SET Note

Volume 12/2566

11 สิงหาคม 2566

บริษัทจดทะเบียนในตลาดหุ้นไทยเตรียมความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์

จัดทำโดย
นางสาวสุมิตรา ตั้งสมวรพงษ์
ฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศไทย

สรุปประเด็นสำคัญ:

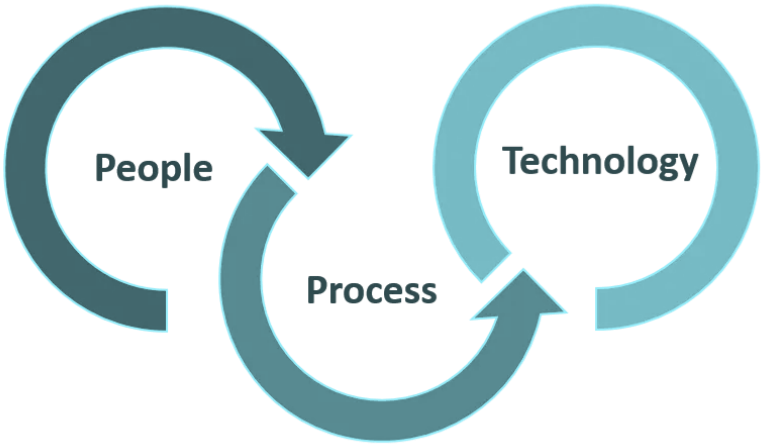
จากการศึกษาเกี่ยวกับการเตรียมความพร้อมด้านความมั่งคงปลอดภัยทางไซเบอร์ จากข้อมูลที่เปิดเผยในแบบแสดงรายการข้อมูลประจำปีและรายงานประจำปี (แบบฟอร์ม 56-1 One Report) ปี 2565 ของบริษัทจดทะเบียนอยู่ในดัชนีราคา SET50 Index จำนวน 50 บริษัท พบว่า

- **บริษัทจดทะเบียนในตลาดหุ้นไทยเตรียมตัวป้องกันและรับมือจากภัยคุกคามทางไซเบอร์ ในรูปแบบ Top-Down Approach** กล่าวคือ วางแผนในระดับนโยบายและกระจายลงไปสู่การปฏิบัติในระดับล่าง มีการเสริมสร้างให้เป็นวัฒนธรรมองค์กร
- **บริษัทจดทะเบียนปฏิบัติตามแนวตามแนวคิด 3 เสาหลักด้านความมั่งคงปลอดภัยทางไซเบอร์ สรุปได้ดังนี้**
  - **เสาหลักต้นที่ 1 บุคลากร (people):** บริษัทจดทะเบียนส่วนใหญ่ที่ทำการศึกษาตระหนักถึงภัยคุกคามทางไซเบอร์ และให้ความสำคัญกับให้ความรู้ สร้างความตระหนักเท่าทันภัยคุกคามทางไซเบอร์ และวางแผนพัฒนาบุคลากรด้านความมั่งคงปลอดภัยทางไซเบอร์
  - **เสาหลักต้นที่ 2 กระบวนการ (process):** บริษัทจดทะเบียนที่ทำการศึกษามีการกำหนดนโยบาย มีการปรับกระบวนงานให้เป็นไปตามมาตราฐานสากลเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ มีการประเมินความเสี่ยง ตลอดจนมีการวางแผนการรับมือ แผนการกู้คืนระบบ ตลอดจนมีการซักซ้อมกรณีที่ต้องโต้ตอบภัยคุกคามทางไซเบอร์
  - **เสาหลักต้นที่ 3 เทคโนโลยี (technology):** บริษัทจดทะเบียนส่วนใหญ่มีการลงทุนในระบบเทคโนโลยีสารสนเทศ และพัฒนาระบบอย่างสม่ำเสมอ รวมถึงการนำเทคโนโลยีสมัยใหม่ อาทิ การใช้ระบบปัญญาประดิษฐ์ มาช่วยในการตรวจจับความผิดพลาด เป็นต้น และมีการสุ่มตรวจสอบระบบต่างๆ ให้พร้อมรับมือและสามารถกู้คืนข้อมูล / ระบบได้
- **ขณะทั่วโลกเผชิญปัญหาขาดแคลนบุคลากรด้านความมั่งคงปลอดภัยทางไซเบอร์ โดยในปี 2565 มีปริมาณความต้องการบุคลากรด้านนี้กว่า 3.43 ล้านคน** และผู้เชี่ยวชาญคาดว่าปริมาณความต้องการบุคลากรด้านนี้จะคงอยู่ต่อไปในปี 2566 **สำหรับประเทศไทยก็มีปัญหาเดียวกัน ดังนั้น ภาครัฐและเอกชนต้องเร่งพัฒนาบุคลากรด้านนี้ เพื่อรองรับภัยคุกคามทางไซเบอร์ที่รุนแรงขึ้น**

บริษัทจดทะเบียนในตลาดหุ้นไทยโดยเฉพาะบริษัทจดทะเบียนขนาดใหญ่ ได้เตรียมตัวประเมินสถานการณ์ เตรียมรับมือภัยคุกคามทางไซเบอร์แล้ว ทั้งในด้านบุคลากร กระบวนการ และเทคโนโลยี และอยู่ระหว่างการพัฒนาอย่างต่อเนื่องเพื่อให้ทันต่อภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไป

ภัยคุกคามทางไซเบอร์ส่งผลกระทบทั้งระดับส่วนบุคคล หน่วยงาน/ องค์กรต่างๆ ทั้งความเสียหายต่อการปฏิบัติงานต่อเนื่องของระบบงาน ความสูญเสียทางการเงิน และความเสื่อมเสียชื่อเสียงของหน่วยงาน / องค์กร และส่งผลกระทบต่อเศรษฐกิจของประเทศ ดังนั้น ในแต่ละประเทศรวมทั้งประเทศไทยได้ออกกฎหมายและ / หรือกฎระเบียบที่เกี่ยวข้อง เพื่อควบคุมดูแลป้องกันภัยคุกคามทางไซเบอร์ (Cyber treats / Cyber Crime) และมุ่งเสริมสร้างความมั่งคงปลอดภัยทางไซเบอร์ (Cyber security)

ภาพที่ 1 The three-pillar approach to cyber security

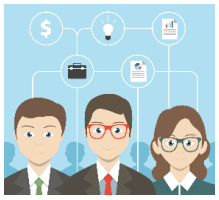


ฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศ ได้ศึกษาข้อมูลจากบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย ในฐานะหน่วยธุรกิจขนาดใหญ่ที่มีผลต่อระบบเศรษฐกิจของของประเทศ ทั้งจากมุมมองการสร้างรายได้ การจ้างงาน การเสริมสร้างนวัตกรรม และการมีส่วนร่วมในการเสียภาษีนิติบุคคลให้แก่ประเทศ ว่ามีการปรับตัวอย่างไรในการตอบรับภัยคุกคามด้านไซเบอร์ โดยทำการศึกษา**จากข้อมูลที่เปิดเผยในแบบแสดงรายการข้อมูลประจำปีและรายงานประจำปี (แบบฟอร์ม 56-1 One Report) ปี 2565 ของบริษัทจดทะเบียน**[1] **ที่อยู่ในดัชนีราคา SET50 Index จำนวน 50 บริษัท**[2] เพื่อทราบถึง**การเตรียมความพร้อมในการจัดการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของบริษัทจดทะเบียนในตลาดหุ้นไทย** ซึ่งจะเป็นข้อมูลเบื้องต้นให้บริษัทจดทะเบียนขนาดกลางและเล็ก และหน่วยงานนอกตลาดหุ้นไทยปฏิบัติตามได้ โดยในการศึกษานี้พิจารณา**ตามแนวคิด 3 เสาหลักด้านความมั่งคงปลอดภัยทางไซเบอร์** (The three-pillar approach to cyber security) ซึ่งเป็นแนวคิดเกี่ยวกับการป้องกันข้อมูลและสารสนเทศภายในองค์กร **โดยพิจารณาข้อมูลจากการดำเนินการ 3 ด้าน ได้แก่ บุคลากร (people) กระบวนงาน (process) และเทคโนโลยี (technology)** สรุปได้ดังนี้

[1] เนื่องจากมีข้อจำกัดด้านเวลาในการศึกษาและการเก็บข้อมูลที่ต้องเก็บรวบรวมด้วยการเก็บมือ จึงพิจารณาเฉพาะบริษัทจดทะเบียนขนาดใหญ่เป็นตัวแทนในการศึกษาเกี่ยวกับการเตรียมความพร้อมในการจัดการเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์

[2] รายชื่อบริษัท ของหลักทรัพย์ที่เป็นองค์ประกอบของดัชนีราคา SET50 Index ณ 3 มกราคม 2566 สำหรับรอบเดือนมกราคม - มิถุนายน 2566

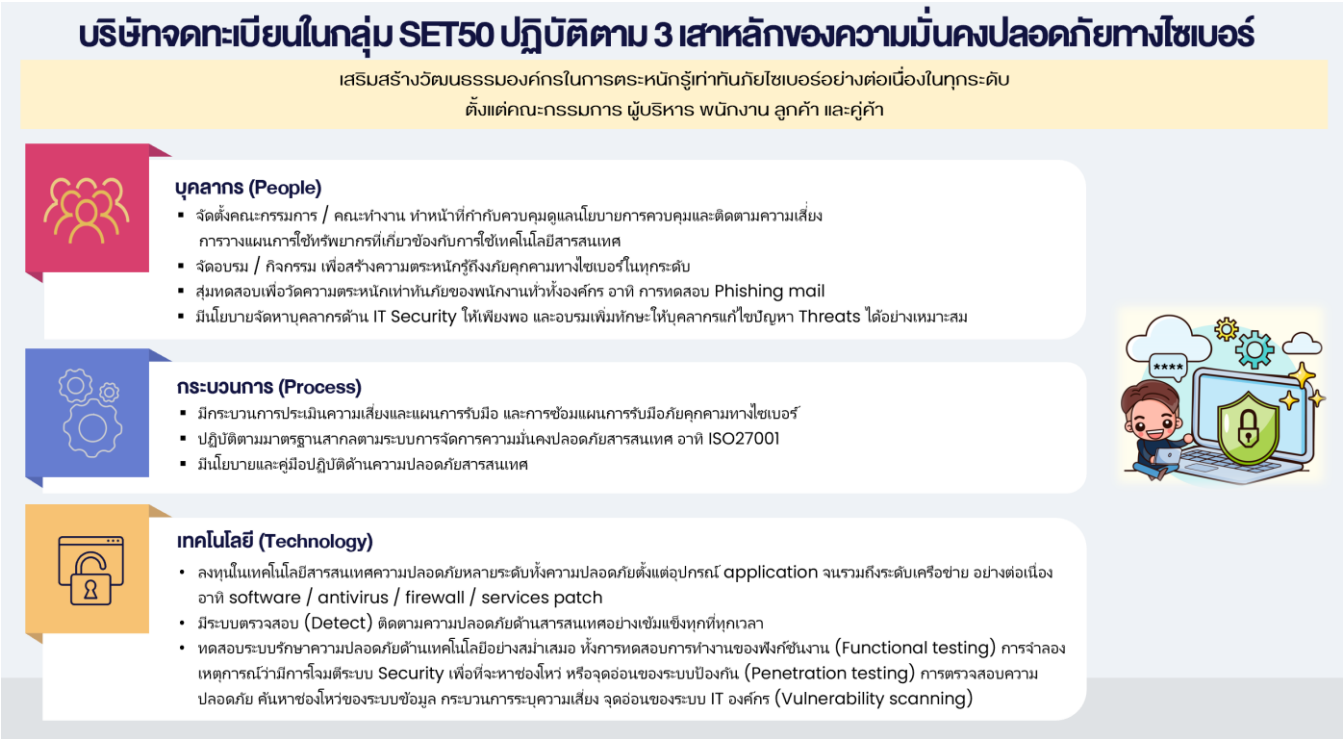
เสาหลักต้นที่ 1 บุคลากร: บริษัทจดทะเบียนส่วนใหญ่ที่ทำการศึกษาตระหนักถึงภัยคุกคามทางไซเบอร์และให้ความสำคัญกับให้ความรู้ สร้างความตระหนักเท่าทันภัยคุกคามทางไซเบอร์ และวางแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์



บริษัทจดทะเบียนที่ทำการศึกษาเกือบทั้งหมด ได้วางแผนการปฏิบัติเกี่ยวกับ**การดำเนินการด้านความมั่งคงปลอดภัยทางไซเบอร์ในรูปแบบ Top-Down Approach กล่าวคือ วางแผนในระดับนโยบายและกระจายลงไปสู่การปฏิบัติในระดับล่าง** และในระดับผู้บริหารพิจารณาว่า **"ความเสี่ยงจากภัยคุกคามด้านไซเบอร์" ถือเป็นกลุ่มความเสี่ยงเกิดใหม่** (Emerging Risk) ซึ่งแต่ละบริษัทต้องมีการประเมินขนาดและโอกาสที่จะได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ พร้อมวางแผนการรับมือ

โดยบริษัทบางจดทะเบียนบางบริษัทให้ความสำคัญในการ**เสริมสร้างให้ความมั่นคงปลอดภัยทางด้านไซเบอร์เป็นวัฒนธรรมขององค์กร** (corporate culture) และ**กำหนดนโยบายด้านความมั่งคงปลอดภัยทางไซเบอร์ และมอบหมายให้คณะกรรมการ คณะอนุกรรมการ คณะผู้บริหาร หรือคณะทำงาน เป็นผู้ควบคุมดูแล**ให้เป็นไปตามนโยบายความมั่งคงปลอดภัยทางไซเบอร์ และเกือบทุกบริษัทที่ทำการศึกษาดำเนินการ**ให้ความรู้ จัดอบรมสัมมนา จัดกิจกรรมเพื่อสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์**[3]

ภาพที่ 1 การปฏิบัติตาม 3 เสาหลักในการเสริมสร้างความมั่งคงปลอดภัยทางไซเบอร์ของบริษัทจดทะเบียนไทยที่อยู่ในดัชนี SET50



ที่มา: แบบฟอร์ม 56-1 One Report ของบริษัทจดทะเบียนที่อยู่ในดัชนี SET50 รวบรวมโดยฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศไทย

บริษัทจดทะเบียนแห่งละแห่งกำหนดผู้รับผิดชอบที่แตกต่างกันในการดูแลเรื่องความมั่งคงปลอดภัยทางไซเบอร์ ซึ่งสรุปผู้รับผิดชอบได้เป็นกลุ่มต่างๆ ดังนี้

[3] บริษัทจดทะเบียน 46 บริษัท จาก 50 บริษัท ที่มีการเปิดเผยข้อมูลเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ / ความเสี่ยงจากภัยคุกคามทางไซเบอร์ ในแบบแสดงรายการข้อมูลประจำปีและรายงานประจำปี (แบบฟอร์ม 56-1 One Report) ปี 2565

- **คณะกรรมการ / คณะอนุกรรมการ ที่มีอยู่แล้วเป็นผู้ดูแล โดยปรับนโยบายเพิ่มเติม**
  อาทิ ปรับเพิ่มเติมเรื่องความเสี่ยงจากภัยคุกคามทางไซเบอร์ในนโยบายการกำกับดูแลกิจการ ภายใต้การดูแลของคณะกรรมการ / คณะอนุกรรมการด้านกำกับดูแลกิจการ หรือ คณะกรรมการบริหารความเสี่ยง หรือ คณะกรรมการตรวจสอบ หรือ คณะกรรมการด้านความยั่งยืนกำกับดูแลกิจการและบริหารความเสี่ยง
- **คณะกรรมการ หรือ คณะอนุกรรมการด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ ที่แต่งตั้งขึ้นมาใหม่เป็นผู้ดูแล** หรือ
- **คณะกรรมการบริหารจัดการ Enterprise Architecture เป็นผู้ดูแล**

ในระดับปฏิบัติการ **บริษัทจดทะเบียนทุกบริษัทที่ทำการศึกษาและเปิดเผยข้อมูลได้ให้ความสำคัญกับการสร้างความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ ผ่านการจัดอบรมสัมมนา และการจัดกิจกรรมภายในองค์กร** รวมถึงฝึกหัดให้บุคลากรมีความระวังภัยในขั้นตอนการปฏิบัติงานจริง โดย**การสุ่มทดสอบอีเมล์หลอกลวง (Phishing mail) อย่างสม่ำเสมอ** และมีการกำหนดจำนวนบุคลากรที่ผ่านการทดสอบเป็นเป้าหมายในการทำการทดสอบอีกด้วย

นอกจากนี้ยังพบว่า จากปัญหาการขาดแคลนบุคลากรที่มีความรู้และความสามารถด้านความมั่งคงปลอดภัยทางไซเบอร์ (จะกล่าวถึงในหัวข้อต่อไป) ส่งผลให้**บริษัทจดทะเบียนบางบริษัทที่ให้บริการด้านเทคโนโลยีอยู่แล้ว หรือบริษัทจดทะเบียนที่มีบริษัทในเครือจำนวนมาก มีการขยายงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในรูปแบบของการจัดตั้งเป็นบริษัทย่อย เพื่อให้บริการเพิ่มเติมแก่ลูกค้า และ / เพื่อดูแลความมั่นคงปลอดภัยทางไซเบอร์ให้แก่บริษัทและบริษัทในเครือ**

ขณะที่บริษัทจดทะเบียนบางบริษัทจัด**กิจกรรมร่วมกับสถาบันการศึกษา หรือให้ข้อมูลสถาบันการศึกษา ในการปรับหรือพัฒนาหลักสูตรเพื่อผลิตบุคลากรด้านความมั่งคงปลอดภัยทางไซเบอร์** หรือ**จัดอบรมเพื่อเสริมสร้างทักษะ (up-skill) ให้บุคลากรด้านมั่งคงปลอดภัยทางไซเบอร์**สามารถบริหารจัดการในการแก้ไขปัญหาจากภัยคุกคามด้านไซเบอร์ได้อย่างเหมาะสมและทันท่วงที ยิ่งไปกว่านั้น **บริษัทจดทะเบียนบางบริษัท มีการจัดทำระบบ พัฒนาเนื้อหา จัดทำสื่อการเรียนการสอนในระบบ e-learning เพื่อให้ความรู้ ตระหนักถึงภัย และเตือนภัยคุกคามทางไซเบอร์ให้แก่ประชาชนทั่วไปอีกด้วย**

เสาหลักต้นที่ 2 กระบวนการ: บริษัทจดทะเบียนที่ทำการศึกษามีการกำหนดนโยบาย มีการปรับกระบวนงานให้เป็นไปตามมาตราฐานสากลเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ มีการประเมินความเสี่ยง ตลอดจนมีการวางแผนการรับมือ แผนการกู้คืนระบบ ตลอดจนมีการซักซ้อมกรณีที่ต้องโต้ตอบภัยคุกคามทางไซเบอร์

บริษัทจดทะเบียนเกือบทั้งหมดที่ทำการศึกษาได้เปิดเผยข้อมูลว่า **มีกระบวนการประเมินความเสี่ยง มีแผนรับรองภัยคุกคามทางไซเบอร์ และบริษัทได้ปฏิบัติตามมาตรฐานสากลตามระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ** อาทิ ISO/IEC27001 เป็นต้น

บริษัทจดทะเบียนที่ทำการศึกษาแต่ละบริษัทมีระดับการปฏิบัติตามมาตรฐานสากลเกี่ยวกับความมั่งคงปลอดภัยทางไซเบอร์ หรือด้านข้อมูลสารสนเทศของแต่ละบริษัทมีความพร้อมรับมือที่แตกต่างกัน โดย

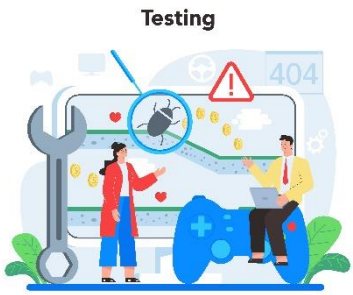
- บางบริษัทได้รับใบรับรองตามมาตรฐานสากลต่อเนื่องหลายปี และอยู่ระหว่างการขอรับรองมาตรฐานในระดับที่สูงขึ้น
- บางบริษัทเพิ่งได้รับการรับรองตามมาตรฐานสากล และ
- บางบริษัทปฏิบัติตามมาตรฐานสากลแต่ยังไม่ยื่นขอใบรับรองมาตรฐาน แต่เกือบทุกบริษัทกำหนดนโยบายและคู่มือปฏิบัติด้านความปลอดภัยสารสนเทศ

และบริษัทจดทะเบียนส่วนใหญ่มีการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ มีการวางแผนและขั้นตอนการปฏิบัติงานในการรับมือ ขั้นตอนในการรับมือ ตลอดจนแผนการในการกู้คืนข้อมูลหรือระบบงาน เมื่อเกิดเหตุจากภัยคุกคามทางไซเบอร์ และมีการกำหนดชัดเจนเกี่ยวกับการซักซ้อมกรณีที่ต้องโต้ตอบภัยคุกคามทางไซเบอร์

เสาหลักต้นที่ 3 เทคโนโลยี: บริษัทจดทะเบียนส่วนใหญ่มีการลงทุนในระบบเทคโนโลยีสารสนเทศ และพัฒนาระบบอย่างสม่ำเสมอ รวมถึงการนำเทคโนโลยีสมัยใหม่ อาทิ การใช้ระบบปัญญาประดิษฐ์ มาช่วยในการตรวจจับความผิดพลาด เป็นต้น และมีการสุ่มตรวบสอบระบบต่าง ๆ ให้พร้อมรับมือและสามารถกู้คืนข้อมูล / ระบบได้

บริษัทจดทะเบียนส่วนใหญ่ที่ทำการศึกษา มีการกำหนดนโยบายการลงทุนด้านเทคโนโลยีสารสนเทศ และด้านความมั่งคงปลอดภัยทางไซเบอร์ ทั้งในด้านอุปกรณ์ แอปพลิเคชัน และเครือข่าย มีการวางแผนนำระบบอัตโนมัติ (Artificial Intelligent / Machine Learning) มาใช้ในกระบวนการตรวจจับความผิดพลาด (Detect process) และมีการตรวจสอบตลอดเวลา

สำหรับระบบต่างๆ ที่ใช้ในการปฏิบัติงาน มีการกำหนดสุ่มตรวจสอบระบบอย่างสม่ำเสมอ ทั้ง



- การทดสอบการทำงานของฟังก์ชันงาน (Functional testing)
- การจำลองเหตุการณ์การโจมตีระบบรักษาความมั่นคงปลอดภัย (Security system) เพื่อที่จะหาช่องโหว่หรือจุดอ่อนของระบบป้องกัน (Penetration testing)
- การตรวจสอบความปลอดภัยเพื่อค้นหาช่องโหว่ของระบบข้อมูล กระบวนการระบุความเสี่ยง จุดอ่อนของระบบ IT องค์กร (Vulnerability scanning) เป็นต้น

และบริษัทจดทะเบียนบางบริษัท นอกจากจะพิจารณาความเสี่ยงของระบบงานภายใน พบว่า บริษัทจดทะเบียนบางบริษัทยังพิจารณาถึงระบบอื่นๆ ที่มีการเชื่อมต่อกับลูกค้าหรือหน่วยงานภายนอกด้วย

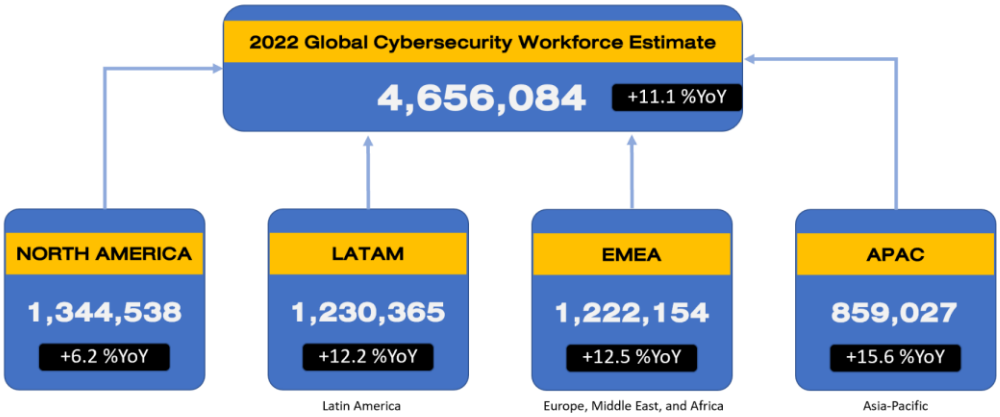
จากที่กล่าวมาข้างต้น อาจกล่าวได้ว่า ขณะนี้บริษัทจดทะเบียนในตลาดหุ้นไทยโดยเฉพาะบริษัทจดทะเบียนขนาดใหญ่ ได้ประเมินสถานการณ์ เตรียมรับมือภัยคุกคามทางไซเบอร์แล้ว และมีการดำเนินการอย่างต่อเนื่องสม่ำเสมอเพื่อให้ทันต่อภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไป ซึ่งแนวทางการดำเนินงานของบริษัทจดทะเบียนขนาดใหญ่นี้จะเป็นข้อมูลเบื้องต้นพอเป็นแนวทางให้บริษัทจดทะเบียนขนาดกลางและเล็ก และหน่วยงานนอกตลาดหุ้นไทยปฏิบัติตามเพื่อพร้อมรับมือภัยคุกคามทางไซเบอร์

ทั่วโลกรวมทั้งประเทศไทยกำลังเผชิญปัญหาการขาดแคลนบุคลากรที่เกี่ยวข้องกับความมั่งคงปลอดภัยทางไซเบอร์ เป็นปัญหาใหญ่ที่องค์กรภาครัฐและธุรกิจกำลังเผชิญและอาจมีแรงกดดันจากการแย่งชิงตัวบุคลากร ดังนั้น ภาครัฐและเอกชนต้องเร่งพัฒนาบุคลากรด้านนี้ เพื่อรองรับภัยคุกคามทางไซเบอร์ที่รุนแรงขึ้น

จากสถานการณ์การแพร่ระบาดของ COVID-19 ส่งผลให้มีการขยายตัวของการทำงานระยะไกล (Remote Workstation) และการใช้บริการคลาวด์แพลตฟอร์ม ขณะที่ปัญหาจากภัยคุกคามทางไซเบอร์มีความรุนแรงขึ้น ซึ่งแน่นอนว่าความต้องการบุคลากรที่มีความเชี่ยวชาญและชำนาญด้านความมั่งคงปลอดภัยทางไซเบอร์ทั่วโลกก็เพิ่มขึ้นตามมาด้วย

ภาพที่ 3 การประมาณการจำนวนบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ทั่วโลก ปี 2565

(หน่วย:คน)



ที่มา: (ISC)² 2022 workforce study

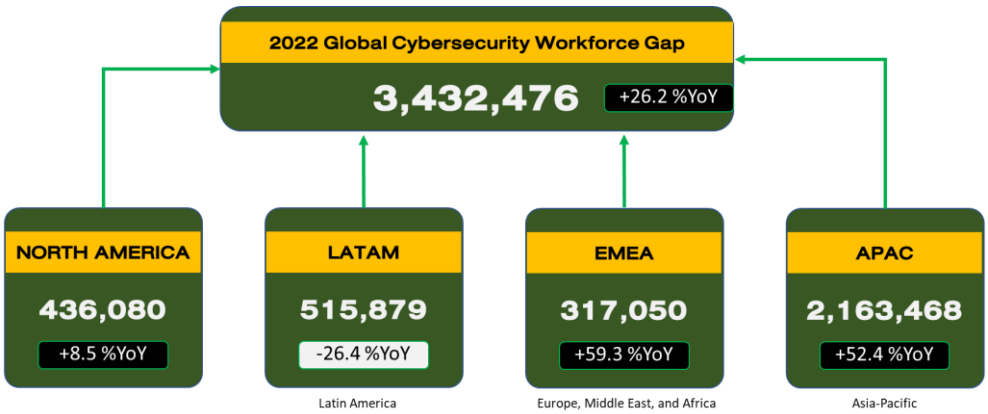
จากรายงาน “(ISC)² 2022 workforce study” ที่จัดทำโดย (ISC)² ซึ่งเป็นองค์กรไม่แสวงหากำไรที่มีสมาชิกประกอบด้วยผู้นำด้านความปลอดภัยทางด้านสารสนเทศทั่วโลก ได้ประเมินว่าในปี 2565 มีบุคลากรทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์ทั่วโลกประมาณ 4.65 ล้านคน เพิ่มขึ้นกว่า 11.1% จากปี 2564 (ภาพที่ 3) และถือว่าเป็นสถิติสูงสุดใหม่นับตั้งแต่ (ISC)² จัดทำรายงาน และมีข้อสังเกตว่า **ในภูมิภาคเอเชียแปซิฟิกที่มีบุคลากรที่ทำงานด้านความมั่งคงปลอดภัยทางไซเบอร์เพิ่มขึ้นจากปีที่ผ่านมาในอัตราที่สูงกว่าภูมิภาคอื่น คือ เพิ่มขึ้น 15.6 % หรือเพิ่มขึ้น 859,000 คน จากปีผ่านมา**[4]

นอกจากนี้ รายงานฉบับนี้ยังเปิดเผยว่า **ในปี 2565 ทั่วโลกมีความต้องการบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์อีกกว่า 3.43 ล้านคน เพิ่มขึ้น 26.2% จากปีที่ผ่านมา** (ภาพที่ 4) **โดยเฉพาะในภูมิภาคเอเชียแปซิฟิกที่มีปริมาณความต้องการบุลากรด้านความมั่งคงปลอดภัยทางไซเบอร์สูงขึ้น 2.16 ล้านคน จากปีที่ผ่านมา หรือคิดเป็น 63% ของจำนวนบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ทั้งหมดที่ทั่วโลกต้องการ นอกจากนี้ ผู้เชี่ยวชาญยังคาดการณ์ปริมาณความต้องการบุคลากรด้านความมั่งคงปลอดภัยทางไซเบอร์จะยิ่งเพิ่มขึ้นในปีนี้** (ปี 2566)

[4] จากการสัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์จำนวนทั่วโลก เพื่อประเมินขนาดบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ ปัญหาการขาดแคลนบุคลากรที่มีความสามารถ ความท้าทายและโอกาส รวมถึงช่องว่างบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ มุมมองเกี่ยวกับการจ้างงาน วัฒนธรรมองค์กร ความพึงพอใจในงาน เส้นทางอาชีพ การพัฒนาวิชาชีพ และอนาคตของงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (https://www.isc2.org/Research/Workforce-Study)

ภาพที่ 4 ประมาณการจำนวนบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ทั่วโลกต้องการเพิ่มขึ้น ในปี 2565

(หน่วย:คน)



ที่มา: (ISC)^2 2022 workforce study

ซึ่งสอดคล้องกับรายงาน “2022 Official Cybercrime Report” ที่จัดทำโดยบริษัท Cybersecurity Ventures[5] ที่เปิดเผยว่า **ทั่วโลกมีความต้องการบุคลากรด้านความมั่งคงปลอดภัยทางไซเบอร์สูงขึ้นมาก โดยในปี 2564 ทั่วโลกมีความต้องการบุคลากรด้านความมั่งคงปลอดภัยทางไซเบอร์สูงถึง 3.5 ล้านคน เพิ่มขึ้นจาก 1 ล้านคนในปี 2556 หรือเพิ่มขึ้น 3.4 เท่าและในรายงานดังกล่าวยังคาดว่าในช่วง 5 ปีข้างหน้า ปริมาณความต้องการบุคลากรด้านนี้จะยังคงอยู่ และนิตยสาร Fortunes ได้ประเมินว่าในประเทศสหรัฐอเมริกาเพียงประเทศเดียวจะมีปริมาณความต้องการบุคลากรด้านนี้มากกว่า 700,000 อัตรา**

สำหรับประเทศไทย ปัญหาการขาดแคลนบุคลากรทางด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นปัญหาใหญ่ที่องค์กรภาครัฐและธุรกิจกำลังเผชิญ โดยเฉพาะหน่วยงานของรัฐ จากจำนวนข้าราชการในองค์กรภาครัฐ มีอยู่ที่ 400,000 คน แต่มีบุคลากรด้านความมั่งคงปลอดภัยทางไซเบอร์รวมกันเพียง 4,000 เท่านั้น[6] ขณะที่ข้อมูลจากบริษัท จัดหางาน จ๊อบส์ ดีบี (ประเทศไทย) จำกัด ณ วันที่ 23 กรกฎาคม 2566 มีบริษัทเอกชนประกาศรับสมัครงานในตำแหน่งเจ้าหน้าที่บุคลากรด้านความมั่งคงปลอดภัยทางไซเบอร์ เจ้าหน้าที่วิเคราะห์ด้านความมั่งคงปลอดภัยทางไซเบอร์ จำนวน 267 อัตรา

แม้ว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้จัดทำโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่งคงปลอดภัยทางไซเบอร์ (Intensive Cybersecurity Capacity Building Program)เพื่อพัฒนาขีดความ สามารถของบุคลากรที่ปฏิบัติหน้าที่รับผิดชอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานต่างๆ ให้มีความชำนาญด้าน

[5] บริษัทวิจัยและสื่อสิ่งพิมพ์ชั้นนำระดับโลกที่เผยแพร่ข้อมูลเศรษฐกิจดิจิทัลโลกและข้อมูลสถิติที่สำคัญเกี่ยวกับความปลอดภัยด้านไซเบอร์

[6] ข้อมูลจากการให้สัมภาษณ์ของเลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ความมั่งคงปลอดภัยทางไซเบอร์ และพัฒนาระบบการเรียนออนไลน์ (NSCA e-learning) เพื่อส่งเสริมการพัฒนาทักษะความรู้ด้านความมั่งคงปลอดภัยทางไซเบอร์ และส่งเสริมการสอบใบประกาศนียบัตรและใบรับรองความเชี่ยวชาญด้านไซเบอร์ที่เป็นที่ยอมรับในระดับสากล[7] **อย่างไรก็ตาม ประเทศไทยจะต้องพัฒนาขีดความสามารถ รวมถึงความรู้และความเข้าใจด้านการรักษาความมั่งคงปลอดภัยทางไซเบอร์ต่อไป ทั้งในระดับนักเรียน นักศึกษา และประชาชนที่สนใจด้านนี้**

อาจกล่าวโดยสรุปได้ว่า บริษัทจดทะเบียนในตลาดหุ้นไทยเตรียมตัวป้องกันภัยคุกคามทางไซเบอร์ ทั้งในด้านบุคลากร กระบวนการ และเทคโนโลยี เพื่อสร้างความตระหนักรู้ และเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์เพื่อรับมือและกู้คืนระบบให้สามารถกลับมาทำงานได้อย่างปกติ เป็นต้น ขณะเดียวกันปัญหาการขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ยังเป็นปัญหาที่เกิดขึ้นทั่วโลกและในประเทศไทย และอาจนำซึ่งปัญหาการแย่งชิงบุคลากร ดังนั้น ภาครัฐและเอกชนควรให้ความสำคัญในการผลิตบุคลากรด้านนี้เพิ่มเติม เพื่อรองรับภัยคุกคามทางไซเบอร์ที่รุนแรงขึ้น

---

[7] https://national-cyber-academy.ncsa.or.th/open-elearning/