แนวปฏิบัติในการรองรับความเสี่ยงจากอุบัติการณ์ที่เกิดขึ้นใหม่ (Emerging risk)

บริษัท เทคลีด เน็กซ์ จำกัด (มหาชน)

บริษัท เทคลีด เน็กซ์ จำกัด (มหาชน)
แนวปฏิบัติในการรองรับความเสี่ยงจากอุบัติการณ์ที่เกิดขึ้นใหม่ (Emerging risk)

ความเสี่ยงจากอุบัติการณ์ที่เกิดขึ้นใหม่ (Emerging risk) คือ ความเสี่ยงที่ยังไม่ได้ปรากฏขึ้นในปัจจุบัน แต่อาจจะเกิดขึ้นได้ในอนาคตเนื่องจากสภาวะแวดล้อมในการดำเนินธุรกิจที่เปลี่ยนแปลงไป เช่น การเปลี่ยนแปลงทางการเมือง เศรษฐกิจ กฎหมาย สังคม เทคโนโลยี สภาพแวดล้อมทางกายภาพ การเปลี่ยนแปลงด้านภูมิอากาศ หรือภาวะโรคอุบัติใหม่ระบาด หรือนโยบายภาครัฐและหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับธุรกิจ โดยบริษัท เทคลีด เน็กซ์ จำกัด (มหาชน) ("บริษัท") ตระหนักถึงความเสี่ยงจากอุบัติการณ์ที่เกิดขึ้นใหม่ โดยเฉพาะการเปลี่ยนแปลงอย่างรวดเร็วทั้งทางด้านเทคโนโลยี ภัยคุกคามไซเบอร์มีการเปลี่ยนแปลงอย่างก้าวกระโดด อาจนำไปสู่การเกิดขึ้นของความเสี่ยงใหม่ที่ไม่เคยเกิดขึ้นในอดีต บริษัทจึงเห็นว่าควรมีการกำหนดกรอบแนวทาง วางมาตรการ และสร้างความความไว้วางใจในยุคที่เทคโนโลยีเปลี่ยนแปลงอย่างรวดเร็ว โดยการสร้างความยืดหยุ่นองค์กรในการคาดการณ์ ป้องกัน และรับมือกับความเสี่ยงที่เกิดใหม่ด้านไซเบอร์ เช่น ภัยคุกคามจากปัญญาประดิษฐ์ (AI-powered threats) ช่องโหว่ในห่วงโซ่อุปทานซอฟต์แวร์ และภัยคุกคามยุคถัดไป เพื่อปกป้องสินทรัพย์ดิจิทัล ข้อมูลลูกค้า และความต่อเนื่องทางธุรกิจของบริษัท

1. <u>ผลกระทบจากความเสี่ยงจากอุบัติการณ์ที่เกิดขึ้นใหม่ (Emerging risk)</u>

บริษัทประเมินผลกระทบจากความเสี่ยงที่เกิดขึ้นใหม่ด้านภัยคุกคามไซเบอร์ ดังนี้

1.1 ผลกระทบด้านการเงินและความต่อเนื่องทางธุรกิจ

- อาจเกิดค่าใช้จ่ายในการฟื้นฟูระบบ รวมถึงค่าจ้างผู้เชี่ยวชาญเข้ามาตรวจสอบ การกู้คืนระบบ และการอัพเกรดระบบรักษาความปลอดภัยใหม่ทั้งหมด
- การหยุดชะงักของธุรกิจ หากระบบมีความเสียหายโดยไม่สามารถให้บริการลูกค้าได้ ส่งผลให้สูญเสียรายได้
- การสูญเสียโอกาสทางธุรกิจ พันธมิตรหรือคู่ค้าอาจชะลอการทำสัญญาหรือยุติการเจรจาเนื่องจากความไม่มั่นใจในระบบความปลอดภัยของบริษัท

1.2 ผลกระทบด้านความน่าเชื่อถือและภาพลักษณ์องค์กร

- ความเชื่อมั่นของลูกค้าลดลง โดยเฉพาะหากมีข้อมูลส่วนบุคคล หรือข้อมูลทางการเงินรั่วไหล

- มูลค่าบริษัทลดลง หากเป็นบริษัทที่อยู่ในตลาดหลักทรัพย์ ข่าวการถูกโจมตีทางไซเบอร์มักส่งผลกระทบเชิงลบต่อราคาหุ้นอย่างรุนแรงในระยะสั้น และส่งผลต่อความเชื่อมั่นของนักลงทุนในระยะยาว
- ผลกระทบต่อภาพลักษณ์แบรนด์ ซึ่งต้องใช้เวลาและงบประมาณในการประชาสัมพันธ์เพื่อกู้คืนชื่อเสียงของบริษัท

1.3 ผลกระทบด้านกฎหมายและการกำกับดูแล

- หากข้อมูลรั่วไหลอาจนำไปสู่โทษปรับทั้งทางแพ่ง ทางอาญา และทางปกครอง
- การฟ้องร้องดำเนินคดี โดยอาจถูกฟ้องร้องจากลูกค้าหรือผู้เสียหายที่ได้รับผลกระทบ
- การตรวจสอบที่เข้มงวดขึ้นจากหน่วยงานกำกับดูแล ซึ่งทำให้กระบวนการทำงานหลังจากนั้นมีความซับซ้อนและมีต้นทุนในการจัดการสูงขึ้น

2. <u>แผนงานรองรับความเสี่ยงจากอุบัติการณ์ที่เกิดขึ้นใหม่ (Emerging risk)</u>

บริษัทมีแผนงานในการรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ (IT Security) เพื่อรองรับความเสี่ยงที่เกิดขึ้นใหม่ด้านภัยคุกคามไซเบอร์ ดังนี้

2.1 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT

- การบริหารจัดการการตั้งค่าระบบ และสอบทานการตั้งค่าระบบอย่างสม่ำเสมอ เพื่อให้การตั้งค่าระบบเป็นไปอย่างถูกต้องและปลอดภัย
- การบริหารจัดการการเปลี่ยนแปลงอย่างรัดกุมเพียงพอ เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วนและป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต
- การบริหารจัดการขีดความสามารถของระบบ IT ให้มีมาตรฐานและวิธีปฏิบัติเรื่องการจัดการขีดความสามารถ การติดตามประสิทธิภาพการทำงานของระบบ และการประเมินแนวโน้มการใช้ทรัพยากรด้าน IT เพื่อให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และสามารถวางแผนการจัดสรรทรัพยากรให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ

- การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่ายและอุปกรณ์ที่ใช้ปฏิบัติงาน ให้สามารถป้องกันการโจมตีด้วยรูปแบบต่าง ๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware) เพื่อลดความเสี่ยงจากการถูกโจมตีระบบ IT ขององค์กร หรือถูกใช้เป็นช่องทางในการโจมตีหน่วยงานอื่น และป้องกันการรั่วไหลของข้อมูลสำคัญ หรือการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต
- กำหนดให้มีมาตรการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก การใช้งานอุปกรณ์เคลื่อนที่ และการใช้งานอุปกรณ์ส่วนตัว
- การสำรองข้อมูลที่สำคัญด้วยวิธีการและความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีสภาพพร้อมใช้งานสอดคล้องกับเป้าหมายการกู้คืนระบบ IT ในกรณีที่ระบบ IT และข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย
- การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (Log) อย่างครบถ้วนและเพียงพอ และสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูล และระบบ IT ย้อนหลังได้ตามที่กฎหมายกำหนด
- การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ
- การประเมินช่องโหว่ทางเทคนิค
- การทดสอบการเจาะระบบ
- การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ โดยจัดให้มีกระบวนการควบคุมการติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบและอุปกรณ์เพื่อลดความเสี่ยงที่จะถูกโจมตีในอนาคต

2.2 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT

- จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง
- กำหนดแผน หรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์
- รายงานเหตุการณ์ที่มีการละเมิดกฎหมาย กฎ และระเบียบที่เกี่ยวข้องกับบริษัท ต่อหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า ภายในระยะเวลาที่กฎหมายกำหนดไว้

- วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไข และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต
- บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT
- ทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างน้อยปีละ 1 ครั้ง

2.3 แผนฉุกเฉินด้าน IT

บริษัทจัดให้มีแผนฉุกเฉินด้าน IT เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ซึ่งส่งผลกระทบให้ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยให้สามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ ดังนี้

- จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT
- กระบวนการจัดทำแผนฉุกเฉินด้าน IT ควรครอบคลุมการดำเนินการ เช่น การประเมินความเสี่ยงที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง และวิเคราะห์ผลกระทบทางธุรกิจ เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ IT ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก เป็นต้น
- จัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็นของระบบที่มีนัยสำคัญ เพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนดไว้
- สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม
- ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง
- กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้าน IT หรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้
- จัดให้มีรายละเอียดในการติดต่อ เพื่อให้สามารถประสานงานในการรายงานเหตุการณ์ผิดปกติด้าน IT หรือขอความช่วยเหลือจากหน่วยงานภายนอกที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ