

NIDA Impacts

02

พฤษภาคม -
สิงหาคม 2567

SPAM!

IRUS!

SCAM!

CYBERSECURITY

ภัยและความมั่นคงทางไซเบอร์กับการจัดการความเสี่ยง

Editor's Note

อาชญากรรมไซเบอร์หรือภัยไซเบอร์ได้กลายเป็นภัยคุกคามใหม่ของทั้งรัฐ เอกชน รวมทั้งพลเมือง ยิ่งเมื่อเทคโนโลยีดิจิทัลเติบโตอย่างรวดเร็วจนไม่ว่าใครก็สามารถเข้าถึงได้อย่างสะดวกตา ดูได้จากดัชนีใกล้ตัวที่สุดอย่างการใช้อินเทอร์เน็ตและสมาร์ทโฟนของภาคครัวเรือนไทยที่เพิ่มสูงขึ้นเป็นลำดับ อ้างอิงจากผลสำรวจของสำนักงานสถิติแห่งชาติที่ระบุไว้ในไตรมาส 2 ของปี 2567 เปรียบเทียบกับไตรมาสเดียวกันของปี 2563 ว่าตัวเลขการเชื่อมต่ออินเทอร์เน็ตภาคครัวเรือน เพิ่มขึ้นจากร้อยละ 77.8 ไปอยู่ที่ร้อยละ 88.5 ขณะที่ตัวเลขการใช้สมาร์ทโฟน เพิ่มขึ้นจากร้อยละ 86.4 ไปอยู่ที่ร้อยละ 96 โดยจำนวนความเสียหายจากภัยไซเบอร์ซึ่งมีหลายรูปแบบ ทั้งจำนวนผู้เสียหายและมูลค่าความเสียหายทางเศรษฐกิจ สังคม ที่เพิ่มเป็นเงาตามตัวเมื่อกลไกการดูแลและป้องกันความปลอดภัยกลับสวนทาง สะท้อนออกมาผ่านผลสำรวจดัชนีโพลเมื่อปี 2566 ที่พบว่า มีกลุ่มตัวอย่างถึงราวร้อยละ 54 ที่เคยถูกลอกโดยแก๊งคอลเซ็นเตอร์ ตามมาด้วยอีกกว่าร้อยละ 45 ถูกแฮกข้อมูลที่อยู่ในคอมพิวเตอร์ เครื่องมือสื่อสาร ถูกลอกให้เปิดเผยข้อมูลส่วนบุคคลสำคัญ ๆ ผ่านโซเชียลมีเดีย และอีกกว่าร้อยละ 24 ถูกโจมตีโดยไวรัสและมัลแวร์ ไม่นับการแฮกข้อมูลองค์กรรัฐและเอกชนที่ทำให้ตัวองค์กรสูญเสียชื่อเสียงและทรัพย์สิน เหล่านี้เป็นสภาพการณ์ที่กำลังสร้างความกังวลแก่สังคมโดยรวมเพราะแสดงให้เห็นว่าการแก้ไขปัญหาเป็นการวิ่งตามหลังเหล่าอาชญากรที่โจมตีผู้ใช้งานและระบบจากช่องโหว่สารพัด

ในขณะที่หลายองค์กรและหน่วยงานที่เกี่ยวข้อง รวมทั้งรัฐบาล ได้มีมาตรการต่าง ๆ ออกมาต่อเนื่อง ยกตัวอย่าง การออก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พ.ร.บ. การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม การที่ธนาคารแห่งประเทศไทยผลักดันการร่างกฎหมายกำหนดแนวปฏิบัติให้สถาบันการเงิน คืนเงินผู้เสียหายเต็มจำนวน หากไม่สามารถปิดช่องโหว่ระบบได้ ฯลฯ สถาบันพัฒนาบริหารศาสตร์ (NIDA) เองก็ได้ร่วมเป็นส่วนหนึ่งที่จะช่วยพัฒนาองค์ความรู้ด้านการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ หรือ Cybersecurity โดยการก่อตั้งหลักสูตร “การจัดการความเสี่ยงความมั่นคงทางไซเบอร์” ภายใต้คณะสถิติประยุกต์ เมื่อปี 2564 โดยมีจุดแข็งในการผสานสองศาสตร์สำคัญ คือการจัดการความเสี่ยงทางเทคโนโลยีในหลักสูตรวิทยาการคอมพิวเตอร์ และสาขาวิชากฎหมายในหลักสูตรนิติศาสตร์ เข้าด้วยกัน NIDA Impacts ฉบับนี้ จึงได้สนทนากับ รองศาสตราจารย์ ดร.ปราโมทย์ กัวเจริญ ผู้อำนวยการสำนักบรรณสารการพัฒนาและผู้อำนวยการหลักสูตร ร่วมกับอาจารย์ ดร.บงกช เจนจรัสสกุล ผู้อำนวยการสำนักเทคโนโลยีดิจิทัลและสารสนเทศ เกี่ยวกับการกิจของการสร้างบุคลากรผู้เชี่ยวชาญในศาสตร์ดังกล่าว รวมทั้งการพัฒนาและโครงสร้างพื้นฐานทางดิจิทัลของสถาบันฯ ที่อาจารย์ทั้งสองท่านได้ร่วมมีประสบการณ์





สารบัญ



Cybersecurity:

ภัยและความมั่นคงทางไซเบอร์กับการจัดการความเสี่ยง

06

Editor's Note

12

ผลสำรวจนิต้าโพล

23

Talk:

รศ.ดร.ปราโมทย์ ก้าวเจริญ และ
อ.ดร.บงกช เจนจรัสสกุล

ภัยไซเบอร์

54.20%

ถูกหลอกโดยแก๊งคอลเซ็นเตอร์

รูปแบบของ
ภัยไซเบอร์
ที่ประชาชนกังวล

45.57%

ถูกแฮกข้อมูลที่อยู่ในคอมพิวเตอร์ แท็บเล็ต
หรือโทรศัพท์มือถือ

45.11%

ถูกขโมยข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัส ATM บัตรเครดิต
รหัสผ่านต่าง ๆ เลขบัตรประชาชน

41.98%

ถูกหลอกให้เปิดเผยข้อมูลส่วนบุคคลที่สำคัญ
ผ่าน Social Media, SMS, Website

24.20%

คอมพิวเตอร์ แท็บเล็ต หรือโทรศัพท์มือถือ ถูกโจมตีด้วยไวรัส
หรือมัลแวร์ชนิดอื่น ๆ จนเกิดความเสียหาย

ศูนย์สำรวจความคิดเห็น «นิด้าโพล» สำรวจความคิดเห็น เรื่อง «ภัยไซเบอร์» ระหว่างวันที่ 27 ต.ค. - 3 พ.ย. 2566 จากประชาชนที่มีอายุ 18 ปีขึ้นไปกระจายทุกภูมิภาค ระดับการศึกษา อาชีพ และรายได้ ทั่วประเทศ จำนวน 1,310 หน่วยตัวอย่าง สุ่มตัวอย่าง

ความกังวลของประชาชน ต่อการรั่วไหลของข้อมูลส่วนบุคคลที่สำคัญ



38.85%

กังวลมาก



32.52%

ค่อนข้างกังวล



17.10%

ไม่กังวลเลย



11.53%

ไม่ค่อยกังวล

ความเสียหายจาก
ภัยไซเบอร์
ที่ประชาชนเคยได้รับ

80.76%

ไม่เคยได้รับความเสียหายใด ๆ เลย

12.06%

ถูกลอกโดยแก๊งคอลเซ็นเตอร์

4.66%

ถูกแฮกข้อมูลที่อยู่ในคอมพิวเตอร์ แท็บเล็ต หรือโทรศัพท์มือถือ

4.20%

ถูกลอกให้เปิดเผยข้อมูลส่วนบุคคลที่สำคัญ
ผ่าน Social Media, SMS, Website

3.21%

ถูกขโมยข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัส ATM บัตรเครดิต
รหัสผ่านต่าง ๆ เลขบัตรประชาชน

แบบหลายขั้นตอน (Multi-stage Sampling) โดยกำหนดค่าความ
เชื่อมั่นที่ร้อยละ 97.0 และสามารถดาวน์โหลดผลสำรวจฉบับเต็ม
ได้ที่ www.nidapoll.nida.ac.th

เมื่อแผนพัฒนาเศรษฐกิจและสังคมฉบับที่ 13 (พ.ศ. 2566-2570) พุ่งเป้าไปที่การวางรากฐานทางเศรษฐกิจบนงานดิจิทัล (Digital Thailand) ความท้าทายที่เราทุกคนต้องเผชิญในการเปลี่ยนผ่านสู่สังคมดิจิทัล (Digital transformation) ในช่วงหลายปีที่ผ่านมา จึงเป็นการปรับโครงสร้างพื้นฐานและการใช้ดิจิทัลในการสร้างความสะดวกสบายในการทำงานและการดำรงชีวิตประจำวัน สิ่งที่เราต้องเตรียมความพร้อมสำหรับอนาคตคือการต้องตอบให้ได้ว่าจะส่งมอบคุณค่าและการตระหนักรู้ในเรื่องใดไปสู่การเป็นสังคมดิจิทัลที่มีคุณภาพ เพื่อที่จะสามารถนำพาเศรษฐกิจและสังคมไทยให้เจริญทัดเทียมนานาชาติได้





สำหรับสถาบันพัฒนบริหารศาสตร์ (นิด้า) นอกจากการมุ่งสู่ Digital University ซึ่งต้องอาศัยการสร้างความร่วมมือภายในองค์กรเพื่อผลักดันให้เกิด digitization ในทุกกระบวนการทำงาน เป้าหมายสำคัญที่ดำเนินไปควบคู่กันก็คือพันธกิจในการเป็นส่วนสำคัญของการเสริมสร้างสังคมดิจิทัลที่มีคุณภาพ โดยเฉพาะในยุคปัจจุบันที่สังคมเศรษฐกิจกำลังอ่อนไหวต่อภัยทางไซเบอร์ในหลายรูปแบบ ทั้งนี้ ภายใต้การขับเคลื่อนอย่างต่อเนื่องของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ร่วมกับคณะสถิติประยุกต์ ในของสังคมเศรษฐกิจ จึงเป็นที่มาของการกำเนิดหลักสูตร **“การจัดการความเสี่ยงความมั่นคงทางไซเบอร์”** ที่มีเป้าหมายในการสร้างและส่งต่อบุคลากรที่มีความรู้ความสามารถในการบริหารจัดการนโยบายในการปกป้องและดูแลความปลอดภัยทางดิจิทัล ในโอกาสนี้ **อาจารย์ ดร.บงกช เจนจรัสสกุล** ผู้อำนวยการสำนักเทคโนโลยีดิจิทัลและสารสนเทศ และ **รองศาสตราจารย์ ดร.ปราโมทย์ กัวเจริญ** ผู้อำนวยการสำนักบรรณสารการพัฒนา ได้ให้เกียรติแบ่งปันมุมมองและประสบการณ์ที่จะเป็นทั้งแนวทางในการพัฒนางานดิจิทัล และส่งเสริมความเชื่อมั่นในการคุ้มครองความปลอดภัยงานดิจิทัลและไซเบอร์ได้อย่างมีประสิทธิภาพ



นับตั้งแต่มีพระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560 สำนักเทคโนโลยีดิจิทัลและสารสนเทศ ต้องพบเจอความท้าทายอะไรบ้างในการข้ามผ่านสู่การเป็นดิจิทัล?



อ.ดร.บงกช.

การเป็นดิจิทัล หรือ Digital transformation ไม่ใช่แค่เรื่องของสร้างบุคลากรหรือเทคโนโลยีเท่านั้น แต่ยังมียานกำกับดูแล และการทำโครงสร้างพื้นฐานให้แข็งแกร่งซึ่งไม่สามารถจะทำให้ลุล่วงในระยะเวลาอันสั้น



ยกตัวอย่างในนี้คือ คือความพยายามของทั้งองค์กรที่จะผลักดันร่วมกัน เช่น งานลงทะเบียนนักศึกษา ซึ่งในตอนเริ่มต้นก็มีความสับสน ขลุกขลัก แต่สิ่งสำคัญก็คือความร่วมมือ ในที่นี้คืองานบริการการศึกษาซึ่งเป็นเจ้าของระบบ โดยระบบใหม่ที่สร้างขึ้นมาจะต้องตอบสนองผู้ใช้งานทุกฝ่าย ต้องออกแบบให้ใช้งานง่าย การที่เราได้รับโอกาสให้เข้าไปทำระบบใหม่นั้นเป็นความท้าทายในการเปลี่ยนแปลงระบบเดิมที่มีความซับซ้อน โดยสิ่งที่เราทำคือออกแบบกระบวนการทุกขั้นตอนให้เข้าถึงง่าย นั่นคือคอนเซ็ปต์แรก



รศ.ดร.ปราโมทย์

การจะทำ Digital transformation ให้ประสบความสำเร็จต้องอาศัย Cybersecurity ด้วย การปรับปรุงเฉพาะโครงสร้างพื้นฐาน [IT infrastructure] อย่างเดียวนั้นไม่เพียงพอ ส่วนในเรื่องของ ROI [Return on Investment] ก็เป็นความท้าทายอย่างหนึ่ง เพราะต้องคำนึงว่าหากไม่มี Cybersecurity หรือเมื่อไม่มีการให้ความสำคัญกับการป้องกันแล้ว เมื่อเกิดความเสียหายขึ้นก็ย่อมต้องเสียค่าปรับ เกิดการฟ้องร้อง เสื่อมเสียชื่อเสียง ไม่ว่าจะเป็นองค์กรขนาดเล็กหรือใหญ่



เช่น หากเกิดกรณีการแฮกข้อมูล ลูกค้าก็เสียความเชื่อมั่น แต่หากเรามีการป้องกันที่ดีพอ เมื่อถูกโจมตีระบบปฏิบัติการส่วนอื่น ๆ ยังสามารถทำงานต่อได้ ลูกค้าก็จะเชื่อถือและอยากร่วมมือกับองค์กรนั้น ๆ องค์กรใหญ่บางแห่งเกิด Downtime risk แค่เพียงไม่กี่นาทีก็สร้างความเสียหายทางธุรกิจจำนวนมาก ดังนั้น จะต้องคำนึงถึงการจัดการความเสี่ยงโดยเริ่มต้นจากที่ว่า เรายอมรับความเสียหายที่อาจจะเกิดขึ้นในอนาคตได้มากน้อยแค่ไหน



การนำเทคโนโลยีมาประยุกต์ใช้ในองค์กร เปลี่ยนกระบวนการแบบแอนะล็อก (Analog) และสิ่งที่เป็นรูปธรรมให้เป็นดิจิทัล (Digitization) ต้องอาศัยความร่วมมือจากหลายฝ่าย เราจะสร้างประสิทธิภาพในการทำงานส่วนนี้อย่างไร

อ.ดร.บงกช: ในตอนเริ่มต้น ต้องคุยกันก่อนว่าเป้าหมายที่เราอยากเห็นจากระบบนี้คืออะไร เรามีเป้าหมายเดียวกัน แม้จะเจอปัญหารายทาง แต่ละจุดก็จะค่อย ๆ แก้ไปได้ •
ขั้นตอนที่ต้องลงแรงค่อนข้างมากคือการคุยกับผู้ใช้ระบบ/เจ้าของระบบ ทีมพัฒนาระบบของเราเอง และนักพัฒนาซอฟต์แวร์ (Developer) ภายนอก ทั้งการให้ข้อมูลและการตรวจทานกระบวนการต่าง ๆ ต้องคอยติดตามว่าระบบที่สร้างขึ้นใหม่จะสามารถตอบสนองความต้องการได้หรือไม่ นอกจากนี้ยังต้องประสานกับฝั่งงานโครงสร้างพื้นฐาน (งาน IT) เพื่อให้การสนับสนุนข้อมูลทางเทคนิคด้วย ดังนั้น เราจึงทำงานคู่ขนานกันไปทั้งทีม นี่เป็นสิ่งสำคัญมาก ๆ ในการขับเคลื่อนไปด้วยกัน

อาจารย์มีโอกาสสอน Design Thinking วันหนึ่งในชั้นเรียน นักศึกษาพูดว่า ประสบการณ์ที่เขาเจอคือ “ระบบถูกสร้างมาเพื่อให้เจ้าหน้าที่ทำงานง่าย” ไม่ได้ทำให้คนที่มาสมัครเรียนใช้งานง่าย นั่นจึงเป็นจุดเริ่มต้นในการทำงานที่เน้นการออกแบบประสบการณ์ (Experience design) ให้ผู้ใช้งานรู้สึกประทับใจ รับฟังความคิดเห็นจากนักศึกษาและผู้ใช้งานจริง ได้ครอบคลุมมากที่สุด

ก่อนการนำผลงาน บริการใด ๆ ออกสู่สาธารณะ นอกจากการดำเนินการทดสอบโดยผู้มีส่วนได้ส่วนเสียภายในแล้ว เรายังมีการนำเสนอแก่ผู้บริหารรวมทั้งนักศึกษาที่เป็นกลุ่มเป้าหมาย เพื่อพิจารณาให้ความเห็นร่วมกันในมุมมอง UX/UI เพื่อให้มั่นใจได้มากยิ่งขึ้นว่าระบบที่จะถูกนำออกมา จะถูกใจและสร้างประสบการณ์ที่ดีให้กับผู้ใช้งานได้มากกว่าเดิม



รศ.ดร.ปราโมทย์: สำหรับการทำงานของบุคลากรในนิต้า การทำ Digital transformation เรียกร้องให้ผู้ปฏิบัติงานเปิดใจรับกระบวนการการเปลี่ยนแปลง เพราะหากยึดกระบวนการเก่า ๆ ก็จะไม่เกิดการเปลี่ยนแปลง สิ่งสำคัญคือเรายังคงใช้กฎเกณฑ์ ระเบียบข้อบังคับตามระบบเดิม แต่เราทำให้ดีขึ้นได้ นำดิจิทัล





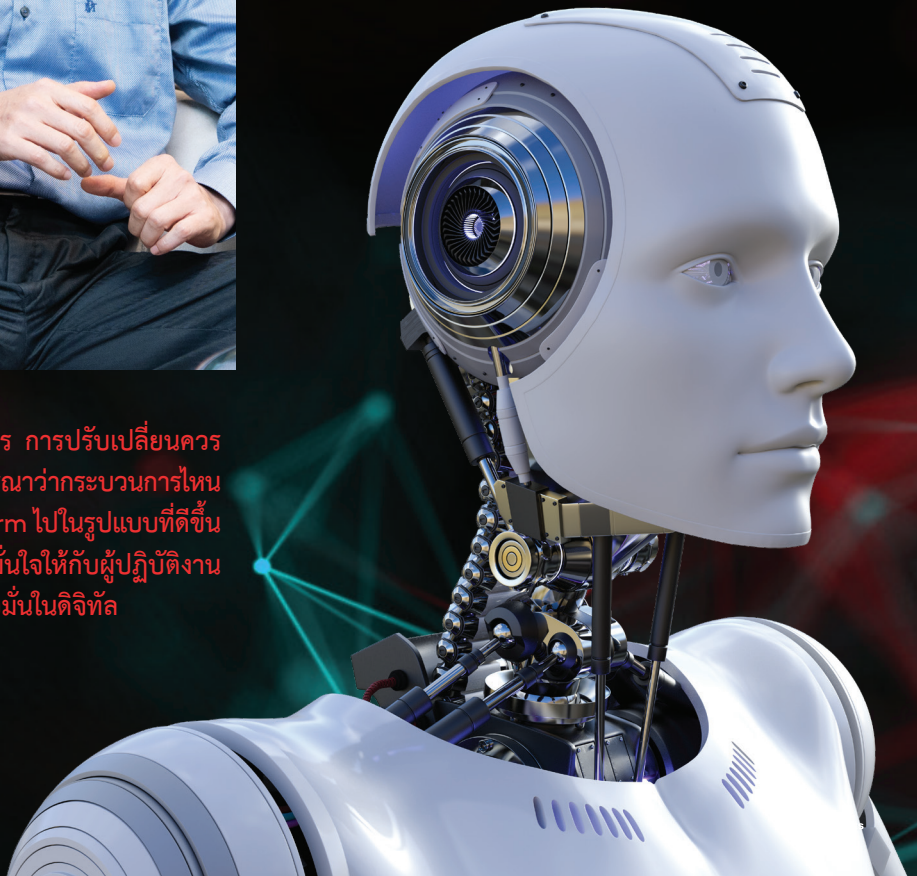
การที่ผู้บริหารเข้ามามีส่วนร่วมเสมอ สะท้อนว่าผู้บริหารของนิต้า
เล็งเห็นถึงความสำคัญของ Digital transformation เป็นอย่างมาก



อ.ดร.บงกช: หนึ่งในพันธกิจสำคัญของผู้บริหารในการ
นำเสนอต่อประชาคมตั้งแต่เข้ามารับตำแหน่ง คือนโยบาย
Digital transformation ที่จะเป็นตัวขับเคลื่อนหลักใน
การทำงาน สนับสนุนทั้งด้านการเรียนการสอน การวิจัย
การบริการการศึกษา และต้องส่งเสริมไปยังนักศึกษาอีก
ด้วย ผู้บริหารต้องการให้ทุกคนมี NIDA's DNA โดยมี
ความรู้ความเข้าใจในดิจิทัล (Digital literacy) เป็นส่วนหนึ่ง
ของ NIDA's DNA



มาใช้ในการประหยัดทรัพยากร การปรับเปลี่ยนควร
ต้องปรับทั้งกระบวนการ พิจารณาว่ากระบวนการไหน
ที่ขาดประสิทธิภาพก็ transform ไปในรูปแบบที่ดีขึ้น
ดิจิทัลจะต้องช่วยสร้างความมั่นใจให้กับผู้ปฏิบัติงาน
ทุกองค์กรก็ต้องสร้างความเชื่อมั่นในดิจิทัล





Cybersecurity จะช่วยสนับสนุนให้การทำงานมีประสิทธิภาพมากขึ้น ปัจจุบันคนกังวลว่า transform ไปแล้วจะเป็นอย่างไร จะมั่นใจในเทคโนโลยีได้หรือไม่ ซึ่งอันที่จริง Cybersecurity สามารถช่วยป้องกัน Digital asset ทั้งข้อมูลและเครื่องมือต่าง ๆ ได้ เป็นส่วนสนับสนุนเป้าหมายและพันธกิจขององค์กร Cybersecurity คือ enabler หรือตัวช่วยให้องค์กรก้าวสู่การเปลี่ยนผ่านได้ดีขึ้น สามารถทำผลิตภัณฑ์ใหม่ นวัตกรรมใหม่ ถ้าเราสร้างความปลอดภัยได้ดีพอก็就会有ความมั่นใจมากขึ้น



การสร้างเชื่อมั่นในดิจิทัลเป็นข้อสังเกตที่หลายองค์กรพบเจอ Cybersecurity จะเข้ามามีบทบาทในเรื่องนี้อย่างไร

รศ.ดร.ปราโมทย์: การดำเนินการตามมาตรฐานความปลอดภัยทางไซเบอร์ Cybersecurity compliance ใช้สอดคล้องกับความต้องการและกฎหมาย เพิ่มความปลอดภัยในการดูแลข้อมูลลูกค้า เราต้องดูแลความปลอดภัย ถ้าเรารู้ระบบมีความปลอดภัยที่ดีพอ ทุกสิ่งทุกอย่างก็สามารถพัฒนาต่อยอดได้ เทคโนโลยีต่าง ๆ ก็จะพัฒนามากขึ้น เกิดความมั่นใจมากขึ้น มีการส่งเสริมนวัตกรรมให้มากยิ่งขึ้น

ในการเก็บข้อมูลลูกค้า ก็ต้องปฏิบัติตามกฎหมาย PDPA ว่าจะเก็บข้อมูลได้มากแค่ไหน ใช้ข้อมูลได้บ้างตามจุดประสงค์ที่ต้องการ อย่างในหลักสูตร “การจัดการความเสี่ยงความมั่นคงทางไซเบอร์” ได้กำหนดให้อิง Industry Standard ทั้ง ISO 27001 หรือกรอบการทำงานด้านความมั่นคงปลอดภัยของ NIST (NIST Cybersecurity) ซึ่งอัปเดตเป็นเวอร์ชัน 2.0 แล้ว โดยหากองค์กรใด ๆ สามารถ transform รวมทั้งปรับปรุงมาตรฐานให้เข้ากับกฎเกณฑ์เหล่านี้ได้ ความปลอดภัยทางไซเบอร์ก็จะดีขึ้น ส่วนกฎหมาย PDPA และ GDPR (General Data Protection Regulation) คือข้อบังคับว่าด้วยการคุ้มครองข้อมูล ใช้ทั้งคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคล) ก็ต้องมีการจัดการอย่างเหมาะสมด้วย

บางคนมองว่า Cybersecurity เป็นการทำงานแบบตั้งรับ แต่อันที่จริงแล้วหากโครงสร้างพื้นฐานแน่น มีการเสริมความปลอดภัยในทุกด้าน การทำงานความปลอดภัยทางไซเบอร์ก็กลายเป็นฝ่ายรุกที่เชื่อมโยงการป้องกันความปลอดภัยทุกส่วนเป็นโครงข่าย ทำให้องค์กรเติบโตได้ภายใต้ความมั่นคงปลอดภัย

รศ.ดร.ปราโมทย์:แน่นอน องค์กรต้องคำนึงถึง Cybersecurity มองเพียงเฉพาะ Digital transformation เชื่อมต่อโครงข่ายโดยไม่สร้างความปลอดภัยไม่ได้ ต้องวิเคราะห์ความเสี่ยงขององค์กรว่าเป็นอย่างไร ก่อนจะขึ้นสู่อินเทอร์เน็ตหรือคลาวด์ (Cloud technology) Cybersecurity จะเข้ามาบทบาทในการปกป้องความเสี่ยง รวมทั้งเพิ่มประสิทธิภาพในการปกป้องข้อมูลและช่วยป้องกันไม่ให้เกิดปัญหาในอนาคต ข้อมูลที่มีอยู่แล้วต้องป้องกันการแฉ ลูกค้าก็มั่นใจว่าข้อมูลจะไม่รั่วไหล แต่หากโดนแฉก็มีผลถึงชื่อเสียงบริษัทและผิดกฎหมายการคุ้มครองข้อมูลด้วย

สถานการณ์อาชญากรรมไซเบอร์ ซึ่งรัฐบาลปัจจุบันจะจริงจังกับการแก้ปัญหามากขึ้น Cybersecurity ในองค์กรจะป้องกันปัญหานี้อย่างไรได้บ้าง

อ.ดร.บงกช: ต้องยอมรับว่า อาชญากรรมไซเบอร์เป็นปัญหาที่ทุกหน่วยงานต้องเจอ แต่เราสามารถป้องกันและเตรียมพร้อมรับมือได้ เช่น มีการกำหนดมาตรการดูแลความปลอดภัย รวมทั้งการเฝ้าสังเกตการณ์ และการสร้างความร่วมมือกับหน่วยงานภายนอก เช่น สำนักงานคณะกรรมการการรักษความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีการสร้างการตระหนักรู้ที่เกี่ยวกับอาชญากรรมไซเบอร์ผ่านสื่อของสำนัก เช่น i-news และ website ของสำนัก ไปยังผู้ใช้งาน (Users)

รศ.ดร.ปราโมทย์: อยากเน้นว่า Security management นั้นสำคัญมากกว่า Security technology ต่อให้เราเทคโนโลยีที่ดีมากแค่ไหน ถ้าจัดการไม่ดีก็หมายความว่าความปลอดภัยของเราไม่ดีพอ ต้องมีการพิจารณาทรัพยากรที่มีอยู่ทั้งหมด ต้องแบ่งคลาสข้อมูล แต่ละประเภทมีความสำคัญอย่างไร ต้องหาวิธีปกป้องข้อมูลในแต่ละชั้น เมื่อสร้างโปรเจกต์ขึ้นมา ในการทำงาน Project Management ต้องให้ Security เข้าไปเกี่ยวข้องตั้งแต่เริ่มต้น เราต้องมีการจัดการที่ดีไปพร้อมกับการมีเทคโนโลยีความปลอดภัยที่เหมาะสม จึงจะเกิดความปลอดภัยแบบครบถ้วนและรอบด้าน หากใส่เรื่องความปลอดภัยเข้าไปทีหลัง การทำงานจะไม่สะดวกและยังอาจเกิดช่องโหว่ได้

การสร้างโปรเจกต์ที่ว่า หมายถึงเราจะต้องคำนึงถึงเรื่องความปลอดภัยของทรัพยากรก่อนเป็นอันดับแรกใช่หรือไม่

รศ.ดร.ปราโมทย์: ใช่ครับ ต้องเป็นส่วนหนึ่งของโปรเจกต์ บุคลากรที่เปลี่ยนหมุนไปยังต้องให้คำแนะนำคนที่มาทำงานต่อด้วย ทั้งการเขียนโปรแกรม การเก็บข้อมูล กระบวนการทำงานทุกอย่าง การสร้างปลอดภัยของข้อมูล ไม่ใช่ข้อมูลรั่วไหลหลังจากสร้างระบบก็ต้องมีกระบวนการทำ Audit มีการทำ Penetration testing ประเมินและค้นหาช่องโหว่ เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ข้อมูลมีความปลอดภัย เพราะการมีคนเข้ามาใช้อยู่เรื่อย ๆ ข้อมูลก็เพิ่มเข้ามา ความเสี่ยงก็ตามมา

Security ต้องมีการดูแลตลอดเวลา Penetration testing จะทำปีละครั้งก็ได้ ซึ่งดีกว่าไม่ทำเลย ส่วนใหญ่มักจะทำเมื่อมีการเปลี่ยนแปลง เช่น เวลาภัยคุกคาม (Threats) เกิดขึ้น หรือหากสิ่งแวดล้อมมีการเปลี่ยนแปลงไปก็ต้องทำ เช่น มีการเอาสิ่งใหม่ใส่เข้ามาในระบบ ก็จะต้องทดสอบ มีโปรดักต์ใหม่ก็ต้องทดสอบว่าการขึ้นระบบ (Implementation) มีความมั่นคงปลอดภัยหรือไม่ หรือต้องมีการทดสอบเมื่อองค์กรสององค์กรมาควบรวมกัน

กฎหมายคุ้มครองข้อมูลส่วนบุคคล PDPA ตอนนี้เป็นอย่างไบ้าง เพราะก่อนหน้านี้ได้รับความสนใจแล้วดูเหมือนจะเจียบหายไป

รศ.ดร.ปราโมทย์: กระแส PDPA สร้างความตระหนักตกใจมากกว่า แต่ประชาชนอาจไม่ได้เข้าใจว่ามันคืออะไร หรืออาจเข้าใจผิด เข้าใจว่าทุกอย่างเป็นข้อมูลส่วนตัว ถ่ายรูปอะไรไม่ได้ ถ่ายรูปติดใครก็ไม่ได้ ที่จริงแล้วกฎหมายในแง่ของความเป็นส่วนตัวหรือ Privacy ดังกล่าวไม่ได้มีจุดประสงค์เช่นนั้น อย่างไรก็ตาม องค์กรต่าง ๆ ก็ต้องตระหนักเรื่องกฎหมายข้อมูลส่วนบุคคล การขอการยินยอม (Consent) และระบุขอบเขตในการนำไปใช้ เพื่อไม่ให้ทำผิดกฎหมาย องค์กรที่น่าเชื่อถือต้องเคารพกฎหมาย อย่างนี้ถ้าเรายังคงทำอยู่ แต่คนอาจจะคิดว่าเป็นเรื่องธรรมดา เช่น การประกาศผลการสอบ เอาขึ้นเว็บ แม้จะสะดวกสบายแต่ต้องดูว่าเป็นข้อมูลส่วนตัวหรือเปล่า เรื่องนี้เป็นเรื่องธรรมดาที่ทำตั้งแต่โบราณ เราสามารถเช็กได้ว่าเราลบได้ไหมในเว็บ แต่ถ้าคิดดี ๆ มันอาจเป็นการละเมิดสิทธิ์ เพราะผู้ที่ลบไม่ผ่านอาจจะรู้สึกอับอายขายหน้า ขึ้นอยู่กับมุมมองความคิดและวัฒนธรรมด้วย ซึ่งก็ต้องมีการปรับเปลี่ยนไป หรือเวลาเลือกตั้ง ทุกคนสามารถดูรายชื่อบัตรประชาชนและที่อยู่ในคูหาเลือกตั้งได้เลย นี่เรียกว่ากฎหมายไม่สอดคล้องกัน ทำไมในหน่วยเลือกตั้งถึงมีข้อมูลส่วนตัวของเราแสดงให้คนอื่นเห็นได้ เราต้องเอาจริงเอาจังว่าเราจะทำอย่างไร



นอกจากนี้ NIDA for Life ก็เป็นอีกหนึ่งช่องทางให้นักศึกษาและบุคคลภายนอกจะได้พัฒนาองค์ความรู้ที่หลากหลาย โดยเราสร้างแพลตฟอร์มออนไลน์ระยะสั้น <https://nidaforlife.nida.ac.th/> ที่สามารถพัฒนาทักษะทั้ง Hard skills และ Soft skills ประกอบด้วยหมวดวิชา AI/ Digital Technology, Environment and SDGs, Language and [Mass] Communication, Management และ Self-Improvement เมื่ออบรมครบตามที่กำหนดจะได้รับใบประกาศนียบัตรด้วย นี่คือทางเลือกหนึ่งในการเรียนรู้ที่มาจากปรัชญาของนิดา นั่นคือ Wisdom for Sustainable Development สร้างปัญญาเพื่อการพัฒนาที่ยั่งยืน โดยมี Lifelong learning หรือการเรียนรู้ตลอดชีวิตเป็นหนึ่งในพันธกิจ

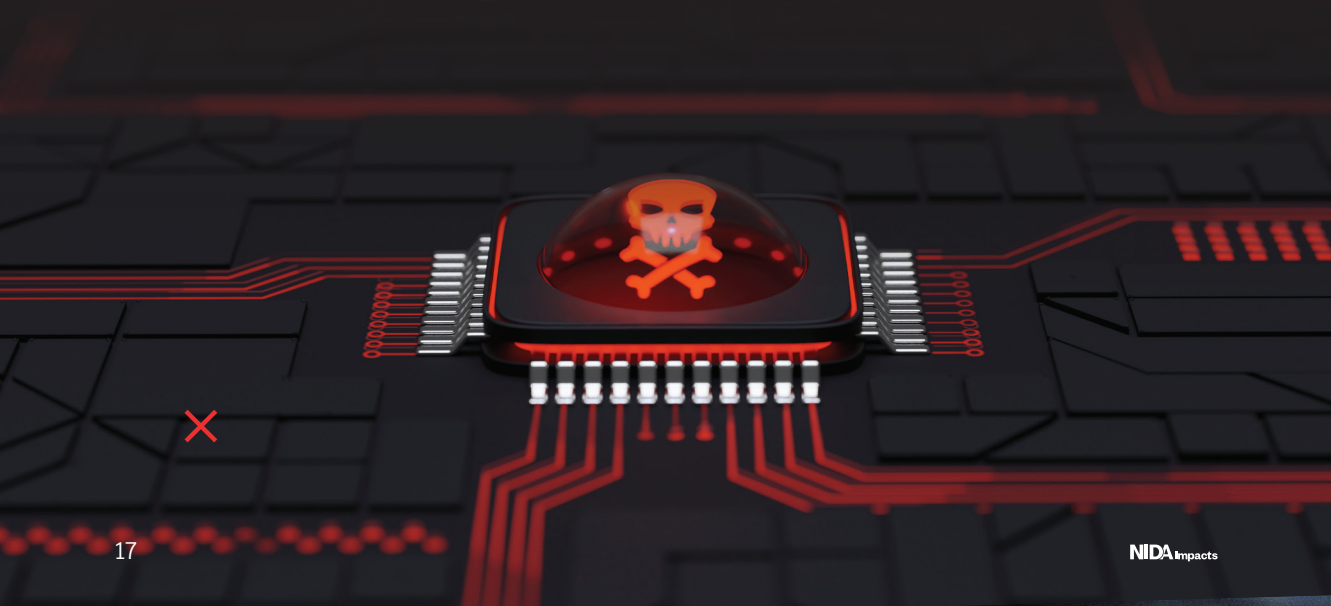


ตอนนี้ทุกคนก็ตระหนักกันมากขึ้นว่าต้องมีทักษะดิจิทัล เพราะเราต้องทันเทคโนโลยี ทันโลก ทุกองค์กรควรส่งเสริมทักษะดิจิทัลอย่างไรบ้าง

อ.ดร.บงกช: หนึ่งในยุทธศาสตร์การดำเนินการภายใต้ยุทธศาสตร์การเป็นดิจิทัลของสถาบัน คือ การดำเนินการในด้านการยกระดับสมรรถนะและทักษะด้านเทคโนโลยี ไม่ได้เน้นเพียงบุคลากรของสถาบันฯ เท่านั้นแต่ยังรวมถึงนักศึกษาด้วย การดำเนินการที่ผ่านมา เช่น การปรับปรุงเนื้อหาวิชา ND4000 ที่เน้นในเรื่องของ Digital skills ที่จำเป็นต่อโลกยุคปัจจุบัน ไม่ว่าจะเป็นการใช้งาน AI การตระหนักรู้และความเข้าใจพื้นฐานเกี่ยวกับ Cybersecurity และจริยธรรมไซเบอร์ การกำหนดสมรรถนะพื้นฐานทางด้านเทคโนโลยีดิจิทัลสำหรับการสร้างบุคลากรใหม่ในตำแหน่งต่าง ๆ ของสถาบัน

ในส่วนหลักสูตรของอาจารย์ปราโมทย์ เห็นว่ามีความแตกต่างจากหลักสูตรในท้องตลาดอีกด้วย

รศ.ดร.ปราโมทย์: หลักสูตร “การจัดการความเสี่ยงความมั่นคงทางไซเบอร์” (Cybersecurity risk management) เป็นการผสมผสาน 3 ศาสตร์เข้าด้วยกันตามลักษณะการใช้งานจริง 1. Information Technology Security หรือ Technical Security 2. Risk management การจัดการความเสี่ยง 3. Cybersecurity law กฎหมายความปลอดภัยทางไซเบอร์





การจัดการความเสี่ยงความมั่นคงทางไซเบอร์ สิ่งสำคัญอย่างแรกคือ Policy driven เน้นให้ความปลอดภัยตั้งแต่เริ่มต้น ใช้นโยบายองค์กรขับเคลื่อนให้มีความปลอดภัยตามความต้องการขององค์กร วิเคราะห์ความเสี่ยงให้ครบถ้วน มีการปฏิบัติตามหลักเกณฑ์ความมั่นคงปลอดภัยที่กำหนด (Compliance) ทั้งมาตรฐานและกฎหมายต่าง ๆ ให้ครอบคลุม การคุ้มครองความปลอดภัยไม่เป็นเพียงผู้ปกป้อง (Preventor) เท่านั้น แต่เน้นไปที่การสร้างนโยบายที่มีมาตรฐานความปลอดภัย ซึ่งจะให้องค์กรสามารถสร้างสรรค์นวัตกรรมใหม่ได้อย่างไม่ติดขัด

ในแง่การทำงานจริง โลกมีปัจจัยแวดล้อมใหม่เข้ามาตลอด การมีความรู้แต่เพียงเรื่องเทคโนโลยีจึงไม่เพียงพออีกแล้ว ต้องมีความรู้ด้านอื่นด้วย ต้องมีการวิเคราะห์ว่าตัวระบบมีประสิทธิภาพแค่ไหน มีปัญหาอะไรเกิดขึ้นบ้าง หลักสูตรก็ปรับเปลี่ยนตามสถานการณ์ทางเศรษฐกิจและอุตสาหกรรม มีการ Compliance กับมาตรฐานอุตสาหกรรมที่เป็นสากลและน่าเชื่อถือ เช่น ISO โดย NIST รวมถึงกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล PDPA หรือ GDPR (General Data Protection Regulation) ซึ่งเป็นข้อบังคับระดับนานาชาติที่ใช้ทั้งคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคล มีงานนิติดิจิทัลและการสืบสวน (Digital Forensics and Investigations) รู้เท่าทันอาชญากรรมทางคอมพิวเตอร์ มีการเชิญผู้เชี่ยวชาญเฉพาะด้านที่มีประสบการณ์ในการทำงานจริงมาให้ความรู้ เช่น เจ้าหน้าที่จากกรมสอบสวนคดีพิเศษ (DSI)



ปัจจุบันเราผลิตนักศึกษาไปแล้วรวม 7 รุ่น นับตั้งแต่เทอมสองของปีการศึกษา 2564 โดยเป็นภาคพิเศษทั้งหมด นักศึกษาสะท้อนว่า ไม่คิดว่าเนื้อหาจะมีมากขนาดที่ต้องครอบคลุม 3 ศาสตร์ ที่เน้นความต้องการทั้งทางด้านเทคนิค ด้านการจัดการ และโดยเฉพาะด้าน Risk Management หรือด้านกฎหมาย จึงเป็นหลักสูตรที่สร้างบุคลากรที่เชี่ยวชาญทั้งด้านเทคนิคและความปลอดภัยต่าง ๆ รวมทั้งงานตรวจสอบ (audit) ด้วย เร็ว ๆ นี้มีนักศึกษาที่สามารถสอบ CISSP ได้เป็นมาตรฐานสากลระดับ Global Standard ที่มีชื่อเสียงมากด้านการรักษาความปลอดภัย ก็ดีใจที่เขาสามารถนำความรู้ไปใช้ประยุกต์กับการทำงานได้





ประเทศไทยนับเป็นประเทศหนึ่งที่ประชากรใช้มือถือกันเป็นสัดส่วนที่สูงมากเป็นอันดับต้น ๆ ของโลก จะดีกว่าไหมถ้าเราจะต่อยอดกิจกรรมที่เราใช้เวลาไปกับมือถือมาสร้างประโยชน์มากขึ้น

รศ.ดร.ปราโมทย์: ยุคนี้เป็นยุคของอินฟลูเอนเซอร์ มีคนทำกิจกรรมออนไลน์เยอะแยะมากมาย ไม่ต้องติดอยู่กับทีวีใคร ๆ ก็เป็นอินฟลูเอนเซอร์ได้ถ้ามีความสามารถมากพอ เป็นผู้สื่อข่าว ทำคอนเทนต์ เราให้ AI ร่างจดหมายให้ได้ ช่วยหาค่าเฉลี่ย คิดเรื่องข้อมูลให้ได้ แต่สิ่งที่ต้องระวังคือ เราต้องมีความรู้ด้วยว่าสิ่งที่ AI ตอบกลับมาเป็นข้อมูลที่ถูกต้องหรือไม่ อีกอย่างที่น่าเป็นห่วงคือเรื่อง Deepfake หรือการสร้างคอนเทนต์ปลอมบุคคล โดย Generative AI ใช้ปัญญาประดิษฐ์ไปเรียนรู้เชิงลึก (Deep Learning) สร้างข้อมูลเนื้อหาใหม่แบบอัตโนมัติ ทำซ้ำข้อมูล เช่น ข้อความ เสียง วิดีโอ จนดูสมจริง ใช้ในหน้าคนดังมาใส่สื่อลามก หรือหลอกให้ลงทุน หลอกให้โอนเงิน ปลอมเป็นตำรวจ มีมีจอาชีพจำนวนมากที่ใช้เทคโนโลยีนี้มาสร้างความเสียหาย

ดังนั้น ทักษะเบื้องต้นที่ทุกคนต้องมีก็คือ การสังเกตและตรวจสอบ นี่ก็คือ Digital literacy ที่สำคัญยิ่ง กรณีนี้ก็ต้องสังเกตความผิดปกติของคลิวิดิโอ เช่น ดวงตาที่ดูไม่เป็นธรรมชาติ การขยับปากไม่ตรงกับเสียง เสียงแห้งหยาบของคลิวิดิโอให้ตึกก่อนแชร์ต่อ เทคโนโลยี AI เข้ามาอยู่ในชีวิตประจำวันของเราแล้ว มันถึงเวลาแล้วที่เราต้องฝึกใช้ AI ด้วย ไม่ว่าจะอยู่ในวิชาชีพไหน AI จะมีผลกระทบต่อเราทุกคน

สำหรับผู้สนใจหลักสูตร
"การจัดการความเสี่ยง
ความมั่นคงทางไซเบอร์"
สามารถศึกษาข้อมูลได้ที่

<https://nida.ac.th/master/cybersecurity-management-special-program/>



SCAN ME

NIDA ADMINISTRATION

1. ศาสตราจารย์ ดร.ศิวัช พงษ์เพียจันทร์
2. รองศาสตราจารย์ ดร.ปริญดา สุขเจริญสิน
3. รองศาสตราจารย์ ดร.สาวิตรี คทกณิช
4. ผู้ช่วยศาสตราจารย์ ดร.ดารารัตน์ อานันทนະສຸວຸນ
5. ผู้ช่วยศาสตราจารย์ ดร.อรรถกฤตย์ เทพมงคล
6. ผู้ช่วยศาสตราจารย์ ดร.สุวิษา เป้าอารีย์
7. ผู้ช่วยศาสตราจารย์ ดร.ประพิน นุชเปี่ยม
8. รองศาสตราจารย์ ดร.พัทธริยา หลัทธิพิช
9. อาจารย์ ดร.กรณ์ คุะนันทน

ประธานคณะกรรมการ

คณะกรรมการ

คณะกรรมการ

คณะกรรมการ

คณะกรรมการ

คณะกรรมการ

คณะกรรมการ

เลขานุการคณะกรรมการ

ผู้ช่วยเลขานุการคณะกรรมการ

นายกมลภพ ปันละมัย

ผู้ประสานงาน

โทร 0 2727 3023



2



3



×

4



5



6



7



8



9





WISDOM *for* Sustainable Development

สถาบันบัณฑิตพัฒนบริหารศาสตร์ (NIDA)

148 ถ.เสรีไทย แขวงคลองจั่น เขตบางกะปิ กรุงเทพมหานคร 10240

โทรศัพท์ 0 2727 3023

อีเมล nidaimpacts2565@gmail.com