งมั่นให้ประชาชนชาวไทยและประเทศไทยของเรามีความปลอดภัยยิ่งขึ้น ภายใต้หลักของสิทธิส่วนบุคคลและความเป็นส่วนตัว ซึ่งหวังว่าทุกท่านจะได้รับประโยชน์ตามที่คาดหวังไว้ จนสามารถแบ่งปันความรู้กับคนอื่น ๆ ต่อไปได้ในยุคที่ข้อมูลและภัยคุกคามนั้นมีผลต่อชีวิตของเรา

ท้ายนี้ขอขอบพระคุณรองศาสตราจารย์คณาธิป ทองรวีวงศ์ ผู้อำนวยการสถาบันกฎหมายสื่อดิจิทัล มหาวิทยาลัยเกษมบัณฑิต ที่ได้ให้คำแนะนำและตรวจทานเนื้อหาเกี่ยวกับกฎหมายเพื่อความสมบูรณ์มากยิ่งขึ้น

คณะผู้เขียนขออุทิศบุญกุศลนี้แด่บิดามารดา ผู้มีพระคุณ ครูบา-อาจารย์ผู้ประสิทธิ์ประสาทวิชา ผู้เขียนหนังสือ รวมถึงผู้ที่เผยแพร่ความรู้ผ่านทางอินเทอร์เน็ตและช่องทางต่าง ๆ และผู้ที่ให้การช่วยเหลือสนับสนุนทุกท่าน หากมีข้อผิดพลาดประการใดในหนังสือเล่มนี้ คณะผู้เขียนพร้อมน้อมรับข้อเสนอแนะจากท่านและรับไปปรับปรุงเพื่อสร้างผลงานที่ดียิ่งขึ้นไป

คณะผู้เขียน

สารบัญ

- **เคสจริงที่เกิดขึ้นแล้วในประเทศไทย**
  - สแกนเช็กอินแอป “ไทยชนะ” แล้วมีโฆษณาแปลก ๆ เข้ามาในมือถือ 107
  - แอป “หมอชนะ” กับคำถามเรื่อง Privacy or Security 108
  - เว็บช็อปปิ้งออนไลน์แอบเก็บรูปของผู้ใช้บริการไว้โดยไม่ได้รับอนุญาต 111
  - ข้อมูลผู้ใช้บริการกว่า 1.1 ล้านบัญชีถูกแฮ็ก 113
  - เว็บรีวิวอาหารถูกดูดข้อมูลกว่า 4 ล้านรายการ 115
  - ค่ายมือถือทำข้อมูลลูกค้าหลุดสู่สาธารณะ 116
  - เว็บจองที่พักทำข้อมูลรั่ว 119
  - แม่บ้านกลายเป็น CIA ประจำองค์กร 122
  - ได้รับลิงก์เว็บไซต์ปลอมหลอกปล้นข้อมูล 124
  - ได้รับ Fake News ว่า KFC แจกอาหารฟรี 125
  - มิจฉาชีพหลอกให้โอนเงิน 4 แสน 126
  - พบรักในโลกออนไลน์แล้วถูกหลอกให้โอนเงิน 128

บทที่ 1

ใช้ชีวิตยากจัง ในยุคดิจิทัล

การใช้ชีวิตโดยปกติทั่วไปก็ว่ายากแล้ว
ยิ่งต้องมาอยู่ในยุคดิจิทัลที่ทุกคนจดจ่ออยู่กับ
การใช้ข้อมูลและชีวิตในสังคมออนไลน์
ก็ยิ่งทำให้ยากขึ้นไปอีกหลายเท่า
มาดูกันว่าการใช้ชีวิตในยุคดิจิทัล
ที่โจรไซเบอร์ผุดขึ้นมากมายต้องทำอย่างไร

นับตั้งแต่เราเข้าสู่ยุคดิจิทัล ข้อมูลส่วนบุคคล ความเป็นส่วนตัว และข้อมูลต่างๆล้วนมีอยู่ทุกหนทุกแห่ง และมีบทบาทกับความเป็นอยู่ของชีวิตเราทุกคนอย่างหลีกเลี่ยงไม่ได้

ในยุคที่ใครๆ ก็พูดกันว่า "Data is the New Oil" ที่ข้อมูลกลายเป็นปัจจัยหลักในการผลักดันเศรษฐกิจ เช่นเดียวกับแหล่งน้ำมันดิบในอดีต ซึ่งเป็นปัจจัยสำคัญในการขับเคลื่อนเศรษฐกิจโลก เรามาทำความรู้จักกับ "ข้อมูลส่วนบุคคล" ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA (Personal Data Protection Act) กันก่อนดีกว่า

ข้อมูลประเภทไหนเรียกว่า "ข้อมูลส่วนบุคคล"

ข้อมูลส่วนบุคคล (Personal Data) คือข้อมูลที่เกี่ยวข้องกับตัวบุคคลผู้เป็นเจ้าของข้อมูลโดยตรง หรือทำให้เชื่อมโยงไปยังเจ้าของข้อมูลได้ง่าย เช่น ชื่อ ที่อยู่ อายุ อาชีพ หมายเลขบัตรประชาชน หรืออีเมล เป็นต้น ซึ่งมีทั้งข้อมูลส่วนบุคคลทางตรง เช่น ข้อมูลจากบัตรประชาชน

หรือทางอ้อมคือไม่ได้ระบุเจาะจงทางตรง แต่สามารถสืบค้นไปถึงตัวบุคคลได้ เช่น IP Address, Login Password ไม่ว่าจะถูกบันทึกในรูปแบบกระดาษหรือรูปแบบอื่น เช่น ในระบบดิจิทัลออนไลน์ โดยไม่คำนึงว่าจะเป็นข้อมูลที่เป็นจริงหรือเท็จ ที่สำคัญพระราชบัญญัตินี้คุ้มครองเฉพาะข้อมูลส่วนบุคคลของคนที่มีชีวิตเท่านั้น ไม่คุ้มครองข้อมูลส่วนบุคคลของคนตาย

นอกจากนี้ยังคุ้มครองไปถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ด้วย เช่น เชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง ความเชื่อ ลัทธิ ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลทางพันธุกรรม และข้อมูลชีวภาพ เป็นต้น

ทุกวันนี้ข้อมูลส่วนบุคคลของเรานั้นถูกนำไปใช้งานต่าง ๆ มากมาย ทั้งโดยรู้ตัว ไม่รู้ตัว ยินยอม หรือไม่ยินยอมก็แล้วแต่ เพราะข้อมูลเป็นหัวใจหลักในการพัฒนาสิ่งต่าง ๆ แต่ทุกอย่างล้วนมีสองด้านเสมอ หากนำไปใช้ในทางที่ถูกก็จะเกิดประโยชน์มหาศาล แต่หากนำไปใช้ในทางที่ผิดก็ส่งผลเสียมากมาย ทั้งต่อทรัพย์สิน อิสรภาพ หรือชีวิต และบางครั้งก็อาจก่อให้เกิดสงครามได้

ชัยชนะแบบพลิกโผของโดนัลด์ ทรัมป์ ในปี 2016 ด้วยการ "ยิงแอด" ไม่ให้คนผิวสีออกไปเลือกตั้ง

หนึ่งในตัวอย่างสำคัญของการนำข้อมูลส่วนบุคคลไปใช้งานแล้วส่งผลให้เกิดการเปลี่ยนแปลงทางการเมืองคือ ชัยชนะแบบพลิกโผของโดนัลด์ ทรัมป์ ในปี 2016 ด้วยการ "ยิงโฆษณาออนไลน์" ไม่ให้ชาวอเมริกันผิวสีออกไปเลือกตั้ง โดยทีมหาเสียงของทรัมป์ได้ใช้บริการบริษัท Cambridge Analytica ของอังกฤษในการสร้างโปรไฟล์คนบนเฟซบุ๊ก แยกเป็นกลุ่ม ๆ และยิงโฆษณาทางการเมืองให้ได้ผลตามต้องการ ลองนึกดูว่าตอนโดนัลด์ ทรัมป์ เป็นประธานาธิบดี เขาพลิกโลกไปแค่ไหน ทั้งท่าทีกับจีนและนานาประเทศ หรือแม้กระทั่งในสหรัฐอเมริกาเอง ส่วนจะดีหรือไม่อย่างไรก็แล้วแต่วิจารณญาณของแต่ละคน แต่ที่แน่ ๆ มันกระทบกับโลกใบนี้มหาศาล!!! นี่แค่ตัวอย่างเดียวเท่านั้น

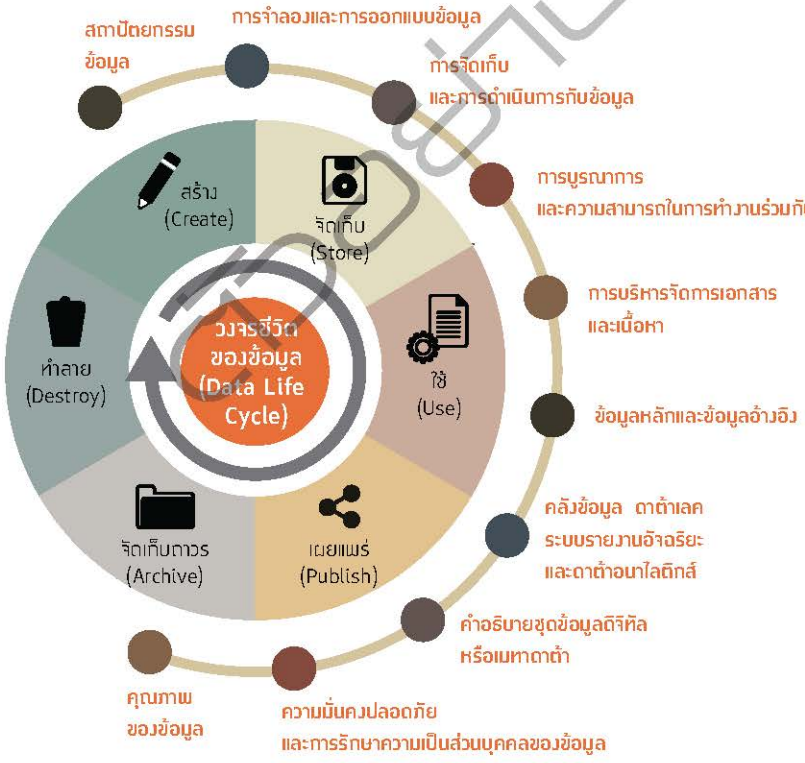
ข้อมูลไม่มีชีวิต แล้วจะสร้างปัญหาให้เราได้ยังไง

ข้อมูลเป็นสิ่งที่มนุษย์สร้างขึ้น ตั้งแต่การจดบันทึกในยุคดึกดำบรรพ์ จนถึงยุคประวัติศาสตร์ จากการแกะสลักไว้ตามผนังถ้ำจนถึงการสลักลงในศิลาจารึก พอมาถึงยุคที่มีกระดาษ เราก็จดบันทึกลงในจดหมายเหตุ ทุกวันนี้ที่เทคโนโลยีทันสมัย เราก็มีการบันทึกลงในรูปแบบดิจิทัล ซึ่งเป็นยุคที่หันไปทางไหนข้อมูลก็อยู่รอบตัวเราไปเสียหมด หากดูเผิน ๆ ก็ไม่น่าก่อให้เกิดปัญหาหรือโทษใด ๆ แต่ในความเป็นจริง **ปัญหาที่เกิดขึ้นกับข้อมูลนั้นล้วนเกิดจากการกระทำของมนุษย์ในทางที่ผิดผ่านวงจรชีวิตของข้อมูล** ไม่ว่าจะขาดความรู้ทั้งโดยตั้งใจนำไปใช้ในทางไม่ดี ขาดความระมัดระวัง หรือประมาทเลินเล่อก็ตาม ยังไม่นับกลุ่ม “อาชญากรไซเบอร์” ซึ่งคอยแสวงหาผลประโยชน์โดยมิชอบในโลกไซเบอร์อีก วิธีการแก้ปัญหาดังกล่าวนั้น เราต้องศึกษาธรรมชาติของข้อมูลก่อน แล้วค่อยไปทำความเข้าใจกับปัญหาของมัน จากนั้นจึงเรียนรู้วิธีใช้เครื่องมือที่เป็นเกราะป้องกันการแก้ปัญหา ซึ่งปัญหาที่เกิดขึ้นนั้นล้วนเกี่ยวกับข้อมูลส่วนบุคคลที่กระทบความเป็นส่วนตัวทั้งสิ้น

วงจรชีวิตของข้อมูล

ถ้าเปรียบข้อมูลเป็นสิ่งมีชีวิต มันก็จะมีวงจรชีวิตของมัน กล่าวคือ มีการเกิดขึ้น ตั้งอยู่ และดับไป เพียงแต่คุณลักษณะพิเศษของมันเป็นสิ่งไม่มีชีวิต จึงมีอายุยืนตราบเท่าที่ไม่มีใครไปทำลายมัน ข้อมูลที่ดีจะถูกพัฒนาเป็นบ่อเกิดองค์ความรู้แก่มนุษย์ทุกชาติทุกภาษาสืบเนื่องต่อกันมา

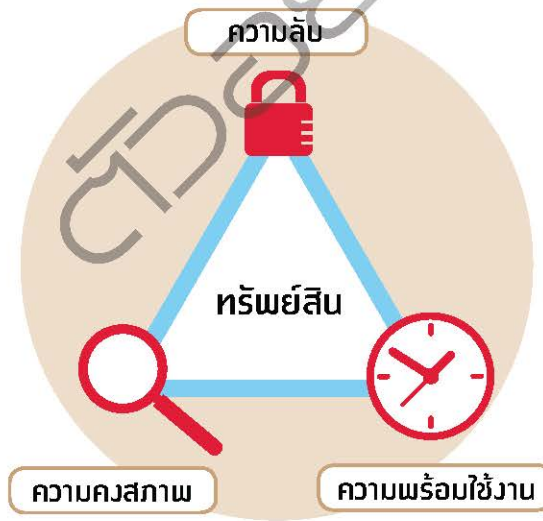
วงจรชีวิตของข้อมูล (Data Life Cycle) คือลำดับขั้นตอนตั้งแต่เริ่มสร้างไปจนถึงการทำลายข้อมูล ซึ่งตลอดทั้งวงจรชีวิตประกอบด้วย 6 ขั้นตอน ดังนี้



ที่มา : Data Governance Framework กรอบการกำกับดูแลข้อมูล เวอร์ชั่น 1.0, สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

1. **การสร้างข้อมูล** (Create) คือการสร้างข้อมูลขึ้นมาใหม่ ทั้งวิธีการจดบันทึกด้วยมือหรือการพิมพ์ข้อความบันทึกในอุปกรณ์อิเล็กทรอนิกส์
2. **การจัดเก็บข้อมูล** (Store) คือการนำข้อมูลที่สร้างขึ้นมาจัดเก็บให้เป็นระเบียบ สะดวกและง่ายต่อการใช้งานตามวัตถุประสงค์ต่าง ๆ รักษาป้องกันไม่ให้สูญหายหรือถูกขโมย ไม่ว่าจะเป็นการจัดเก็บลงแฟ้มเอกสารข้อมูลหรือระบบการจัดการฐานข้อมูลในระบบคอมพิวเตอร์
3. **การใช้ข้อมูล** (Use) คือการนำข้อมูลที่จัดเก็บมาใช้ประมวลผลให้เกิดประโยชน์ตรงตามวัตถุประสงค์ด้านการใช้งานต่าง ๆ เช่น การศึกษาค้นคว้า การวิเคราะห์ข้อมูล การจัดทำรายงาน เป็นต้น
4. **การเผยแพร่ข้อมูล** (Publish) คือการนำข้อมูลไปเปิดเผย ไม่ว่าจะเป็นการส่งมอบเอกสาร หนังสือที่มีการบันทึกข้อมูล หรือการแลกเปลี่ยนข้อมูล การแชร์ข้อมูล การกระจายข้อมูลระหว่างบุคคล องค์กร ตลอดจนการโอนข้อมูลข้ามพรมแดนผ่านระบบคอมพิวเตอร์
5. **การจัดเก็บข้อมูลถาวร** (Archive) คือการคัดลอกข้อมูลเพื่อทำสำเนาสำหรับเก็บรักษา โดยไม่มีการลบ ปรับปรุง หรือแก้ไขข้อมูลนั้นอีก และนำกลับไปใช้งานได้ใหม่เมื่อต้องการ
6. **การทำลายข้อมูล** (Destroy) คือการทำลายข้อมูลไม่ให้มีสภาพการใช้งาน เนื่องจากมีอายุนานเกินไป จนไม่เหมาะสมกับการใช้ประโยชน์ในยุคปัจจุบัน เช่น ทำลายเอกสาร หนังสือ วัตถุที่จดบันทึก ตลอดจนไฟล์ข้อมูลต่าง ๆ ในระบบคอมพิวเตอร์

หากถามว่าในฐานะเจ้าของข้อมูลส่วนบุคคล เราได้อะไรจากเรื่องนี้บ้าง คำตอบคือ "ไม่!" เพราะที่ผ่านมาเราไม่เคยให้ความสำคัญกับการปกป้องข้อมูลส่วนตัวต่าง ๆ ซึ่งอาจทำให้สูญเสียอิสรภาพหรือเป็นอันตรายต่อชีวิต เพราะไม่เคยใส่ใจถึงอันตรายที่เรียกว่า **"ภัยคุกคาม"** (Threat) ซึ่งจะส่งผลต่อตัวเราแม้แต่น้อย ที่สำคัญภัยคุกคามนั้นทวีความรุนแรงขึ้นทุกวัน ยิ่งปัจจุบันเราเชื่อมต่อกันทางไซเบอร์มากขึ้น จากภัยคุกคามทั่วไปก็กลายเป็น **"ภัยคุกคามทางไซเบอร์"** ซึ่งส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยของทรัพย์สินทั้งที่จับต้องได้ เช่น ร่างกายของเรา คอมพิวเตอร์ สมาร์ทโฟน เป็นต้น และจับต้องไม่ได้ เช่น ชื่อเสียง ความลับทางการค้า ความลับส่วนตัว แผนกลยุทธ์ หรือข้อมูลส่วนบุคคล เป็นต้น



การรักษาความมั่นคงปลอดภัย (Security) มีเป้าหมายเพื่อรักษาทรัพย์สินของเราให้มีคุณสมบัติ 3 ประการ หรือเรียกว่า CIA ได้แก่

● **ความลับ** (Confidentiality) คือมาตรการป้องกันเพื่อให้ผู้ได้รับอนุญาตเท่านั้นที่เข้าถึงข้อมูลได้ เช่น การตั้งชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าระบบต่างๆ การใช้รหัส Pin ที่เป็นตัวเลข 4-6 หลัก การสแกนนิ้วมือหรือใบหน้า การใช้บัตรเครดิตคู่กับรหัส Pin เพื่อดูยอดเงินหรือถอนเงินจากตู้ ATM

● **ความคงสภาพ** (Integrity) คือความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม โดยมี 2 กลไกหลัก คือ การป้องกันและการตรวจสอบ เช่น การยืนยันตัวตนด้วยใบหน้า หรือการใช้ตัวเลขหลักสุดท้ายในบัตรประชาชนตรวจสอบความถูกต้องของหมายเลขบัตรประชาชนทั้งหมดที่เรากรอก แต่ต้องใช้สูตรคำนวณเฉพาะ

● **ความพร้อมใช้งาน** (Availability) คือการเข้าถึงและใช้ข้อมูลได้ตามต้องการโดยผู้ใช้หรือระบบที่ได้รับอนุญาตเท่านั้น เช่น การทำระบบสำรองที่มีมากกว่า 1 ระบบทำงานพร้อมกัน หากระบบใดเสีย อีกระบบก็ให้บริการต่อได้

หากยังไม่เห็นภาพว่าการรักษา CIA สำคัญแค่ไหน ให้ลองคิดเล่นๆ ดูว่าถ้าข้อมูลที่เป็นความลับของเราถูกเปิดเผยจะส่งผลเสียอย่างไร หากผลการตรวจเลือดของเราถูกแก้ไขจะส่งผลเสียแค่ไหน หากโปรแกรมที่เราต้องใช้เพื่อทำงานส่งลูกค้าใช้การไม่ได้ ชีวิตหรือธุรกิจของเราจะเป็นอย่างไร นี่คือเหตุผลว่าทำไม CIA หรือการรักษาความมั่นคงปลอดภัยถึงสำคัญมาก

ทุกระบบล้วนมีช่องโหว่

ความจริงแล้วทุกทรัพย์สินมักมีจุดอ่อนหรือช่องโหว่ (Vulnerability) ที่ถูกโจมตีได้ เช่น เรามีเครื่องคอมพิวเตอร์แต่กลับใช้ซอฟต์แวร์เถื่อนก็อาจถูกแฮ็กเข้าระบบได้ง่าย ๆ หรือมีสมาร์ทโฟนแต่ตั้งรหัสผ่านเป็น 123456 ก็อาจทำให้คนอื่นปลดล็อกเครื่องเราได้

สาเหตุของภัยคุกคามนั้นมีมากมายหลายทาง อาจจะเป็นจากคนคุ้นเคย คนแปลกหน้า หรือแฮ็กเกอร์ โดยภัยคุกคามที่เข้าถึงอุปกรณ์คอมพิวเตอร์ของเราโดยตรงจะมุ่งเป้าโจมตีจุดอ่อนหรือช่องโหว่ของระบบหรืออุปกรณ์ซึ่งทำให้เกิดผลลัพธ์เป็นผลกระทบต่อระบบหรืออุปกรณ์นั้น เช่น ทำให้อุปกรณ์เสียหาย ไม่สามารถให้บริการได้ หรือขโมยข้อมูล เป็นต้น

ความสัมพันธ์ของความมั่นคงปลอดภัยและการโจมตีภัยคุกคาม

หลายคนคิดว่า **"ภัยคุกคามทางไซเบอร์"** เป็นเรื่องไกลตัว คงเกิดขึ้นกับคนที่มีชื่อเสียง คนรวย หรือมหาเศรษฐีมากกว่าเราที่เป็นคนธรรมดา หากคุณเป็นคนหนึ่งที่คิดแบบนี้ ถือว่าเป็นความคิดที่ผิดมหันต์และมีความเสี่ยงถูกโจมตีได้มาก เพราะ **"ภัยคุกคาม"** เกิดขึ้นได้กับทุกคนและทุกวัย ทั้งยังเกิดขึ้นทุกวันแทบจะทุกวินาทีเลยก็ว่าได้ บทเรียนในอดีตมีเหตุการณ์ต่าง ๆ เกิดขึ้นมากมาย ตั้งแต่ผลกระทบเล็กน้อยไปจนถึงผลกระทบที่กระจายเป็นวงกว้าง จากแค่บุคคลเดียวไปจนถึงระดับนานาชาติ และภัยคุกคาม

ที่เกิดขึ้นก็ไม่ได้เพิ่งเกิดเมื่อ 2-3 ปีที่แล้ว แต่มีมาเป็นสิบปี และบางทีอาจมีมามากกว่า 50 ปีแล้วด้วยซ้ำ

ก่อนที่จะไปไกลกว่านี้ ผู้เขียนอยากอธิบายความแตกต่างของคำว่า **"ความปลอดภัย"** (Safety) กับ **"ความมั่นคงปลอดภัย"** (Security) ที่หลายคนมักเรียกสลับกันเพื่อให้เข้าใจตรงกันเสียก่อน ความปลอดภัยหมายถึง การพ้นภัย การปราศจากภัย รวมถึงปราศจากอันตรายที่มีโอกาสจะเกิดขึ้น แต่ความมั่นคงปลอดภัยคือการตั้งเป้าหมายเพื่อรักษาทรัพย์สินของเราให้มีคุณสมบัติ 3 ประการตามที่กล่าวไปแล้วคือ การรักษาความลับ การรักษาความคงสภาพ และความพร้อมใช้งาน ที่อธิบายในที่นี้เพื่อให้มองเห็นความแตกต่างระหว่างสองคำนี้ แต่สุดท้ายจะเลือกใช้อย่างไรก็แล้วแต่

เราโดนจารกรรมข้อมูลกันตั้งแต่เมื่อไหร่

"ภัยคุกคามทางไซเบอร์" หรือ "ภัยไซเบอร์" เกิดขึ้นช่วงปี ค.ศ. 1940 โดยเริ่มต้นจากการทดลองแนวคิดที่ว่า **"ไวรัสคอมพิวเตอร์คืออะไร"** แนวคิดนี้ได้รับการกล่าวถึงเป็นครั้งแรกโดยนักคณิตศาสตร์ชื่อจอห์น ฟอน นอยมันน์ (John von Neumann) ซึ่งตีพิมพ์บทความเรื่อง "Theory of Self-Reproducing Automata" เพื่อเป็นการทดลองว่า "สิ่งมีชีวิตเชิงกล" เช่น รหัสคอมพิวเตอร์ที่จะทำให้เครื่องจักรเสียหายนั้นสามารถคัดลอกตัวเองและแพร่เชื้อไปยังคอมพิวเตอร์เครื่องใหม่ได้ และจากทฤษฎีต้นกำเนิดเพียงเรื่องเดียวนี้ ก็ทำให้เกิดเหตุการณ์มากมายภายหลังที่พวกเราคาดไม่ถึง ทั้งเรื่องดีและไม่ดี เช่น การพัฒนาไวรัสคอมพิวเตอร์ขึ้นมาตามหลักการ "การคัดลอกตัวเอง" เป็นต้น

ไวรัสคอมพิวเตอร์มีหลายประเภทและทำงานแตกต่างกันตามหลักการและวิธีการพัฒนาของโปรแกรมเมอร์ แต่ไวรัสคอมพิวเตอร์ทุกตัวล้วนมุ่งเน้นที่จะจารกรรมข้อมูลสำคัญและทำลายระบบการทำงานภายในเครื่องคอมพิวเตอร์ของเรา

ไวรัสคอมพิวเตอร์

เป็นนิยามของโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นมาโดยมีจุดมุ่งหมายเพื่อทำให้ระบบหรือเครื่องคอมพิวเตอร์นั้นไม่สามารถใช้งานได้หรือหยุดชะงัก รวมถึงเพื่อขโมยข้อมูลสำคัญอันมีค่าที่อยู่ในเครื่องคอมพิวเตอร์ ซึ่งสมาร์ทโฟนที่เราใช้งานกันทุกวันก็ทำงานเสมือนเป็นคอมพิวเตอร์เช่นกัน

ในอดีตไวรัสคอมพิวเตอร์ยังมีการทำงานที่ไม่หลากหลายมากนัก เพราะเป็นช่วงเริ่มต้นจากการพัฒนาตามทฤษฎี "Theory of Self-Reproducing Automata" และการใช้งานอินเทอร์เน็ตยังไม่เยอะมาก รวมถึงเครื่องคอมพิวเตอร์ก็มีราคาแพง

ปัจจุบันคำว่า "**มัลแวร์**" (Malware) ซึ่งย่อมาจาก "Malicious Software" หรือซอฟต์แวร์ที่เป็นอันตราย ถูกใช้เป็นชื่อเรียกของโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกสร้าง ออกแบบ และพัฒนาขึ้นโดยมีเจตนามุ่งร้ายต่อระบบคอมพิวเตอร์และระบบเครือข่ายทุกประเภท รวมถึงอุปกรณ์คอมพิวเตอร์ ซึ่งมีหลายรูปแบบ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) สปายแวร์ (Spyware) ไวรัสเรียกค่าไถ่หรือแรนซัมแวร์ (Ransomware) เป็นต้น (อ่านเพิ่มเติมในบทที่ 2)

เนื่องจากไวรัสคอมพิวเตอร์เป็นภัยคุกคามที่เกิดขึ้นบ่อยกับระบบเครือข่ายหรือระบบคอมพิวเตอร์ เราจึงพยายามยับยั้งด้วยการพัฒนา

โปรแกรมป้องกันไวรัส (Antivirus) ขึ้นมา เพื่อศึกษาและเรียนรู้พฤติกรรมการทำงานของไวรัสคอมพิวเตอร์ รวมถึงกระจายข้อมูล และเป็นศูนย์กลางสำหรับใช้พัฒนาซึ่งกันและกันเพื่อหยุดยั้งภัยคุกคามจากไวรัสคอมพิวเตอร์ แต่ถึงอย่างนั้นก็ยังมีภัยคุกคามทางไซเบอร์ที่เราหาวิธีป้องกันหรือยับยั้งได้ยากคือ **"การจารกรรมข้อมูล"** ซึ่งเป็นภัยคุกคามจากการอาศัยช่องโหว่ของซอฟต์แวร์ (เช่น ใช้ซอฟต์แวร์เถื่อน ซอฟต์แวร์หมดอายุ) การตั้งค่าระบบเครือข่ายและระบบคอมพิวเตอร์ (เช่น การตั้งรหัสผ่านที่เดาได้ง่าย) อุปกรณ์เครือข่าย (เช่น เปิดให้เชื่อมต่อจากระยะไกลโดยใช้รหัสผ่านง่าย ๆ) ความผิดพลาดของผู้ใช้งาน (เช่น นำแฟลชไดร์ฟมาต่อเข้าเครื่องคอมพิวเตอร์โดยที่มีไวรัสแฝงอยู่) เป็นต้น

การจารกรรมข้อมูลหรือเจาะระบบคอมพิวเตอร์

เป็นนิยามของกรณีที่แฮ็กเกอร์ (Hacker) ใช้โปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นมาโดยมีจุดประสงค์เพื่อทำให้ระบบหรือเครื่องคอมพิวเตอร์นั้นไม่สามารถใช้งานได้หรือหยุดชะงัก รวมถึงเพื่อขโมยข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์ โดยอาศัยช่องโหว่ของซอฟต์แวร์ การตั้งค่าระบบเครือข่ายและคอมพิวเตอร์ อุปกรณ์เครือข่าย และความผิดพลาดของผู้ใช้งาน เป็นต้น

การจารกรรมข้อมูลหรือการเจาะระบบนั้นเกิดขึ้นตั้งแต่เมื่อร้อยกว่าปีก่อน ซึ่งตั้งแต่ปี ค.ศ. 1900 จนถึงปัจจุบัน ทั่วโลกมีเหตุการณ์อะไรบ้างและมีวิวัฒนาการอย่างไร ผู้เขียนขอยกประเด็นที่เกิดขึ้นในช่วงสำคัญ ๆ ออกมาเป็นตัวอย่าง เพื่อให้ทุกคนเข้าใจวิธีการที่เหล่าแฮ็กเกอร์ใช้เจาะระบบความมั่นคงปลอดภัยดังต่อไปนี้

● **ปี ค.ศ. 1955** "Hacker Meaning" เกิดขึ้นที่ MIT เมื่อพบว่ามีเครื่องจักรทำงานผิดปกติ โดยตรวจสอบพบจากรายงานการประชุมของ

Tech Model Railroad Club ในเดือนเมษายน ค.ศ. 1955 ซึ่งระบุว่า Mr. Eccles พยายามขอให้ใครก็ได้ช่วย "แฮ็ก" (Hacked) หรือหยุดยั้งระบบไฟฟ้าเพื่อปิดเครื่องจักรที่ทำงานผิดปกติ และในเหตุการณ์นี้เองจึงเกิดคำว่า "แฮ็กเกอร์" ขึ้นเป็นครั้งแรก (น่าเสียดายที่คำว่า "แฮ็กเกอร์" นั้นมีจุดเริ่มต้นที่ดี หมายถึงผู้เชี่ยวชาญด้านคอมพิวเตอร์ แต่ในปัจจุบันกลับเป็นคำที่มีความหมายเชิงลบ ซึ่งหมายถึงผู้ไม่ประสงค์ดีที่พยายามเข้าสู่ระบบคอมพิวเตอร์)

- **ปี ค.ศ.** 2010 - 2020 มีเหตุการณ์เกิดขึ้นมากมายและเป็นช่วงที่เหล่าแฮ็กเกอร์จารกรรมและปล่อยข้อมูลออกสู่สาธารณะเพื่อเรียกเงินค่าไถ่ รวมถึงล่มระบบสื่อสารและโครงข่ายพื้นฐานมากมาย เช่น

  - **พฤษภาคม ค.ศ.** 2017 เกิดเหตุการณ์สำคัญขึ้นแทบจะเรียกว่าเป็นชนวนของการเข้าสู่ยุคจารกรรมข้อมูลเลยก็ว่าได้ เพราะเกิดการระบาดของไวรัสเรียกค่าไถ่หรือแรนซัมแวร์ที่ชื่อ "WannaCry" (เรามักเรียกกันเล่น ๆ ว่าอยากจะร้องไห้ ก็น่าจะร้องจริง ๆ เพราะผลกระทบที่เกิดขึ้นนั้นมหาศาล) ที่สร้างความเสียหายแก่เครื่องคอมพิวเตอร์ไปมากกว่า 300,000 เครื่องทั่วโลก (ติดมากกว่า 100,000 เครื่องในวันแรก) จากช่องโหว่และเครื่องมือที่ถูกแฮ็กเกอร์ขโมยไปจากสำนักงานความมั่นคงแห่งชาติ (NSA) ของสหรัฐอเมริกา

  - **สิงหาคม ค.ศ.** 2020 เกิดการโจมตีจากหลายแหล่งเพื่อทำให้เป้าหมายไม่สามารถให้บริการได้ การโจมตีแบบนี้เรียกว่า DDoS (Distributed Denial of Service) โดยเป้าหมายคือตลาดหุ้นของนิวซีแลนด์ ส่งผลให้ตลาดหุ้นต้องปิดตัวลงชั่วคราว

- **กันยายน ค.ศ.** 2020 มีรายงานการเสียชีวิตครั้งแรกหลังจากอาชญากรไซเบอร์ใช้ไวรัสเรียกค่าไถ่โจมตีโรงพยาบาลในเมืองดึสเซลดอร์ฟ (Düsseldorf) ประเทศเยอรมนี แม้ว่าจะไม่ตั้งใจก็ตาม แต่ผลกระทบที่เกิดขึ้นทำให้ผู้ป่วยต้องย้ายไปรักษาตัวยังโรงพยาบาลที่อยู่ไกลออกไปและเสียชีวิตในที่สุด

- **ตุลาคม ค.ศ.** 2020 มีการโจมตีจากไวรัสเรียกค่าไถ่เพิ่มขึ้นโดยมุ่งเป้าไปยังโรงพยาบาลในอเมริกาเพื่อขโมยข้อมูลด้านสุขภาพและข้อมูลส่วนตัวของผู้ป่วย เพื่อแลกกับการจ่ายค่าไถ่

- **ธันวาคม ค.ศ.** 2020 "SolarWinds" ผู้ให้บริการยักษ์ใหญ่ของโลกด้านระบบบริหารจัดการและตรวจสอบสถานะการทำงานของอุปกรณ์เครือข่าย ถูกเข้าถึงโดยไม่ได้รับอนุญาตและถูกแก้ไขโดยฝังมัลแวร์ไว้ ส่งผลให้เกิดการละเมิดความมั่นคงปลอดภัยที่ร้ายแรงและครอบคลุมไปทั่วโลกต่อผู้ใช้งานซอฟต์แวร์ดังกล่าว

นี่คือตัวอย่างที่ยกขึ้นมาบางส่วนเพื่อให้เห็นภาพว่าทำไมข้อมูลถึงสำคัญกับเรามาก นอกจากนี้หลายประเทศยังมีการบันทึกเหตุการณ์หรือสิ่งผิดปกติทั่วโลกเพื่อใช้ประเมินความเสี่ยงและพยากรณ์เพื่อหาวิธีป้องกันภัยคุกคามที่เกิดขึ้น รวมทั้งยังช่วยกันหาวิธีป้องกัน จึงเกิดเป็นองค์กรหรือหน่วยงานต่าง ๆ เพื่อระดมทุนและทรัพยากรที่มีของตนเองในการสร้างมาตรฐาน เช่น

- **สภาเศรษฐกิจโลก** (World Economic Forum) ซึ่งเป็นองค์กรไม่แสวงหากำไร ได้จัดทำรายงานความเสี่ยงต่าง ๆ ที่เกิดขึ้นทั่วโลก และมีการจัดทำรายงานประจำปีเพื่อสรุปความเสี่ยงต่าง ๆ

จากภัยคุกคามหรือ “เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์” ที่เกิดขึ้นทั่วโลก รวมทั้งให้ความสนใจว่านานาชาติกำลังกังวลหรือมีมุมมองต่อความเสี่ยงเรื่องใดอยู่ และให้ความสำคัญกับความเสี่ยงใดบ้าง โดยสำรวจจากผู้มีส่วนได้ส่วนเสียและกลุ่มที่เป็นอาสาสมัคร เพื่อรวบรวมความคิดเห็นสรุปออกมาเป็นความเสี่ยงที่มีแนวโน้มที่รุนแรงมากขึ้น

ที่มา : http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

รายงานประจำปี ค.ศ. 2020 ของสภาเศรษฐกิจโลกแสดงให้เห็นว่าการโจมตีทางไซเบอร์เกี่ยวกับโครงสร้างพื้นฐาน (Cyberattacks: infrastructure) ส่งผลกระทบต่อกลุ่มผู้มีส่วนได้ส่วนเสีย 76.1% และการโจมตีทางไซเบอร์เกี่ยวกับการขโมยเงินหรือข้อมูล (Cyberattacks: theft of money/data) ส่งผลกระทบต่อกลุ่มผู้มีส่วนได้ส่วนเสีย 75.0% ซึ่งผลกระทบที่เกิดขึ้นนั้นทำให้สูญเสียข้อมูลส่วนบุคคลในส่วนของบริษัท 76.2% และสูญเสียข้อมูลส่วนบุคคลในส่วนของภาครัฐ 76.1% จะเห็นว่าในระดับโลก

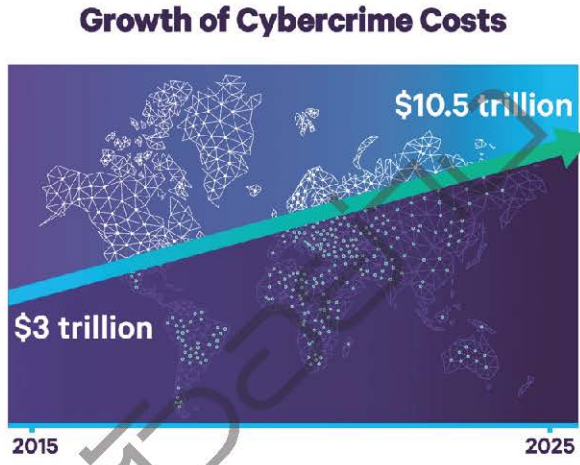
หรือประเทศไทยเอง ภัยคุกคามทางไซเบอร์นั้นน่ากลัวมากแค่ไหน ทั้งยังส่งผลโดยตรงถึงข้อมูลส่วนบุคคลอีกด้วย ดังนั้นการตระหนักและมีความรู้เรื่องความมั่นคงปลอดภัยจึงสำคัญอย่างยิ่งต่อการปกป้องข้อมูลส่วนบุคคลหรือความเป็นส่วนตัว

การลงทุนในตลาดการรักษาความมั่นคงปลอดภัยไซเบอร์ของโลก (Global Cyber Security Spending)

จากแนวโน้มภัยคุกคามที่รุนแรงมากขึ้นทุกปี ทำให้เกิดความตื่นตัวทั่วโลกที่ต้องดำเนินการหรือออกกฎหมายต่าง ๆ เพื่อปกป้องประชาชน ข้อมูล ทรัพย์สิน เศรษฐกิจ และความมั่นคงของแต่ละประเทศ ประเทศไทยเองก็ตื่นตัวเช่นกัน ซึ่งก่อนหน้านี้เรามี "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์" อยู่แล้ว และได้ออกพระราชบัญญัติเพิ่มอีก 2 ฉบับ ในเดือนพฤษภาคม พ.ศ. 2562 คือ "พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์" และ "พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล" ที่เกี่ยวข้องกับการคุ้มครองข้อมูลของประชาชนอย่างเราโดยตรง ซึ่งมีโทษทั้งจำและปรับ ทำให้หน่วยงานทั้งภาครัฐและเอกชนต้องปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยกันยกใหญ่ เพื่อดูแลระบบและข้อมูลของลูกค้าและประชาชน

ดังนั้นหากใครหรือหน่วยงานไหนต้องการข้อมูลของเราไปใช้ต้องขออนุญาตและได้รับอนุญาตจากเราก่อนเท่านั้น เราต้องพิจารณาว่าอีกฝ่ายจะนำข้อมูลของเราไปใช้ทำอะไรบ้างและอยู่ในขอบเขตที่กำหนดหรือไม่ เรามีสิทธิ์ระงับการใช้งาน การเข้าถึง เรียกคืนข้อมูล หรือลบข้อมูลได้ ซึ่งเป็นเรื่องที่ทุกคนต้องรู้

จากรูปด้านล่างจะเห็นว่าแม้พยากรณ์ว่าจะมีการลงทุนเรื่องนี้สูงขึ้นเรื่อย ๆ จาก 3 ล้านล้านดอลลาร์สหรัฐ ($3 trillion) ในปี ค.ศ. 2015 และเพิ่มขึ้นเป็น 10.5 ล้านล้านดอลลาร์สหรัฐ ($10.5 trillion) ในปี ค.ศ. 2025 แต่ภัยคุกคามกลับไม่ลดลงเลย



ที่มา : https://www.embroker.com/blog/cyber-attack-statistics/

เมื่อข้อมูลของเราถูกปล้นจะส่งผลเสียแค่ไหน

โดยทั่วไปแล้วภัยคุกคามมักจะโจมตีหน่วยงานและภาคธุรกิจเพื่อสร้างความเสียหายหรือความเสื่อมเสีย แต่ในช่วงหลังมีการเปลี่ยนแปลงมากมายเกิดขึ้นและส่งผลโดยตรงกับเรา เนื่องจากภัยคุกคามทางไซเบอร์เริ่มมุ่งเน้นไปทางข้อมูลความเป็นส่วนตัวและข้อมูลที่มีความสำคัญต่าง ๆ มาดูกันว่าผลกระทบตามหลักการด้านความมั่นคงปลอดภัยนั้นมีอะไรบ้างและใครที่ได้รับผลกระทบจากภัยคุกคามที่เกิดขึ้น

ผลกระทบทางตรงที่เรารู้ว่าต้องเจอ

ผลกระทบทางตรงที่เกิดขึ้นจากการถูกโจมตีโดยภัยคุกคาม หรือแม้แต่เหตุการณ์ข้อมูลรั่วไหลก็ส่งผลกระทบให้เราต้องกลับมานั่งคิดว่าจะป้องกันได้อย่างไร ที่สำคัญสิ่งที่ต้องดำเนินการเพื่อไม่ให้เหตุการณ์เหล่านี้เกิดขึ้นซ้ำอีก ล้วนแล้วแต่มีค่าใช้จ่ายทั้งสิ้นและเป็นสิ่งที่ไม่สามารถหลีกเลี่ยงได้ เพราะหากปล่อยไว้ย่อมส่งผลกระทบกับข้อมูลหรือระบบของเราและลูกค้า ซึ่งมีค่าใช้จ่ายต่าง ๆ ตามรายการดังต่อไปนี้

● การสืบสวนทางเทคนิค

แน่นอนว่าหากเกิดภัยคุกคามขึ้นกับองค์กรของเรา หลาย ๆ กรณี จำเป็นต้องจ้างผู้เชี่ยวชาญเข้ามาช่วยตรวจสอบ ซึ่งมีค่าใช้จ่ายที่สูงพอสมควร เพราะการเก็บหลักฐานต้องอาศัยผู้เชี่ยวชาญทางเทคนิคเพื่อให้มีความน่าเชื่อถือในชั้นศาล นอกจากผู้เชี่ยวชาญจะต้องมีความสามารถด้านเทคนิคแล้ว ยังต้องมีจรรยาบรรณด้วย เพราะสามารถเข้าถึงข้อมูลที่สำคัญและอ่อนไหว โดยผู้เชี่ยวชาญจะดำเนินการตั้งแต่ต้นเหตุ วิเคราะห์ และเข้าถึงข้อมูลต่าง ๆ ทั้งหมดเพื่อหาสาเหตุของภัยคุกคามที่เกิดขึ้นว่ามาจากอะไร เช่น เกิดจากพนักงานนำแฟลชไดร์ฟที่มีไวรัสมาเสียบเข้าเครื่องคอมพิวเตอร์ ทำให้เครื่องติดไวรัสและส่งข้อมูลออกไปยังภายนอก เป็นต้น

● การแจ้งเตือนการละเมิดกับลูกค้า

หลังจากเกิดภัยคุกคามขึ้นแล้ว เราจำเป็นต้องแจ้งเตือนเหตุการณ์ที่เกิดขึ้นกับลูกค้าของเรา ซึ่งต้องมานั่งคิดว่าจะทำอย่างไรให้ลูกค้ารู้สึกสบายใจและกังวลใจน้อยที่สุด ดังนั้นการจ้างผู้เชี่ยวชาญหรือหน่วยงานที่ดำเนินการอย่างมืออาชีพจึงเป็นสิ่งจำเป็น ถึงแม้ค่าใช้จ่ายจะแสนแพงก็ตาม แต่เพื่อความสบายใจของลูกค้า เราจำเป็นต้องทำ ผู้เชี่ยวชาญจะพิจารณาเลือกช่องทางในการสื่อสารกับลูกค้าของเราเพื่อลดผลกระทบและแรงปะทะกับลูกค้า

● การปฏิบัติตามกฎข้อบังคับ

บางธุรกิจจะมีกฎข้อบังคับซึ่งองค์กรต้องปฏิบัติตามหน่วยงานที่กำกับดูแล เช่น ธนาคารต้องปฏิบัติตามธนาคารแห่งประเทศไทย (ธปท.) บริษัทประกันต่าง ๆ ต้องปฏิบัติตามสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) บริษัทในตลาดหลักทรัพย์ต้องปฏิบัติตามสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

เป็นต้น ซึ่งหน่วยงานกำกับดูแลเหล่านี้จะออกกฎระเบียบเพื่อช่วยให้การดำเนินการของธุรกิจต่าง ๆ มีความมั่นคงปลอดภัยและลดผลกระทบที่จะเกิดต่อผู้บริโภคให้น้อยที่สุด

อย่างไรก็ตาม หากมี "เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์" เกิดขึ้น องค์กรยังต้องมีค่าใช้จ่ายอีกมากสำหรับค่าจ้างที่ปรึกษาหรือผู้เชี่ยวชาญ เพื่อดำเนินการต่าง ๆ ให้เป็นไปตามขั้นตอนของกฎระเบียบข้อบังคับที่เกี่ยวข้อง ซึ่งอาจรวมถึงการปรับปรุงด้านนโยบาย ด้านกระบวนการ ด้านเทคโนโลยี รวมถึงการสร้างความตระหนักรู้ด้านไซเบอร์ ด้านความมั่นคงปลอดภัยของข้อมูลและภัยคุกคาม ที่ปรึกษาจะช่วยให้องค์กรกลับเข้าสู่ขั้นตอนการปฏิบัติที่ดีให้สอดคล้องกับกฎระเบียบข้อบังคับ และตรวจสอบการดำเนินการในขั้นตอนต่าง ๆ เพื่อป้องกันการเกิดเหตุการณ์ซ้ำอีกในอนาคต

● ค่าธรรมเนียมทนายความและการดำเนินคดี

หากเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ขึ้น จะต้องเป็นคดีอย่างแน่นอน องค์กรต้องรายงานต่อหน่วยงานที่กำกับดูแล รวมถึงอาจถูกฟ้องร้อง ซึ่งต้องเข้าสู่กระบวนการยุติธรรมที่อาจมีทั้งโทษปรับและจำคุก องค์กรจึงต้องมีทนายที่มีความรู้ความสามารถในด้านความมั่นคงปลอดภัยของข้อมูล หากองค์กรไม่มีความรู้หรือทนายที่มีความสามารถ อาจตกเป็นจำเลยที่ไม่สามารถผ่อนปรนความรุนแรงจากการถูกลงโทษได้ เพราะสิ่งที่ต้องเจอก็คือค่าปรับซึ่งแต่ละข้อกฎหมายในแต่ละประเทศนั้นไม่เหมือนกัน และการจ้างทนายก็มีค่าใช้จ่าย "ยิ่งเก่ง ยิ่งแพง" แต่ก็เป็นสิ่งที่ควรทำ

● การคุ้มครองผู้บริโภคหลังการละเมิด

การเกิดเหตุการณ์ข้อมูลรั่วไหลส่งผลกระทบต่อความไว้วางใจของเจ้าของข้อมูล สิ่งที่ต้องเร่งดำเนินการคือ เตรียมกระบวนการหรือช่องทางสำหรับติดต่อสื่อสาร ขั้นตอนการตอบสนองต่อเหตุการณ์ผิดปกติ หรือแม้แต่

ช่องทางสำหรับเจ้าของข้อมูลที่สามารถเข้าถึงข้อมูลของตน และช่วยตรวจสอบการใช้งานข้อมูล เพื่อเพิ่มความมั่นใจให้กับเจ้าของข้อมูลมากขึ้นหลังจากเกิดเรื่องขึ้น รวมถึงการชดเชยความเสียหายที่เกิดขึ้นแก่เจ้าของข้อมูลด้วย

● การประชาสัมพันธ์

การประชาสัมพันธ์เป็นสิ่งที่ดีและเป็นการกู้ชื่อเสียงรวมทั้งภาพลักษณ์ที่ดีให้เกิดขึ้นกับเรา ฉะนั้นค่าใช้จ่ายย่อมสูงพอสมควร การใช้ทีมประชาสัมพันธ์มืออาชีพจะทำให้เราดูดีในสายตาคนอื่น โดยสามารถวัดเสียงตอบรับได้ว่าการที่เราให้ทีมช่วยแล้วมีผลลัพธ์เป็นอย่างไร มีข้อบกพร่องตรงไหนบ้าง ถือเป็นการยิงปืนนัดเดียวได้นกสองตัว ซึ่งเป็นการลงทุนที่คุ้มค่า

● การปรับปรุงความมั่นคงปลอดภัยทางไซเบอร์

การยกระดับและการปรับปรุงด้านความมั่นคงปลอดภัยทางไซเบอร์นั้นมีค่าใช้จ่ายมหาศาลและไม่สามารถหลีกเลี่ยงได้ เพราะหลังจากเกิดภัยคุกคามขึ้น เราจะตกเป็นเป้าหมายต่อไปเรื่อย ๆ แม้แต่หน่วยงานที่กำกับดูแลก็จับตามองว่าเรามีการเปลี่ยนแปลง ปรับปรุง และยกระดับตัวเองอย่างไรบ้าง เพราะหากเกิดเรื่องขึ้นซ้ำอีก ค่าปรับก็จะแพงขึ้นเป็นเท่าตัว ฉะนั้นการปรับปรุงจุดอ่อนที่เป็นช่องโหว่ต่อการโจมตีจึงเป็นเรื่องที่สมควร เช่น หากไม่มีอุปกรณ์ตรวจสอบหรือตรวจจับภัยคุกคาม ก็ต้องดำเนินการจัดซื้อ ไม่ว่าจะเป็นการจ้างหรือติดตั้งเอง เป็นต้น

สิ่งหนึ่งที่สำคัญคือ บุคลากรที่ปฏิบัติงานรักษาความมั่นคงปลอดภัย เพราะหากไม่มีบุคลากรที่เชี่ยวชาญด้านนี้ เราก็ไม่สามารถเฝ้าระวังหรือป้องกันความมั่นคงปลอดภัยได้ โดยค่าใช้จ่ายของทั้งสองส่วนก็มีราคาแพงพอสมควร ซึ่งประเทศไทยยังไม่สามารถผลิตบุคลากรด้านนี้ได้เพียงพอต่อความต้องการ ถือเป็นอีกช่องทางหนึ่งที่เราจะพัฒนาตัวเองขึ้นมาเป็นบุคลากรที่ตลาดแรงงานต้องการ

ผลกระทบทางอ้อมที่ซ่อนอยู่โดยไม่รู้

หัวข้อนี้เป็นผลกระทบที่ซ่อนอยู่ในผลกระทบหลัก ซึ่งเราอาจไม่ทันสังเกตจนกว่าจะเกิดความเสียหายขึ้น เช่น ลูกค้าหาย รายได้ลด ข่าวเสียเพิ่มขึ้น คู่แข่งแซงหน้าหรือโจมตีเรา ซึ่งความเสียหายเหล่านี้ส่งผลกระทบที่ไม่อาจแก้ไขได้ทันทีหรือกำหนดระยะเวลาได้ เรามาดูกันว่ามีอะไรบ้าง

● เบี้ยประกันเพิ่มขึ้น

ปกติแล้วเราจะพยายามเลี่ยงด้วยการจ่ายเงินเอง เพราะหากเรานำเงินทุนมาใช้จะทำให้ขาดสภาพคล่อง การทำประกันภัยไซเบอร์นั้นดูเหมือนเป็นทางออกที่ดีที่สุด แต่ทว่ามีค่าใช้จ่ายแพงพอสมควรและเบี้ยประกันก็อาจสูงขึ้นทุกปี เพราะภัยคุกคามเกิดเยอะขึ้นเรื่อย ๆ

นอกจากนี้การทำประกันภัยยังขึ้นอยู่กับเงื่อนไขด้วย ซึ่งเราไม่อาจรู้ได้เลยว่าค่าปรับหรือค่าไถ่จะอยู่ที่เท่าไหร่ ต้องทำทุนประกันแค่ไหนถึงจะเพียงพอ และความเสี่ยงของเรามีมากน้อยแค่ไหน ดังนั้นการทำประกันภัยจึงมีค่าใช้จ่ายเพิ่มขึ้น ซึ่งเป็นผลกระทบที่ซ่อนอยู่อย่างแน่นอน หากปีไหนเราถูกโจมตีด้วยภัยคุกคามสำเร็จ เบี้ยประกันจะสูงเป็นเท่าตัว เพราะเป็นค่าความเสี่ยงที่เกิดขึ้น (ใช้หลักการเดียวกับประกันภัยรถยนต์ หากชนเมื่อไหร่ก็น้ำตานองเมื่อนั้น)

● ค่าใช้จ่ายที่เพิ่มขึ้นจากการเป็นหนี้

หากเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางข้อมูลขึ้น สิ่งหนึ่งที่เกิดขึ้นแน่นอนคือ ค่าปรับและอาจมีค่าใช้จ่ายอื่น ๆ ตามมาอีกไม่รู้จบ จึงต้องหาแหล่งเงินทุนต่าง ๆ เพื่อเป็นทุนหมุนเวียนภายใน ทำให้ขาดสภาพคล่องทางการเงินและส่งผลกระทบในเรื่องอื่น ๆ

● ผลกระทบจากการหยุดชะงักในการดำเนินงานหรือการทำลายล้าง

ผลกระทบที่เห็นชัดคือ ทำให้การทำงานหรือการให้บริการหยุดชะงัก เพราะในการสืบสวนหาสาเหตุและผลกระทบจากเหตุการณ์ที่เกิดขึ้น เราจะถูกสั่งห้ามดำเนินการใดๆ ทั้งสิ้น การหยุดชะงักของบริการจะทำให้เราขาดรายได้และความมั่นใจของลูกค้าก็ลดลง เพราะเราไม่สามารถส่งมอบสินค้าหรือบริการได้ ดังนั้นการจ้างที่ปรึกษาเพื่อแก้ไขและตรวจสอบเรื่องที่เกิดขึ้นก็เป็นเรื่องด่วนที่ต้องดำเนินการ

● มูลค่ารายได้จากสัญญาที่หายไป

ตั้งแต่อดีตจนถึงปัจจุบัน มูลค่าหรือรายได้ของเรานั้นเป็นสิ่งดึงดูดนักลงทุน แต่สิ่งที่กระทบกับรายได้คือ "ภัยคุกคาม" หากใครถูกจารกรรมหรือข้อมูลรั่วไหล เพียงแค่นาทีแรกที่ข่าวออก หุ้นของกิจการนั้นก็ตกฮวบทันที และบางครั้งอาจถึงขั้นล้มละลายจนไม่สามารถฟื้นกลับมาได้อีก ดังนั้นสิ่งที่ต้องให้ความสำคัญคือ "การป้องกันการเกิดภัยคุกคาม" และ "งบประมาณการลงทุนด้านความมั่นคงปลอดภัยทางไซเบอร์และข้อมูล"

● ชื่อเสียงทางการค้า

ชื่อเสียงเป็นสิ่งที่ทุกคนหรือองค์กรล้วนสั่งสมมาเป็นเวลานานและการสร้างมันขึ้นมาก็ไม่ใช่เรื่องง่าย แต่การทำให้พังลงนั้นง่ายในพริบตาเพียง "คลิกเดียว" จากแฮ็กเกอร์หรือคนในองค์กรที่ไม่หวังดี ก็ทำให้ลูกค้าที่ใช้บริการของเราแทบจะเดินหนีไปเลย และคู่แข่งก็พร้อมแทนที่ทันที ซึ่งเหตุการณ์เหล่านี้มีให้เห็นกันอยู่บ่อยๆ จึงต้องหาวิธีรับมือและแก้ไขกันทุกวิถีทาง เพราะการที่ชื่อเสียงทางการค้าของเราเสื่อมเสีย ก็หมายถึงรายได้ที่หายไป รวมถึงความเชื่อมั่นจากนักลงทุนด้วย

● การสูญเสียทรัพย์สินทางปัญญา

หากถูกจารกรรมข้อมูล สิ่งหนึ่งที่จะเกิดขึ้นแน่นอนคือ ข้อมูลสำคัญ (เช่น ข้อมูลสินค้า หรือข้อมูลอื่นๆ ที่เป็นความลับทางธุรกิจ) มักถูกคู่แข่งหรือผู้ไม่ประสงค์ดีนำไปสร้างมูลค่าเพิ่มต่อ จึงต้องมีการรักษาความมั่นคงปลอดภัยที่ดีเพียงพอและต้องไม่ประมาทในการดูแลรักษาความปลอดภัยของข้อมูล เพราะหากข้อมูลเหล่านี้หลุดไปอยู่ในมือผู้ไม่ประสงค์ดีจะส่งผลเสียมากมาย และอาจหมายถึงจุดจบของเราก็เป็นได้

● ความสัมพันธ์กับลูกค้าที่หายไป

จากหัวข้อทั้งหมดที่กล่าวมานั้น สิ่งที่ต้องระวังเป็นพิเศษก็น่าจะเป็นหัวข้อนี้ เพราะกว่าที่เราจะสร้างชื่อเสียงขึ้นมาได้ ก็มาจากความไว้ใจของลูกค้าด้วยเช่นกัน หากไม่มีลูกค้าแล้วเราจะอยู่ได้อย่างไร รายได้ของเราจะมีไหม รวมถึงการตอบรับเกี่ยวกับผลิตภัณฑ์หรือการให้ข้อมูลสำหรับพัฒนาผลิตภัณฑ์ต่างๆ ของเราก็น่าจะเป็นไปไม่ได้เลย เพราะลูกค้ามักกระจายข่าวอย่างรวดเร็วแบบปากต่อปาก ยิ่งในยุคดิจิทัล การใช้สื่อโซเชียลเพื่อกดดันหรือต่อต้านผลิตภัณฑ์นั้นรวดเร็วและกระจายวงกว้างมาก ปัจจุบันทุกองค์กรยังกังวลกับเรื่องนี้ เพราะกว่าจะลงมือแก้ไข ข่าวเสียหายก็ลามไปไกลกว่าที่จะจัดการได้ และถึงแก้ไขได้ ก็ต้องลุ้นอีกว่าผลตอบรับจะเป็นอย่างไร

ลูกค้า "ค่ายมือถือ" ฉุนหนัก พลาดสิทธิ์โครงการ "คนละครึ่ง"

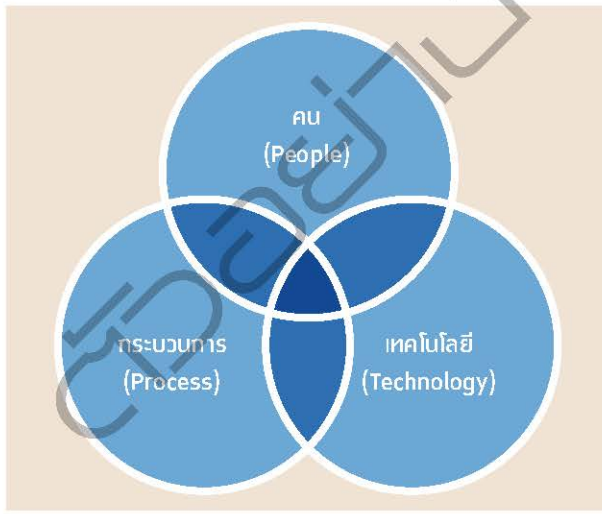
เหตุการณ์ที่ถือว่าเป็นที่สุดของการส่งท้ายปี ค.ศ. 2020 ก็น่าจะเป็นเรื่องที่เกิดขึ้นในโครงการ "คนละครึ่ง" โดยหนึ่งในผู้ให้บริการเครือข่ายโทรศัพท์มือถือรายใหญ่ได้เกิดปัญหาขัดข้อง ทำให้ผู้ลงทะเบียนไม่สามารถรับรหัสผ่านแบบใช้ครั้งเดียวหรือ OTP (One Time Password) ได้ ส่งผลให้ผู้ใช้บริการพลาดโอกาสการรับสิทธิ์จากโครงการ จึงเรียกร้องให้เครือข่ายโทรศัพท์มือถือเจ้านั้นรับผิดชอบในสิ่งที่เกิดขึ้น ซึ่งทางค่ายมือถือได้รับผิดชอบโดยชดเชยเป็น **"ส่วนลด"** จำนวน "3,500 บาท" ในการซื้อผลิตภัณฑ์ของตน แต่สิ่งที่ผู้ใช้บริการต้องการคือ **"เงินสด"** จำนวน "3,500 บาท" เพื่อนำมาใช้ในชีวิตประจำวัน

ผลตอบรับที่เกิดขึ้นจากเหตุการณ์นี้คือ "การขู่ประกาศย้ายค่าย" ของผู้ใช้บริการจนเป็นกระแสไปทั่วโลกโซเชียล สังเกตได้จากราคาหุ้นที่ร่วงลงไปประมาณ 2.92% ในเดือนธันวาคม ค.ศ. 2020 เราไม่รู้ว่าสถานการณ์ต่อไปจะเป็นอย่างไร ซึ่งเป็นการบ้านใหญ่ที่ผู้บริหารค่ายมือถือนี้ต้องแก้ไขอย่างเร่งด่วนแน่นอน โดยต้องปรับปรุงทั้งด้านเทคนิค ภาพลักษณ์ การลงทุน และความเชื่อใจจากลูกค้าที่เสียไป

จากผลกระทบต่าง ๆ ที่กล่าวมาทั้งหมด บางคนอาจคิดว่าแล้วมันเกี่ยวกับเรายังไง หากลองพิจารณาอย่างถี่ถ้วน จะพบว่าถ้าเราหรือองค์กรตกเป็นเหยื่อของภัยคุกคามทางไซเบอร์จะเสียหายแค่ไหน นอกจากเสียเงินเสียเวลาแล้ว ยังมีกระบวนการทางชั้นศาลตามมาอีกมาก กว่าจะเรียก

ความเชื่อมั่นจากลูกค้าให้กลับมาใช้บริการอีกครั้งไม่ใช่เรื่องง่าย ซึ่งจากการสำรวจพบว่า หลายองค์กรล้มหายตายจากไปก่อนที่จะกู้สถานการณ์กลับมาได้ซะอีก หากเราทำงานอยู่ในองค์กรนั้น ก็จะกระทบต่อรายได้และส่งผลไปถึงครอบครัว และถ้ามีหลายองค์กร หลายคน ตกเป็นเหยื่อภัยคุกคามทางไซเบอร์ จะส่งผลกระทบต่อเศรษฐกิจและความมั่นคงของประเทศขนาดไหน

3 ผู้พิทักษ์ที่ช่วยต่อกรกับภัยคุกคาม



องค์ประกอบสำคัญ 3 ประการที่ช่วยให้เราและองค์กรบรรลุเป้าหมายต่างๆ ได้ รวมถึงเป้าหมายในการรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัว คือ

● **คน** (People) เป็นจุดเริ่มต้นและเป็น "ลำดับแรกเสมอ" ที่ก่อให้เกิดภัยคุกคามขึ้น โดยอาจเกิดจากความประมาทเลินเล่อในการใช้งาน

ทั้งตั้งใจและไม่ตั้งใจ หรือเป็นจุดแรกที่เหล่าผู้ไม่ประสงค์ดีจะโจมตีข้อมูลส่วนบุคคล เช่น ชื่อ-นามสกุล ที่อยู่ เลขบัตรประจำตัวต่างๆ พฤติกรรม รสนิยม แนวคิด เป็นต้น ซึ่งข้อมูลเหล่านี้มักถูกนำมาตั้งเป็นรหัสผ่าน นอกจากนี้ยังนำไปเชื่อมโยงเพื่อย้อนกลับมาทำร้ายตัวเจ้าของข้อมูลหรือองค์กรที่สังกัดอยู่ได้

● **กระบวนการ** (Process) กระบวนการของหน่วยงานหรือองค์กร เช่น นโยบาย ระเบียบ ข้อบังคับ ก็เป็นอีกหนึ่งสาเหตุที่ทำให้การป้องกันความมั่นคงปลอดภัยของระบบสารสนเทศลดลงและเสี่ยงต่อการถูกโจมตีจากภัยคุกคาม เช่น การจารกรรมข้อมูล โดยหากเป็นเหตุการณ์ที่เกิดขึ้นก่อน “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์” หรือ “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์” และ “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล” บังคับใช้ก็คงไม่เป็นอะไรนัก เพราะไม่ต้องดำเนินการแก้ไขใดๆ อย่างมากก็ถูกลูกค้าหรือบุคคลทั่วไปเขียนตำหนิในสื่อโซเชียล แต่หลังจากมีพระราชบัญญัติที่กล่าวมาข้างต้น บุคคลหรือหน่วยงานที่รับผิดชอบจะต้องปรับปรุงการดำเนินงานต่าง ๆ ให้สอดคล้องกับที่กำหนดไว้ เพราะหากไม่ทำตามจะมีบทลงโทษตามมาทั้งโทษปรับและจำคุก

● **เทคโนโลยี** (Technology) เป็นความจริงที่ว่า “บนโลกนี้ไม่มีอะไรมั่นคงปลอดภัย 100%” แม้ว่าเทคโนโลยีนั้นจะเคยแข็งแกร่งแค่ไหนในอดีต ก็อาจถูกโจมตีได้ในอนาคต และ “ภัยคุกคามมักตามมาคู่กับเทคโนโลยีเสมอ” เพราะภัยคุกคามและเทคโนโลยีมีการพัฒนาตลอดเวลา มีผู้ทดสอบและผู้ไม่ประสงค์ดีมากมายที่พยายามเจาะระบบการรักษาความมั่นคงปลอดภัยและการป้องกันของเทคโนโลยี

การที่เราไม่มีซอฟต์แวร์หรือเทคโนโลยีสำหรับป้องกันภัยคุกคามก็ยิ่งทำให้เสี่ยงมากกว่าคนอื่น อย่างไรก็ตาม สิ่งสำคัญคือการตระหนักรู้ถึงภัยคุกคามและหลีกเลี่ยงพฤติกรรมเสี่ยงต่าง ๆ ที่ก่อให้เกิดภัยคุกคาม ดังนั้น หากขาดความรู้ ลำพังเพียงกระบวนการและเทคโนโลยีที่ใช้ป้องกันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ก็ไม่อาจป้องกันภัยคุกคามเหล่านั้นได้อย่างมีประสิทธิภาพ ทำให้มีโอกาสเสี่ยงที่จะตกเป็นเหยื่อของผู้ไม่ประสงค์ดีที่เข้ามาจารกรรมข้อมูล

หลายครั้งที่เรามักลงทุนทางเทคโนโลยีเพื่อป้องกันข้อมูลสำคัญและลดความเสี่ยงจากภัยคุกคาม เช่น ค่าบริการของระบบปฏิบัติการต่าง ๆ (OS License Software) โปรแกรมป้องกันไวรัส (Antivirus) ประกันความเสี่ยงภัยทางไซเบอร์ (Cyber Insurance) แต่ไม่มีกระบวนการในการป้องกันให้ความรู้ หรือสร้างความตระหนักรู้ให้กับผู้ใช้งาน ก็ทำให้เทคโนโลยีที่เราอุตส่าห์ลงทุนจัดหามาช่วยป้องกันภัยคุกคามทางไซเบอร์ได้ไม่เต็มประสิทธิภาพ หากเราใส่ใจที่จะศึกษาหาความรู้และอัปเดตสิ่งต่าง ๆ ที่เกิดขึ้นบนโลก รวมถึงสร้างกระบวนการหรือวิธีการที่ปลอดภัย ก็จะช่วยลดค่าใช้จ่ายเรื่องเทคโนโลยีสำหรับป้องกันภัยคุกคามและความเสี่ยงที่เกิดขึ้นได้

ไมโครซอฟท์ออกโรงเตือน "ภัยออนไลน์" อาจทำไทยเสียหาย 2.86 แสนล้านบาท

ปี ค.ศ. 2017 ไมโครซอฟท์ร่วมกับฟรอสต์ แอนด์ ซัลลิแวน เผยมูลค่าความเสียหายต่อเศรษฐกิจที่อาจเกิดขึ้น ว่า ถ้าองค์กรธุรกิจในไทยไม่ให้ความสำคัญในการวางแผนรับมือกับอาชญากรไซเบอร์ จะส่งผลกระทบราว 2.2% ของ GDP หรือคิดเป็นมูลค่า 2.86 แสนล้านบาทเลยทีเดียว

“หนังสือเล่มนี้เป็นหนังสือที่เขียนเรื่องยากให้เข้าใจง่าย
แต่ยังคงความกว้างและลึกของเนื้อหาที่เป็น ‘แก่น’ ของภัยคุกคามทางไซเบอร์
ทั้งข้อมูลส่วนบุคคลและความเป็นส่วนตัว ช่วยส่งเสริมความเข้าใจได้อย่างดีเยี่ยม”
ดร. นพ.บดินทร์ ทรัพย์สมบูรณ์
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“การสร้างความตระหนักรู้ถึงความสำคัญเรื่องการใช้ชีวิตอย่างมั่นคงปลอดภัย
ในโลกไซเบอร์เป็นเรื่องสำคัญ และจำเป็นที่ประชาชนชาวไทยต้องรู้เท่าทัน
เพื่อเป็นส่วนหนึ่งในการแก้ปัญหาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ”
ปริญญา หอมเอนก
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“นอกจากการเล่าความรู้เชิงลึกแล้ว ผู้เขียนยังกล้าตีแผ่ด้วยตัวอย่างจริง
ทั้งที่เป็นข่าวโด่งดังเสียหายรุนแรงในต่างประเทศ
จนถึงเหตุการณ์ที่เกิดขึ้นใกล้ตัวในประเทศ ที่สำคัญเล่าด้วยภาษาที่คนทั่วไปเข้าใจได้ง่าย
และด้วยความเป็นกลาง เต็มไปด้วยคติเตือนใจให้เราฉุกคิด”
ดร.ชัย วุฒิวิวัฒน์ชัย
ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค-สวทช.)

“หนังสือเล่มนี้เปรียบเสมือนอริยทรัพย์ที่ต้องอ่านและแชร์บอกต่อให้คนที่เรารัก
‘รีบทำความเข้าใจและทำทันที’ เปรียบเสมือนเข็มทิศนำทางสู่
‘นิสัยความมั่นคงปลอดภัยไซเบอร์ที่ยั่งยืน’ เพราะช่วยให้คุณลดความเสี่ยง
และโอกาสถูก Hack ได้ โดยไม่ต้องอาศัยโชคใดๆ”
สุรชัย ฉัตรเฉลิมพันธุ์
ผู้อำนวยการฝ่ายกลยุทธ์และการบริหารจัดการควบคุมดูแล
ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ธนาคารกรุงไทย จำกัด (มหาชน)

“หนังสือเล่มนี้ช่วยจุดประกายในการสร้างความตระหนักรู้ถึงความสำคัญ
ของข้อมูลส่วนบุคคล ภัยคุกคามทางไซเบอร์ในยุคดิจิทัลที่อาจเกิดขึ้นได้ในชีวิตประจำวัน
รวมทั้งให้ความรู้เบื้องต้นเกี่ยวกับกฎหมายข้อมูลส่วนบุคคลซึ่งเป็นประโยชน์อย่างยิ่งแก่ผู้สนใจ”
ดร.สุธาทิพ ยุทธโยธิน
ผู้พิพากษาศาลชั้นต้นประจำสำนักประธานศาลฎีกา

ปัจจุบันเราเชื่อมต่อกันทางไซเบอร์มากขึ้นจนกลายเป็นภัยคุกคาม
หากไม่อยากตกเป็นข่าวดัง ไม่อยากถูกแฮ็กเฟซบุ๊ก หรือติดคุกฟรีจากสิ่งที่ไม่ได้ทำ
ต้องรู้เท่าทันและป้องกันไว้ก่อน อย่าปล่อยให้ใครขโมยข้อมูลของคุณไปใช้ได้ตามใจ

หมวดธุรกิจ
ISBN 978-616-18-4201-7
9 786161 842017
Design by eleventh rabbit
245 บาท