คู่มือการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) สำหรับกรรมการบริษัท ในภาคตลาดทุน

จัดทำโดย:

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

สิงหาคม 2568

EXECUTIVE SUMMARY

การกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) สำหรับกรรมการบริษัทในภาคตลาดทุน ในยุคดิจิทัลที่ภัยคุกคามทางไซเบอร์ทวีความซับซ้อนและรุนแรงขึ้นอย่างต่อเนื่อง Cybersecurity จึงไม่ใช่เรื่องของฝ่าย IT เท่านั้น แต่เป็นวาระสำคัญระดับกรรมการบริษัท โดยเฉพาะในภาคตลาดทุนที่ต้องรักษาความเชื่อมั่นของผู้ลงทุนและผู้มีส่วนได้เสีย

คู่มือฉบับนี้จัดทำโดยสำนักงาน ก.ล.ต. เพื่อสนับสนุนกรรมการบริษัทให้สามารถกำกับดูแลด้านไซเบอร์อย่างมีประสิทธิภาพ ครอบคลุม 7 ประเด็นสำคัญ ได้แก่:

1. บทบาทกรรมการต่อ Cybersecurity กรรมการบริษัทควรมีส่วนร่วมในการกำหนดนโยบายและติดตามความเสี่ยงไซเบอร์อย่างใกล้ชิด ไม่ควรมองว่าเป็นหน้าที่ของฝ่าย IT เพียงฝ่ายเดียว
2. การบริหารความเสี่ยงความทางไซเบอร์ ควรผนวกความเสี่ยงไซเบอร์เข้ากับการบริหารความเสี่ยงองค์กร (ERM) โดยใช้มาตรฐานสากล เช่น ISO/IEC 27001, NIST CSF
3. ความเสี่ยงจากบุคคลภายนอก (Third Party Risk) ต้องมีการประเมินและติดตามผู้ให้บริการภายนอกที่เข้าถึงข้อมูลสำคัญ พร้อมกำหนดข้อกำหนดด้านความปลอดภัยในสัญญา
4. การตอบสนองต่อภัยคุกคามไซเบอร์ องค์กรควรมีแผนรับมือเหตุการณ์ไซเบอร์ที่ชัดเจน พร้อมระบบเตือนภัยและเครื่องมือที่ทันสมัย เช่น SIEM, EDR
5. การสื่อสารในภาวะวิกฤติไซเบอร์ กรรมการบริษัทควรกำกับดูแลให้มีแผนการสื่อสารที่โปร่งใสและมีประสิทธิภาพในกรณีเกิดเหตุร้ายแรง
6. วัฒนธรรมและความตระหนักรู้ในองค์กร ส่งเสริมให้บุคลากรทุกระดับมีส่วนร่วมในการรักษาความปลอดภัยไซเบอร์ผ่านการอบรมและกิจกรรมสร้างความตระหนักรู้
7. การกำกับดูแล AI กรรมการบริษัทควรมีบทบาทในการกำกับดูแลการใช้ AI ให้สอดคล้องกับหลักธรรมาภิบาล ความปลอดภัย และจริยธรรม

เครื่องมือประกอบ เช่น แบบประเมินตนเอง รายงานความเสี่ยง และคำถามเชิงกลยุทธ์ ด้าน AI Governance ช่วยให้กรรมการบริษัทสามารถนำไปใช้จริงในการประชุมและกำหนดนโยบายองค์กร

การกำกับดูแลด้านไซเบอร์อย่างรอบด้านไม่เพียงช่วยลดความเสี่ยง แต่ยังเป็นส่วนสำคัญของ ESG ที่เสริมสร้างความไว้วางใจและความยั่งยืนขององค์กรในระยะยาว

สารบัญ

บทนำ

ในยุคดิจิทัลที่ภัยคุกคามทางไซเบอร์ทวีความซับซ้อนและรุนแรงมากขึ้นอย่างต่อเนื่องความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) จึงไม่ใช่เพียงหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ (IT) เท่านั้น แต่เป็นวาระสำคัญที่ระดับคณะกรรมการบริษัทต้องให้ความสำคัญ เพราะเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้นกับองค์กร ไม่เพียงจะส่งผลกระทบโดยตรงต่อการดำเนินธุรกิจ แต่มันยังกระทบต่อความน่าเชื่อถือ และความยั่งยืนขององค์กรอีกด้วย

คู่มือฉบับนี้จัดทำขึ้นโดยสำนักงาน ก.ล.ต. เพื่อเป็นเครื่องมือสนับสนุนกรรมการบริษัทในภาคตลาดทุนให้สามารถกำกับดูแลความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิภาพ โดยครอบคลุมทั้งมิติของความเสี่ยง กลยุทธ์ การบริหารจัดการ และธรรมาภิบาลด้านไซเบอร์

เนื้อหาในคู่มือแบ่งเป็นประเด็นสำคัญ 7 ด้าน พร้อมตัวอย่างแนวปฏิบัติ “สิ่งที่ควรทำ” และ “สิ่งที่ไม่ควรทำ” รวมถึงเครื่องมือประกอบ เช่น แบบประเมินตนเอง รายงานตัวชี้วัดความเสี่ยง และคำถามเชิงกลยุทธ์สำหรับกรรมการ ทั้งนี้ เพื่อให้กรรมการสามารถนำไปประยุกต์ใช้ในการประชุม การติดตามการบริหารความเสี่ยง และการกำหนดนโยบายองค์กรได้จริง

การกำกับดูแลด้านไซเบอร์อย่างรอบด้าน นอกจากจะช่วยลดความเสี่ยงแล้ว ยังเป็นองค์ประกอบสำคัญของหลักธรรมาภิบาล (Governance) ซึ่งช่วยเสริมสร้างและธำรงไว้ซึ่งความไว้วางใจของผู้ใช้บริการที่มีให้กับองค์กร และสอดคล้องกับบริบท ESG ที่ผู้มีส่วนได้เสียให้ความสำคัญมากขึ้นเรื่อย ๆ ดังนั้น คู่มือนี้จึงเป็นหนึ่งในก้าวสำคัญเพื่อยกระดับการบริหารจัดการความเสี่ยงไซเบอร์ขององค์กรในภาคตลาดทุนไทยให้ทัดเทียมมาตรฐานสากลและช่วยคณะกรรมการบริษัทพร้อมรับมือความท้าทายจากเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

1 บทบาทกรรมการบริษัทต่อความมั่นคงปลอดภัยทางไซเบอร์ (CYBERSECURITY)

ความเสี่ยงทางไซเบอร์ ไม่ใช่แค่สิ่งที่อาจมีผลกระทบเพียงระบบ IT ของบริษัทเท่านั้น แต่อาจส่งผลกระทบถึงทรัพย์สิน ระบบงาน และชื่อเสียงขององค์กร กรรมการบริษัทจึงควรให้ความสำคัญกับบทบาทในการกำกับดูแลนโยบาย กลยุทธ์ และติดตามสถานะความมั่นคงปลอดภัยไซเบอร์อย่างใกล้ชิด

สิ่งที่ควรทำ DO

01 คณะกรรมการบริษัทควรบรรจุ Cyber Risk เป็นวาระการประชุมประจำเพื่อให้มีการนำเสนอและติดตามความเสี่ยงด้านไซเบอร์อย่างต่อเนื่องในทุกการประชุมคณะกรรมการบริษัท

02 จัดตั้งคณะกรรมการหรืออนุกรรมการเฉพาะกิจด้านไซเบอร์ เพื่อประเมิน ตอบสนอง และตรวจสอบ ให้เป็นไปตามกฎหมาย เช่น ประกาศ/แนวปฏิบัติของหน่วยงานกำกับดูแล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เป็นต้น

03 กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite[1]) หากเกิดภัยคุกคามด้านไซเบอร์ให้ชัดเจน อนุมัติแผนจัดการความเสี่ยงโดยอ้างอิงมาตรฐานสากล (เช่น ISO/IEC 27001 Information Security Management Systems (ISMS) หรือ NIST Cybersecurity Framework (CSF) 2.0, ISACA Control Objectives for Information and Related Technologies (COBIT), COSO Enterprise Risk Management (ERM) เป็นต้น)

04 กำหนดให้ผู้บริหารรายงานสถานะและตัวชี้วัดสำคัญ (KPIs) ด้านไซเบอร์ต่อคณะกรรมการบริษัทเป็นระยะ เช่น เหตุการณ์ผิดปกติ การสำรองข้อมูล ความพร้อมของระบบ ผลการตรวจสอบด้าน IT เป็นต้น

05 ส่งเสริมให้กรรมการบริษัทเพิ่มพูนความรู้ด้านไซเบอร์อย่างสม่ำเสมอ เพื่อช่วยให้สามารถกำกับดูแลและรับมือกับความเสี่ยงทางไซเบอร์ได้อย่างมีประสิทธิภาพ

06 กำหนดบทบาทหน้าที่ตามโครงสร้าง 3 Lines of Defense[2] โดยคณะกรรมการบริษัทเป็นผู้กำหนดนโยบายภาพรวม

สิ่งที่ไม่ควรทำ DON'T

01 มองว่าเรื่องไซเบอร์เป็นหน้าที่ของฝ่าย IT เพียงฝ่ายเดียว

02 มองข้ามกฎหมาย/ระเบียบที่เกี่ยวข้อง

03 รอให้เกิดเหตุการณ์ก่อนจึงค่อยพูดคุยถึงมาตรฐานความปลอดภัย

04 ตัดสินใจโดยขาดข้อมูลจากหลายฝ่ายหรือไม่ตรวจสอบหรือติดตามรายงานจากผู้บริหาร

05 มองข้ามการพัฒนาทักษะความรู้ด้านไซเบอร์โดยมองว่าเป็นเรื่องของฝ่าย IT เท่านั้น

06 ไม่ได้วางโครงสร้างในการกำกับดูแลภายในองค์กรอย่างเหมาะสม ปล่อยให้การดูแลความเสี่ยง IT/Cyber Risk เป็นของฝ่าย ITเพราะคิดว่าเป็นประเด็นเทคนิค

[1] ความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ ระดับหรือประเภทของความเสี่ยงโดยรวมที่คณะกรรมการบริหารและผู้บริหารยอมรับได้ในการดำเนินการเพื่อให้บรรลุวิสัยทัศน์และพันธกิจขององค์กร สามารถแสดงได้ทั้งเชิงคุณภาพหรือเชิงปริมาณหรือทั้งสองรูปแบบรวมกัน

1 บทบาทกรรมการบริษัทต่อความมั่นคงปลอดภัยทางไซเบอร์ (CYBERSECURITY)

นอกจากนี้ บทบาทของคณะกรรมการบริษัทในด้านความมั่นคงปลอดภัยทางไซเบอร์ถือเป็นองค์ประกอบสำคัญภายใต้หลักการ ESG (Environmental, Social, and Governance) โดยเฉพาะในมิติของ Governance ที่เน้นการบริหารจัดการองค์กรอย่างมีธรรมาภิบาล โปร่งใส และรับผิดชอบต่อผู้มีส่วนได้เสีย กรรมการบริษัทควรตระหนักถึงความเสี่ยงและผลกระทบจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลต่อข้อมูล ทรัพย์สิน ชื่อเสียงขององค์กร และความไว้วางใจที่ได้รับจากผู้ใช้บริการ

กรรมการบริษัท ควรมีส่วนร่วมในการกำหนดนโยบายและแนวทางปฏิบัติด้าน Cybersecurity ให้สอดคล้องกับมาตรฐานสากล รวมถึงบูรณาการ Cybersecurity เข้าเป็นส่วนหนึ่งของกลยุทธ์ ESG เพื่อสร้างความเชื่อมั่นให้แก่ผู้ถือหุ้น นักลงทุน ลูกค้า และพันธมิตรทางธุรกิจ ตลอดจนสนับสนุนให้องค์กรสามารถดำเนินงานได้อย่างยั่งยืนในยุคดิจิทัล ทั้งนี้ การกำกับดูแลด้าน Cybersecurity อย่างมีประสิทธิภาพจะช่วยลดความเสี่ยง เพิ่มขีดความสามารถในการแข่งขัน และเสริมสร้างภาพลักษณ์ที่ดีให้แก่องค์กรในระยะยาว

ข้อมูลเพิ่มเติม ภาคผนวก A : แบบประเมินตนเองของกรรมการบริษัทในด้านการกำกับดูแล Cybersecurity (Cybersecurity Governance Self-Assessment Checklist)

[2] โครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ควรมีการถ่วงดุลอำนาจ (Check and Balance) และมีการแบ่งแยกหน้าที่ (Segregation of Duties) อย่างเหมาะสม ตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense) ได้แก่
1. การปฏิบัติงาน (First Line of Defense) หมายถึง หน่วยงานปฏิบัติงานด้าน IT และผู้ที่ใช้ระบบ IT ปฏิบัติงาน
2. การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องในการปฏิบัติงานด้าน IT (Second Line of Defense) หมายถึง หน่วยงานบริหารความเสี่ยงด้าน IT และหน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ด้าน IT
3. การตรวจสอบด้าน IT (Third Line of Defense) หมายถึง หน่วยงานตรวจสอบด้าน IT ซึ่งมีหน้าที่ในการตรวจสอบการปฏิบัติงานของหน่วยงานที่ทำหน้าที่ First Line of Defense และ Second Line of Defense เพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบาย มาตรฐาน และกฎหมายทางด้าน IT ที่เกี่ยวข้อง หน่วยงานในระดับนี้อาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ First Line of Defense และ Second Line of Defense

2 การกำหนดกรอบการบริหารความเสี่ยงทางไซเบอร์

คณะกรรมการบริษัทควรมีส่วนร่วมอย่างใกล้ชิดในการกำหนดกรอบการบริหารความเสี่ยงทางไซเบอร์ โดยสามารถนำความเสี่ยงด้านไซเบอร์ ผนวกเป็นส่วนหนึ่งของการกำกับดูแลองค์กรและการจัดการความเสี่ยงด้านไซเบอร์ขององค์กร (Enterprise Risk Management - ERM) ได้ เพื่อระบุและประเมินความเสี่ยงต่าง ๆ ที่อาจกระทบองค์กร โดยอาจอ้างอิงมาตรฐานสากล เช่น COSO Enterprise Risk Management – Integrating with Strategy and Performance (ERM), ISO/IEC 27001 Information Security Management Systems (ISMS), ISO 31000 (Risk Management) หรือ NIST Cybersecurity Framework 2.0 (CSF 2.0)

สิ่งที่ควรทำ DO

01 นำกรอบการบริหารความเสี่ยงทางไซเบอร์รวมเป็นส่วนหนึ่งของการบริหารจัดการความเสี่ยงองค์กร (ERM)

02 แยกบทบาทหน้าที่ตาม 3 Lines of Defense ให้ชัดเจน ตรวจสอบและปรับปรุงโครงสร้างตามความเหมาะสม

03 มีการจัดทำทะเบียนจัดการความเสี่ยง (Risk Register[3]) และคัดเลือกระดับความเสี่ยงอย่างชัดเจน เพื่อให้ง่ายต่อการตัดสินใจจัดลำดับความสำคัญ

04 มีการนำเสนอข้อมูลความเสี่ยงด้าน IT ที่ส่งผลกระทบต่อองค์กรในภาพรวม ให้คณะกรรมการบริษัทพิจารณา โดยควรนำเสนอในรูปแบบที่เข้าใจได้ง่าย (Heatmap, Key Risk Indicator - KRI) เพื่อให้คณะกรรมการบริษัทมองเห็นภาพรวมความเสี่ยงได้เร็ว

05 มีการพิจารณาแนวทางในการจัดการความเสี่ยง (Risk Treatment[4]) ส่วนการโอนย้ายความเสี่ยงให้กับผู้อื่น (Risk Transference) เช่น การทำประกันภัยไซเบอร์ เป็นต้น

สิ่งที่ไม่ควรทำ DON'T

01 ดำเนินการโดยไม่มีความเชื่อมโยงกับความเสี่ยงใดภายในองค์กร และไม่มีมาตรฐานหรือ Framework อ้างอิง

02 ให้ฝ่ายเดียวรับผิดชอบทั้งควบคุมและตรวจสอบเองจนขาดสมดุล/อาจเกิด Conflict Of Interest

03 ข้อมูลความเสี่ยงถูกจัดเก็บอย่างกระจัดกระจายและขาดระบบในการติดตามหรือปรับปรุงข้อมูลอย่างต่อเนื่อง

04 รายงานแต่ตัวเลขทางเทคนิคหรือข้อมูลด้าน Technical มากเกินไป จนคณะกรรมการบริษัทไม่เข้าใจสาระสำคัญของความเสี่ยง

05 มองข้ามประเด็นการจัดการความเสี่ยง (Risk Treatment) หรือไม่สนับสนุนทรัพยากรที่จำเป็นและเหมาะสมต่อการจัดการความเสี่ยง

ข้อมูลเพิ่มเติม ภาคผนวก B: ตัวอย่างรายงานความเสี่ยงไซเบอร์ที่ควรเสนอเข้าสู่คณะกรรมการบริษัท(Cybersecurity Risk Dashboard)

[3] การจัดทำทะเบียนความเสี่ยง (Risk Register) เพื่อบันทึกผลการประเมินความเสี่ยง และแนวทางในการจัดการความเสี่ยง โดยมีตัวอย่างรายละเอียด ดังนี้ 1. วันที่ประเมินความเสี่ยง 2. รายละเอียดเหตุการณ์ความเสี่ยง 3. โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (Likelihood) 4. ความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (Potential Impact) 5. ระดับค่าความเสี่ยงก่อนการควบคุม (Inherent Risk) 6. แนวทางจัดการความเสี่ยง (Risk Treatment) 7. เจ้าของความเสี่ยง (Risk Owner) 8. ระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) 9. สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) เป็นต้น โดยควรครอบคลุมถึง ความเสี่ยงจากบุคคลภายนอก (Third-Party/Vendor Risk) ความเสี่ยงจากเทคโนโลยีเก่า (Legacy System Risk) ความเสี่ยงจากบุคลากรภายใน (Insider Threat) ความเสี่ยงจากเหตุการณ์ซ้ำซ้อน (Recurring Incident) ความเสี่ยงจากภัยไซเบอร์รูปแบบใหม่ (Emerging Cyber Threats) เป็นต้น

[4] การจัดการความเสี่ยง (Risk Treatment) ควรกำหนดให้มีแนวทางในการจัดการความเสี่ยงด้าน IT อย่างเหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยง (Risk Assessment) เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) โดย การกำหนดแนวทางในการจัดการความเสี่ยง โดยพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมกับผู้ประกอบธุรกิจ เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การลดหรือบรรเทาความเสี่ยง (Risk Mitigation) การโอนย้ายความเสี่ยงให้กับผู้อื่น (Risk Transference) และการยอมรับความเสี่ยงโดยการเสนอเหตุผลต่อผู้บริหารเพื่อตัดสินใจ (Risk Acceptance) เป็นต้น

3 การบริหารความเสี่ยงจากบุคคลภายนอก (THIRD PARTY RISK)

กรรมการบริษัทควรให้ความสำคัญกับความเสี่ยงที่เกิดจากผู้ให้บริการภายนอก (Third Party) โดยเฉพาะผู้ที่เข้าถึงข้อมูลสำคัญหรือระบบหลักขององค์กร เช่น ผู้ให้บริการ Cloud ผู้รับเหมาพัฒนาระบบ หรือ AI Platform จากภายนอก องค์กรควรกำหนดกระบวนการทำคัดเลือก การทำ Due Diligence และการประเมินความเสี่ยงก่อนการใช้บริการจากผู้ให้บริการภายนอก และมีการกำกับติดตามตามรอบระยะเวลาที่กำหนด และระบุบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอก กรณีเกิดเหตุภัยคุกคามไซเบอร์ รวมถึงข้อกำหนดด้านความมั่นคงปลอดภัยด้านไซเบอร์ต่าง ๆ ไว้ในสัญญาอย่างชัดเจน

สิ่งที่ควรทำ DO

01 กำหนดให้ “ความเสี่ยงจาก Third Party” เป็นส่วนหนึ่งของกรอบการบริหารความเสี่ยงขององค์กร และอยู่ในวาระการประชุมคณะกรรมการบริษัท

02 สอบถามผู้บริหารว่าองค์กรมีนโยบายและกระบวนการประเมินความเสี่ยงของ Third Party ในด้าน Cybersecurity/Data Security อย่างไร

03 ตรวจสอบว่าในรายงานความเสี่ยง มีข้อมูล Third Party รวมอยู่ด้วยหรือไม่ เช่น Vendor สำคัญที่ผ่าน/ไม่ผ่านการประเมิน

04 สนับสนุนให้มีการจัดทำข้อกำหนดด้าน Cybersecurity และ Data Security ในสัญญากับ Third Party (ผ่านการกำหนดนโยบายหรือแนวทางของคณะกรรมการบริษัท)

05 ส่งเสริมให้มีรายงานสรุปความเสี่ยงจาก Third Party นำเสนอต่อคณะกรรมการบริษัทเป็นระยะ โดยเฉพาะในกรณีที่มีความเสี่ยงระดับสูง

สิ่งที่ไม่ควรทำ DON’T

01 มองข้ามความเสี่ยงจากผู้ให้บริการภายนอก โดยคิดว่าไม่ใช่เรื่องสำคัญระดับคณะกรรมการบริษัท

02 ไม่ตั้งคำถามหรือติดตามความเสี่ยงจาก Third Party ที่เข้าถึงข้อมูลหรือระบบสำคัญขององค์กร

03 รับรายงานด้าน IT หรือความเสี่ยงโดยไม่ตรวจสอบว่าครอบคลุมถึงผู้ให้บริการภายนอกหรือไม่

04 ปล่อยให้ฝ่ายปฏิบัติการดำเนินการเรื่องสัญญาโดยไม่มีกรอบนโยบายหรือ Oversight

05 รอให้เกิดเหตุเสียหายจาก Third Party ก่อนจึงเริ่มสนใจหรือติดตาม

4 การติดตามและตอบสนองต่อภัยคุกคามไซเบอร์

ภัยไซเบอร์เปลี่ยนแปลงอย่างรวดเร็ว ต้องมีระบบเตือนภัย เครื่องมือที่ทันสมัย และแผนตอบโต้เหตุการณ์ที่ฝึกซ้อมที่ปฏิบัติได้จริงและเหมาะสมกับสถานการณ์ พร้อมแนวทางการรายงานเหตุการณ์ถึงผู้บริหารระดับสูงสุดเมื่อจำเป็น ทั้งนี้ คณะกรรมการบริษัทควรติดตาม และสอบถามถึงระบบเตือนภัยและกระบวนการตอบสนองขององค์กรเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้น รวมถึงทักษะและความพร้อมของบุคลากรภายในองค์กรในการตอบสนองต่อเหตุการณ์

สิ่งที่ควรทำ DO

01 มี Incident Response Plan ที่เป็นรูปธรรม พร้อมกำหนดบทบาทชัดเจน เช่น ใครเป็นผู้รายงานถึงคณะกรรมการบริษัท และฝึกซ้อม Tabletop Exercise/Drill อย่างสม่ำเสมอ

02 ใช้เครื่องมือทันสมัย และเหมาะสมกับธุรกิจ เพื่อให้มั่นใจได้ว่าองค์กรจะสามารถตรวจจับภัยคุกคามได้อย่างทันการณ์ เช่น Security Information and Event Management (SIEM), Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), Endpoint Detection and Response (EDR) และ Threat Intelligence[5] Platform และ Update สม่ำเสมอทั้งนี้ หากองค์กรตรวจจับภัยคุกคามได้อย่างทันการณ์ ก็สามารถตอบสนองได้อย่างเท่าทัน

03 กำหนดเกณฑ์ Severity ว่าเหตุการณ์ลักษณะใดควรยกระดับและมีการรายงานถึงคณะกรรมการบริษัทโดยไม่ชักช้า

04 นำบทเรียนจากเหตุการณ์จริงมาทบทวนและปรับปรุงแผนงานอย่างต่อเนื่อง

สิ่งที่ไม่ควรทำ DON'T

01 1) ไม่กำหนดแบบแผน เน้นแก้ปัญหาเฉพาะหน้า ละเลยฝึกซ้อม หรือคิดว่ามีแผน Business Continuity Plan (BCP) แล้วเพียงพอ
2) ไม่ทบทวนแผน BCP/Disaster Recovery Plan (DRP) หรือแผนเผชิญเหตุต่าง ๆ เพราะคิดว่า "ไม่น่าเกิด"

02 พึ่งพาเครื่องมือประเภทใดประเภทหนึ่งเพียงอย่างเดียว เช่น มีแต่ Firewall หรือระบบป้องกัน โดยไม่มีกระบวนการตรวจจับหรือตอบสนองที่เหมาะสม เมื่อเกิดเหตุองค์กรจะไม่สามารถตอบสนองได้อย่างทันการณ์และเหตุการณ์ที่เกิดขึ้นอาจจะขยายวงกว้างและสร้างความเสียหายมากขึ้นได้

03 รอให้เกิดเหตุการณ์ความเสียหายรุนแรงแล้วจึงเริ่มรายงานหรือดำเนินการแก้ไข

04 ไม่ถอดบทเรียนเพราะคิดว่า "ไม่น่าเกิดซ้ำ"

ข้อมูลเพิ่มเติม ภาคผนวก C : ตัวอย่าง Template รายงานเหตุการณ์ด้านความมั่นคงไซเบอร์ (Cybersecurity Incident Notification Template)

[5] Security Information and Event Management (SIEM) ทำหน้าที่รวบรวมและวิเคราะห์ข้อมูลจากแหล่งต่าง ๆ เพื่อตรวจจับภัยคุกคาม
Intrusion Detection System (IDS) ทำหน้าที่ตรวจจับกิจกรรมที่น่าสงสัยหรือการโจมตีที่เกิดขึ้นในเครือข่าย
Intrusion Prevention System (IPS) ทำหน้าที่ป้องกันการโจมตีโดยการบล็อกหรือสกัดกั้นกิจกรรมที่ไม่พึงประสงค์
Endpoint Detection and Response (EDR) ทำหน้าที่ตรวจจับและตอบสนองต่อภัยคุกคามที่เกิดขึ้นบนอุปกรณ์ปลายทาง และ
Threat Intelligence คือข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ที่รวบรวมและวิเคราะห์จากแหล่งต่าง ๆ เช่น ข่าวกรอง การวิจัย และการแบ่งปันข้อมูล ช่วยให้องค์กรเข้าใจและเตรียมพร้อมรับมือกับภัยคุกคามที่อาจเกิดขึ้น

5 การสื่อสารในภาวะวิกฤติด้านไซเบอร์ (CYBER CRISIS COMMUNICATION)

องค์กรควรมีแผนการสื่อสารในภาวะวิกฤติไซเบอร์ (Cyber Crisis Communication Plan) ที่ชัดเจน โดยควรกำหนดว่าใครจะเป็นผู้สื่อสารกับสาธารณะ หน่วยงานกำกับดูแล และลูกค้า โดยต้องเตรียมเนื้อหาข้อความและแนวทางตอบคำถามล่วงหน้า (Pre-Statement) เพื่อให้พร้อมในการตอบสนองต่อเหตุการณ์ นอกจากนี้ กรรมการบริษัทควรมีบทบาทในการกำหนดกรอบนโยบายและแนวทางการสื่อสารที่ชัดเจน รวมถึงติดตามการดำเนินการของฝ่ายบริหาร ในการเตรียมพร้อมเรื่องดังกล่าวไว้ล่วงหน้า เพื่อให้การตอบสนองต่อเหตุการณ์เป็นไปอย่างมีประสิทธิภาพ โปร่งใส และลดความเสียหายให้ได้มากที่สุด

สิ่งที่ควรทำ DO

01 กำหนดให้ “การสื่อสารในภาวะวิกฤติไซเบอร์” เป็นส่วนหนึ่งของแผนบริหารความเสี่ยง และติดตามให้ฝ่ายบริหารจัดเตรียมแผนการตอบสนองต่อเหตุการณ์ไว้ล่วงหน้า

02 สอบถามและทบทวนแผน Crisis Communication ว่ามีการกำหนดผู้รับผิดชอบ ช่องทาง และรูปแบบข้อความสื่อสารในกรณีฉุกเฉินหรือไม่

03 กำกับดูแลและติดตามให้แน่ใจว่า องค์กรมี Incident Handling Plan หรือแผนรับมือภัยคุกคาม ที่สามารถตอบสนองต่อเหตุการณ์และจำกัดผลกระทบให้อยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite)

04 กำกับดูแลและติดตามให้แน่ใจว่า ฝ่ายบริหารขององค์กรได้ให้ความสำคัญและเข้าร่วมในการฝึกซ้อมแผนรับมือเหตุการณ์ดังกล่าวอย่างสม่ำเสมอ (Incident Response Drill)

สิ่งที่ไม่ควรทำ DON’T

01 มองว่าเรื่องการสื่อสารเป็นหน้าที่ของฝ่ายประชาสัมพันธ์เพียงอย่างเดียว โดยไม่เกี่ยวข้องกับระดับคณะกรรมการบริษัท

02 เพิกเฉยต่อวิธีการที่องค์กรจะสื่อสารกับลูกค้า/หน่วยงานกำกับดูแลในขณะเกิดเหตุร้ายแรง

03 รอให้เกิดเหตุการณ์จริงก่อนจึงพิจารณาวิธีการสื่อสารหรือการแถลงข่าว

04 องค์กรมีแผนรับมือเหตุการณ์แล้วจึงไม่ต้องฝึกซ้อม

6 วัฒนธรรมและความตระหนักรู้ภายในองค์กร

"บุคลากร" คือองค์ประกอบสำคัญของการสร้างความมั่นคงปลอดภัยไซเบอร์ และในขณะเดียวกันก็อาจเป็นจุดเปราะบางได้เช่นกัน กรรมการบริษัทควรส่งเสริมให้เกิดวัฒนธรรมองค์กรที่ทุกคนภายในองค์กรมีความตระหนักรู้และมีส่วนร่วมในการดูแลความปลอดภัยของข้อมูลและระบบ (Cyber Hygiene) อย่างต่อเนื่องและยั่งยืน

สิ่งที่ควรทำ DO

01 แสดงบทบาทผู้นำ (Tone from the Top) ด้วยการปฏิบัติตนให้เป็นแบบอย่างที่ดีในเรื่อง Cyber Hygiene เช่น ปฏิบัติตาม IT Security Policy ที่อนุมัติไปอย่างเคร่งครัด เป็นต้น

02 กำกับและสนับสนุนให้องค์กรจัดกิจกรรมเสริมสร้างความตระหนักรู้ด้านไซเบอร์อย่างต่อเนื่อง เช่น การอบรม ฝึกจำลองสถานการณ์ (Phishing Simulation) และการประเมินระดับความตระหนักรู้และพฤติกรรมความปลอดภัยด้านไซเบอร์ของบุคลากรทุกระดับภายในองค์กร อย่างน้อยปีละ 1 ครั้ง

03 สนับสนุนให้มีการสื่อสารด้วยภาษาเข้าใจง่าย เน้นว่า "เราทุกคนคือเจ้าของข้อมูล"

04 สนับสนุนระบบสร้างแรงจูงใจ เช่น การยกย่องหรือให้รางวัล สำหรับผู้แจ้งเตือนภัยได้ทันท่วงที

05 กำกับดูแลให้องค์กร มีช่องทางแจ้งเหตุผิดปกติที่ปลอดภัย ไม่ลงโทษผู้แจ้งเหตุ และมีมาตรการตอบสนองหากเกิดเหตุการณ์จริง

สิ่งที่ไม่ควรทำ DON'T

01 เพิกเฉย หรือทำในสิ่งที่ขัดกับแนวทาง Cyber Hygiene หรือละเลยต่อ IT Security Policy ขององค์กร

02 1) มองว่าการให้ความรู้ไซเบอร์เป็นเรื่องของฝ่าย IT หรือฝ่าย HR เท่านั้น โดยไม่ติดตามผลหรือสนับสนุนให้เกิดการพัฒนาอย่างต่อเนื่องทั่วทั้งองค์กร
2) ผู้บริหารไม่มีส่วนร่วมฝึกอบรม หรือสร้างความตระหนักรู้ เพราะคิดว่าไม่เกี่ยวกับตน

03 ใช้ศัพท์เทคนิคมากเกินไปจนบุคลากรไม่เข้าใจสาระสำคัญ

04 เพิกเฉยเมื่อพบพฤติกรรมสุ่มเสี่ยงในองค์กร ปล่อยให้ละเมิดซ้ำโดยไม่ดำเนินการใด ๆ

05 ไม่ควรสร้าง หรือสนับสนุนให้เกิดวัฒนธรรม"ไม่พูดเท่ากับไม่ผิด" เพราะต้นทุนในการตรวจสอบและสืบหาสาเหตุเพื่อหา Root Cause มักสูงมากกว่าการกล้ายอมรับความผิดพลาดที่เกิดจากบุคลากรเอง

7 การกำกับดูแล AI ในบทบาทของกรรมการบริษัท

ในยุคที่ปัญญาประดิษฐ์ (AI) กลายเป็นเทคโนโลยีสำคัญในการขับเคลื่อนธุรกิจ การกำกับดูแล AI จึงไม่ใช่เรื่องของเทคนิคเท่านั้น แต่เป็นประเด็นด้านธรรมาภิบาลและความมั่นคงปลอดภัยที่คณะกรรมการบริษัทไม่อาจละเลยได้ โดยเฉพาะเมื่อการนำ AI ไปใช้ อาจนำมาซึ่งความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การรั่วไหลของข้อมูลการตัดสินใจผิดพลาด หรือแม้แต่การละเมิดกฎหมายและจริยธรรม คณะกรรมการบริษัทจึงต้องกำหนดกรอบการกำกับดูแลที่ครอบคลุมทั้งมิติของความเสี่ยง การคุ้มครองข้อมูล และการตรวจสอบการทำงานของ AI อย่างต่อเนื่อง เพื่อสร้างความเชื่อมั่นและความโปร่งใสในการใช้เทคโนโลยีดังกล่าวในองค์กร

สิ่งที่ควรทำ DO

01 กำกับดูแลให้มีการประเมินและบริหารความเสี่ยงด้าน Cybersecurity ที่เกี่ยวข้องกับกิจกรรมที่จะนำ AI มาใช้งาน เช่น การควบคุมสิทธิ์การเข้าถึง การตรวจสอบ Input/Output ของระบบ AI และการเฝ้าระวังพฤติกรรมของ Model ติดตามผลกระทบจาก AI ที่มีอคติ (AI Bias) รวมถึง Security Risk อย่างใกล้ชิด

02 สนับสนุนการจัดทำนโยบายและแนวปฏิบัติด้าน AI Governance ที่สอดคล้องกับแนวปฏิบัติ/มาตรฐานสากล/กฎหมายที่เกี่ยวข้อง (เช่น ETDA AI Governance Guideline, OECD AI Principles, NIST AI RMF, ISO/IEC 42001 AI Management System, PDPA) โดยคำนึงถึงปัจจัยด้านกฎหมาย จริยธรรม ธรรมาภิบาล ความโปร่งใส ความมั่นคงปลอดภัย สิทธิเสรีภาพ และความเป็นส่วนตัว ความน่าเชื่อถือ และความรับผิดชอบต่อผู้มีส่วนได้เสีย

03 กำกับดูแลและติดตามให้มีคณะทำงานหรือกลไก Oversight ที่มีหลายฝ่ายร่วมกันกำกับดูแลความเสี่ยงเกี่ยวกับการใช้งาน AI เช่น AI Governance Committee หรือ AI Ethics Committee พร้อมกำหนดแนวทางทบทวน/ประเมิน AI เป็นระยะ

04 สนับสนุนให้จัดอบรมความเข้าใจด้านความเสี่ยงของ AI แก่บุคลากร รวมถึงกรรมการบริษัทและผู้บริหาร

สิ่งที่ไม่ควรทำ DON'T

01 มองว่า AI เป็นเรื่องของฝ่ายเทคนิคเพียงฝ่ายเดียว โดยไม่วางกรอบนโยบายหรือกลไก Oversight ในระดับองค์กร

02 ปล่อยให้ใช้ AI จาก Third Party หรือ AI-as-a-Service โดยไม่ประเมินความเสี่ยงล่วงหน้า หรือไม่มีนโยบาย และการควบคุมการส่งข้อมูลภายในออกไปยังระบบภายนอก

03 เชื่อว่าเมื่อเลือกใช้ AI สำเร็จรูปแล้ว ผู้ให้บริการจะเป็นผู้รับผิดชอบความปลอดภัยและจริยธรรมโดยสมบูรณ์ ไม่จำเป็นต้องมีมาตรการขององค์กรเอง

04 เพิกเฉยต่อการเปลี่ยนแปลงของเทคโนโลยี AI ที่อาจเพิ่มความเสี่ยงใหม่ให้กับองค์กร โดยไม่มีการประเมินหรือปรับมาตรการควบคุมที่เหมาะสมตามรูปแบบธุรกิจที่เปลี่ยนแปลงไป

ข้อมูลเพิ่มเติม ตามภาคผนวก D : คำถามเชิงกลยุทธ์ที่กรรมการควรถาม ด้าน AI Governance (AI Oversight Questions for the Board)

เอกสารอ้างอิง

- Committee of Sponsoring Organizations of the Treadway Commission (COSO), (2017). Enterprise risk management – Integrating with strategy and performance.

- Information Systems Audit and Control Association (ISACA). (2019). Control Objectives for Information and Related Technologies (COBIT).

- Ivano Bongiovanni, Sergeja Slapničar, Micheal Axelsen, & David Stockdale. (2024). The Three Lines Model in Cybersecurity Governance and Risk Management. Information Systems Audit and Control Association (ISACA).

- National Institute of Standards and Technology (NIST) U.S. Department of Commerce. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

- National Institute of Standards and Technology. (2024). The NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1.

- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29.

- Noah P. Barsky, & Keri Pearlson. (2025). Boards Need a More Active Approach to Cybersecurity. Harvard Business Review.

- Organization for Economic Co-operation and Development (OECD). (2024). OECD AI Principles.

- Tara K. Giunta ,& Lex Suvanto, (2024). Board Oversight of Artificial Intelligence. Harvard Law School Forum on Corporate Governance.

- The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements.

- The National Institute of Standards and Technology (NIST). (2024). AI risk management framework (AI RMF 1.0). U.S. Department of Commerce.

ภาคผนวก
เครื่องมือสำหรับ
กรรมการบริษัท

ภาคผนวก A : แบบประเมินตนเองด้านการกำกับดูแล Cybersecurity (Cybersecurity Governance Self-Assessment Checklist)

คณะกรรมการบริษัทสามารถใช้ Checklist นี้เพื่อตรวจสอบระดับการมีส่วนร่วมของตนในประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร

คำถาม	ใช่/ไม่ใช่	หมายเหตุ/ การติดตาม
1. องค์กรของท่านมีการกำหนด Cybersecurity เป็นวาระในการประชุมคณะกรรมการบริษัทอย่างสม่ำเสมอหรือไม่		
2. มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ด้านไซเบอร์อย่างชัดเจนหรือไม่		
3. ท่านได้รับรายงานสถานะและตัวชี้วัดสำคัญ (KPIs) ด้านไซเบอร์จากผู้บริหารเป็นประจำหรือไม่		
4. มีคณะกรรมการ/อนุกรรมการเฉพาะกิจด้าน Cybersecurity หรือไม่		
5. องค์กรมีการนำ Framework มาตรฐานสากล เช่น ISO/IEC 27001 ISMS, NIST CSF, ISACA COBIT, COSO ERM เป็นต้น มาใช้อย่างเป็นระบบหรือไม่		
6. มีแผนรับมือภัยคุกคามทางไซเบอร์ หรือแผนเผชิญเหตุด้านไซเบอร์หรือไม่ ทั้งนี้ แผนดังกล่าวอาจจะรวมอยู่ในแผน Business Continuity Plan (BCP)/ Disaster Recovery Plan (DRP) ขององค์กรได้		
7. ผู้บริหารองค์กรมีส่วนร่วมในการฝึกซ้อมรับมือเหตุการณ์ (Incident Response Drill) อย่างสม่ำเสมอหรือไม่		
8. มีการประเมินความเสี่ยงของผู้ให้บริการภายนอก (Third Party Risk) อย่างรอบด้านหรือไม่		
9. ท่านได้รับข้อมูลและแผนการตอบสนองเมื่อเกิดภัยไซเบอร์ร้ายแรงหรือไม่		
10. มีการกำกับดูแลด้าน AI Ethics และ AI Risk ในระดับคณะกรรมการบริษัทหรือไม่		
11. คณะกรรมการบริษัทมีการอบรม/สัมมนาด้าน Cybersecurity หรือ AI Governance เป็นประจำหรือไม่		

ภาคผนวก B : ตัวอย่างรายงานความเสี่ยงไซเบอร์ที่ควรเสนอเข้าสู่คณะกรรมการบริษัท (Cybersecurity Risk Dashboard)

ตัวอย่างภาพรวมที่คณะกรรมการบริษัทควรเห็นจากผู้บริหารด้าน IT หรือ CISO

Executive Cyber Risk Dashboard

หมวด	ตัวชี้วัด (KPI)	ค่าเป้าหมาย	ค่าสถานะล่าสุด	หมายเหตุ
ระดับความเสี่ยงขององค์กรด้านไซเบอร์	ระดับความเสี่ยงไซเบอร์องค์กร (โดยรวม)	ปานกลาง	ปานกลาง	
ความเสี่ยงบุคคลภายนอก	จำนวนผู้ให้บริการสำคัญที่ผ่านการประเมินความเสี่ยง	ประเมินแล้วเสร็จ ≥ 80% ของจำนวนผู้ให้บริการสำคัญ	60%	อยู่ระหว่างประเมินผู้ให้บริการรายใหม่ 2 ราย
ความพร้อมของระบบ	ระยะเวลาที่ระบบงานทำงานได้ตามปกติ (Up Time)	ระบบสำคัญ: ≥ 99%	99.75%	
		ระบบอื่น: > 95%	98%	
การทดสอบการกู้คืนระบบ	เวลาในการกู้คืนระบบ (Recovery Time Objective (RTO))	ระบบสำคัญ: ≤ 6 ชั่วโมง	4 ชั่วโมง ทดสอบเมื่อ...	
		ระบบอื่น: ≤ 24 ชั่วโมง	23-25 ชั่วโมง	ระบบสำรองบางส่วนไม่ผ่าน
การทดสอบการกู้คืนข้อมูล	ระยะเวลาที่ยอมให้ข้อมูลสูญหายได้ (Recovery Point Objective (RPO))	ข้อมูลสำคัญ: Near Real-Time	ทดสอบผ่านเมื่อ...	
		ข้อมูลอื่น: 24 ชั่วโมง	ทดสอบผ่านเมื่อ...	
คุณภาพการให้บริการ	ความพึงพอใจพนักงานภายในและลูกค้าต่อการใช้บริการระบบงาน	พนักงานภายใน: ≥ 80%	พนักงานภายใน: 95%	
		ลูกค้า: ≥ 80%	ลูกค้า: 90%	
การฝึกอบรม Cyber Awareness	จำนวนพนักงานผ่านการฝึกอบรม Cyber Awareness	จำนวนพนักงาน: ≥ 90%	86%	พนักงานใหม่บางส่วนอยู่ระหว่างฝึกอบรม
การตรวจพบภัยคุกคามไซเบอร์	จำนวนครั้งที่ตรวจพบ	พยายามคุกคามองค์กรแต่ไม่สำเร็จ	50 ครั้ง	
		ผลกระทบไม่ร้ายแรง ≤ 5 ครั้ง	3 ครั้ง	
		ผลกระทบร้ายแรง ≤ 1 ครั้ง	0 ครั้ง	
		ผลกระทบวิกฤต ≤ 1 ครั้ง	0 ครั้ง	

ภาคผนวก B :

ตัวอย่างรายงานความเสี่ยงไซเบอร์ที่ควรเสนอเข้าสู่คณะกรรมการบริษัท (Cybersecurity Risk Dashboard)

ตัวอย่างภาพรวมที่คณะกรรมการบริษัทควรเห็นจากผู้บริหารด้าน IT หรือ CISO

Executive Cyber Risk Dashboard

หมวด	ตัวชี้วัด (KPI)	ค่าเป้าหมาย	ค่าสถานะล่าสุด	หมายเหตุ
การประเมินช่องโหว่ทางเทคนิค (Vulnerability Assessment)	ความสม่ำเสมอในการประเมินช่องโหว่	มีการประเมินเดือนละ ≥ 1 ครั้ง	มีการประเมินประจำเดือนนี้แล้ว	
การทดสอบการเจาะระบบ (Penetration Testing)	ความสม่ำเสมอในการทดสอบการเจาะระบบ	มีการทดสอบการเจาะระบบปีละ ≥ 1 ครั้ง	มีการทดสอบประจำปีนี้แล้ว	

ผลการตรวจสอบด้าน IT	ระดับความเสี่ยง	จำนวนประเด็น			อยู่ระหว่างการจัดซื้อระบบและอุปกรณ์ด้านไอที
		ตรวจพบ/ข้อบกพร่อง	แก้ไขแล้ว	คงเหลือ	
	วิกฤต	2	2	0	
	ร้ายแรง	4	3	1	
	ปานกลาง	8	5	3	
	ต่ำ	12	4	8	

ภาคผนวก C :

ตัวอย่าง Template รายงานเหตุการณ์ด้านความมั่นคงไซเบอร์
(Cybersecurity Incident Notification Template)

[ชื่อองค์กร]

1. รายละเอียดเหตุการณ์
- วันเวลาที่ตรวจพบ:
- ประเภทของผลกระทบ: (เช่น การรักษาความลับของข้อมูล, ความถูกต้องครบถ้วนของข้อมูล, ความพร้อมใช้งาน)
- ลักษณะของเหตุการณ์: (เช่น Ransomware, Data Breach, Unauthorized Access)
- ระบบงานหรือบริการที่ได้รับผลกระทบ:

2. การประเมินเบื้องต้น
- ระดับความรุนแรง: (เช่น ร้ายแรง/ปานกลาง/ต่ำ)
- ข้อมูลที่อาจรั่วไหล: (ถ้ามี)
- ระยะเวลาที่คาดว่าจะต้องใช้แก้ไขปัญหา:
- ระยะเวลาที่ธุรกิจหยุดชะงัก: (ถ้ามี)
- ความเสียหายคิดเป็นมูลค่าโดยประมาณ: (เช่น บาทต่อชั่วโมง)
- จำนวนลูกค้าที่ได้รับผลกระทบ:
- จำนวนลูกค้าที่ร้องเรียน: (ถ้ามี)
- กฎหมายที่เกี่ยวข้อง: (เช่น ต้องรายงานหน่วยงานใดบ้าง)

3. การตอบสนอง
- สาเหตุเบื้องต้น: (ถ้าทราบ)
- สิ่งที่ได้ดำเนินการในเบื้องต้น:
- การสื่อสารหน่วยงานภายใน: (เช่น บริษัทแม่ พนักงานที่ได้รับผลกระทบ ฝ่ายจัดการความเสี่ยง)
- การสื่อสารหน่วยงานภายนอก: (ถ้ามี เช่น ตำรวจ, ก.ล.ต., ตลท., สคส., สกมช.)
- การสื่อสารต่อลูกค้าที่ได้รับผลกระทบ: (ถ้ามี)
- การสื่อสารต่อสาธารณะ: (ถ้ามี)

4. สิ่งที่ต้องการให้คณะกรรมการบริษัทพิจารณา
- เช่น การอนุมัติทรัพยากร การเรียกประชุมวิสามัญ การสื่อสารกับผู้ถือหุ้นและผู้มีส่วนได้ส่วนเสีย

5. การดำเนินการถัดไป
- การจำกัดความเสียหาย: (เช่น สามารถควบคุมได้แล้ว)
- แนวทางการแก้ไข:
- การกู้คืนระบบ: (ถ้ามี)

ภาคผนวก D : คำถามเชิงกลยุทธ์ที่กรรมการควรถามด้าน AI Governance (AI Oversight Questions for the Board)

คำถาม	ใช่/ไม่ใช่	หมายเหตุ/ การติดตาม
กลยุทธ์การใช้ AI		
มีกลยุทธ์ระดับองค์กรในการใช้ AI หรือไม่		
มีการนำ AI มาใช้เพื่อเพิ่มประสิทธิภาพหรือเพื่อลดภาระในการปฏิบัติงานของมนุษย์ หรือไม่		
ความเสี่ยงและจริยธรรม		
มีการประเมินความเสี่ยงด้าน Bias และความโปร่งใสของ AI หรือไม่		
มีการทดสอบ Model ก่อนนำไปใช้งานจริงหรือไม่		
ข้อมูลส่วนบุคคล		
AI ที่องค์กรใช้มีการประมวลผลข้อมูลส่วนบุคคลหรือไม่		
มีกระบวนการประมวลผลข้อมูลเท่าที่จำเป็น (Data Minimization) และการขอความยินยอมหรือไม่		
Third-Party AI		
มีการใช้ AI จากผู้ให้บริการภายนอกหรือไม่		
มีการกำกับและจำกัดการส่งข้อมูลหรือไม่		
การกำกับดูแลและการฝึกอบรม		
องค์กรมีคณะทำงานด้าน AI Ethics หรือไม่		
บุคลากรทุกระดับได้รับการฝึกอบรมด้าน AI Governance หรือไม่		