Checklist : คำถามที่กรรมการควรพูดคุยเกี่ยวกับ Cybersecurity เพิ่มเติม

คำถามดังต่อไปนี้เป็นรายการคำถามตัวอย่างที่ท่านสามารถนำไปใช้พูดคุยในองค์กรของท่านเพื่อวางกลยุทธ์หรือตรวจสอบการดำเนินงานด้าน Cybersecurity ภายในองค์กรของท่านได้ โดยอาจเป็นการพูดคุยระหว่างกรรมการบริษัทเป็นการภายใน หรือมีการเชิญผู้บริหารขององค์กรหรือที่ปรึกษามาร่วมประชุมด้วย โดยท่านสามารถเพิ่มเติมคำถามนอกเหนือจากรายการเบื้องต้นเหล่านี้ได้

หมวดที่ 1: การทำให้ Cybersecurity กลายเป็นส่วนหนึ่งขององค์กร

ลำดับ	คำถาม	Self-check
1.	มีการประเมินความเสี่ยงด้าน Cybersecurity จากผู้เชี่ยวชาญภายนอกหรือผู้ที่เป็นอิสระต่อการดำเนินงานภายในหรือไม่?	☐ เคย ☐ ไม่เคย หมายเหตุ:
2.	องค์กรของท่านมีการกำหนดนโยบายและแผนกลยุทธ์ด้าน Cybersecurity และมีการทบทวนเป็นประจำหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
3.	ความเสี่ยงด้าน Cybersecurity ถูกจัดลำดับให้มีความสำคัญสูง สำหรับทุกฝ่ายภายในองค์กรหรือไม่?	☐ ใช่ ☐ ไม่ใช่ หมายเหตุ:
4.	องค์กรของท่านมีการกำหนดผู้รับผิดชอบด้าน Cybersecurity และผู้ที่เกี่ยวข้องไว้อย่างชัดเจนหรือไม่	☐ มี ☐ ไม่มี หมายเหตุ:
5.	กรรมการบริษัททุกท่านมีความรู้พื้นฐานด้าน Cybersecurity ที่เพียงพอสำหรับการประชุมหารือเพื่อตัดสินใจ กำหนดนโยบาย หรือการลงทุนด้าน Cybersecurity หรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:

หมวดที่ 2: การสร้างวัฒนธรรมด้าน Cybersecurity ในเชิงบวก

ลำดับ	คำถาม	Self-check
1.	การประชุมกำหนดนโยบายด้าน Cybersecurity และกระบวนการที่เกี่ยวข้อง มีผู้รับผิดชอบที่เกี่ยวข้องกับแต่ละนโยบายหรือกระบวนการมาร่วมประชุมด้วยหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
2.	องค์กรของท่านมีวัฒนธรรมที่ทุกฝ่ายจะประสานความร่วมมือกันเพื่อป้องกันและรับมือกับภัยคุกคามทางไซเบอร์หรือไม่ ตัวอย่างเช่น มีการแบ่งแยกหน้าที่ความรับผิดชอบชัดเจน เมื่อเกิด Cyber Incident ขึ้นกับองค์กร ฝ่ายสื่อสาร ฝ่ายงานหลัก ฝ่ายความเสี่ยง ฝ่ายกฎหมาย และฝ่าย IT	☐ มี ☐ ไม่มี หมายเหตุ:
3.	องค์กรของท่านมีตัวชี้วัดความร่วมมือด้าน Cybersecurity ของผู้บริหารและพนักงานภายในองค์กรในเชิงรุก (เช่น การเข้าร่วมอบรมด้าน Cybersecurity, การแจ้งฝ่ายที่ดูแลด้าน Cybersecurity ถึงข้อกังวลหรือพฤติกรรมต้องสงสัยที่พบเจอ เป็นต้น) หรือไม่	☐ มี ☐ ไม่มี หมายเหตุ:
4.	องค์กรของท่านมีการสร้างแรงจูงใจให้พนักงานทุกฝ่ายรายงานปัญหาหรือความเสี่ยงทางด้านไซเบอร์ที่พบหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
5.	องค์กรของท่านมีการแบ่งปันความรู้หรือถอดบทเรียนที่ได้รับจากเหตุการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้นภายในองค์กรหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:

หมวดที่ 3: การสร้างความเชี่ยวชาญด้าน Cybersecurity

ลำดับ	คำถาม	Self-check
1.	ฝ่ายบุคคลขององค์กรสามารถระบุทักษะด้านไซเบอร์ที่จำเป็นในองค์กรได้หรือไม่? และมีแผนเพื่อเร่งสร้างพนักงานที่มีทักษะที่จำเป็นเหล่านี้หรือไม่?	☐ ได้ ☐ ไม่ได้ หมายเหตุ:
2.	ท่านได้รับทราบถึงแนวโน้มที่ดีขึ้นในการที่พนักงานทั่วไปทำการแจ้งเหตุซึ่งอาจเป็นความเสี่ยงด้านไซเบอร์ที่เกิดขึ้นในองค์กรหรือไม่?	☐ ทราบ ☐ ไม่เคยทราบ หมายเหตุ:
3.	องค์กรของท่านสามารถรักษาผู้บริหารหรือพนักงานด้าน Cybersecurity ให้ทำงานอยู่กับท่านได้เป็นเวลาต่อเนื่องยาวนานหลายปี โดยไม่ลาออกบ่อยๆ ได้หรือไม่?	☐ ได้ ☐ ไม่ได้ หมายเหตุ:
4.	องค์กรของท่านมีการตรวจสอบทบทวนทักษะด้านไซเบอร์ที่ยังขาดแคลนอยู่เป็นประจำหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
5.	กรรมการบริษัทมีความรู้ความเข้าใจเพียงพอในการตัดสินใจเชิงกลยุทธ์ด้าน Cybersecurity หรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
6.	ปัจจุบันองค์กรของท่านมีบุคลากรด้านไซเบอร์ที่เพียงพอต่อการบริหารจัดการความเสี่ยง และการจัดการรับมือกับภัยคุกคามได้หรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
7	ท่านทราบหรือไม่ว่า องค์กรท่านพึ่งพาความเชี่ยวชาญด้าน cybersecurity จากผู้ให้บริการภายนอก (3rd party หรือ vendor) มากน้อยเพียงใด	☐ ทราบ ☐ ไม่เคยทราบ หมายเหตุ:

หมวดที่ 4: การระบุสินทรัพย์สำคัญในองค์กร

ลำดับ	คำถาม	Self-check
1.	องค์กรของท่านมีการระบุสินทรัพย์สำคัญทั้งในส่วนของ Hardware, Software และ Data เพื่อให้สามารถประเมินความเสี่ยงทางด้านไซเบอร์ได้หรือไม่? และการปกป้องสินทรัพย์เหล่านั้นให้มีความมั่นคงปลอดภัยเพียงพอแล้วหรือไม่?	☐ มี และเพียงพอ ☐ มี แต่ไม่เพียงพอ ☐ ไม่มี หมายเหตุ:
2.	ท่านเคยได้รับรายงานเกี่ยวกับ การบริหารจัดการทรัพย์สินสารสนเทศสำคัญทั้งด้าน Hardware, Software และ Data รวมถึงผู้ที่รับผิดชอบในแต่ละสินทรัพย์เหล่านั้นหรือไม่?	☐ เคย ☐ ไม่เคย หมายเหตุ:
3.	องค์กรของท่านมีข้อมูลระดับความสำคัญและวัตถุประสงค์ในการใช้งานของแต่ละสินทรัพย์ รวมถึงข้อมูลอย่างชัดเจน เพื่อใช้ตัดสินใจดำเนินการทางด้าน Cybersecurity ได้อย่างเพียงพอหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:

หมวดที่ 5: การทำความเข้าใจเกี่ยวกับภัยคุกคามทางด้าน Cybersecurity

ลำดับ	คำถาม	Self-check
1.	ท่านเคยได้รับรายงาน เกี่ยวกับภัยคุกคามด้านไซเบอร์ที่องค์กรต้องเผชิญบ่อยหรือไม่? และทราบถึงวิธีการจัดการรับมือกับภัยคุกคามเหล่านี้หรือไม่?	☐ เคย และทราบ ☐ เคย แต่ไม่ทราบ ☐ ไม่เคย หมายเหตุ:
2.	การประเมินความเสี่ยงด้านภัยคุกคามไซเบอร์มีผู้ที่เกี่ยวข้องจากฝ่ายอื่นๆ นอกเหนือจากฝ่าย IT หรือ Cybersecurity เข้าร่วมหรือไม่ เช่น การประเมินความเสี่ยงสำหรับ Software ที่แผนกหนึ่งใช้งาน มีการเชิญผู้บริหารหรือเจ้าหน้าที่จากแผนกนั้นมาร่วมประเมินความเสี่ยงด้านภัยคุกคามไซเบอร์ด้วยหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
3.	องค์กรของท่านมีความร่วมมือด้าน Cybersecurity กับตัวแทนจากหน่วยงานอื่นๆ ในอุตสาหกรรมเดียวกัน เพื่อแบ่งปันข่าวสารด้านความเสี่ยงหรือภัยคุกคามทางไซเบอร์ที่อาจจะเป็นภัยคุกคามต่อภาคอุตสาหกรรม หรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
4.	องค์กรของท่านมีการส่งเสริมความรู้ให้กับกรรมการบริษัท ผู้บริหาร และพนักงานในองค์กร เกี่ยวกับภัยคุกคามทางไซเบอร์รูปแบบใหม่ๆ และแนวทางป้องกันและรับมือกับภัยคุกคามดังกล่าวเป็นประจำหรือไม่	☐ มี ☐ ไม่มี หมายเหตุ:
5.	กรรมการบริษัทเคยได้รับรายงานถึงภัยคุกคามใหม่ๆ ที่องค์กรกำลังเผชิญโดยมีเนื้อหาที่อ่านเข้าใจได้ง่ายหรือไม่?	☐ เคย ☐ ไม่เคย หมายเหตุ:

หมวดที่ 6: การบริหารความเสี่ยงสำหรับ Cybersecurity

ลำดับ	คำถาม	Self-check
1.	กรรมการบริษัทเคยทราบถึงความเสี่ยงปัจจุบันที่องค์กรกำลังเผชิญจากเหตุการณ์การโจมตีด้านทางไซเบอร์แต่ละครั้งหรือไม่?	☐ เคย ☐ ไม่เคย หมายเหตุ:
2.	องค์กรของท่านมีกระบวนการเพื่อให้มั่นใจว่า ความเสี่ยงทางด้านไซเบอร์นั้นจะถูกประเมินร่วมในฐานะของความเสี่ยงทางธุรกิจหรือไม่?	☐ ใช่ ☐ ไม่ใช่ หมายเหตุ:
3.	องค์กรของท่านมีแนวทางในการรับมือกับภัยคุกคามทางด้านไซเบอร์ที่มีประสิทธิภาพหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
4.	กรรมการบริษัทได้เคยมีการหารือร่วมกับผู้เกี่ยวข้องถึงระดับความเสี่ยงทางด้านไซเบอร์ใดที่องค์กรสามารถยอมรับได้ (Acceptable Risk) และความเสี่ยงใดที่ไม่สามารถยอมรับได้ (Unacceptable Risk) หรือไม่?	☐ เคย ☐ ไม่เคย หมายเหตุ:

หมวดที่ 7: การดำเนินการด้าน Cybersecurity ที่เหมาะสม

ลำดับ	คำถาม	Self-check
1.	กรรมการบริษัทเคยได้รับทราบข้อมูลหรือการรายงานสถานะการดำเนินงานด้าน Cybersecurity ขององค์กรอย่างสม่ำเสมอ และได้รับข้อมูลที่เป็นประโยชน์ต่อการตัดสินใจหรือไม่?	☐ เคย ☐ ไม่เคย หมายเหตุ:
2.	กรรมการบริษัทเคยได้รับทราบวัตถุประสงค์และความสำคัญในการดำเนินการหรือการลงทุนใหม่ๆ ด้าน Cybersecurity ขององค์กรหรือไม่	☐ เคย ☐ ไม่เคย หมายเหตุ:
3.	การกำหนดตัวชี้วัดของการดำเนินการด้าน Cybersecurity มีความสอดคล้องกับความเสี่ยงด้าน Cybersecurity ที่องค์กรต้องบริหารจัดการหรือไม่?	☐ สอดคล้อง ☐ ไม่สอดคล้อง หมายเหตุ:
4.	กรรมการบริษัทมีการตรวจสอบติดตามการดำเนินการด้าน Cybersecurity ขององค์กรเป็นประจำหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:

หมวดที่ 8: การทำงานร่วมกับ Supply Chain และคู่ค้า

ลำดับ	คำถาม	Self-check
1.	กรรมการบริษัททราบถึงผลการประเมินศักยภาพ การประเมินความเสี่ยง และการบริหารจัดการความเสี่ยงด้านไซเบอร์สำหรับผลิตภัณฑ์หรือบริการจากคู่ค้า หรือ 3rd party หรือ vendor หรือไม่?	☐ ทราบ ☐ ไม่ทราบ หมายเหตุ:
2.	องค์กรของท่านมีการพัฒนาแนวทางการประเมินผลกระทบและการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ร่วมกับคู่ค้า หรือ 3rd party หรือ vendor หรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
3.	องค์กรท่านมีการติดตามความเสี่ยงด้าน Cybersecurity ของ Supply Chain และรายงานมายังกรรมการบริษัทหรือไม่?	☐ มี และรายงาน ☐ มี แต่ไม่รายงาน ☐ ไม่มี หมายเหตุ:
4.	การตัดสินใจในการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น คู่ค้า หรือ 3rd party หรือ vendor ที่มีความเสี่ยงหรือมีนัยสำคัญ ได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายหรือไม่?	☐ เคย ☐ ไม่เคย หมายเหตุ:

หมวดที่ 9: การวางแผนตอบสนองต่อเหตุการณ์ภัยคุกคามไซเบอร์

ลำดับ	คำถาม	Self-check
1.	องค์กรของท่านมีการทบทวนแผนรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) และแผน Disaster Recovery Plan (DRP) และมีการซักซ้อมการดำเนินการตามแผนเป็นประจำหรือไม่?	☐ มี ☐ ไม่มี หมายเหตุ:
2.	กรณีที่องค์กรท่านมีเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้น องค์กรท่านมีการจัดทำรายงานเกี่ยวกับแนวทางปรับปรุงระบบหรือกระบวนการเพื่อป้องกันไม่ให้เกิดเหตุในลักษณะดังกล่าวหรือเหตุการณ์คล้ายคลึงกันในอนาคตหรือไม่	☐ มี ☐ ไม่มี หมายเหตุ:
3.	กรรมการบริษัทท่าน มีความเข้าใจถึงแนวทางปฏิบัติที่จำเป็น ในสถานการณ์เกิดเหตุการณ์ภัยคุกคามทางไซเบอร์กับองค์กร เพื่อให้การแก้ไขปัญหาเป็นไปอย่างเหมาะสมและลดความสับสนวุ่นวาย เพื่อให้องค์กรสามารถจำกัดผลกระทบและความเสียหายได้อย่างรวดเร็วและทันกาล หรือไม่?	☐ เข้าใจ ☐ ไม่เข้าใจ หมายเหตุ:
4.	หากเกิดเหตุการณ์ด้าน Cybersecurity องค์กรของท่านทราบว่าจะสามารถติดต่อขอความช่วยเหลือจากหน่วยงานภายนอกใดได้บ้าง? และต้องรายงานเหตุการณ์ดังกล่าวต่อหน่วยงานใดบ้าง?	☐ ทราบ ☐ ไม่ทราบ หมายเหตุ:
5.	องค์กรของท่านมีแผนการสื่อสาร และมีการกำหนดผู้รับผิดชอบและช่องทางในการสื่อสารกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์กับองค์กรของท่านหรือไม่?	☐ มีแผนสื่อสาร ☐ ไม่มีแผนสื่อสาร หมายเหตุ:

เกณฑ์การคิดคะแนน

หากท่านตอบตัวเลือกแรก = 1 คะแนน

(เช่น มี/เคย/ใช่/ทราบ/เข้าใจ/มีแผนการสื่อสาร/มี และเพียงพอ/มี และรายงาน/เคย และทราบ)

ตัวเลือกอื่น = 0 คะแนน

ระดับคะแนน และคำอธิบาย

ระดับคะแนน	คำอธิบาย
น้อยกว่า 10	องค์กรท่านอาจมีความเสี่ยงด้านการบริหารจัดการ cybersecurity risk ได้อย่างไม่เหมาะสม
10 - 30	ท่านพอเข้าใจถึงความเสี่ยงด้าน cybersecurity risk อยู่บ้าง อย่างไรก็ดีองค์กรท่านอาจมีความเสี่ยงด้านการบริหารจัดการ cybersecurity risk ได้อย่างไม่เหมาะสม ท่านสามารถใช้ checklist นี้ เพื่อเป็นแนวทางในการสื่อสารและกำหนดเป็นวาระในการประชุมภายในองค์กรท่านได้
31 - 38	ท่านมีความเข้าใจความเสี่ยงด้าน cybersecurity ว่าจะกระทบต่อการดำเนินธุรกิจขององค์กรท่านได้อย่างไร อย่างไรก็ดี เพื่อให้การบริหารความเสี่ยงด้าน cybersecurity ถูกจัดการอย่างเหมาะสม ท่านสามารถใช้ checklist นี้ เพื่อเป็นแนวทางในการสื่อสารและกำหนดเป็นวาระในการประชุมภายในองค์กรท่าน เพิ่มเติมได้
38 ขึ้นไป	ท่านมีความเข้าใจความเสี่ยงด้าน cybersecurity ว่าจะกระทบต่อการดำเนินธุรกิจขององค์กรท่านได้อย่างไร อย่างไรก็ดี ท่านควรติดตามการปฏิบัติงานและผลการปฏิบัติงาน รวมถึงการบริหารจัดการความเสี่ยงด้าน cybersecurity risk อย่างต่อเนื่อง