

# พลิกมุมมองความเสี่ยง ยิ่งหลีกเลียง ยิ่งเสียโอกาส

ภูมิทัศน์ความเสี่ยงโลก 2568



# คำนำ

ในยุคที่เกิดการเปลี่ยนแปลงอย่างรวดเร็ว การบริหารความเสี่ยงเชิงรุกคือ กฎแห่งความสำเร็จ

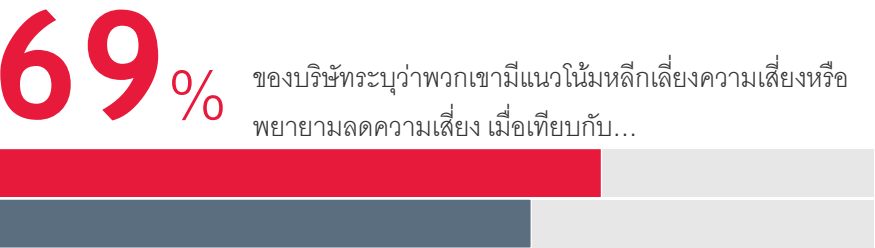


**Koen Claessens**  
Global Head of Risk  
Advisory Services,  
BDO Belgium

[koen.claessens@bdo.be](mailto:koen.claessens@bdo.be)

บทเรียนจากปีที่ผ่านมา ชัดเจนยิ่งกว่าที่เคย: อย่าเพียงแค่ "ตั้งรับ" และรอให้ความปั่นป่วนสิ้นสุดลงในยุคที่วิกฤตการณ์เกิดขึ้นอย่าง ต่อเนื่องและไม่หยุดหย่อน (Pemacrisis) ธุรกิจที่ต้องการ ก้าวหน้าและบรรลุเป้าหมาย จำเป็นต้องเปลี่ยนไปใช้แนวทางเชิงรุก ในการบริหารจัดการความเสี่ยงอย่างจริงจัง ปัญหาที่กำลังทวีความรุนแรงขึ้นคือ: มีองค์กรส่วนน้อยเท่านั้นที่นำกลยุทธ์เชิงรุกมาใช้ และสถานการณ์ก็ดูจะแยลงเรื่อย ๆ จากรายงานประจำปีครั้งที่ 10 ว่าด้วยความเสี่ยงระดับโลกของเราได้เผยตัวเลขที่สนใจคือ จากการสำรวจผู้นำระดับสูง 500 คนทั่วโลก พบว่า 69% ระบุว่าองค์กรของตนมีแนวโน้ม "หลีกเลี่ยงความเสี่ยง" หรือ "พยายามลดความเสี่ยงให้เหลือน้อยที่สุด" ตัวเลขนี้เพิ่มขึ้นจาก 61% ในปีที่ผ่านมา และมีแนวโน้มว่าสัดส่วนนี้จะ สูงขึ้นไปอีก นับตั้งแต่การสำรวจ เนื่องจากความเสี่ยงจากสงครามการค้าโลกและการเปลี่ยนแปลงนโยบายของสหรัฐฯ อย่างต่อเนื่อง ผู้นำระดับสูงจำนวนมากยังไม่พอใจกับความพยายามในการบริหารความเสี่ยงขององค์กรตนเอง โดยผู้บริหารโดยเฉลี่ยยอมรับว่า ครึ่งหนึ่ง ของข้อบกพร่องด้านความเสี่ยงที่ระบุไว้ ได้เกิดขึ้นในองค์กรของตน และ ไม่มีผู้บริหารคนใดเลย จากกลุ่มตัวอย่าง 500 คนที่ให้คะแนนการบริหารความเสี่ยงของตนว่า "สมบูรณ์แบบ" ที่น่าสนใจคือผู้บริหารหลายท่านวิจารณ์ว่ามีการใช้ภัยเกินควรในการปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance) ซึ่งเป็นสัญญาณชัดเจนว่า กลยุทธ์ความเสี่ยงในปัจจุบันยังไม่สามารถสร้างคุณค่าได้เท่าที่ควร

ปัญหาหลักคือ องค์กรส่วนใหญ่ใช้แนวทางการบริหารความเสี่ยงที่มุ่งเน้นเพียงการ "ติดถูกในช่อง" เพื่อให้สอดคล้องกับข้อกำหนด มากกว่าการบริหารความเสี่ยงอย่างแท้จริง โชคดีที่ผู้บริหารส่วนใหญ่ตระหนักถึงประเด็นนี้ โดย 74% เชื่อว่าการ ปลุกฝังแนวคิดเรื่องความเสี่ยงให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร จะช่วยเปลี่ยนจุดโฟกัสจากการปฏิบัติตามกฎข้อบังคับ ไปสู่กลยุทธ์ความเสี่ยงที่แท้จริง ซึ่ง สามารถสร้างคุณค่าและโอกาส ให้กับธุรกิจได้มากขึ้น นั่นหมายถึง การเติบโตต้องมาพร้อมกับการเปลี่ยนแปลง และการเปลี่ยนแปลงนี้จะทำให้ภูมิทัศน์ความเสี่ยงเปลี่ยนตามไปด้วย ซึ่งอาจนำไปสู่การเผชิญกับปัจจัยเสี่ยงใหม่ ๆ เช่น ความเสี่ยงด้านห่วงโซ่อุปทาน หรือความมั่นคงทางไซเบอร์ ดังนั้น จึงไม่เคยมีช่วงเวลาใดที่สำคัญไปกว่านี้ในการที่องค์กรต้อง ปรับใช้แนวทางเชิงรุก ในการบริหารความเสี่ยง และทำให้แน่ใจว่ากลยุทธ์ความเสี่ยงของตน จะไม่ถูกล่วงด้วยการทำงานเชิงรูปแบบ หากสามารถปรับเปลี่ยนได้ องค์กรก็จะสามารถ พัฒนาการรับมือกับความเสี่ยง และพร้อมที่จะ ใช้ประโยชน์จากโอกาสมากมาย ที่ภูมิทัศน์ความเสี่ยงระดับโลกในปัจจุบันกำลังเกิดขึ้น ■



สารบัญ

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| บทสรุปสำหรับผู้บริหาร                                                              | 03 |
| การวิเคราะห์ความเสี่ยงสำคัญ ปี 2568: สภาวะวิกฤตการณ์ที่ทำลายการเติบโต              | 06 |
| ระเบียบและกฎหมายช่วยชี้นำแนวปฏิบัติการบริหารความเสี่ยงในองค์กรได้จริงหรือไม่       | 09 |
| ความเสี่ยงด้านบุคลากรกลับมาเป็นประเด็นสำคัญอีกครั้ง                                | 11 |
| ช่องว่างเชิงความเสี่ยง: แนวคิดการมุ่งเน้นเพียงข้อปฏิบัติกำลังจำกัดศักยภาพการเติบโต | 12 |
| ภัยไซเบอร์ที่ไม่มีวันสิ้นสุด: ความท้าทายที่ต้องเผชิญต่อไป                          | 16 |
| เชื่อมช่องว่างระหว่างความเสี่ยงและโอกาสจาก AI                                      | 21 |
| ‘Flexsourcing’: กลยุทธ์ใหม่เพื่อฝ่าวิกฤตห่วงโซ่อุปทาน                              | 25 |
| จัดการความเสี่ยงทุจริต: ปิดทุกช่องโหว่                                             | 27 |



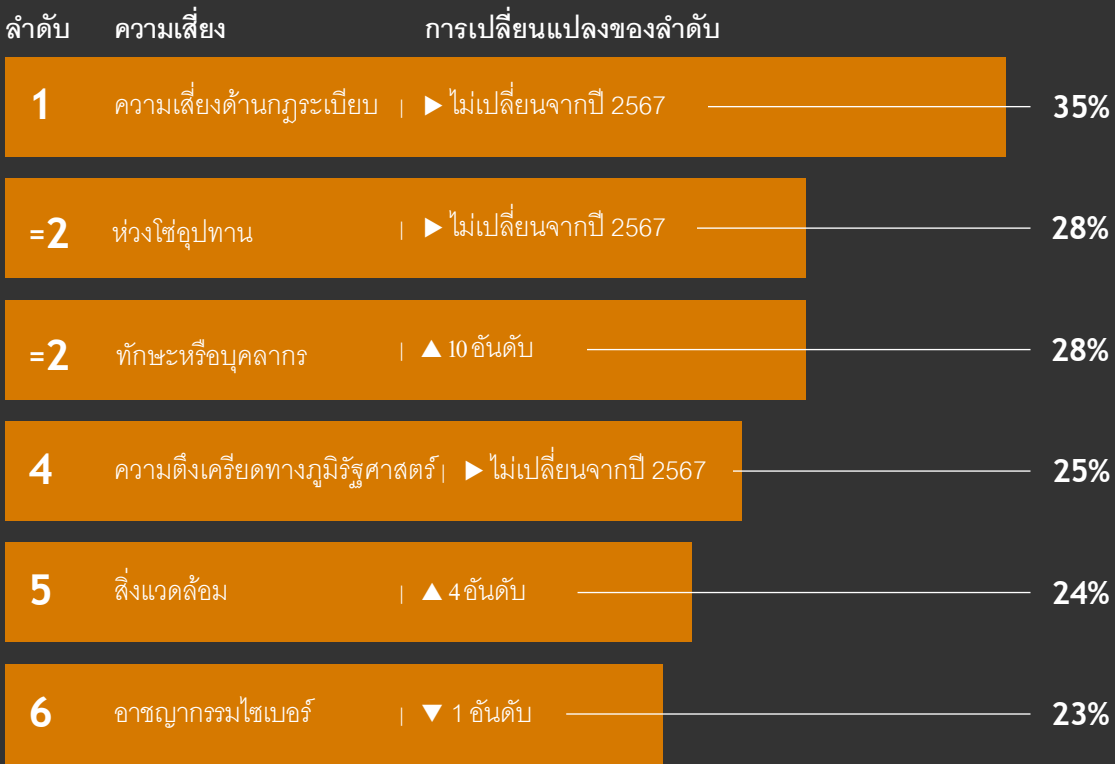
# บทสรุปสำหรับผู้บริหาร

## การวิเคราะห์ความเสี่ยงสำคัญ ปี 2568: สภาวะวิกฤตถาวรที่ท้าทายการเติบโต

ผู้บริหารถึง 84% เห็นพ้องว่า ภูมิทัศน์ความเสี่ยงของโลกในปัจจุบันถูกกำหนดโดย "วิกฤต" ที่มีความเข้มข้นสูงกว่าในอดีตอย่างชัดเจนแนวทางปฏิบัติของธุรกิจส่วนใหญ่จึงมุ่งเน้นที่การ "ลดความเสี่ยงเป็นหลัก" ทั่ว การหลีกเลี่ยงความเสี่ยงโดยสิ้นเชิง อาจเป็นอุปสรรคสำคัญที่ทำให้องค์กร ไม่สามารถคว้าโอกาสใหม่ ๆ เพื่อสร้างการเติบโตได้

อ่านต่อหน้า 06

### ความเสี่ยงสำคัญที่องค์กรยังไม่พร้อมรับมือ



การสำรวจผู้บริหารระดับ C-suite จำนวน 500 คนทั่วโลก จัดทำขึ้นสำหรับ BDO ในเดือนมกราคม 2568 รายละเอียดการสำรวจฉบับเต็มดูได้ที่หน้า 30

### กฎข้อบังคับ VS การบริหาร

#### ความเสี่ยงที่แท้จริง

หน่วยงานกำกับดูแลได้เรียกร้อง

ข้อมูลเกี่ยวกับความเสี่ยงอย่าง

ต่อเนื่อง ผู้บริหารบางส่วนเห็นว่าการ

รายงานนี้อาจช่วยให้ บริษัทปลอดภัย

ยิ่งขึ้นได้ แต่สิ่งนี้อาจสร้างข้อจำกัด

อ่านต่อหน้า 09

ข้อเรียกร้องด้านกฎข้อบังคับในการรายงานเพิ่มเติม กำลังช่วยลดระดับความเสี่ยงที่แท้จริงขององค์กรได้จริงหรือไม่?



39%

ใช่

57%

ค่อนข้างใช่

ความเสี่ยงด้านบุคลากรกลับมาเป็นประเด็นสำคัญ

อีกครั้ง

นับตั้งแต่การระบาดของโควิด-19ผู้นำองค์กรถึง 28% จัดให้

ความเสี่ยงด้านบุคลากรและทักษะอยู่ในกลุ่ม 3 ความเสี่ยง

สูงสุดตัวเลขนี้ เพิ่มขึ้นกว่าสองเท่า เมื่อเทียบกับปี 2567 ที่

มีผู้บริหารระบุเพียง 12% เท่านั้น การเข้ามาของ

ปัญญาประดิษฐ์ (AI) อาจยิ่งทำให้ประเด็นนี้มีความ

เร่งด่วนมากขึ้น เพราะมันไม่ได้เป็นเพียงความเสี่ยงด้าน การ

ดึงดูดและรักษามูลค่าเท่านั้น แต่ยังรวมถึงความเสี่ยง

ด้าน ช่องว่างทักษะ (Skill Gap) ที่บุคลากรอาจไม่พร้อม

รับมือกับเทคโนโลยีใหม่ ๆ อย่างทัน่วงที่

อ่านต่อหน้า 11

อุตสาหกรรมใดที่ผู้นำยังขาดความพร้อมในการรับมือกับความเสี่ยงด้านบุคลากร/ทักษะ?

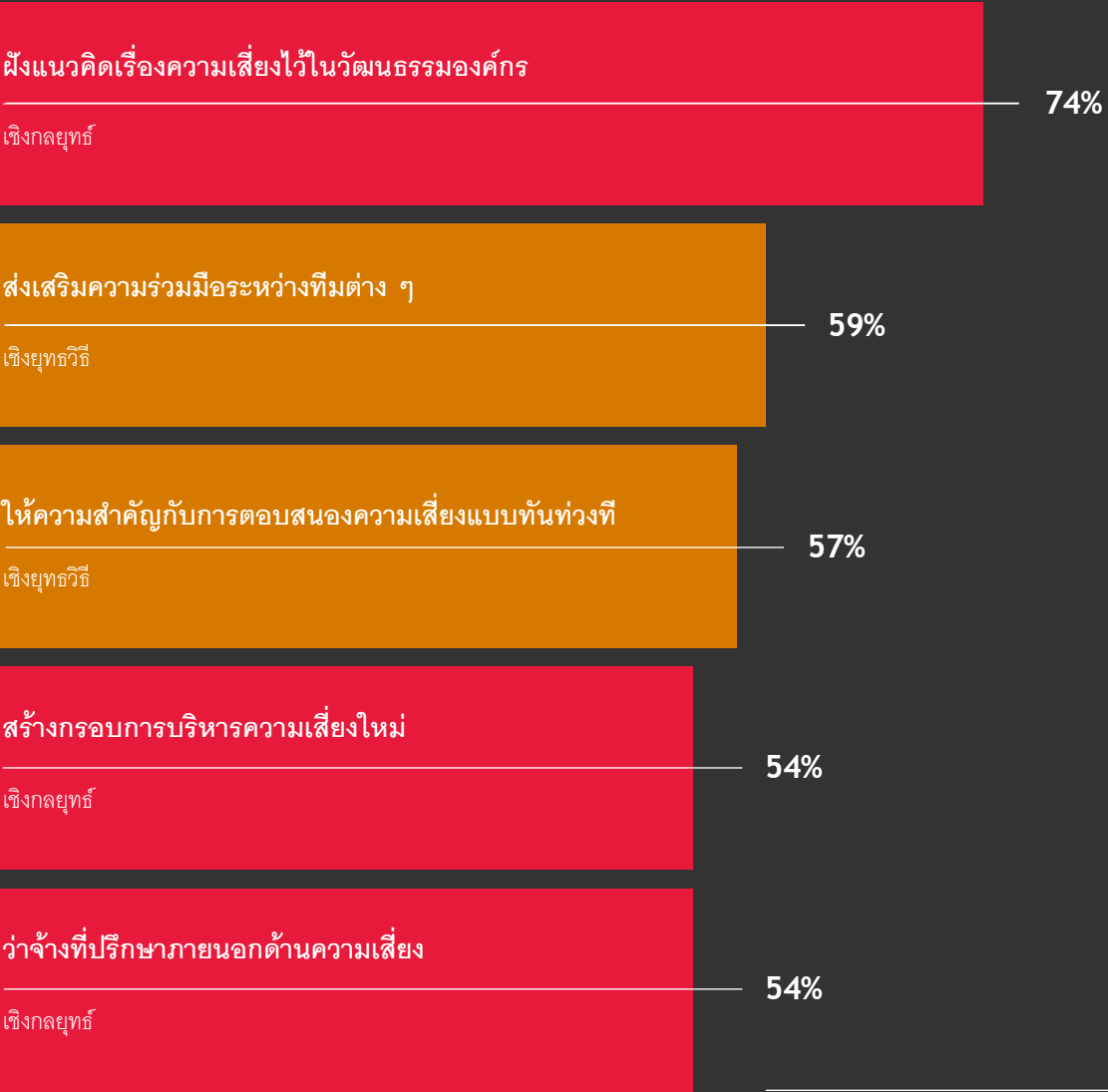


ช่องว่างแห่งความเสี่ยง

แม้ว่าข้อเรียกร้องด้านข้อมูลความเสี่ยงจากหน่วยงานกำกับดูแลจะสามารถ กระตุ้นให้เกิดการลดความเสี่ยง ในองค์กรได้ แต่การปฏิบัติตามนั้นก็มี ขอบเขตจำกัด บริษัทต้องระมัดระวังไม่ให้สร้างสภาพแวดล้อมที่เน้นแต่การ "ทำเครื่องหมายในช่อง" (Check-the-box mentality) เพื่อให้เป็นไปตามกฎระเบียบเท่านั้น เพราะแนวทางเชิงรูปแบบเช่นนี้อาจ เบี่ยงเบนความสนใจ และบั่นทอนความพยายามในการนำกลยุทธ์ การจัดการความเสี่ยงที่แท้จริง มาใช้ ซึ่งเป็นสิ่งสำคัญสำหรับการสร้างคุณค่าและการเติบโตในระยะยาว

อ่านต่อหน้า 12

องค์กรต่าง ๆ มีแนวทางอย่างไรในการเปลี่ยนทิศทางไปสู่การจัดการความเสี่ยงอย่างแท้จริง?



ภัยไซเบอร์ที่ไม่มีวันสิ้นสุด: ความท้าทายที่ต้องเผชิญต่อไป

การโจมตีทางไซเบอร์ กำลังพุ่งสูงสุดสูงสุดในฐานะประเด็นความเสี่ยงที่สำคัญ เนื่องจาก ภูมิทัศน์ภัยคุกคามที่เปลี่ยนแปลงอย่างต่อเนื่อง และถูกเร่งให้รุนแรงขึ้นด้วย ปัญญาประดิษฐ์ (AI) อย่างไรก็ตาม, ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) แสดงความกังวลว่า การมุ่งเน้นที่การ ปฏิบัติตามกฎหมายข้อกำหนดด้านไซเบอร์ ที่เข้มงวดมากขึ้นเรื่อย ๆ อาจ เบี่ยงเบนความพยายาม การดำเนินมาตรการ ลดความเสี่ยงอย่างเป็นรูปธรรม

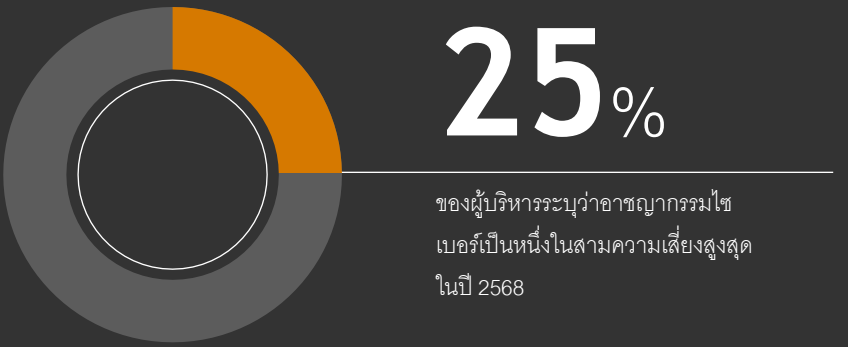
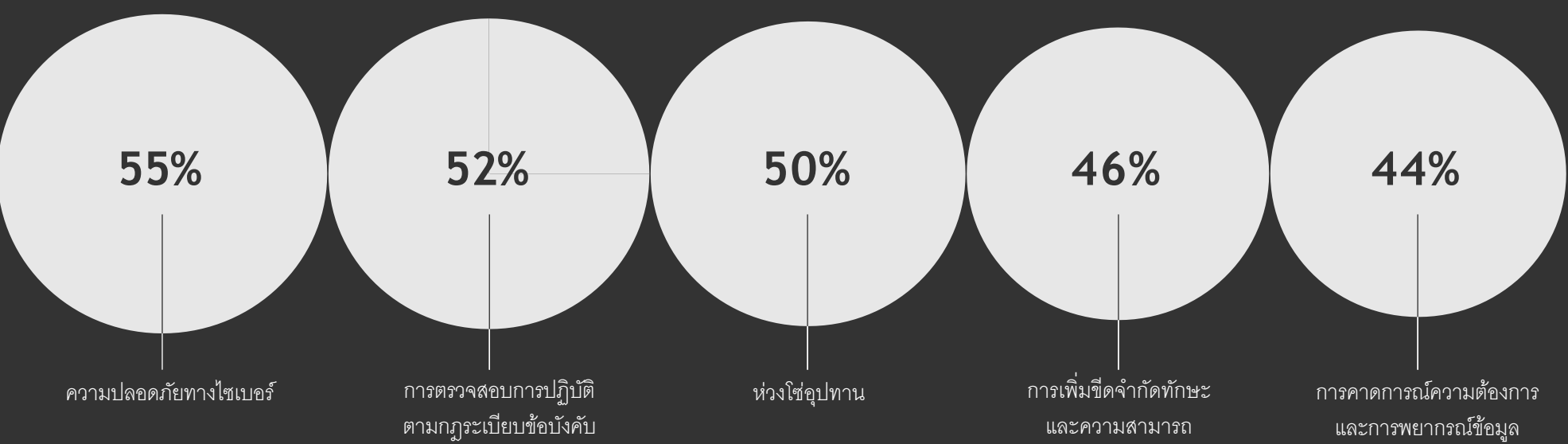
อ่านต่อหน้า 16

เชื่อมช่องว่างระหว่างความเสี่ยงและโอกาสจาก AI

ในปีที่ผ่านมา ทิศนคติต่อปัญญาประดิษฐ์ (AI) ได้เปลี่ยนไปอย่างชัดเจน ผู้บริหารส่วนใหญ่เริ่มมองว่า AI เป็น "โอกาส" มากกว่า "ความเสี่ยง" (แม้ว่าบางส่วนจะมองว่าเป็นทั้งสองด้านพร้อมกัน)ผู้นำองค์กรเชื่อว่า AI สามารถเป็นเครื่องมือสำคัญในการ ช่วยปรับปรุงและยกระดับการจัดการความเสี่ยง ได้อย่างมีนัยสำคัญ

อ่านต่อหน้า 21

ผลกระทบที่คาดว่าจะเกิดขึ้นจาก AI ภายใน 12 เดือนข้างหน้า

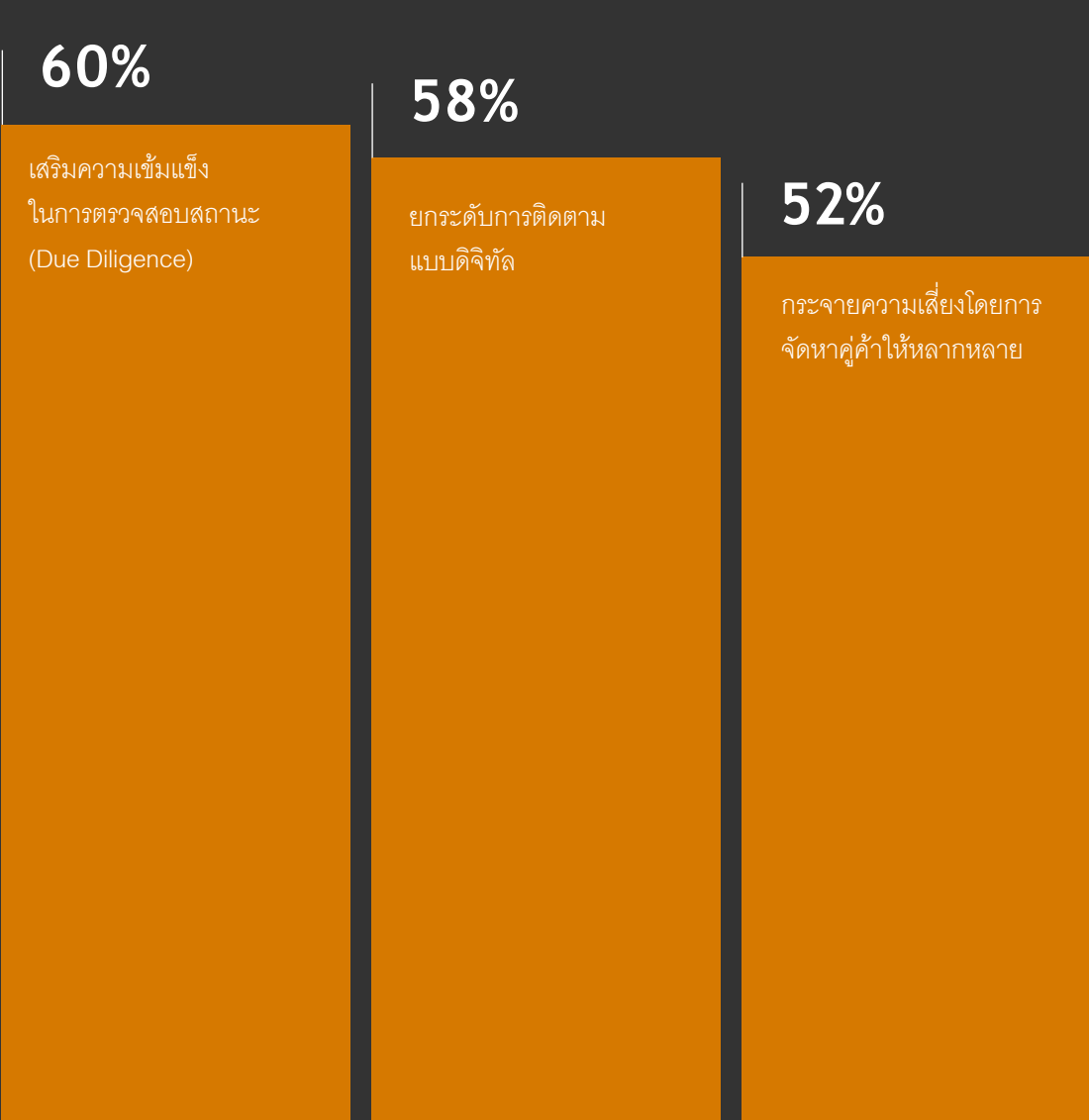


‘Flexsourcing’ : กลยุทธ์ใหม่เพื่อฝ่าวิกฤตห่วงโซ่อุปทาน

ห่วงโซ่อุปทาน กำลังเผชิญกับแรงกดดันมหาศาล ซึ่งมีแนวโน้มจะแย่ลงจากการ ขึ้นภาษีนำเข้า และความจำเป็นในการ เปลี่ยนแหล่งจัดซื้อ อย่างเร่งด่วน ด้วยเหตุนี้ บริษัทจึงจำเป็นต้องพิจารณาใช้แนวทาง 'Flexsourcing' ซึ่งเป็นกลยุทธ์แบบผสมผสานเพื่อสร้างความยืดหยุ่น โดย 'Flexsourcing' คือการรวม Nearshoring (การจัดซื้อจากประเทศใกล้เคียง) เข้ากับ Friendshoring (การจัดซื้อจากประเทศพันธมิตรที่ไว้ใจได้) วิธีนี้จะช่วย เสริมความคล่องตัว ในการสลับแหล่งจัดซื้อไปยังประเทศที่มี ความน่าเชื่อถือสูงกว่า หรือมี ภาษีนำเข้าที่ต่ำกว่า ได้อย่างรวดเร็ว ทำให้ธุรกิจมีความพร้อมในการรับมือกับความผันผวนทางภูมิรัฐศาสตร์และเศรษฐกิจโลก

อ่านต่อหน้า 25

3 กลยุทธ์หลักที่บริษัทต่างๆ กำลังใช้เพื่อให้ ห่วงโซ่อุปทานทางกายภาพ (Physical Supply Chains) แข็งแกร่งและยืดหยุ่นขึ้น



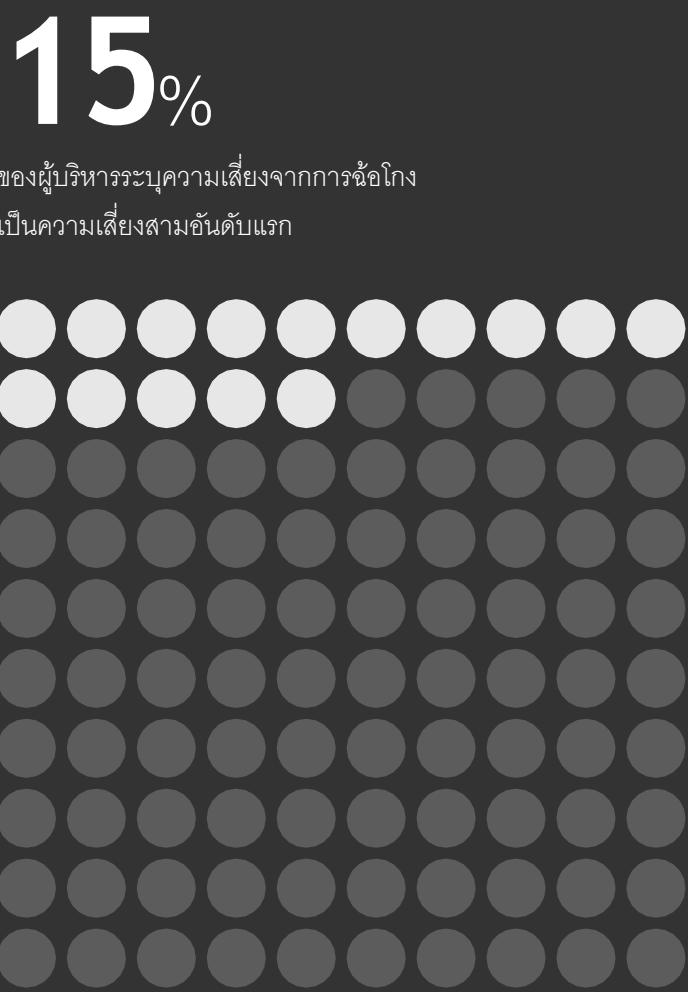
และ 3 กลยุทธ์หลักที่บริษัทต่างๆ กำลังใช้เพื่อให้ ห่วงโซ่อุปทานดิจิทัล Digital Supply Chains) แข็งแกร่งและยืดหยุ่นขึ้น



จัดการความเสี่ยงทุจริต: ปิดทุกช่องโหว่

ความเสี่ยงจากการทุจริต กำลังถูก ประเมินค่าต่ำเกินไป และถูกเข้าใจผิดอย่างน่ากังวล โดยมีผู้บริหารเพียง 15% เท่านั้นที่จัดให้ความเสี่ยงนี้เป็นหนึ่งในสามความเสี่ยงสูงสุดในขณะนี้เช่นกัน, ผู้ทุจริต ก็กำลังใช้ปัญญาประดิษฐ์ (AI) เพื่อค้นหาช่องโหว่และจุดอ่อนใหม่ ๆ ได้อย่างมีประสิทธิภาพและรวดเร็วยิ่งขึ้นถึงเวลาแล้วที่บริษัทต้อง ให้ความสำคัญกับความเสี่ยงนี้อย่างจริงจัง และยกระดับมาตรการป้องกันให้เท่าทันเครื่องมือสมัยใหม่ที่ไม่หวังดีกำลังใช้งานอยู่

อ่านต่อหน้า 27



# การวิเคราะห์ความเสี่ยงสำคัญ ปี 2568: สภาวะวิกฤตถาวรที่ท้าทายการเติบโต

องค์กรอาจเผชิญกับการหยุดชะงักหรือความเสียหายเปรียบในการแข่งขันหากไม่ดำเนินการบริหารความเสี่ยงอย่างจริงจัง

ภาพรวม

สิ่งที่กำลังเปลี่ยนแปลง

ภูมิทัศน์ความเสี่ยงทั่วโลกกำลังเผชิญกับ ความไม่แน่นอนที่สูงขึ้น กว่าที่เคยเป็นมาอย่างชัดเจน ผลกระทบที่ตามมาคือบริษัทส่วนใหญ่เลือกใช้แนวทางจัดการความเสี่ยงที่ระมัดระวัง (Safety-First Approach) มากกว่าที่เคย

ทำไมเรื่องนี้จึงสำคัญ

แนวทางแบบ 'รอดูสถานการณ์ไปก่อน' นี้ไม่เหมาะสมอย่างยิ่งกับยุคสมัยที่เรากำลังเผชิญกับ 'วิกฤตถาวร' (pemacrisis) เพราะจะจำกัดโอกาสในการเติบโต และอาจเป็นอุปสรรคต่อความก้าวหน้าของบริษัท

ควรทำอะไร

แม้ว่าความระมัดระวังนี้จะเข้าใจได้ แต่ธุรกิจต้องมีแนวทางเชิงรุก โดยประเมินความเสี่ยงที่ตนรับได้ (risk appetite) เทียบกับผลลัพธ์ที่อาจเกิดขึ้น และวางแผนรับมืออย่างเหมาะสม เพื่อให้มั่นใจว่าการรับความเสี่ยงทุกครั้งจะนำมาซึ่งโอกาสในการเติบโต ไม่ใช่แค่ภัยคุกคาม

ตั้งแต่ความตึงเครียดทางการค้าระหว่างประเทศที่ทวีความรุนแรงขึ้นไปจนถึงการเปลี่ยนแปลงในความสัมพันธ์ทางภูมิรัฐศาสตร์ ภูมิทัศน์ความเสี่ยงระดับโลกได้เปลี่ยนแปลงอย่างต่อเนื่องมากกว่าสิบปีแล้ว และยังไม่มีสัญญาณว่าจะกลับเข้าสู่ภาวะเสถียร ผู้เชี่ยวชาญด้านความเสี่ยงและผู้บริหารระดับสูงส่วนใหญ่ยังคงมองเห็นระดับวิกฤตที่สูงเป็นประวัติการณ์ โดย 84% ของผู้ตอบแบบสอบถามในครั้งนี้นับว่า ภูมิทัศน์ความเสี่ยงโลกในปัจจุบันถูกกำหนดด้วยวิกฤตมากกว่าที่เคยเป็นมา

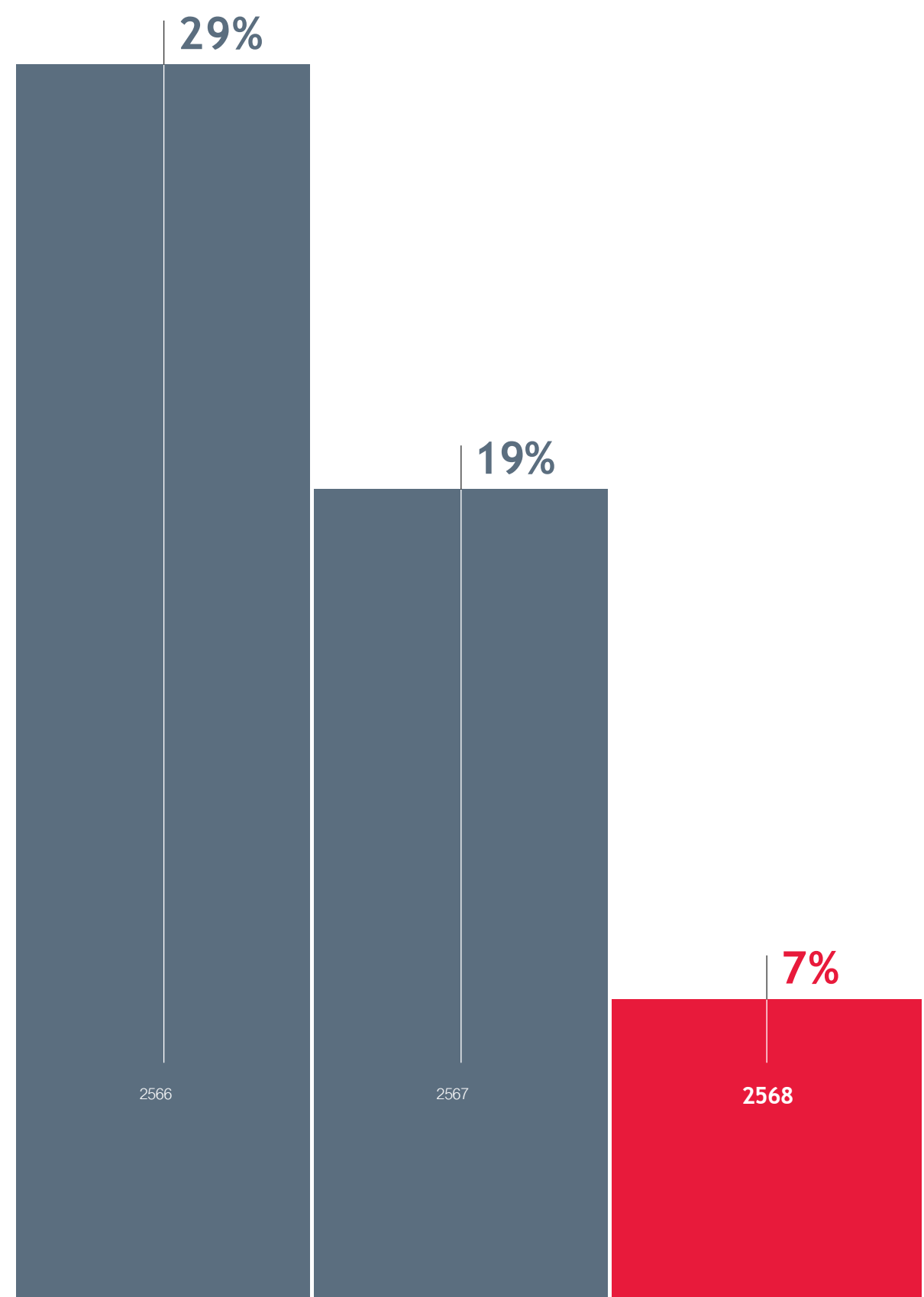
ในสถานการณ์เช่นนี้ ธุรกิจกำลังประสบความยากลำบากในการกำหนดทิศทางเพื่อก้าวไปข้างหน้า

ปัจจุบัน มีผู้บริหารเพียง 7% ที่ระบุว่าการบริหารความเสี่ยงของตน 'เชิงรุกอย่างแท้จริง' ซึ่งลดลงอย่างต่อเนื่องจาก 19% ในปี 2567 และ 29% ในปี 2566 แนวโน้มนี้เป็นปัญหา เพราะความระมัดระวังที่มากเกินไปขององค์กรจะชะลอการเติบโต และนำมาซึ่งแรงกดดันที่เพิ่มขึ้นจากผู้มีส่วนได้ส่วนเสีย ▶



การจัดการความเสี่ยงเชิงรุกเริ่มกลายเป็นเรื่องที่พบได้น้อยลง

เปอร์เซ็นต์ของผู้บริหารที่ได้ระบุว่าการจัดการความเสี่ยงของตนเป็น "เชิงรุกอย่างแท้จริง"



“ความวุ่นวายและความผันผวนที่เกิดขึ้นรอบตัวเราในตอนนี้ กำลังส่งผลกระทบต่อธุรกิจอย่างแน่นอน” Dave Arick กรรมการผู้จัดการฝ่ายบริหารความเสี่ยงระดับโลกของ Sedgwick บริษัทบริหารจัดการเคลมและประเมินความเสียหายกล่าว “เราจะเห็นว่าหลายธุรกิจลังเลเมื่อต้องตัดสินใจลงทุนหรือขยายกิจการ เพราะไม่รู้ว่าความไม่แน่นอนครั้งต่อไปจะมาจากทิศทางใด จึงมีท่าทีแบบ ‘รอดูสถานการณ์ก่อน’ เกิดขึ้นเยอะมาก”

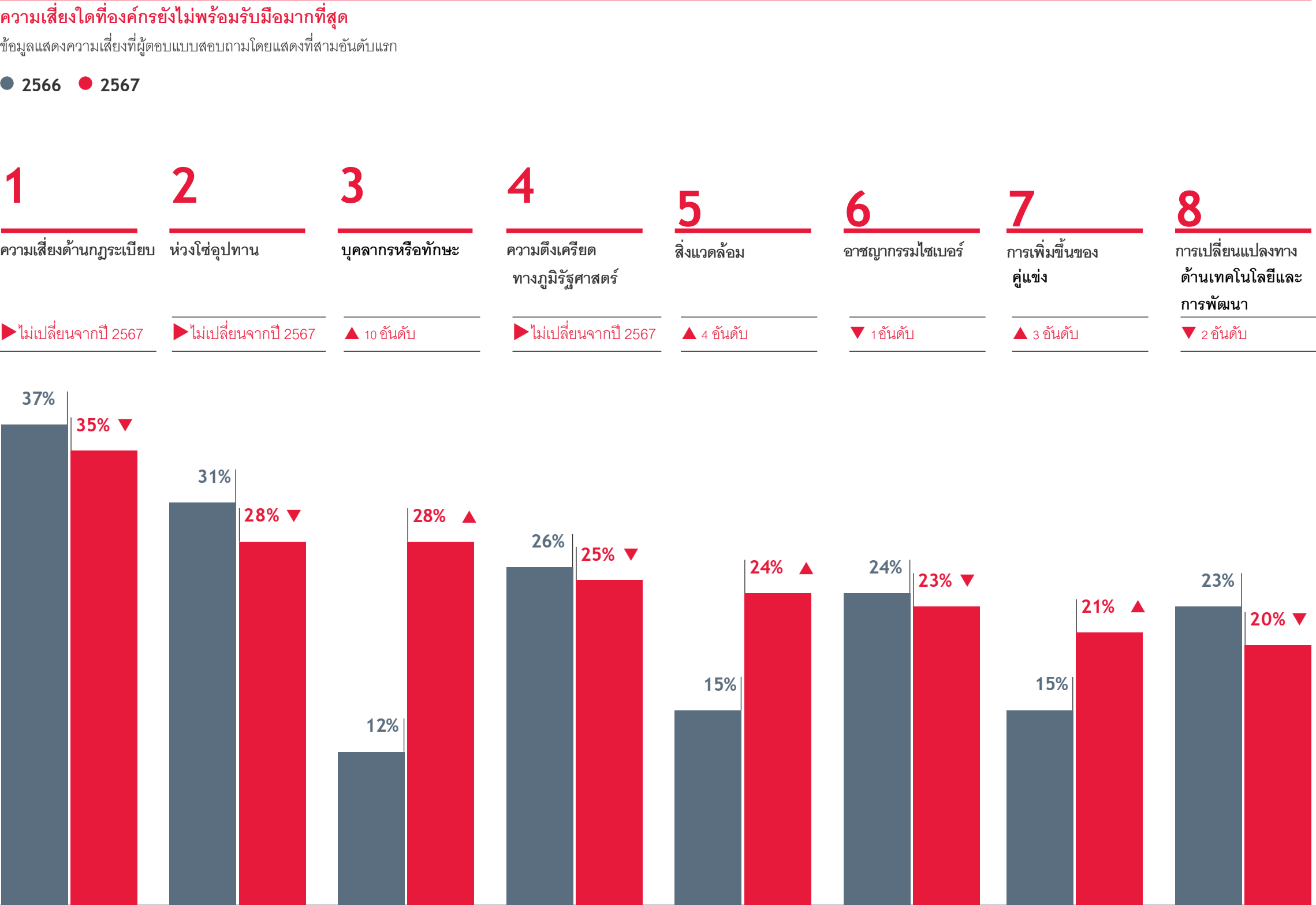
อย่างไรก็ตาม ปัญหาของแนวทางนี้คือ ถ้าความท้าทายยังคงทวีความรุนแรงขึ้น ธุรกิจก็จะหยุดนิ่ง

“การรอให้สถานการณ์คลี่คลาย อาจทำให้หลายธุรกิจตกอยู่ในภาวะเป็นอัมพาต เพราะกลัวว่าทุกอย่างอาจผิดพลาดได้” อาริกกล่าว “แม้ว่าจะมีเหตุผลมากมายให้เราชะงักงัน แต่การตั้งเป้าหมายของธุรกิจไม่สามารถทำได้ด้วยความกลัว”

แนวทางที่ดีกว่าในสภาพแวดล้อมเช่นนี้ คือการใช้ การวางแผนตามสถานการณ์ (Scenario Planning) เพื่อคาดการณ์ถึงสิ่งที่อาจผิดพลาด และเตรียมพร้อมรับมือ เพื่อให้ธุรกิจสามารถคว้าโอกาส แทนที่จะนั่งเฉยรอให้ความวุ่นวายผ่านไป

“แม้แต่บริษัทที่ต้องการเดินหน้าอย่างกล้าหาญ หรือมองหาแนวทางที่อาจเปลี่ยนแปลงธุรกิจโดยสิ้นเชิง ก็ยังสามารถวางแผนเพื่อรับมือกับสิ่งที่อาจผิดพลาดได้” อาริกกล่าว “คำถามคือ เราจะเตรียมตัวอย่างไรให้พร้อม เพื่อไม่ให้เราถูกจับได้ว่าประมาท หากสิ่งเหล่านั้นเกิดขึ้นจริง?”

การวางแผนตามสถานการณ์ ไม่ใช่สิ่งที่ทำเพียงครั้งเดียวแล้วจบ เพราะภูมิทัศน์ความเสี่ยงทั่วโลกในปัจจุบันยังคงเปลี่ยนแปลงอย่างรวดเร็ว ▶



"ตอนนี้เรากำลังตั้งเป้าหมายและวางกลยุทธ์สำหรับปีนี้ ซึ่งหนึ่งในขั้นตอนสำคัญคือการวิเคราะห์และทบทวน ความเสี่ยงหลักในช่วงเวลานี้ เพื่อให้มั่นใจว่าเรามีมาตรการจัดการที่เหมาะสม" ลีแอน แอปเพลต์ (Lianne Appelt) หัวหน้าฝ่ายบริหารความเสี่ยงองค์กรของ Salesforce กล่าว "ภูมิทัศน์ของความเสี่ยงได้เปลี่ยนไปอย่างมีนัยสำคัญนับตั้งแต่การประเมินความเสี่ยงภายในครั้งล่าสุดเมื่อเดือน ธันวาคม และฉันคิดว่าการเปลี่ยนแปลงที่ใหญ่ที่สุดคือด้านกฎข้อบังคับ"

ภาระด้านกฎข้อบังคับที่เพิ่มขึ้นนี้อาจเป็นปัจจัยที่ผลักดันให้หลายธุรกิจเลือกใช้แนวทาง "ปลอดภัยไว้ก่อน" ในการปฏิบัติ ตามกฎข้อบังคับ ซึ่งทำให้ผู้จัดการความเสี่ยงมีแนวโน้มจะตอบสนองเชิงรับมากกว่ารุก

"ภูมิทัศน์ความเสี่ยงมีขนาดใหญ่ เปลี่ยนแปลงอย่างรวดเร็ว และพัฒนาอย่างต่อเนื่อง ด้วยเหตุผลมากมาย จึง เป็นเรื่องยากที่บริษัทจะตามทันกับทุกความท้าทายที่เกิดขึ้น"

“บริษัทต่าง ๆ มักรู้สึกว่าการระเบียบเป็นภาระส่วนหนึ่งเป็นเพราะหน่วยงานกำกับดูแลคาดเดาทิศทางค่อนข้างยาก”

**Emanuel Van Zandvoort,**  
Partner, Risk Advisory Services –  
Enterprise Risk Management, BDO Netherlands

แกรี สตูริสกี (Gary Sturisky) หัวหน้าฝ่ายให้คำปรึกษาด้านความเสี่ยงของ BDO USA กล่าว "แต่ในระยะยาว หากบริษัทลงทุนล่วงหน้าเพื่อระบุและจัดการความเสี่ยง แทนที่จะรอให้ปัญหาเกิดขึ้นก่อนค่อย แก้ไข ค่าใช้จ่ายโดยรวมอาจน้อยกว่ามาก นั่นคือข้อดีที่ชัดเจนของการมีแนวทางเชิงรุก"

ความเสี่ยงด้านกฎระเบียบยังคงเป็นอันดับหนึ่งในบรรดาความเสี่ยงที่ผู้บริหารระดับ C-suite รู้สึกว่าไม่พร้อมรับมือมากที่สุด โดย 35% เลื่อนให้เป็นหนึ่งในสามอันดับแรก

"บริษัทต่างรู้สึกว่าการข้อบังคับเป็นภาระ เพราะผู้กำกับดูแลสามารถคาดเดาได้น้อยลง" เอมานูเอล ฟาน ซานด์วูร์ต (Emanuel Van Zandvoort) หัวหน้าฝ่ายที่ปรึกษาความเสี่ยง – บริหารความเสี่ยงองค์กร ที่ BDO Netherlands กล่าว "ในยุโรป

บริษัทต้องลงทุนอย่างมากในด้านการปฏิบัติตามกฎระเบียบ แต่กฎหมายกลับสามารถเปลี่ยนแปลงได้ ในช่วงข้ามคืน"

โดย 52% ของผู้ตอบแบบสำรวจ ระบุว่า กฎระเบียบด้านความเป็นส่วนตัวของข้อมูล เป็นข้อบังคับที่สำคัญที่สุดต่อธุรกิจของตน มากกว่ากฎระเบียบประเภทอื่น ๆ

ในขณะที่ ความเสี่ยงด้านห่วงโซ่อุปทาน และ บุคลากรหรือความสามารถ (Talent Risk) ตามมาเป็นอันดับสองร่วมกัน – ซึ่งถือเป็นการเพิ่มขึ้นอย่างมากของความเสี่ยงด้านทรัพยากรมนุษย์เพราะในปี 2567 ยังอยู่แค่อันดับที่ 12 (ดูหน้า 11) และความเสี่ยงด้านภูมิรัฐศาสตร์ ยังคงเป็นประเด็นสำคัญอยู่อันดับที่ 4

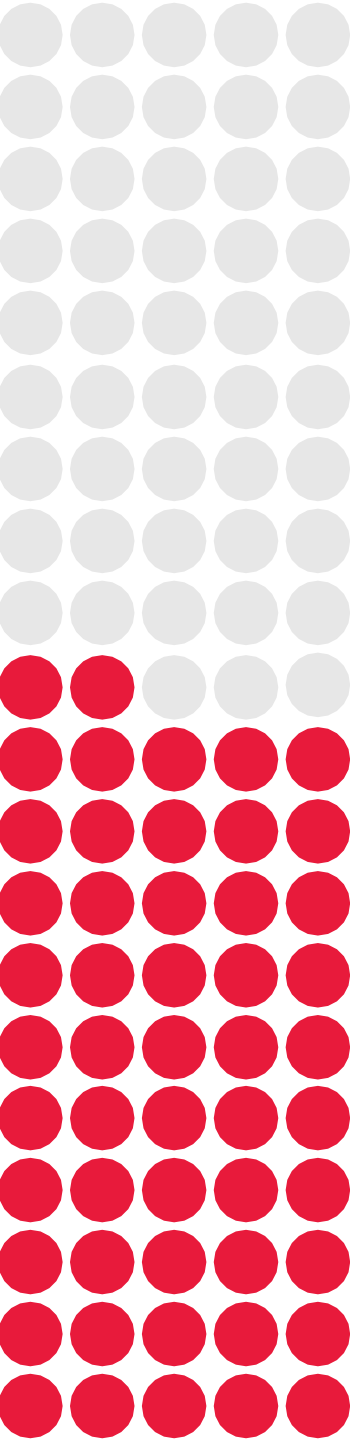
ความตึงเครียดทางภูมิรัฐศาสตร์ยังส่งผลให้เกิดความไม่แน่นอนมากขึ้นทั่วโลก ธุรกิจต้องเผชิญกับความสับสนเกี่ยวกับ ภาษีศุลกากร และความตึงเครียดด้านการค้า ซึ่งยิ่งทำให้แนวคิด "รอดูสถานการณ์" ทวีความรุนแรงความขัดแย้งระหว่างสหรัฐฯ และจีน ยังเป็นแรงกดดันอย่างมากต่อธุรกิจ โดยเฉพาะในภูมิภาคเอเชียแปซิฟิก (APAC)

"ประเด็นแรกคือสงครามการค้าระหว่างจีนกับสหรัฐฯ ส่วนประเด็นที่สองคือความสัมพันธ์ระหว่างไต้หวัน สหรัฐฯ และจีน ทำให้สถานการณ์ในภูมิภาค APAC ค่อนข้างตึงเครียด" Ricky Cheng ผู้อำนวยการและหัวหน้าฝ่ายให้คำปรึกษาความเสี่ยงของ BDO ฮองกง กล่าว

ความเสี่ยงด้านสิ่งแวดล้อม ก็เป็นอีกหนึ่งประเด็นที่กำลังมาแรง โดยขยับขึ้น 4 อันดับ มาอยู่อันดับที่ 5 ซึ่ง 24% ระบุว่า ยังไม่พร้อมรับมือกับความเสี่ยงนี้ อาชญากรรมไซเบอร์ (Cybercrime) ก็ยังคงเป็นประเด็นที่ต้องจับตามอง โดยอยู่ในอันดับที่ 6 ■

52%

มองว่าความเป็นส่วนตัวของข้อมูลเป็นหนึ่งในกฎระเบียบสามประการที่สำคัญที่สุดสำหรับธุรกิจ



# การปฏิบัติตามกฎระเบียบช่วยให้เราเห็นภาพการจัดการความเสี่ยงที่แท้จริงได้ไหม?

แม้ว่า ข้อกำหนดการรายงาน ที่เพิ่มขึ้นจะช่วย มุ่งความสนใจ ของผู้บริหารไปยังความเสี่ยงได้อย่างมีประสิทธิภาพ แต่ก็มีความเสี่ยงที่ซ่อนอยู่คือการเน้นการรายงานมากเกินไปอาจสร้าง ความประมาท ได้ เพราะองค์กรอาจเข้าใจผิดว่าการปฏิบัติตามกฎเกณฑ์อย่างเป็นทางการถือเป็นการจัดการความเสี่ยงที่แท้จริง

ภาพรวม

สิ่งที่กำลังเปลี่ยนแปลง

การเน้นที่กฎข้อบังคับมักเกินไป อาจสร้างสภาพแวดล้อมแบบทำตามขั้นตอนเพียงผิวเผินซึ่งเบี่ยงเบนความสนใจจากการจัดการความเสี่ยงที่แท้จริง

ทำไมเรื่องนี้จึงสำคัญ

การเน้นที่กฎข้อบังคับมากเกินไป อาจสร้างสภาพแวดล้อมแบบทำตามขั้นตอนเพียงผิวเผินซึ่งเบี่ยงเบนความสนใจจากการจัดการความเสี่ยงที่แท้จริง

ควรทำอะไร

กฎข้อบังคับการกำกับดูแลสามารถเป็นส่วนหนึ่งของการคิดวิเคราะห์ความเสี่ยงได้ แต่ทุกองค์กรต้องให้ความสำคัญกับความเสี่ยงทั้งในภาพรวมและรายละเอียดปลีกย่อยที่ธุรกิจเผชิญอยู่เสมอ

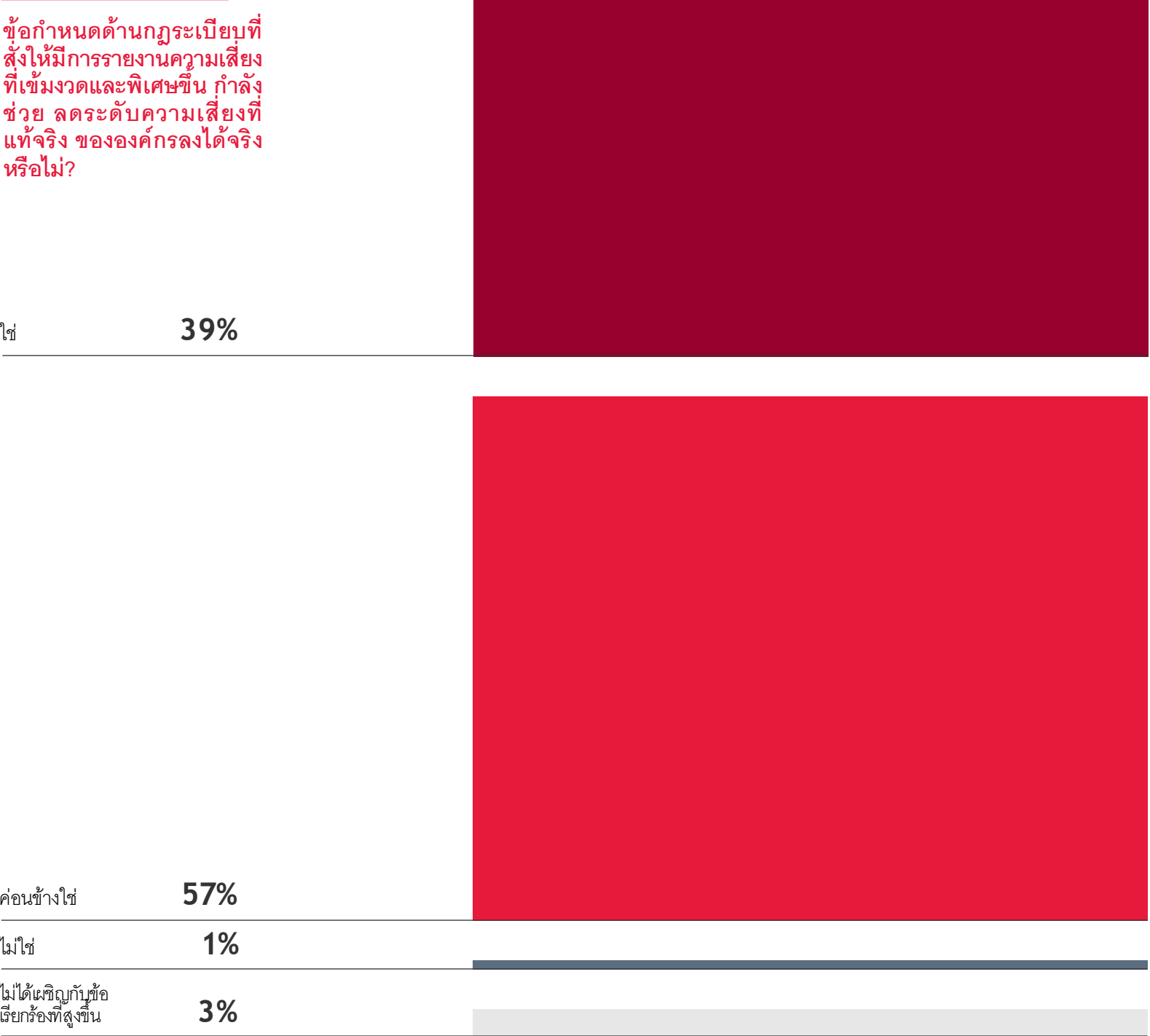
ธุรกิจต่างๆ เผชิญกับกฎระเบียบที่เพิ่มขึ้น โดยเฉพาะธุรกิจที่ดำเนินงานข้ามประเทศ

แม้ว่าจะเพิ่มภาระการปฏิบัติตามกฎสำหรับผู้จัดการความเสี่ยง แต่ผู้บริหารระดับสูงส่วนใหญ่ระบุว่าความต้องการรายงานเพิ่มเติมจากหน่วยงานกำกับดูแลนั้นช่วยลดความเสี่ยงโดยรวมได้

มากกว่าหนึ่งในสามของผู้ตอบแบบสอบถาม (39%) ระบุว่ากฎระเบียบการกำกับดูแลที่เพิ่มขึ้นช่วยลดโปรไฟล์ความเสี่ยงของพวกเขา ขณะที่อีก 57% กล่าวว่า ช่วยลดความเสี่ยงในระดับหนึ่ง

อย่างไรก็ตาม ความมองการกำกับดูแลเป็นเพียงส่วนหนึ่งของกลยุทธ์การจัดการความเสี่ยงขององค์กรเท่านั้น

“การกำกับดูแลในส่วนของกฎระเบียบเป็นแง่มุมหนึ่งของการจัดการความเสี่ยง แต่ผมไม่คิดว่าการกำกับดูแลจะให้ภาพรวมของสภาพแวดล้อมความเสี่ยงทั้งหมดแก่คุณ มันช่วยได้ แต่ถ้าคุณมองแค่จากมุมของการปฏิบัติตามกฎเท่านั้น คุณจะพลาดการวิเคราะห์เหตุการณ์และภัยคุกคามในภาพรวมและรายละเอียดภายในองค์กรนั้น ” ▶

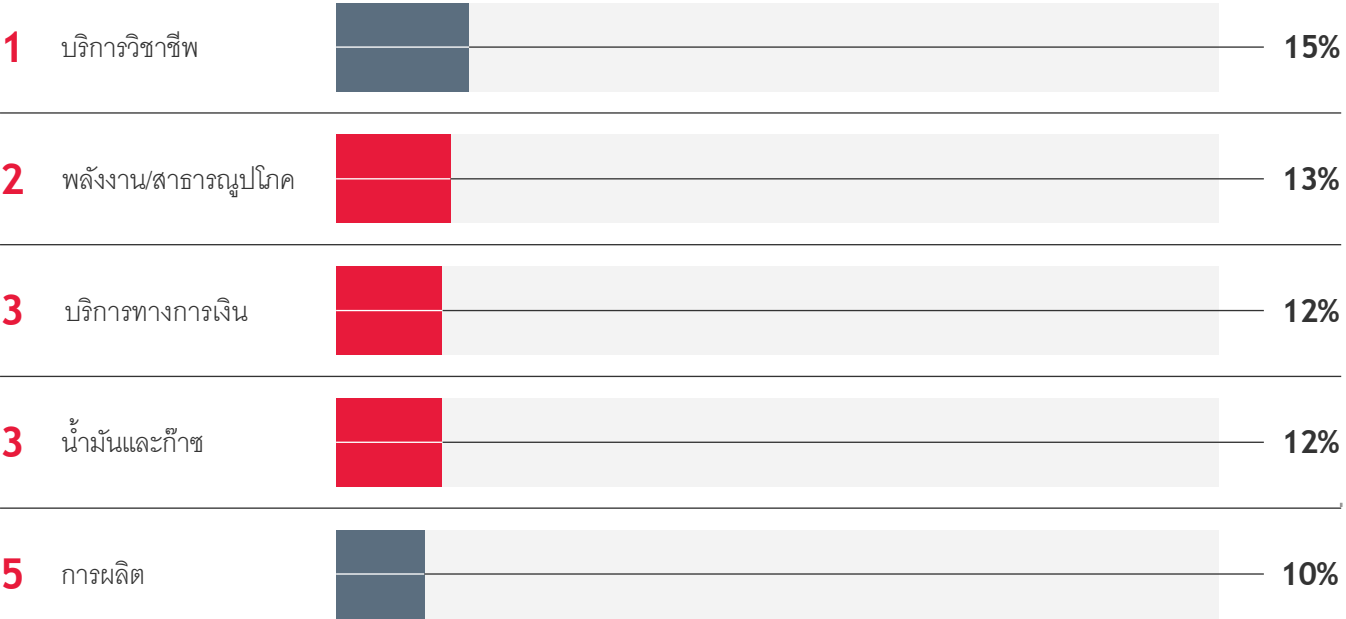




ศักยภาพของการกำกับดูแลที่จะสนับสนุนการจัดการความเสี่ยงเชิงรุกมากขึ้น อาจขึ้นอยู่กับปริมาณของกฎระเบียบที่ธุรกิจต้องเผชิญ บริษัทในอุตสาหกรรมที่ถูกควบคุมอย่างเข้มงวดระบุว่าพวกเขามีแนวโน้มที่จะจัดการกับความเสี่ยงอย่างเชิงรุกมากขึ้น โดยธุรกิจด้านพลังงานและสาธารณูปโภค (13%) รวมถึงบริการทางการเงินและน้ำมันกับก๊าซ (12% ทั้งคู่) ได้ดำเนินมาตรการเพื่อก้าวหน้าความเสี่ยงอยู่เสมอ ซึ่งเป็นไปได้ว่าเนื่องจากความเร็วของการเปลี่ยนแปลงด้านกฎระเบียบ ทำให้บริษัทในภาคส่วนเหล่านี้ต้องปรับตัวอย่างต่อเนื่องตามเกณฑ์ความเสี่ยงที่เปลี่ยนแปลงไป ซึ่งกำหนดโดยไม่เพียงแค่คณะกรรมการบริษัทเท่านั้น

5 อันดับภาคส่วนที่ระบุว่าการรับมือกับความเสี่ยงโดยวิธีการในรูปแบบ 'เชิงรุกมาก'

● อุตสาหกรรมที่มีการควบคุมอย่างเข้มงวด



แต่ยังรวมถึงหน่วยงานกำกับดูแลด้วย — เอนริค โตเมเนซ หัวหน้าฝ่ายให้คำปรึกษาความเสี่ยง BDO ประเทศสเปน กล่าว

แม้ว่าจะไม่ใช่อุตสาหกรรมที่ถูกควบคุมอย่างเข้มงวด แต่ 15% ของบริษัทที่ให้บริการวิชาชีพกล่าวว่าพวกเขาจัดการความเสี่ยงอย่างเชิงรุกมาก ซึ่งเป็นไปได้ว่าไม่ใช่เพียงเพราะความกังวลด้านกฎระเบียบเท่านั้น แต่ยังเป็นเพราะการรั่วไหลของข้อมูลลูกค้าอาจส่งผลเสียต่อชื่อเสียงอย่างร้ายแรงต่อบริษัท ■

# ความเสี่ยงด้านบุคลากรกลับมาเป็นประเด็นสำคัญอีกครั้ง

## ผู้บริหารวิตกกังวลมากขึ้นเกี่ยวกับการเข้าถึงบุคลากรที่มีความสามารถ

การเปลี่ยนแปลงที่เห็นได้ชัดที่สุดในอันดับความเสี่ยงประจำปี 2568 คือความกังวลที่เพิ่มขึ้นอย่างรวดเร็วเกี่ยวกับบุคลากรและทักษะของพนักงาน โดยมากกว่าหนึ่งในสี่ของผู้บริหาร (28%) ระบุว่า "ศักยภาพของบุคลากร" หรือ "ความสามารถในการดึงดูดและรักษาบุคลากรที่มีคุณภาพ" เป็นหนึ่งในสามอันดับแรกของความเสี่ยง ซึ่งเพิ่มขึ้นจาก 12% ในปี 2567 แม้ว่า "ศักยภาพของบุคลากร" และ "ความสามารถด้านบุคลากร" จะจัดอยู่ในอันดับค่อนข้างต่ำในรายการความเสี่ยงที่ผู้บริหารรู้สึกที่ไม่พร้อมรับมือ แต่เมื่อรวมกันแล้ว ความเสี่ยงด้านบุคลากรนั้นกลับขึ้นมาอยู่ในอันดับที่ 2 เทียบเท่ากับความเสี่ยงหลักอื่นๆ และสูงกว่าปัญหาที่มีมาอย่างยาวนาน เช่น ความตึงเครียดทางภูมิรัฐศาสตร์และอาชญากรรมทางไซเบอร์

ความกังวลจะแตกต่างกันไปในแต่ละภาคธุรกิจ โดยอุตสาหกรรมสุขภาพและวิทยาศาสตร์ชีวภาพมีความกังวลด้านบุคลากร/ทักษะมากที่สุด (44%) รองลงมาคือภาคอสังหาริมทรัพย์และก่อสร้าง (39%) และต่อด้วยกลุ่มเทคโนโลยี สื่อ และโทรคมนาคม (34%)



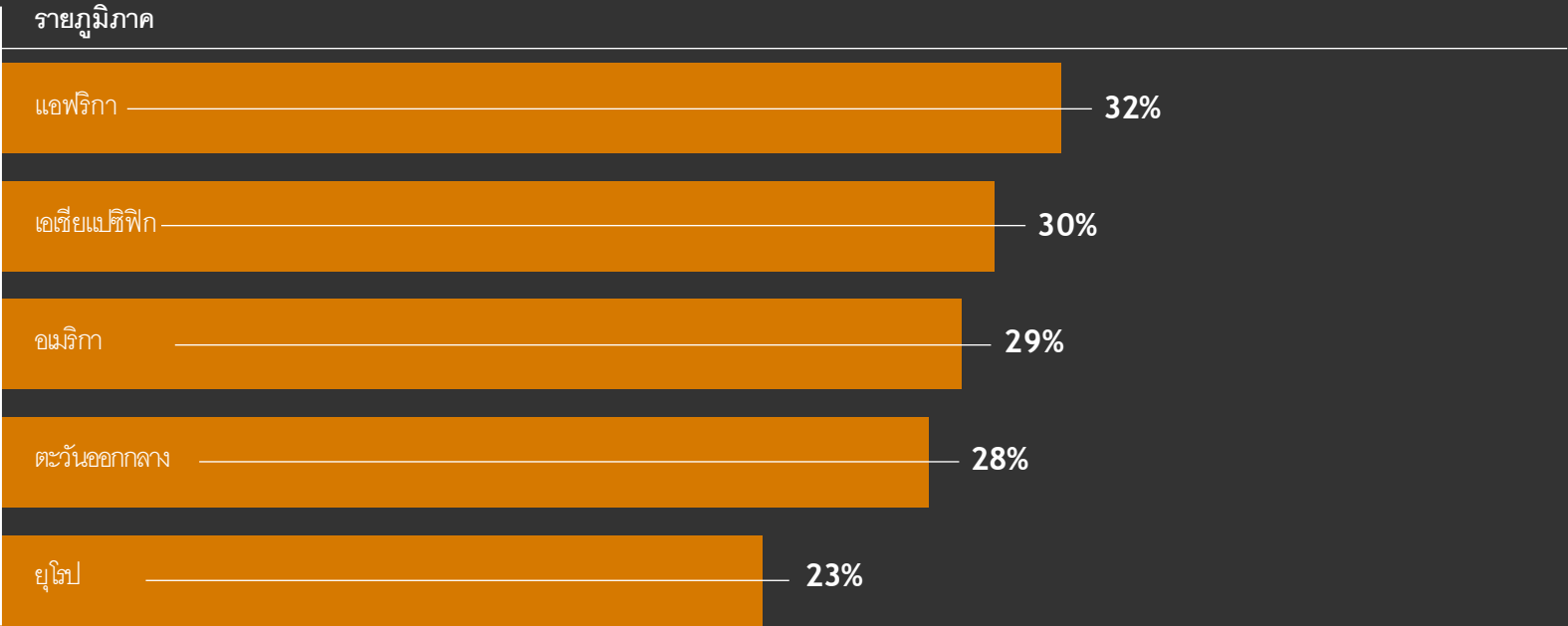
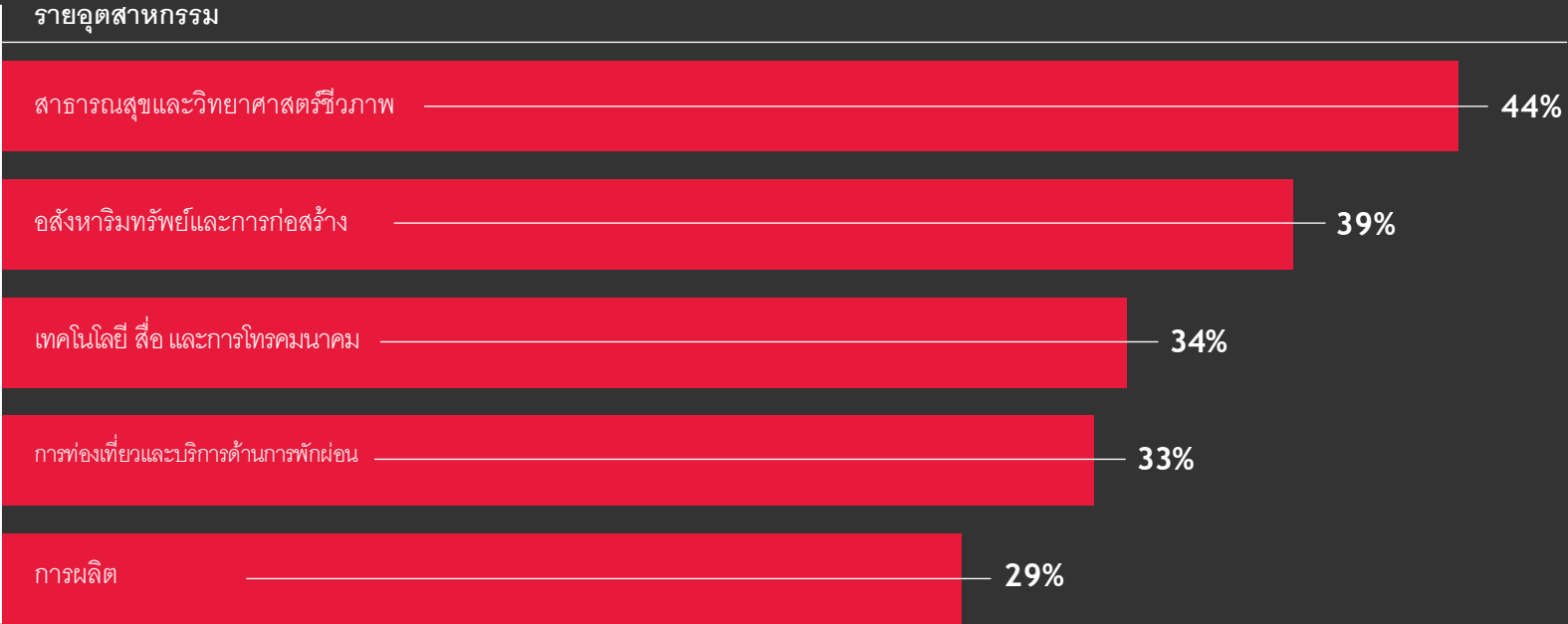
“ตอนนี้เราขาดแคลนบุคลากรที่มีความสามารถ และการรักษาคคนเก่งให้อยู่กับเรา หรือการหาคนที่มีความกาพสูงมาร่วมงานเป็นเรื่องที่ยากมาก” เดฟ อาริก ผู้อำนวยการบริหาร ฝ่ายบริหารความเสี่ยงระดับโลก บริษัท Sedgwick กล่าว “การที่เราสามารถพูด ‘ภาษาของความเสี่ยง’ ได้ เป็นสิ่งสำคัญมากสำหรับทุกคนในโลกที่เราอยู่ตอนนี้”

“แค่การหาคนที่ใช่เข้ามาร่วมทีม คนที่สามารถเฝ้าระวังและสังเกตเห็นความเสี่ยงรอบตัว แม้ว่าจะงานประจำของเขาจะไม่ใช่งานด้านความเสี่ยงก็ตาม ก็กลายเป็นเรื่องยากขึ้นเรื่อย ๆ สำหรับผม เราทุกคนล้วนเป็นผู้จัดการความเสี่ยงในระดับหนึ่งทั้งนั้น”

ปัญหาด้านความเสี่ยงเกี่ยวกับบุคลากรยังได้รับผลกระทบจาก AI ไม่ใช่เพียงเพราะองค์กรต้องการคนที่มีความรู้ด้าน AI มากขึ้น ไม่ว่าจะในฐานะผู้ใช้หรือผู้พัฒนา แต่เพราะเทคโนโลยีที่เติบโตอย่างรวดเร็วนี้ อาจทำให้ “ความรู้เชิงสถาบัน” หรือประสบการณ์เฉพาะตัวในองค์กรค่อย ๆ ลดลง และส่งผลต่อการฝึกอบรมกับพัฒนาทักษะของพนักงานในระยะยาว

“ทุกวันนี้ งานที่ต้องทำด้วยมือกำลังถูกตัดออกไป แต่นั่นคือวิธีที่คนเรียนรู้ เมื่อพวกเขาเริ่มต้นทำงานในสายงานความเสี่ยง”อลิชา ไชชนายา หัวหน้าผู้นำสายงานที่ปรึกษา BDO สำนักงานลอนดอน กล่าว“คุณต้องให้คนเข้าใจสิ่งที่เกิดขึ้นจริงในรายละเอียดหน้างาน เพราะถ้าคุณตัดกระบวนการเหล่านั้นออกไป คุณก็จะสูญเสียโอกาสในการฝึกคนให้เข้าใจภาพจริง และเราก็ไม่อยากสูญเสีย ‘ความทรงจำของกล้ามเนื้อ’ (muscle memory) แบบนั้นไป”

## ความเสี่ยงด้านความสามารถ/ทักษะ กระทบต่อกลุ่มอุตสาหกรรมหรือภูมิภาคใดบ้าง



# ช่องว่างเชิงความเสี่ยง: แนวคิดการมุ่งเน้นเพียงข้อปฏิบัติกำลังจำกัดศักยภาพการเติบโต

การทำตามเช็กลิสต์ (Check-the-box mentality) อาจกลายเป็นอุปสรรคสำคัญที่บดบังแนวทางการจัดการความเสี่ยงที่มีประสิทธิภาพ

ภาพรวม

สิ่งที่กำลังเปลี่ยนแปลง

การกำกับดูแลที่เพิ่มขึ้นและสภาพแวดล้อมในการดำเนินธุรกิจที่ไม่แน่นอน กำลังผลักดันให้ธุรกิจมุ่งเน้นการจัดการความเสี่ยงในเชิงการปฏิบัติตามกฎระเบียบมากขึ้น

ทำไมเรื่องนี้จึงสำคัญ

แนวทางนี้มักมีความสำคัญเหนือกว่าการจัดการความเสี่ยงอย่างแท้จริง ซึ่งอาจทำให้ธุรกิจพลาดหรือมองข้ามโอกาสในการเติบโตที่เป็นไปได้

ควรทำอะไร

การปลูกฝังวัฒนธรรมด้านความเสี่ยง (risk culture) ในองค์กร จะช่วยเปลี่ยนมุมมองจากการมุ่งเน้นแค่การปฏิบัติตามกฎระเบียบ ไปสู่การเปิดรับความเสี่ยงอย่างมีวิจารณญาณ เพื่อมองเห็นและใช้ประโยชน์จากโอกาสทางธุรกิจที่สามารถขับเคลื่อนการเติบโตได้

ผู้บริหารเชื่อว่าพวกเขามีสมดุลที่เหมาะสมระหว่างการจัดการความเสี่ยงอย่างแท้จริง ความเสี่ยงในวงกว้างที่อาจเป็นภัยคุกคามต่อองค์กร และการปฏิบัติตามกฎระเบียบ แต่เมื่อพิจารณาอย่างลึกซึ้งจะพบว่า มีความไม่สอดคล้องกันภายในองค์กรอยู่

แม้ว่าผู้ตอบแบบสำรวจส่วนใหญ่ (54%) จะกล่าวว่ามีความสำคัญกับทั้งความเสี่ยงและการปฏิบัติตามกฎอย่างเท่าเทียมกัน แต่ผลสำรวจแสดงให้เห็นว่า CEO หรือกรรมการผู้จัดการ (MD) กลับมีมุมมองไม่ตรงกับ Chief Risk Officer (CRO) ผู้นำองค์กรมองว่า ปัญหาใหญ่ที่สุดคือการใช้จ่ายเงินจำเป็นด้านการปฏิบัติตามกฎระเบียบรองลงมาก็คือแนวคิดการทำงานแบบ “ติดถูกตามช่อง” โดยไม่เข้าใจภาพรวมของความเสี่ยงในทางตรงกันข้าม CROs มองว่าปัญหาใหญ่ที่สุดคือการปรับตัวที่จำกัดต่อความเสี่ยงใหม่ ๆ รองลงมาก็คือการใช้เทคโนโลยีสำหรับติดตามความเสี่ยงในระดับต่ำมาก

นอกจากนี้ จากหลังด้านกฎระเบียบยังอาจบีบบังคับให้บริษัทต้องมุ่งเน้นการจัดการความเสี่ยงในเชิงการปฏิบัติตามกฎระเบียบมากขึ้น เนื่องจากความไม่แน่นอนในตลาดที่กว้างมากกว่าเดิม ทำให้เกิดความเสี่ยงที่ไม่สามารถคาดการณ์ได้มากขึ้นในการตัดสินใจทางธุรกิจ

“สภาพแวดล้อมด้านกฎระเบียบในปัจจุบันมีการเปลี่ยนแปลงอย่างรวดเร็วและในบางกรณีถึงขั้นกลับทิศทางอย่างสิ้นเชิง แทนที่จะค่อย ๆ เปลี่ยนแปลงแบบค่อยเป็นค่อยไปภายใต้รัฐบาลปัจจุบัน” Polly James, Senior Director of Risk Management at Feld Entertainment in the US. กล่าว “การมุ่งลดภาระของรัฐบาลลง ▶



การกำกับดูแลจากส่วนกลางและการผลักดันให้การกำกับดูแลกระจายลงไปยังระดับรัฐนั้น ไม่เป็นประโยชน์ต่อธุรกิจที่ดำเนินงานทั่วประเทศ”

การหาจุดสมดุลระหว่างการบริหารความเสี่ยงอย่างแท้จริงและการปฏิบัติตามข้อกำหนดเป็นสิ่งสำคัญ หากบริษัทต้องการมีแนวทางเชิงรุกมากขึ้นในการจัดการความเสี่ยง

“ความเสี่ยงด้านกฎระเบียบและการปฏิบัติตามกฎระเบียบถือเป็นส่วนสำคัญมาโดยตลอดในภาพรวมความเสี่ยงของเรา แต่สิ่งที่เกิดขึ้นในปีนี้มีพิเศษและแตกต่างออกไป จึงเป็นเรื่องสำคัญมากที่ต้องติดตามสถานการณ์อย่างใกล้ชิด เพราะมันช่วยให้เราไม่ต้องหยุดหรือชะลอกิจกรรมอื่น ๆ หรือนวัตกรรมต่าง ๆ เพียงเพื่อไปมุ่งเน้นแต่เรื่องการปฏิบัติตามกฎ” Lianne Appelt, Head of Enterprise Risk Management, Salesforce กล่าว

ธุรกิจส่วนใหญ่ตระหนักถึงความจำเป็นที่ต้องให้ความสำคัญกับความเสี่ยงที่แท้จริงมากขึ้น โดยถึง 74% ของผู้บริหารกล่าวว่า การปลูกฝังแนวคิดเรื่องความเสี่ยงลงในวัฒนธรรมองค์กรเป็นสิ่งที่มีความสำคัญในลำดับต้น ๆ

“ความเสี่ยงด้านกฎระเบียบและการปฏิบัติตามข้อกำหนดถือเป็นหัวใจหลักของภูมิทัศน์ความเสี่ยงของเราเสมอมา แต่สิ่งที่เกิดขึ้นในปีนี้มีพิเศษและแตกต่างออกไป”

Lianne Appelt,  
Head of Enterprise Risk Management, Salesforce

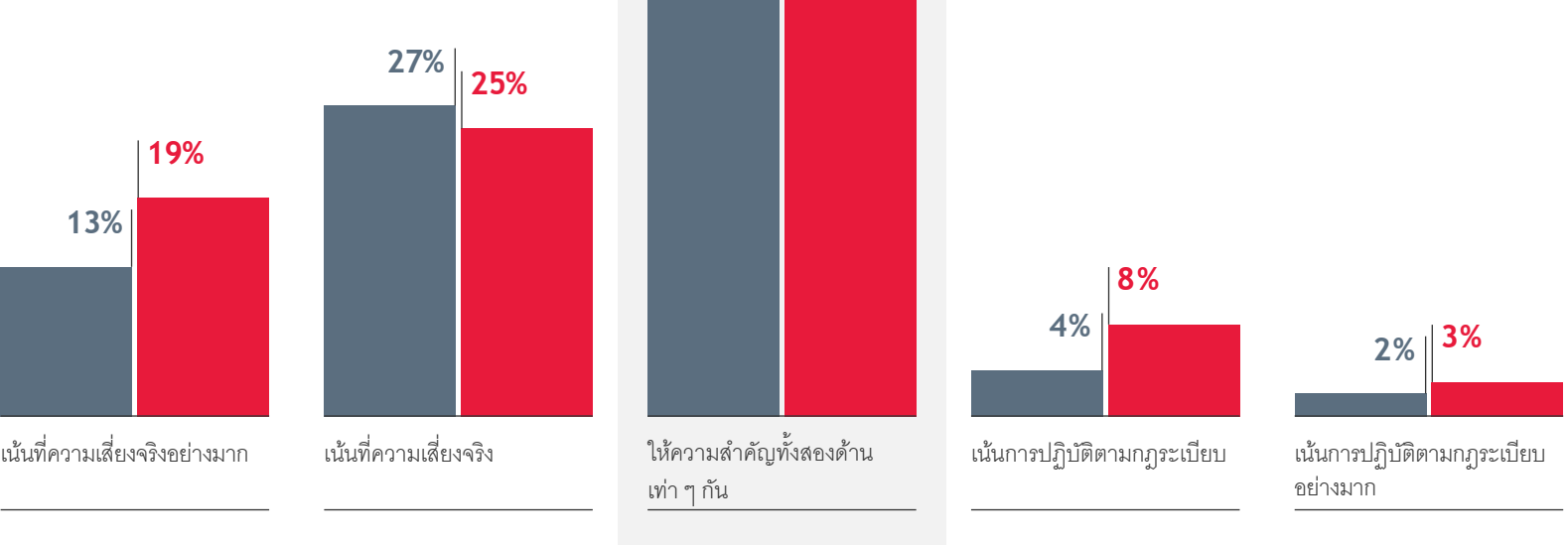
“จำเป็นอย่างยิ่งที่ทุกคนต้องมีความเข้าใจว่า ‘ความเสี่ยง’ หมายถึงอะไร ทั้งในระดับบุคคลและระดับธุรกิจ รวมถึงต้องตระหนักถึงข้อดีของการดำเนินธุรกิจโดยมีกรอบความคิดที่สอดคล้องกับเป้าหมายเชิงกลยุทธ์และค่านิยมขององค์กร” Matt Williams, a National Leader in BDO Australia’s Risk Advisory Services team. กล่าว

อีกประเด็นหนึ่งคือทัศนคติที่ดูจะขัดแย้งกันของผู้ในระดับสูง โดย 63% ของ ซีอีโอและกรรมการผู้จัดการกล่าวว่า ความเสี่ยงด้านกฎระเบียบเป็นหนึ่งในสามอันดับแรกของความเสี่ยงที่พวกเขาไม่พร้อมรับมือ ขณะเดียวกัน 60% ก็กล่าวว่าการใช้ภัยด้านการปฏิบัติตามกฎระเบียบมากเกินไปเป็นปัญหาใหญ่

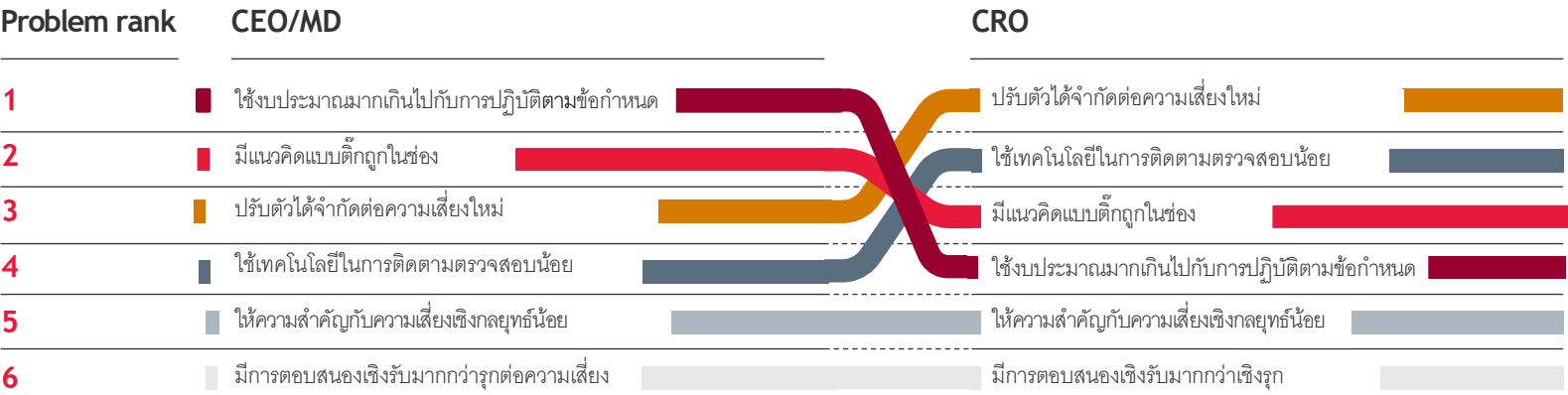
หนึ่งในเหตุผลที่อาจทำให้เกิดความไม่สอดคล้องนี้ คือผู้นำองค์กรเชื่อว่าบริษัทของตนไม่ได้รับคุณค่าที่ดีที่สุดจากความพยายามด้านการปฏิบัติตามและการควบคุมกฎระเบียบ เพราะยังคงมุ่งเน้นไปที่การทำตามขั้นตอนแบบ “ดีถูกในช่อง” มากกว่าการหาวิธีเปลี่ยนการบริหารความเสี่ยงให้กลายเป็นโอกาสทางธุรกิจ ▶

โฟกัสที่ความเสี่ยงจริง VS การปฏิบัติตามกฎระเบียบ :ผู้บริหารจำนวนมากจะพอใจกับการประเมินประนีประนอมที่จุดกึ่งกลาง

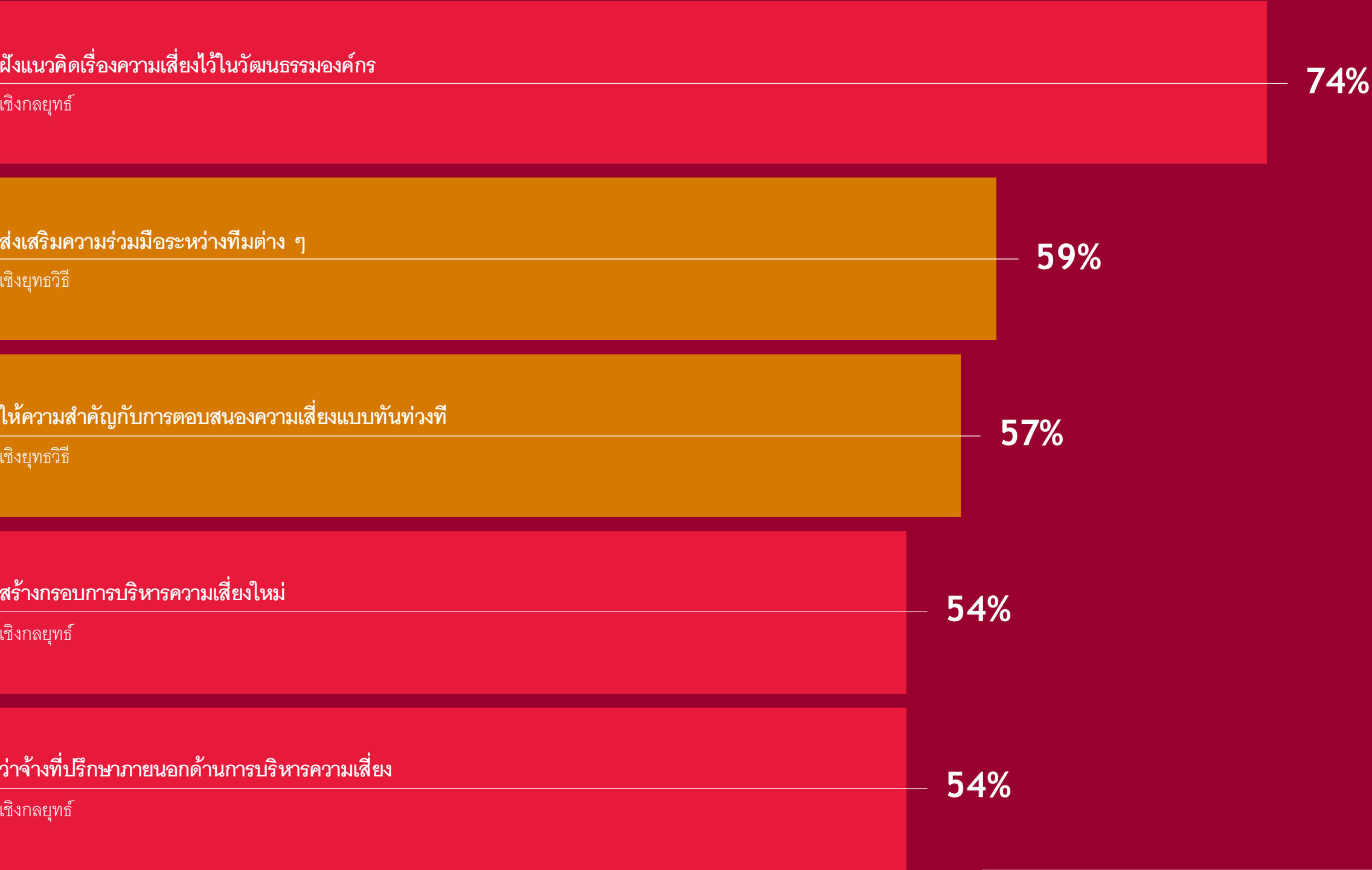
- ลำดับปัจจุบัน
- ลำดับที่ควรจะเป็น



หากมองอย่างเจาะลึก, จะพบว่า ซีอีโอ/กรรมการผู้จัดการมีทัศนคติที่ไม่ค่อยสอดคล้องตามกับการบริหารความเสี่ยงซึ่งไม่สอดคล้องกับมุมมองของหัวหน้าฝ่ายบริหารความเสี่ยง (CRO) ที่รับผิดชอบโดยตรง



องค์กรต่าง ๆ กำลังทำอะไรเพื่อปรับสมดุลไปสู่การบริหารความเสี่ยงที่แท้จริง?



แม้ CEO บางรายจะมองว่าการปฏิบัติตามข้อกำหนดมีต้นทุนสูง และไม่สร้างรายได้โดยตรง แต่การ “ใช้เงินน้อยเกินไป” ก็อาจก่อให้เกิดผลเสียอย่างร้ายแรง”

Richard Walker, Head of Risk Advisory Services, BDO South Africa กล่าวว่

“ธุรกิจต้องชั่งน้ำหนักระหว่างความเสี่ยงและโอกาส แม้การประหยัดงบด้านการปฏิบัติตามข้อกำหนดจะดูน่าสนใจ แต่หากถูกตรวจพบ อาจต้องเผชิญกับค่าปรับจำนวนมากและความเสียหายต่อชื่อเสียง”

ธุรกิจบางแห่งเลือกลงทุนในด้านความเสี่ยงในรูปแบบอื่น เช่น การว่าจ้างที่ปรึกษา อย่างไรก็ตาม ความเต็มใจที่จะดำเนินกลยุทธ์นี้มักขึ้นอยู่กับโครงสร้างความเป็นเจ้าของของกิจการ

- 67% ของบริษัทที่มีผู้บริหารมืออาชีพหรือกลุ่มทุนเอกชน (PE) เป็นเจ้าของ กล่าวว่า พวกเขาใช้ที่ปรึกษาเพื่อให้ความสำคัญกับการบริหารความเสี่ยงที่แท้จริง
- ขณะที่บริษัทที่เจ้าของเป็นผู้ก่อตั้งเอง มีแนวโน้มใช้ที่ปรึกษาน้อยกว่าอย่างชัดเจน (เพียง 43% เท่านั้น) ■

## ข้อมูลเชิงลึก

# ยกระดับการเปลี่ยนจากรูปแบบเป็นการสร้างคุณค่า

## Alisa Voznaya

Partner leading BDO's Consulting practice in London

“บางครั้งองค์กรรู้สึกว่ แนวทางแบบ 'ปฏิบัติตามข้อกำหนด' (Compliance) นั้น ง่ายและสะดวกกว่า เพราะคุณเพียงแค่ทำตามขั้นตอนให้ครบถ้วน ก็รู้สึกเหมือนว่า งานเสร็จสมบูรณ์"ได้รับความพึงพอใจทันทีในทางตรงกันข้าม การสร้างวัฒนธรรมด้านความเสี่ยง (Risk Culture) ที่แข็งแกร่งกลับเป็นสิ่งที่ผู้บริหารส่วนใหญ่รู้สึกว่า ยากที่สุด ที่จะทำให้สำเร็จลงได้จริง”

องค์กรจำเป็นต้อง ตระหนักถึงความแตกต่างนี้ และตั้งคำถามกับตัวเองว่า "เรากำลัง 'พูดถึงความเสี่ยง' อย่างมีกลยุทธ์ เพื่อขับเคลื่อนธุรกิจ หรือแค่พูดถึงมันในฐานะรายการที่ต้องทำตามเช็กลิสต์ (Check-the-box mentality) เท่านั้น?" สัญญาณที่ชัดเจนที่สุด ที่บ่งชี้ว่าองค์กรยังคงมองความเสี่ยงแบบ ทำตามเช็กลิสต์ คือ หน่วยงานต่าง ๆ ใช้เวลาส่วนใหญ่ไปกับ กรอกเอกสารด้าน Complianceแต่ ไม่เคยนำผลการประเมินความเสี่ยง ที่ได้มาพูดคุยหรือตัดสินใจใน ระดับผู้บริหารสูงสุด อย่างจริงจัง

สิ่งนี้หมายความว่า ผู้บริหารไม่ได้พิจารณาประเด็นด้านความเสี่ยงเป็นส่วนหนึ่งของวาระเชิงกลยุทธ์เลย

“เมื่อทีม การปฏิบัติตามกฎ (Compliance) และทีม บริหารความเสี่ยง (Risk) ทำงานแยกขาดจากกัน โดยเฉพาะในองค์กรที่ไม่ได้อยู่ในอุตสาหกรรมที่ถูกกำกับเข้มงวด นั่นคือปัญหาที่แท้จริง"เพราะในท้ายที่สุดแล้ว ทั้งสองฝ่ายต่างก็มี เป้าหมายเดียวกันคือการปกป้องและสร้างคุณค่าให้กับองค์กร เพียงแต่พวกเขามองเป้าหมายนั้นผ่านมุมมองที่แตกต่างกันเท่านั้นการบูรณาการการทำงานของทั้งสองทีมจึงเป็นกุญแจสำคัญสู่การบริหารความเสี่ยงที่ครอบคลุมและมีประสิทธิภาพ” ■

“องค์กรจำเป็นต้อง ตระหนักถึงความแตกต่างนี้ และตั้งคำถามกับตัวเองว่า "เรากำลัง 'พูดถึงความเสี่ยง' อย่างมีกลยุทธ์ เพื่อขับเคลื่อนธุรกิจ หรือแค่พูดถึงมันในฐานะรายการที่ต้องทำตามเช็กลิสต์ (Check-the-box mentality) เท่านั้น?"

# ภัยไซเบอร์ที่ไม่มีวันสิ้นสุด: ความท้าทายที่ต้องเผชิญต่อไป

ภัยคุกคามทางไซเบอร์ที่พัฒนาอย่างต่อเนื่อง กำลังทำให้ผู้บริหารต้องตื่นตัวตลอดเวลา

ภาพรวม

สิ่งที่กำลังเปลี่ยนแปลง

อาชญากรไซเบอร์มีความซับซ้อนมากขึ้นเรื่อย ๆ จนทำให้ CEO จำนวนมากเริ่มหันมาให้ความสนใจอย่างจริงจัง โดยเฉพาะเมื่อคู่แข่งทางธุรกิจของตนตกเป็นเป้าหมายของการโจมตี

ทำไมเรื่องนี้จึงสำคัญ

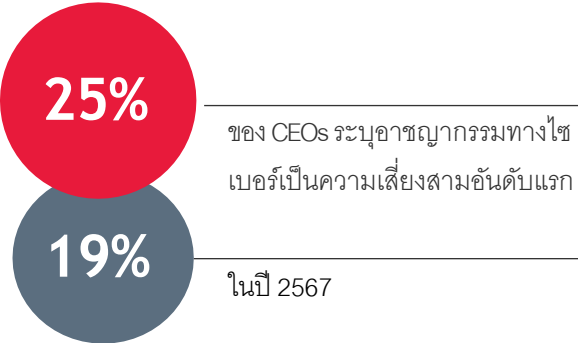
การโจมตีทางไซเบอร์สามารถสร้างความเสียหายต่อชื่อเสียงขององค์กรอย่างรุนแรง และอาจนำไปสู่บทลงโทษจากหน่วยงานกำกับดูแล หากบริษัทไม่มีมาตรการรักษาความปลอดภัยที่เพียงพอ

ควรทำอย่างไร

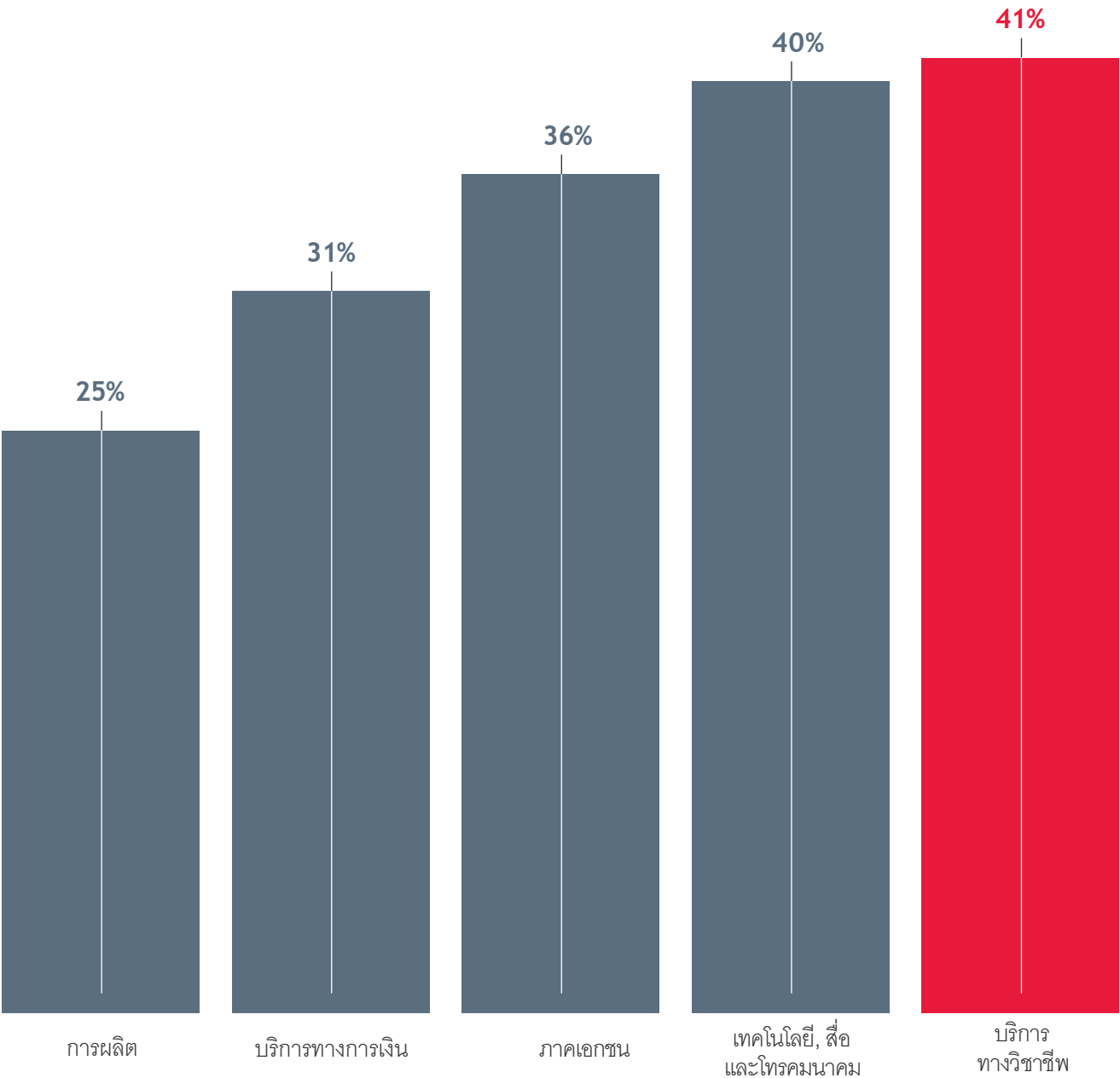
องค์กรที่มีความแข็งแกร่งด้านไซเบอร์มากที่สุด มักจะเป็นองค์กรที่มองความปลอดภัยทางไซเบอร์เป็นตัวขับเคลื่อนธุรกิจ (enabler) ไม่ใช่เพียงต้นทุนที่หลีกเลี่ยงไม่ได้ในการดำเนินงาน

ภัยคุกคามจากการโจมตีทางไซเบอร์กำลังทำให้ CEO รู้สึกวิตกกังวลมากกว่าที่เคย รายงานของ IBM/Ponemon Institute ระบุว่า ค่าเสียหายเฉลี่ยจากเหตุข้อมูลรั่วไหลในปี 2567 อยู่ที่เกือบ 5 ล้านดอลลาร์สหรัฐ ท่ามกลางสถานการณ์นี้ CEO จำนวนหนึ่งในสี่ระบุว่าการโจมตีทางไซเบอร์เป็นหนึ่งในสามความเสี่ยงสูงสุดของพวกเขา เพิ่มขึ้นจาก 19% เมื่อปีที่แล้ว

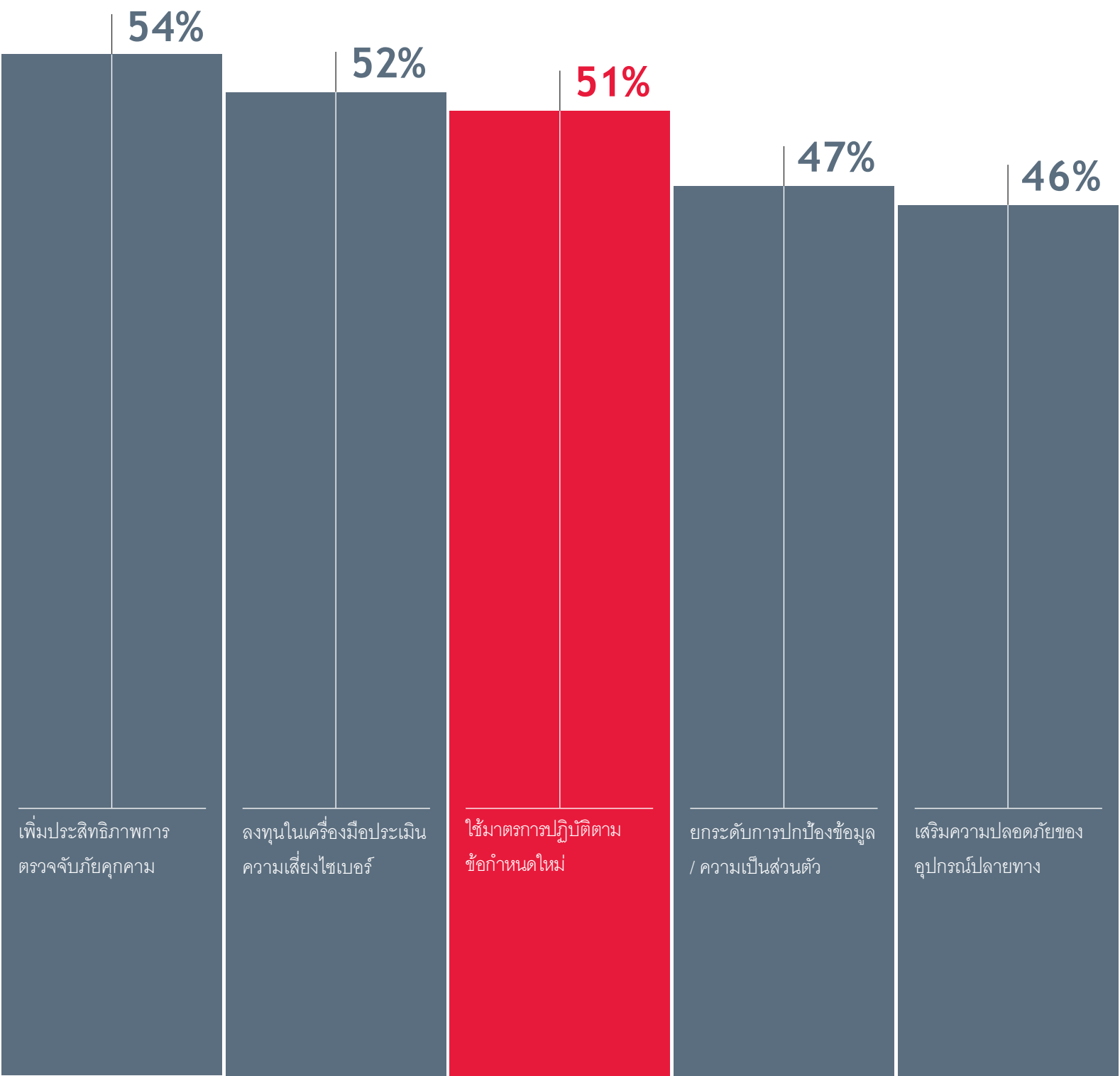
“ไม่มีอะไรใหม่มากนัก สิ่งที่เปลี่ยนไปคือความซับซ้อนและความเร็วที่การโจมตีทางไซเบอร์บางประเภทสามารถเจาะเข้าระบบและส่งผลกระทบต่อบริษัทได้” Lianne Appelt, Head of Enterprise Risk Management กล่าว ▶



อุตสาหกรรมที่ให้ความสำคัญกับภัยไซเบอร์มากที่สุด



ลำดับความสำคัญด้านความปลอดภัยไซเบอร์ของผู้นำธุรกิจ  
ในอีก 2 ปี ข้างหน้า



Salesforce: “ในฐานะที่เราเป็นบริษัทเทคโนโลยี ความเสี่ยงด้านไซเบอร์คือสิ่งที่เราให้ความสำคัญสูงสุดเราจึงทำทุกอย่างที่สามารถทำได้เพื่อให้มั่นใจว่า ผลิตภัณฑ์ บริการ และระบบภายในของเรามีความปลอดภัย”

แม้ว่า แคมเปญฟิชชิงผ่านอีเมล (email phishing) ที่มีเป้าหมายเพื่อติดตั้งมัลแวร์หรือหลอกหลวงให้โอนเงิน ยังคงเป็น ความเสี่ยงด้านไซเบอร์หลัก อยู่ในปัจจุบัน แต่ตอนนี้มีแนวโน้มเพิ่มขึ้นของการโจมตีแบบ Social Engineering ซึ่งมุ่งเป้าไปที่ “ตัวบุคคล” ภายในองค์กร

“ผู้ไม่หวังดีใช้เทคโนโลยีชนิดเดียวกับที่เรานำมาเพิ่มประสิทธิภาพการทำงาน มาช่วยในการสอดแนม (reconnaissance) และเรียนรู้ข้อมูลเกี่ยวกับองค์กรและพนักงาน” กล่าวโดย Rocco Galletto, Partner and Global Head of Cyber, BDO Canada “ทีมของเราทดสอบทั้งระบบความปลอดภัยด้านกายภาพและระบบความปลอดภัยด้านดิจิทัล และตอนนี้เครื่องมือตรวจจับมัลแวร์สามารถจับภัยได้เกือบทั้งหมดแล้ว แต่เมื่อเป็น Social Engineering ผ่านพนักงานเรามักพลาดอยู่ตรงนี้เสมอ” ▶

“เมื่อทีมไซเบอร์สามารถสร้างความสอดคล้องกับเป้าหมายระดับองค์กรได้อย่างแท้จริงพวกเขาจะไม่เพียงแต่ช่วยให้องค์กร ปลอดภัย เท่านั้น แต่ยังทำได้อย่าง รวดเร็วและมีประสิทธิภาพ สูงสุดด้วย”

**Rocco Galletto,**  
Partner and Global Head of Cyber, BDO Canada

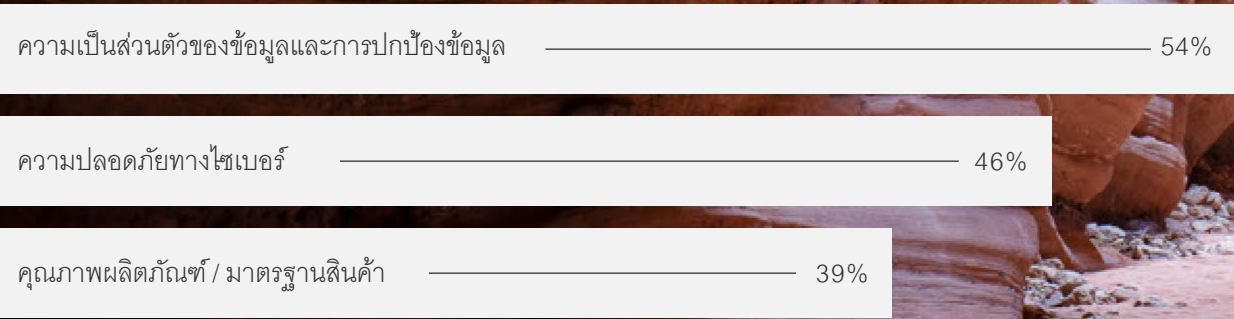
บางอุตสาหกรรมมีความเปราะบางต่อความเสี่ยงไซเบอร์เป็นพิเศษ และพบว่าตัวเองยังขาดความพร้อมอย่างรุนแรง:กลุ่มบริการวิชาชีพ (Professional Services): เป็นกลุ่มที่มีแนวโน้ม ไม่พร้อมรับมือกับความเสียหายไซเบอร์สูงสุด (41%)ตามมาด้วยกลุ่ม เทคโนโลยี, สื่อ และโทรคมนาคม (Tech, Media, Telecom) ที่ 40%และกลุ่ม Private Equity ที่ 36%

ภัยคุกคามทางไซเบอร์มีการ พัฒนาอย่างรวดเร็ว ซึ่งนำไปสู่ ช่องว่างที่กว้างขึ้น ระหว่างองค์กรที่มี "ความยืดหยุ่นทางไซเบอร์" (Cyber Resilience) กับองค์กรที่ปรับตัวไม่ทันนอกจากนี้ ความเร็วของการเปลี่ยนแปลงด้านเทคโนโลยี ยังเป็นอีกหนึ่งความเสี่ยงหลัก:20% ของผู้ตอบแบบสอบถามระบุว่า “การเปลี่ยนแปลงทางเทคโนโลยี” เป็น 1 ใน 3 ความเสี่ยงหลักที่พวกเขาไม่พร้อมรับมือแต่มี CEO เพียง 9% เท่านั้นที่มองเห็นนั้น ซึ่งแสดงให้เห็นถึงความไม่สอดคล้องในการรับรู้ความเสี่ยงระดับผู้นำ

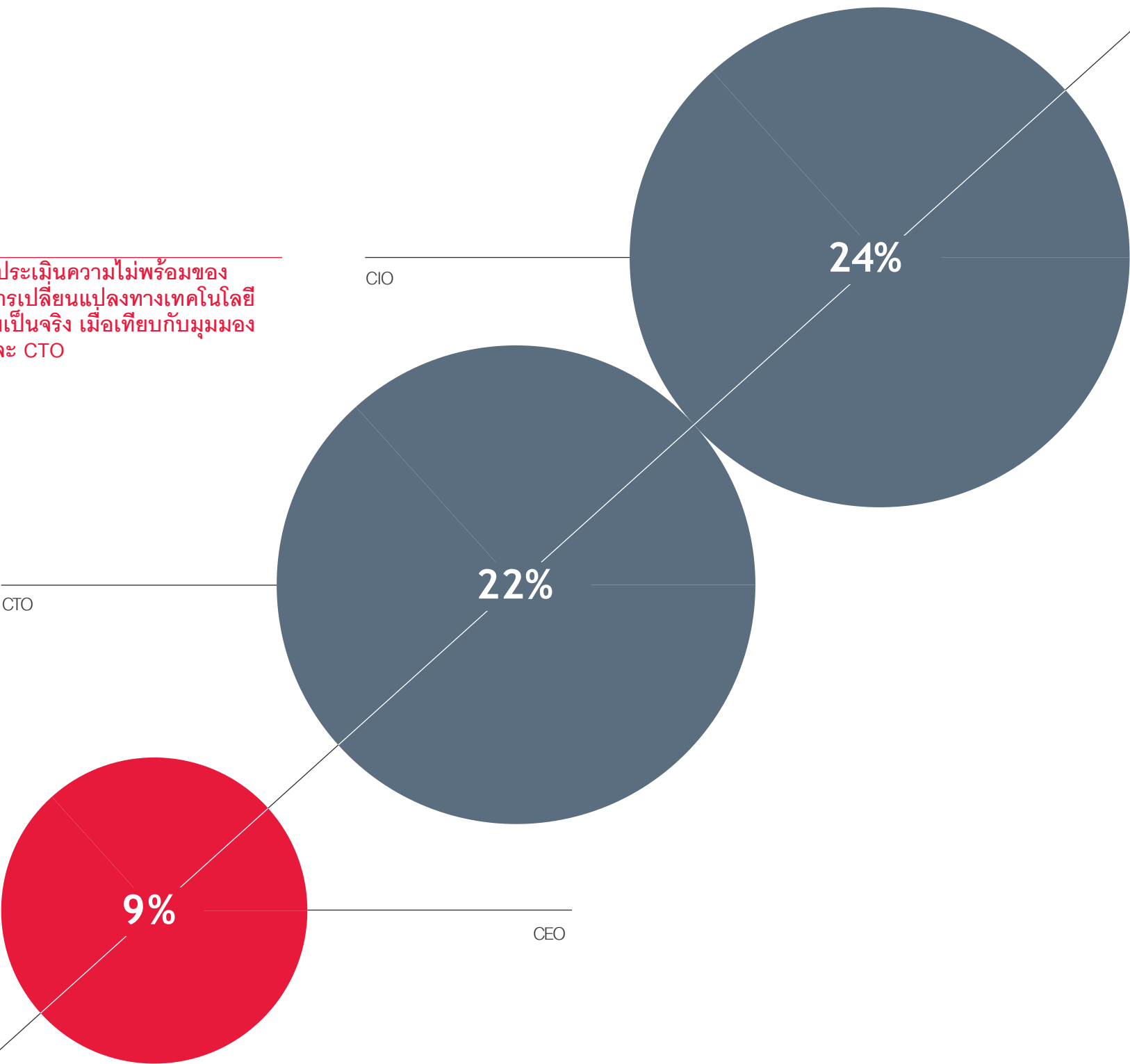
“เมื่อเทคโนโลยีเปลี่ยนแปลง ความเสี่ยงของธุรกิจก็เปลี่ยนไปด้วย ไม่ใช่แค่เพราะเทคโนโลยีเปลี่ยน แต่เพราะวิธีการดำเนินงานของธุรกิจก็เปลี่ยนเช่นกัน”

Galletto กล่าว ▶

ผู้บริหารกำลังประสบปัญหาในการจัดการกับความเสี่ยงใดมากที่สุด?



CEO มักจะประเมินความไม่พร้อมขององค์กรต่อการเปลี่ยนแปลงทางเทคโนโลยีต่ำกว่าความเป็นจริง เมื่อเทียบกับมุมมองของ CIO และ CTO



“เนื่องจากเทคโนโลยีเปลี่ยนแปลงเร็วขึ้น ธุรกิจก็ต้องปรับตัวให้เร็วขึ้น และทีมไซเบอร์มักจะตามไม่ทัน ดังนั้นช่องว่างด้านความพร้อมจึงอาจใหญ่ขึ้นกว่าในอดีต และช่องว่างนั้นก็ดูเหมือนจะขยายกว้างขึ้นเรื่อย ๆ”

ความแตกต่างสำคัญระหว่างองค์กรที่มี “ความยืดหยุ่นด้านไซเบอร์” (Cyber Resilience) สูง กับองค์กรที่ตามไม่ทัน คือ: องค์กรที่ปรับตัวได้ดีจะ มองความปลอดภัยไซเบอร์เป็นตัวสนับสนุนธุรกิจ ไม่ใช่อุปสรรค

Galletto กล่าวว่า “เมื่อทีมไซเบอร์มีเป้าหมายที่ สอดคล้องกับเป้าหมายขององค์กรโดยรวม พวกเขาจะสามารถช่วยให้องค์กรปลอดภัยได้อย่าง รวดเร็วและมีประสิทธิภาพ” ซึ่งช่วยให้องค์กรสามารถ คาดการณ์สิ่งที่อาจผิดพลาดได้ล่วงหน้า และ ฟื้นตัวได้อย่างรวดเร็ว หากเกิดเหตุไม่คาดคิด

นอกเหนือจากความเสี่ยงการโจมตี ไซเบอร์ยังสร้าง ความท้าทายด้านการปฏิบัติตามกฎระเบียบ (Compliance) ที่เพิ่มขึ้น โดย 52% ของ CTO ระบุว่าองค์กรของตนมี “แนวคิดแบบติดถูกในกล่อง” ซึ่งเบี่ยงเบนจากกลยุทธ์บริหารความเสี่ยงที่แท้จริง

“นอกจาก ความเสี่ยงที่แท้จริงของการถูกโจมตีทางไซเบอร์แล้ว ความปลอดภัยไซเบอร์ยังได้กลายเป็น ภาระที่หนักขึ้นเรื่อย ๆ ในแง่ของ การปฏิบัติตามกฎระเบียบ (Compliance)”

Galletto กล่าวว่า “องค์กรจำนวนมากมัก ทำตามเช็กลิสต์ให้ครบ แต่กลับละเลย ความปลอดภัยที่ต้องดูแลในชีวิตจริงแบบวันต่อวัน” เมื่อทรัพยากรมีไม่เพียงพอ ความรับผิดชอบด้าน Compliance จึงกลายเป็นการ ‘ติดถูกในกล่อง’ ไปโดยปริยาย ไม่มีใครรับผิดชอบงานเหล่านี้อย่างจริงจัง นอกจากช่วงเวลาที่ต้องเตรียมตัวสำหรับการตรวจสอบเท่านั้น” ■

ข้อมูลเชิงลึก

## ความท้าทายด้านไซเบอร์สำหรับธุรกิจขนาดกลาง

Rocco Galletto

Partner, Global Head of Cyber, BDO Canada

“สิ่งที่เราพบเป็นประจำในกลุ่มลูกค้าธุรกิจขนาดกลาง คือ พวกเขาต้องปฏิบัติตามกฎระเบียบที่คล้ายคลึงกับองค์กรขนาดใหญ่แต่มีทีมรักษาความปลอดภัยทางไซเบอร์ขนาดเล็กมาก อาจมีเพียง 5 ถึง 10 คน ที่รับหน้าที่ดูแลความปลอดภัยของทั้งองค์กร”

“ในบางกรณี องค์กรอาจมีพนักงานถึง 2,000 ถึง 4,000 คน แต่มีผู้เชี่ยวชาญด้านความปลอดภัยเพียงไม่กี่คนในการปกป้องธุรกิจทั้งหมด”

ในสถานการณ์เช่นนี้ เราจึงเห็นแนวโน้มที่เพิ่มขึ้นของธุรกิจประเภทนี้ ที่หันมาขอคำปรึกษาจากบริษัทผู้ให้บริการระดับมืออาชีพ เช่น BDO เพื่อช่วยชี้แนะแนวทางในด้านที่องค์กรอาจขาดทรัพยากร

หรือยังไม่มีความเข้าใจเพียงพอว่า องค์กรอื่น ๆ ที่มีขนาดใกล้เคียงกันนั้นจัดการกับความเสี่ยงด้านไซเบอร์อย่างไร

การมี “โปรแกรมความปลอดภัยทางไซเบอร์ที่มีโครงสร้างชัดเจน” เป็นสิ่งสำคัญเพื่อให้องค์กรสามารถ นำหน้าหรืออย่างน้อยทันต่อความเสี่ยงทางไซเบอร์ที่เปลี่ยนแปลงอยู่เสมอ

องค์กรควรพิจารณาความพร้อมในหลายระดับ เช่น: ระบุทรัพย์สินหรือข้อมูลสำคัญทั้งหมดที่ต้องปกป้องในองค์กร ประเมินว่าปัจจุบันมีมาตรการป้องกันอย่างไรบ้าง วางแผนการพัฒนให้สอดคล้องกับการเติบโตขององค์กร “เมื่อองค์กรพัฒนาและเปลี่ยนแปลง มาตรการด้านความปลอดภัยก็ต้องพัฒนาไปพร้อมกัน เพื่อรักษาความมั่นคงปลอดภัยในระดับที่เข้มแข็งอยู่เสมอ” ■

“เมื่อองค์กรพัฒนาและเปลี่ยนแปลง มาตรการด้านความปลอดภัยก็ต้องพัฒนาไปพร้อมกันเพื่อรักษาความมั่นคงปลอดภัยในระดับที่เข้มแข็งอยู่เสมอ”

# เชื่อมช่องว่างระหว่างความเสี่ยงและโอกาสจาก AI

ในขณะที่ ความมุ่งมั่นเชิงบวก กำลังเป็นแรงผลักดันให้เกิด การแข่งขันด้าน AI อย่างดุเดือด บริษัทก็จำเป็นต้อง วางกรอบการจัดการความเสี่ยงให้เหมาะสม

ภาพรวม

สิ่งที่กำลังเปลี่ยนแปลง

บริษัทต่างๆ มองโลกในแง่ดีมากขึ้นเกี่ยวกับโอกาสที่ AI สร้าง และมองว่า AI เป็นความเสี่ยงน้อยลง

ทำไมเรื่องนี้จึงสำคัญ

ธุรกิจอาจมองข้ามหรือประเมินความเสี่ยงจาก AI ต่ำเกินไป ซึ่งอาจส่งผลเสียต่อชื่อเสียงในระยะยาว หรืออาจพัวพันกับปัญหาด้านกฎระเบียบที่ร้ายแรง

ควรทำอย่างไร

ธุรกิจจำเป็นต้องมีกรอบการจัดการความเสี่ยงที่เป็นระบบ เพื่อสามารถนำนวัตกรรม AI มาใช้ได้ อย่างปลอดภัย เพราะหากประเมินผิดพลาด การลงทุนที่ลงไปอาจสูญเปล่าได้ในทันที

ตลอดระยะเวลา 12 เดือนที่ผ่านมา ในขณะที่เทคโนโลยี AI ยังคงพัฒนาอย่างต่อเนื่อง ทศนคติของผู้บริหารต่อความเสี่ยงของ AI ก็ได้เปลี่ยนไปอีกครั้ง โดยปัจจุบันผู้บริหารส่วนใหญ่เริ่มมองเห็น "โอกาส" มากกว่า "ความเสี่ยง"การเปลี่ยนแปลงนี้สะท้อนให้เห็นจากผลการจัดอันดับความเสี่ยงของ AI บนสเกล 1 ถึง 5 (โดย 5 คือความเสี่ยงสูงสุด):ปัจจุบันผู้ตอบแบบสอบถามส่วนใหญ่ (57%) ให้คะแนนความเสี่ยงของ AI ที่ ระดับ 3ในขณะที่ปีก่อน ผู้ตอบแบบสอบถามถึง 52% เคยจัดให้ความเสี่ยงน้อยอยู่ในระดับที่สูงกว่า คือ ระดับ 4

Kirstie Tieman, AI Leader, BDO USA กล่าวว่า: “ตอนนี้อยู่ในจุดเปลี่ยนที่ AI ไม่ใช่เรื่องในเชิงทฤษฎีอีกต่อไป มันอยู่ในมือของทุกคนแล้ว การเข้าถึงได้ง่ายนี้กำลังขับเคลื่อนนวัตกรรม แต่ขณะเดียวกันก็สร้าง 'จุดบอด' ด้วย" ความเสี่ยงที่แท้จริงในตอนนี้คือการมองว่า AI เป็น เครื่องมือสำเร็จรูปที่ใช้ได้ทันที โดยไม่ต้องวางแผน หากไม่มี กรอบการจัดการความเสี่ยงที่แข็งแกร่ง บริษัทอาจ เพิ่มการเปิดรับความเสี่ยงเร็วกว่า ที่พวกเขาจะสามารถสร้างมูลค่าจากมันได้"

Vernie Balasubramaniam, Director of AI, Privacy and Data Protection, BDO UK กล่าวว่า: "อีกหนึ่งเหตุผลของการเปลี่ยนแปลงทัศนคตินี้คือ หลายบริษัทอาจเชื่อว่าความเสี่ยงที่จะ 'ตกขบวน' หากไม่คว้าโอกาสจาก AI นั้น สูงกว่าความเสี่ยงของการใช้งาน AI เสียอีก"

อีกหนึ่งปัญหาที่สำคัญคือ AI ได้ เข้ามามีบทบาทในแทบทุกด้านของธุรกิจ จนทำให้ ผู้บริหารระดับสูงหลายคนอาจไม่ตระหนัก ว่ามีการใช้งาน AI อยู่มากเพียงใด หรือในลักษณะที่ เสี่ยงภัย มากแค่ไหน ▶

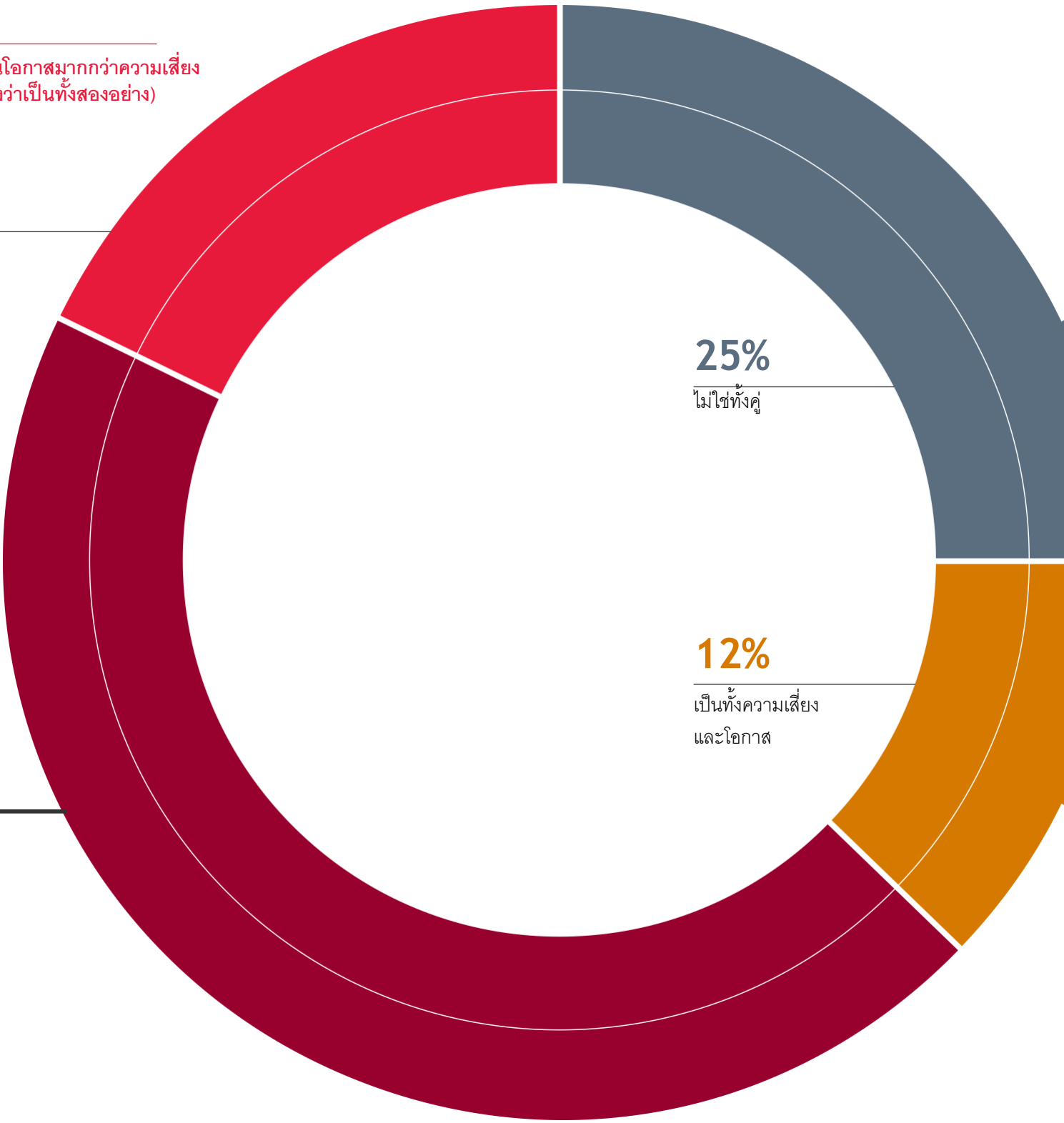
AI ถูกมองว่าเป็นโอกาสมากกว่าความเสี่ยง (แต่บางท่านก็มองว่าเป็นทั้งสองอย่าง)

18%

ความเสี่ยง

45%

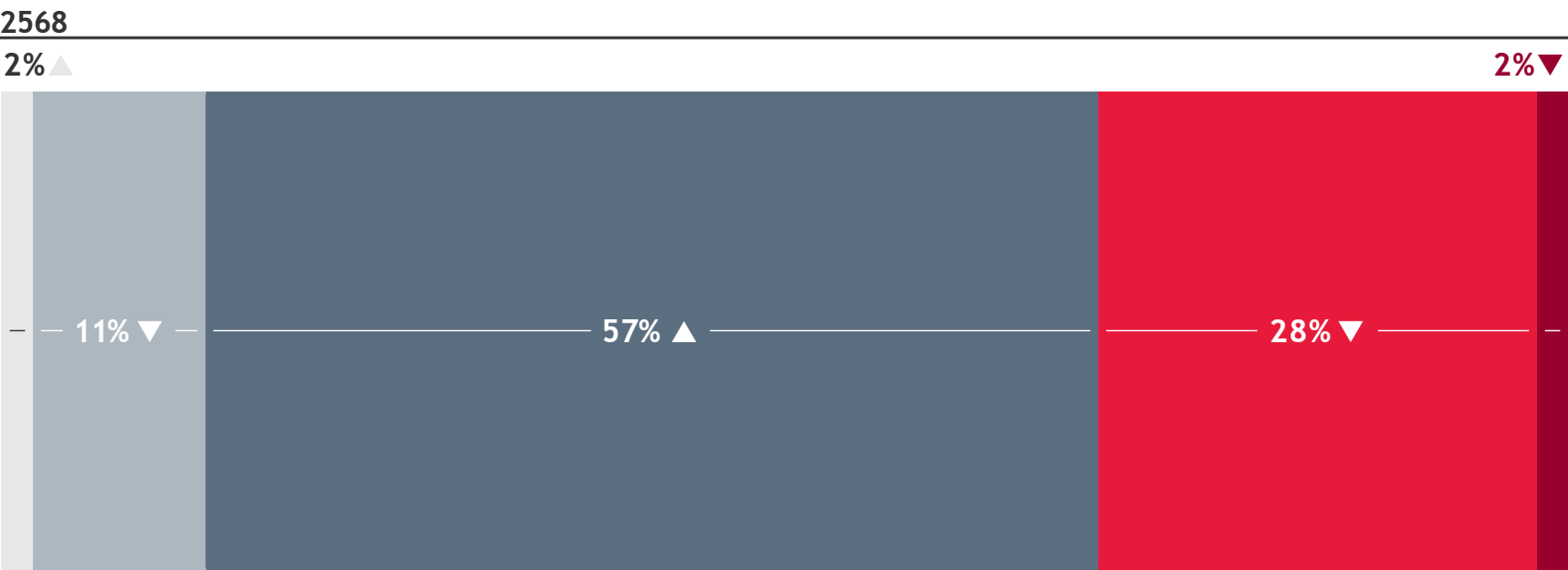
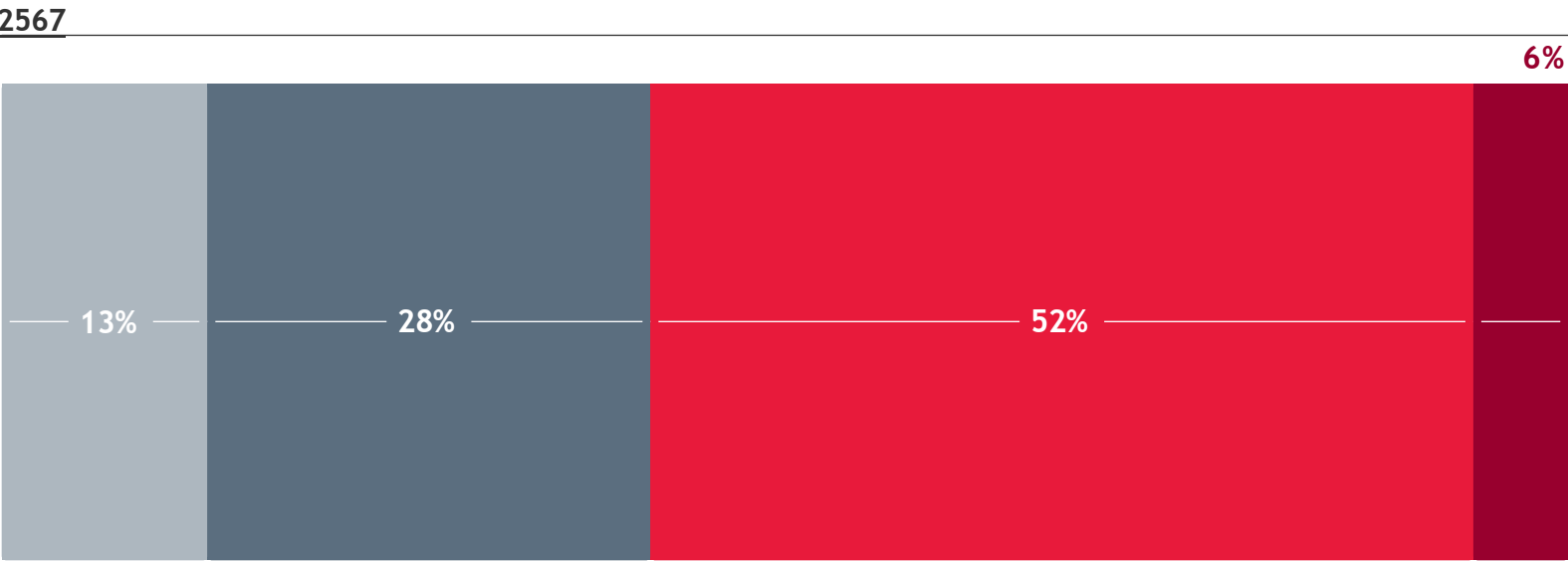
โอกาส



ความกังวลเกี่ยวกับความเสี่ยงด้าน AI ลดลงตั้งแต่ปี 2567

มาตราส่วน

ไม่มีความเสี่ยง 1 2 3 4 5 มีความเสี่ยงอย่างมีนัยสำคัญ



"ทุกอย่างที่มีอยู่และทำให้พวกเขากังวลว่าตนเองอาจเสียเปรียบเพื่อนร่วมงาน" เธอกล่าว มีหลายด้านที่ผู้บริหารเชื่อว่า AI จะส่งผลกระทบต่อธุรกิจของพวกเขาใน 12 เดือนข้างหน้า โดยด้านความปลอดภัยทางไซเบอร์เป็นอันดับหนึ่ง (55%) ตามมาด้วยการตรวจสอบการปฏิบัติตามกฎระเบียบ (52%) และห่วงโซ่อุปทาน (50%)

"การใช้ AI ในการตรวจสอบการปฏิบัติตามกฎเป็นเรื่องดี คุณจะมีข้อมูลมากขึ้นที่ให้ข้อมูลเชิงลึกที่ละเอียดขึ้นเกี่ยวกับความเสี่ยงเฉพาะและใครที่ทำให้องค์กรเสี่ยง" Balasubramaniam กล่าว "นี่หมายความว่า คุณสามารถจัดการความเสี่ยงแบบเรียลไทม์ในด้านต่างๆ เช่น การตรวจจับการฉ้อโกง"

แม้จะมีโอกาสนี้ มีเพียง 31% ของผู้ตอบแบบสอบถามเชื่อว่า AI สามารถช่วยในการระบุความเสี่ยง หรือการตรวจจับและป้องกันการฉ้อโกงได้ ซึ่งเป็นโอกาสที่อาจถูกพลาด และชี้ให้เห็นถึงการขาดความตระหนักถึงเครื่องมือที่มีอยู่

แม้ว่าจะมีความมองโลกในแง่ดีมากขึ้นในกลุ่มผู้บริหาร แต่ก็ยังมีการยอมรับถึงความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีนี้ ผู้ตอบแบบสอบถาม 62% กล่าวว่า AI อาจเพิ่มความเสี่ยงด้านความเป็นส่วนตัว ขณะที่ 56% กล่าวว่า AI อาจเพิ่มความเสี่ยงด้านความปลอดภัยทางไซเบอร์

Tierman กล่าวว่าเป็นไปได้ว่าความเสี่ยงอื่น ๆ อาจถูกมองข้ามไป

"ยังคงมีการประเมินต่ำเกินไปโดยเฉพาะอย่างยิ่งเกี่ยวกับความเสี่ยงจากการทำงานและอคติด้านจริยธรรม" เธอกล่าว "ผู้นำหลายคนเทียบความเสี่ยงของ AI กับความเป็นส่วนตัวของข้อมูลหรือแค่ความลำเอียงของโมเดล และหยุดแค่นั้น ความจริงคือความเสี่ยงตอนนี้รวมถึงความเสี่ยงต่อชื่อเสียง การหยุดชะงักของแรงงาน การทำงานอัตโนมัติมากเกินไป และบางครั้งอาจรวมถึงการสูญเสียความรู้ขององค์กรด้วย"

ในแนวทางเดียวกัน บริษัทบางแห่งอาจประเมินความเสี่ยงโดยรวมต่อบริษัทต่ำเกินไปหากวางกลยุทธ์ AI ผิดพลาด

"พวกเขาไม่เห็นว่าคุณอาจทำให้บริษัทล้มเหลวได้ เช่น ถ้าคุณรวบรวมข้อมูลทั้งหมดไว้ในที่เดียว หากเกิดการละเมิด คุณไม่ได้สูญเสียแค่ฐานข้อมูลเดียว แต่คุณสูญเสียข้อมูลทั้งหมดของคุณ" Balasubramaniam กล่าว

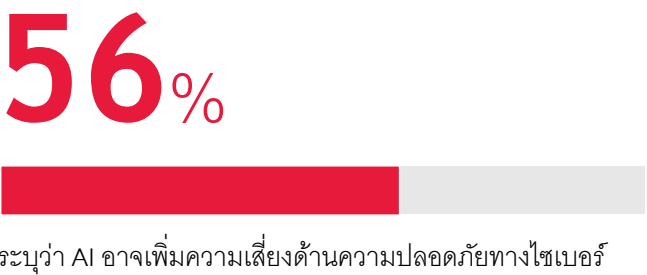
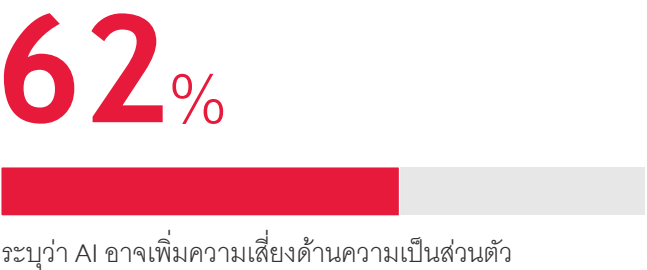
เพื่อหลีกเลี่ยงกับดักเหล่านี้ ธุรกิจจำเป็นต้องทำให้มีการมีส่วนร่วมอย่างกว้างขวางในการสนทนาเกี่ยวกับการลงทุนใน AI โดยเฉพาะในมุมมองของความเสี่ยง

Polly James, Senior Director for Risk Management, Feld Entertainment กล่าวว่า ธุรกิจของเธอมีทีมข้ามสายงานที่ประเมินความเสี่ยงและประโยชน์ร่วมกัน และตกลงกันในกรอบการป้องกันสำหรับโครงการ AI ใหม่ ๆ ▶

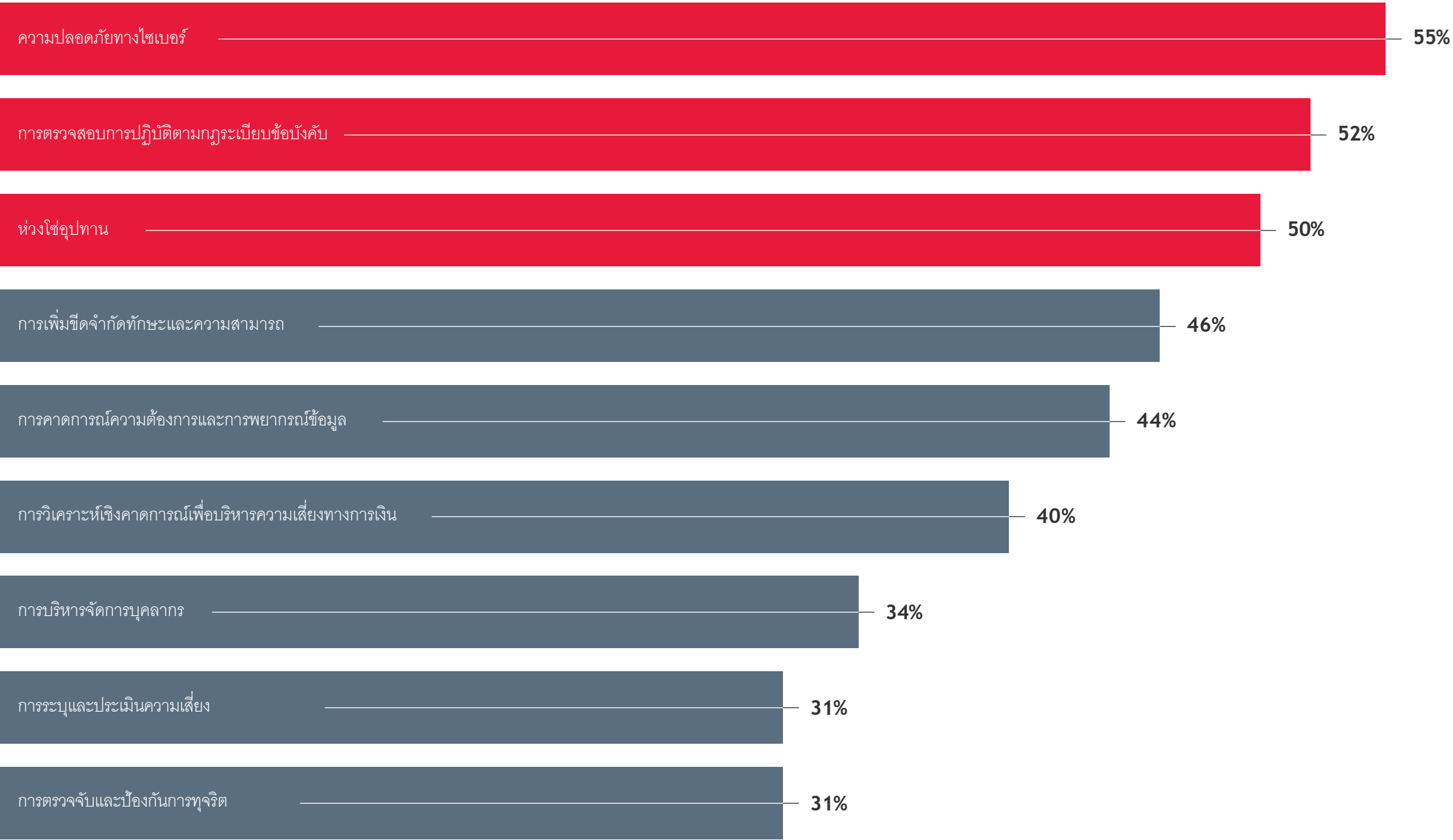
เธอกล่าวว่า: "เราดำเนินการอย่างระมัดระวังและทดลองอย่างค่อยเป็นค่อยไป ไม่ได้กระโดดลงไปอย่างเต็มตัว" "เราได้ จำกัดจำนวนผู้ใช้ และสร้าง มาตรการป้องกัน ที่ชัดเจนเกี่ยวกับผู้ที่สามารถเข้าถึงได้ รวมถึงให้ความมั่นใจว่า ข้อมูลสำคัญจะไม่ถูกป้อนเข้าสู่โมเดลสาธารณะ อย่างแน่นอน"

นอกจากนี้ยังมีความเสี่ยงที่ธุรกิจขนาดเล็กและขนาดกลางอาจพึ่งพาเครื่องมือ AI มากเกินไป เพราะการใช้ AI อาจมีต้นทุนสูงกว่าการจ้างพนักงานเพิ่ม

"ในบริษัทขนาดใหญ่ พวกเขาน่าจะจัดสมดุลได้ถูกต้อง เพราะมีแนวทางที่เป็นระบบมากขึ้นในการยอมรับ AI ดังนั้นธุรกิจขนาดกลางและเล็กจึงน่าจะเสี่ยงที่สุด"Balasubramaniam กล่าว ■



ผลกระทบที่คาดว่าจะเกิดขึ้นจาก AI ภายใน 12 เดือนข้างหน้า



ข้อมูลเชิงลึก

# แนวทางการกำกับดูแลและบริหารจัดการความเสี่ยงจาก AI

## Vernie Balasubramaniam

Director of AI, Privacy and Data Protection, BDO UK

“เราขอแนะนำให้ทุกองค์กรมี ‘กลยุทธ์ด้าน AI’ อย่างชัดเจน มีบุคคลที่รับผิดชอบโดยตรงเกี่ยวกับ AI และจัดตั้ง ‘คณะกรรมการกำกับดูแล AI’ ที่ประกอบด้วยผู้มีส่วนได้ส่วนเสียจากหลายฝ่ายเพื่อให้แน่ใจว่าการบริหารความเสี่ยงจะไม่ขึ้นอยู่กับบุคคลใดบุคคลหนึ่งเพียงคนเดียว แต่มีหลายคนที่รับรู้ และมอง AI ผ่านมุมมองความเสี่ยงและโอกาสที่หลากหลาย”

“อีกหนึ่งสิ่งที่สำคัญคือ การดำเนินโปรแกรมการปฏิบัติตามกฎระเบียบ (compliance) อย่างเป็นระบบตั้งแต่เนิ่น ๆ เพื่อระบุว่ามีการควบคุมใดในปัจจุบันที่สามารถช่วยลดความเสี่ยงจาก AI ได้ โดยไม่ต้องเริ่มต้นจากศูนย์

องค์กรยังต้องทำการเชื่อมโยง (mapping) กฎระเบียบเพื่อให้เข้าใจผลกระทบในระดับโลก ไม่ใช่เพียงเฉพาะในประเทศที่ตนดำเนินธุรกิจอยู่”

## Kirstie Tiernan

AI Leader and Member of Board of Directors, BDO USA

“ความเสี่ยงจาก AI ไม่ใช่ปัญหาทางเทคโนโลยี แต่มันคือจุดอ่อนของภาวะผู้นำ ถ้าคณะกรรมการบริหารไม่รู้ว่าจะต้องถามคำถามอะไรเกี่ยวกับ AI พวกเขาก็ไม่สามารถกำกับดูแลได้อย่างมีประสิทธิภาพ

องค์กรไม่ควรมีแค่หัวหน้าฝ่าย AI เท่านั้น แต่ควรมี รูปแบบการกำกับดูแล (Governance Model) ที่ช่วยให้ผู้นำสามารถพูดและเข้าใจภาษาของความเสี่ยงได้อย่างถูกต้อง พร้อมได้รับการสนับสนุนจากการตรวจสอบอิสระในประเด็นด้านจริยธรรม, อคติ, และความรับผิดชอบต่อ” “หากไม่มีสิ่งเหล่านี้ ความมองโลกในแง่ดีจะกลายเป็นความเสี่ยงที่เปิดช่องให้เกิดปัญหา” ■



# ‘Flexsourcing’: กลยุทธ์ใหม่เพื่อฝ่าวิกฤตห่วงโซ่อุปทาน

ความเสี่ยงทางภูมิรัฐศาสตร์ที่เพิ่มมากขึ้นหมายความว่าองค์กรต่างๆ จำเป็นต้องประเมินห่วงโซ่อุปทานของตนเองอีกครั้ง

ภาพรวม

สิ่งที่กำลังเปลี่ยนแปลง

ความตึงเครียดทางภูมิรัฐศาสตร์และท่าทีสงครามการค้ากำลังเพิ่มความกังวลเกี่ยวกับความยืดหยุ่นของห่วงโซ่อุปทาน และทำให้หลายองค์กรเริ่มทบทวนความสัมพันธ์กับคู่ค้าอีกครั้ง

ทำไมเรื่องนี้จึงสำคัญ

ธุรกิจจำนวนมากได้รับผลกระทบอย่างหนักในช่วงโควิด-19 เพราะพึ่งพาคู่ค้ารายเดียวที่อยู่ห่างไกลจากผู้บริโภค ส่งผลต่อความพร้อมของสินค้าและผลกำไรของธุรกิจ

ควรทำอะไร

ธุรกิจต่างๆ จำเป็นต้อง ลงทุนในแนวทางใหม่ ๆ เพื่อลดความเสี่ยงใน ห่วงโซ่อุปทานทางกายภาพ โดยใช้กลยุทธ์แบบ 'Flexsourcing' ซึ่งเป็นการผสมผสาน ระหว่างการจัดหาจากแหล่งใกล้เคียง (Nearshoring) และการจัดหาจากประเทศที่เป็นมิตร (Friendshoring)

ความเสี่ยงในห่วงโซ่อุปทานยังคงติดอันดับ 2 ในรายการความเสี่ยงที่ผู้นำธุรกิจรู้สึก ว่า “ไม่พร้อมรับมือมากที่สุด” นับตั้งแต่การสำรวจนั้น สถานการณ์ทั่วโลกยังมีแนวโน้มเลวร้ายลง โดยเฉพาะจากความตึงเครียดทางการค้า เช่น สงครามการค้าระหว่างสหรัฐฯ กับประเทศที่เคยเป็นพันธมิตรทางเศรษฐกิจ

หลังโควิด-19 แนวโน้มของ Nearshoring เริ่มเติบโตขึ้น เพราะองค์กรต้องการลดระยะห่างระหว่างคู่ค้ากับลูกค้าล่าสุด หลายบริษัทเริ่มหันมาใช้รูปแบบผสมที่ยืดหยุ่นมากขึ้น เช่น Flexsourcingซึ่งผสมผสานความคล่องตัว ทั้งจากการใช้คู่ค้าเดิมและการหาทางเลือกใหม่

“Flexsourcing มีความสำคัญเพิ่มขึ้นอย่างมาก เพราะด้วยภาษีใหม่ที่กำลังถูกเสนอในหลายประเทศ บริษัทต่าง ๆ กำลังพิจารณาย้ายฐานการผลิต ซึ่งจะนำมาซึ่งประเด็น compliance ชุดใหม่ทั้งหมด” Dave Arick, Managing Director for Global Risk Management at Sedgwick กล่าว “เราคงเห็นแล้วว่าจากช่วงโควิดว่า การพึ่งพาคู่ค้าเพียงรายเดียว คือสูตรแห่งหายนะ ดังนั้นความยืดหยุ่น ไม่ใช่แค่การใช้คู่ค้าให้มีประสิทธิภาพ แต่รวมถึงการหาแหล่งใหม่กลายเป็นเรื่องจำเป็นมากในโลกปัจจุบัน”

อย่างไรก็ตาม ผู้นำธุรกิจส่วนใหญ่ระบุว่าแนวทางหลักในการลดความเสี่ยงในห่วงโซ่อุปทานทางกายภาพใน 2 ปีข้างหน้า ได้แก่: การตรวจสอบสถานะคู่ค้า (Due diligence) เพิ่มขึ้น 60%การใช้เครื่องมืออนิเตอร์ดิจิทัลเพิ่มขึ้น 58%ซึ่งอาจจะสะท้อนให้เห็นว่าการปรับเปลี่ยนห่วงโซ่อุปทานจริง ๆ ยังเป็นเรื่องยาก(โดย Nearshoringอยู่ท้ายสุดในลิสต์ เพียง 41% เท่านั้นที่ให้ ความสำคัญ)

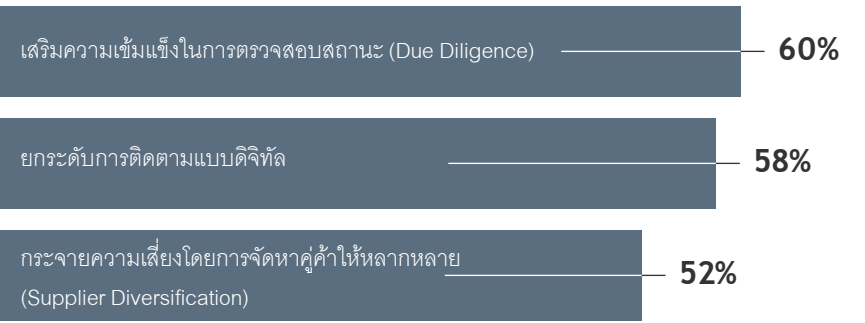
“มันไม่ใช่ทางลัดที่ได้ผลทันที แต่มันคือเกมเชิงกลยุทธ์ระยะยาว” Fraser Paget, Head of Supply Chain and Logistics Advisory at BDO UK. กล่าว “และมันก็เกี่ยวข้อง กับต้นทุนด้วย Nearshoring อาจจะดีกว่าในระยะยาว แต่แน่นอนว่าราคาแพงกว่า”

ผู้บริหารยังกล่าวเพิ่มเติมว่าพวกเขากำลัง เสริมความแข็งแกร่งของห่วงโซ่อุปทานด้านดิจิทัล ด้วยการ:ตรวจสอบผู้ให้บริการดิจิทัลเป็นประจำ (62%)ลงทุนในเครื่องมืออนิเตอร์ดิจิทัลขั้นสูง (56%)เสริมความแข็งแกร่งให้ข้อตกลงการแบ่งปันข้อมูล (56%)

ในอดีต การลงทุนด้านดิจิทัลมักเน้นไปที่ระบบการเงินและการตลาดแต่ตอนนี้ ฝ่ายไอซิสติกส์กำลังเริ่มไล่ตามให้ทัน

“เมื่อมองย้อนกลับไปที่ตลอด 5 ปีที่ผ่านมา ผมคิดว่าแนวคิดของผู้บริหารกำลังเปลี่ยนไปอย่างชัดเจน” Paget กล่าวเสริม

## 3 วิธีหลักที่บริษัทต่างๆ กำลังเสริมสร้างห่วงโซ่อุปทานทางกายภาพของตน



## 3 วิธีหลักที่บริษัทต่างๆ กำลังเสริมสร้างห่วงโซ่อุปทานดิจิทัลของตน



ข้อมูลเชิงลึก

## การปรับเปลี่ยนห่วงโซ่อุปทาน

### Fraser Paget

Head of Supply Chain and Logistics Advisory, BDO UK

“เป็นที่น่าสังเกตว่า ห่วงโซ่อุปทาน (Supply Chain) มักเป็นส่วนที่ ได้รับการลงทุนด้านเทคโนโลยีน้อยเกินไป แต่ปัจจุบันกลับต้องเร่งปรับตัว เนื่องจากเป็น จุดที่มีความเสี่ยงสูงยิ่งแม้ว่า ปัญญาประดิษฐ์ (AI) จะมีศักยภาพสูงในการช่วยงานด้าน การพยากรณ์ แต่ก็มีความท้าทายที่สำคัญ ยิ่งองค์กรมีขนาดใหญ่ การนำเทคโนโลยีใหม่เข้ามา หรือการเปลี่ยนแปลงระบบเดิมที่ฝังรากลึกยิ่งทำได้ยากลำบากด้วยเหตุนี้ บริษัทขนาดใหญ่ จำนวนมากจึงยังคง ยึดติดกับระบบเก่า เพราะมองว่า "การจัดการกับการเปลี่ยนแปลงครั้งใหญ่นั้นเป็นภาระที่เกินกำลัง" และมักตัดสินใจด้วยประโยชน์สั้น ๆ ว่า "ขอใช้ของเดิมไปก่อน”

ธุรกิจขนาดใหญ่มัก ปรับตัวได้ยาก เมื่อต้องเผชิญกับการเปลี่ยนแปลงและลงทุนใหม่ ๆ อยู่ตลอดเวลา เนื่องจากไม่พร้อมรับมือกับความเปลี่ยนแปลงครั้งใหญ่ที่เกิดขึ้น

โครงการเปลี่ยนแปลงขนาดใหญ่ (Large-scale transformation projects) สามารถส่งผลกระทบให้ ผลประกอบการทางการเงินของธุรกิจหยุดชะงัก ได้อย่างรุนแรงกรณีศึกษาที่เห็นได้ชัด กรณี Mothercare เผชิญกับความล้มเหลวส่วนหนึ่งเนื่องจาก สินค้าขาดตลาด หลังจากการติดตั้งระบบบริหารจัดการคลังสินค้าใหม่ กรณี KFC ประสบปัญหาใหญ่ในการ จัดส่งไก่ตามคำสั่งซื้อ เมื่อมีการเปลี่ยนผู้ให้บริการด้านโลจิสติกส์ผู้นำระดับสูงจึงต้องตระหนักว่าการลงทุนในเทคโนโลยีส่งผลกระทบต่อโครงสร้างพื้นฐานทางธุรกิจทั้งหมด (Business Infrastructure) ไม่ใช่แค่ตัวเทคโนโลยีเองเท่านั้น การเปลี่ยนแปลงใด ๆ จึงต้องได้รับการจัดการด้วยความรอบคอบสูงสุด

“หากคุณเป็น ร้านขายของชำ (Grocer) แล้ว ไม่สามารถนำสินค้าไปถึงซูเปอร์มาร์เก็ตได้ หรือเป็น ธุรกิจอีคอมเมิร์ซ ที่ ไม่สามารถจัดส่งสินค้าให้ลูกค้าได้ตามคำสั่งซื้อ... คุณก็ไม่มีธุรกิจเหลืออยู่ดังนั้น คุณต้อง ทดสอบความเสี่ยงทางเทคโนโลยี (Stress Test) และ วิเคราะห์ความเสี่ยง อย่างถี่ถ้วน เพื่อให้มั่นใจว่าคุณสามารถ ย้อนกลับไปใช้ระบบเดิม (Roll Back) ได้ หากทุกอย่างไม่เป็นไปตามแผนที่วางไว้” ■

“เมื่อคุณอยู่ในวัฏจักรของ การจัดการการเปลี่ยนแปลง และ การลงทุนใหม่อย่างต่อเนื่อง ธุรกิจขนาดใหญ่มักจะลำบาก เพราะรับมือกับความไม่แน่นอนเหล่านั้นได้ยาก”

# จัดการความเสี่ยงทุจริต: ปิดทุกช่องโหว่

กระแสความนิยมและการเติบโตของเทคโนโลยี AI ที่กำลังเกิดขึ้นอย่างต่อเนื่อง อาจทำให้ องค์กรต่าง ๆ ตกอยู่ในความเสี่ยงต่อภัย Deepfake มากยิ่งขึ้น

ภาพรวม

สิ่งที่กำลังเปลี่ยนแปลง

การเติบโตของเทคโนโลยี AI กำลังเพิ่มความซับซ้อนในภูมิทัศน์ความเสี่ยงด้านการทุจริต โดยช่วยให้มิจฉาชีพสามารถหลอกลวงพนักงานได้ง่ายขึ้นผ่านเทคโนโลยี Deepfake

ทำไมเรื่องนี้จึงสำคัญ

พนักงานอาจถูกหลอกให้มอบข้อมูลสำคัญ หรือแม้กระทั่งอนุมัติการโอนเงินโดยไม่ตั้งใจ

ควรทำอย่างไร

การฝึกอบรมอย่างต่อเนื่องเกี่ยวกับการควบคุมภายใน (Internal Controls) เป็นสิ่งสำคัญในการลดความเสี่ยงจากการทุจริต เนื่องจากเหตุการณ์ส่วนใหญ่เกิดจากการไม่ปฏิบัติตามขั้นตอนควบคุมอย่างถูกต้อง

การฉ้อโกง (Fraud) เป็นความเสี่ยงที่อาจ ถูกประเมินค่าต่ำไป และบางครั้งก็ ถูกเข้าใจผิด ในองค์กรมีผู้บริหารเพียง 15% เท่านั้น ที่ระบุว่า การฉ้อโกงเป็นหนึ่งใน สามความเสี่ยงสูงสุด ของตน ซึ่งถือเป็นระดับความสำคัญที่ เท่าเทียมกับปัญหาอื่น ๆ เช่น ความเสียหายต่อแบรนด์ หรือการเข้าถึงแหล่งเงินทุน

การฉ้อโกงนำมาซึ่ง ต้นทุนที่สูงมากสำหรับธุรกิจ ผู้ตรวจสอบการฉ้อโกงประเมินว่า องค์กรต่าง ๆ สูญเสียรายได้ถึง 5% ต่อปี กับการฉ้อโกงภายใน (Occupational Fraud) ซึ่งเป็นการฉ้อโกงที่กระทำโดยพนักงานของตนเอง (อ้างอิงจาก ACFE)ยิ่งไปกว่านั้น การเกิดขึ้นของเทคโนโลยี AI ยังได้สร้างโอกาสให้ กลุ่มมิจฉาชีพมืออาชีพ สามารถแทรกซึมเข้าสู่บริษัทโดยใช้ Deepfake ได้อย่างแนบเนียนทั้งหมดนี้หมายความว่า: บริษัทต่าง ๆ จำเป็นต้อง ให้ความสำคัญกับความเสี่ยงจากการฉ้อโกงมากขึ้น อย่างเร่งด่วน โดยเฉพาะการจัดการกับช่องโหว่ที่เกิดจากเทคโนโลยีใหม่

Glenn Pomerantz, Partner และ Global Head of Forensics ที่ BDO USA กล่าวว่า "บางครั้งมันต้องเกิดจากคู่แข่งในอุตสาหกรรม ถูกโจมตี หรือ ขาวใหญ่ หรือแม้แต่เหตุการณ์เล็ก ๆ ที่กระทบองค์กรของตนเองโดยตรง จึงจะสามารถ 'ปลุก' องค์กรให้ตื่นตัวได้" "ไม่มีการเฉลิมฉลองใหญ่โตสำหรับการ ป้องกันการฉ้อโกง ที่สำเร็จ แต่หากคุณตกเป็นเหยื่อของการรัยยกเงิน 50 ล้านดอลลาร์ เรื่องนั้นจะ เป็นที่รับรู้กันอย่างแพร่หลาย"

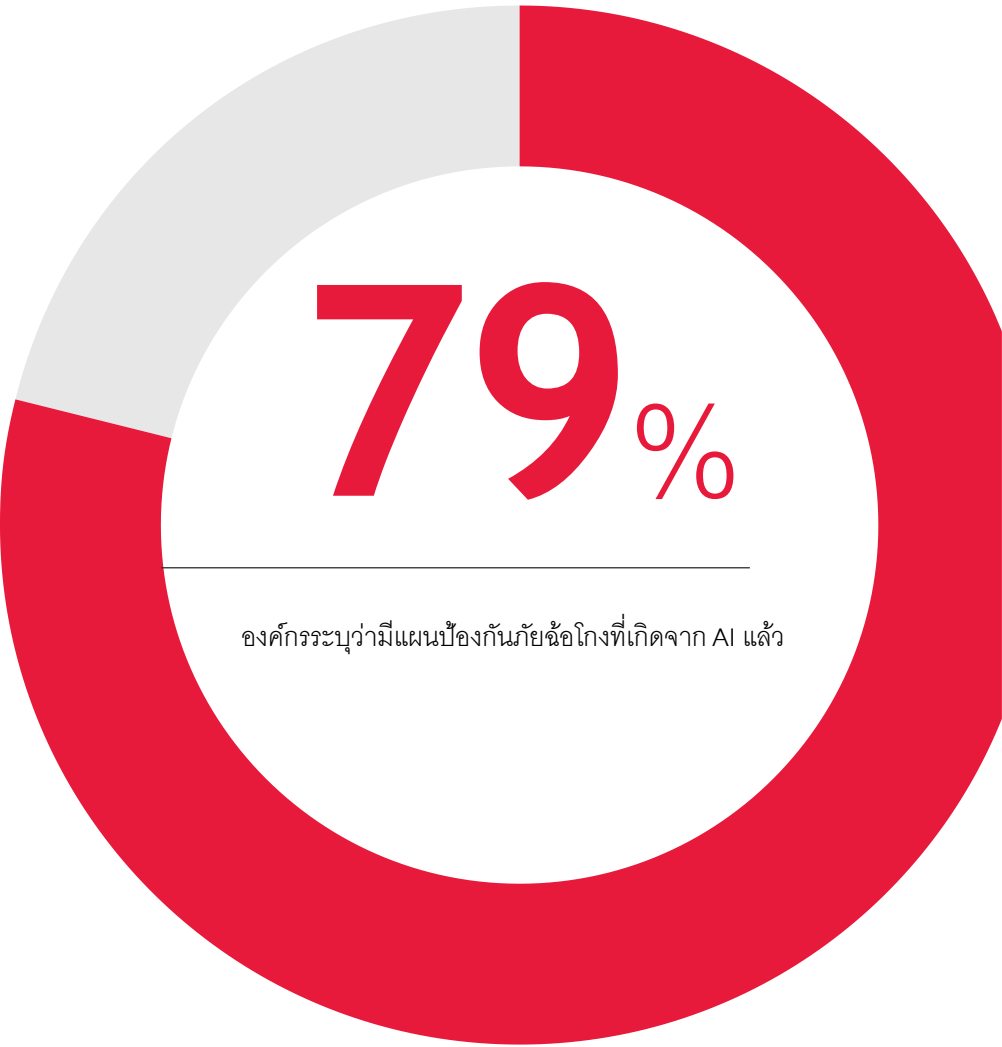
Pomerantz กล่าวว่า การฉ้อโกง มักเกิดขึ้น ไม่ใช่เพราะขาดมาตรการควบคุม (Controls) ที่เหมาะสม แต่เป็นเพราะมาตรการเหล่านั้น ไม่ได้ถูกปฏิบัติตามอย่างถูกต้อง

เขากล่าวว่า: "ความเสียหาย (Breakdown) มักเกิดขึ้นเสมอ มันเกือบจะเหมือนกับ ความตายและการเสียภาษี (Death and Taxes) ที่ไม่มีวันหายไปไหน แต่บางบริษัทก็พยายามมากกว่าบริษัทอื่น"

ปัจจุบัน องค์กรส่วนใหญ่ ได้ให้ความสำคัญกับภัยคุกคามจาก AI อย่างจริงจัง โดย 79% ระบุว่าพวกเขามี แผนรับมือการฉ้อโกงที่ใช้ AI เป็นเครื่องมือ (AI-enabled fraud) อย่างไรก็ตาม ตัวเลขนี้ยังคงหมายความว่า หนึ่งในห้าของบริษัท (21%) อาจยัง มีความเปราะบาง และเสี่ยงต่อการถูกโจมตีจากการฉ้อโกงรูปแบบใหม่นี้

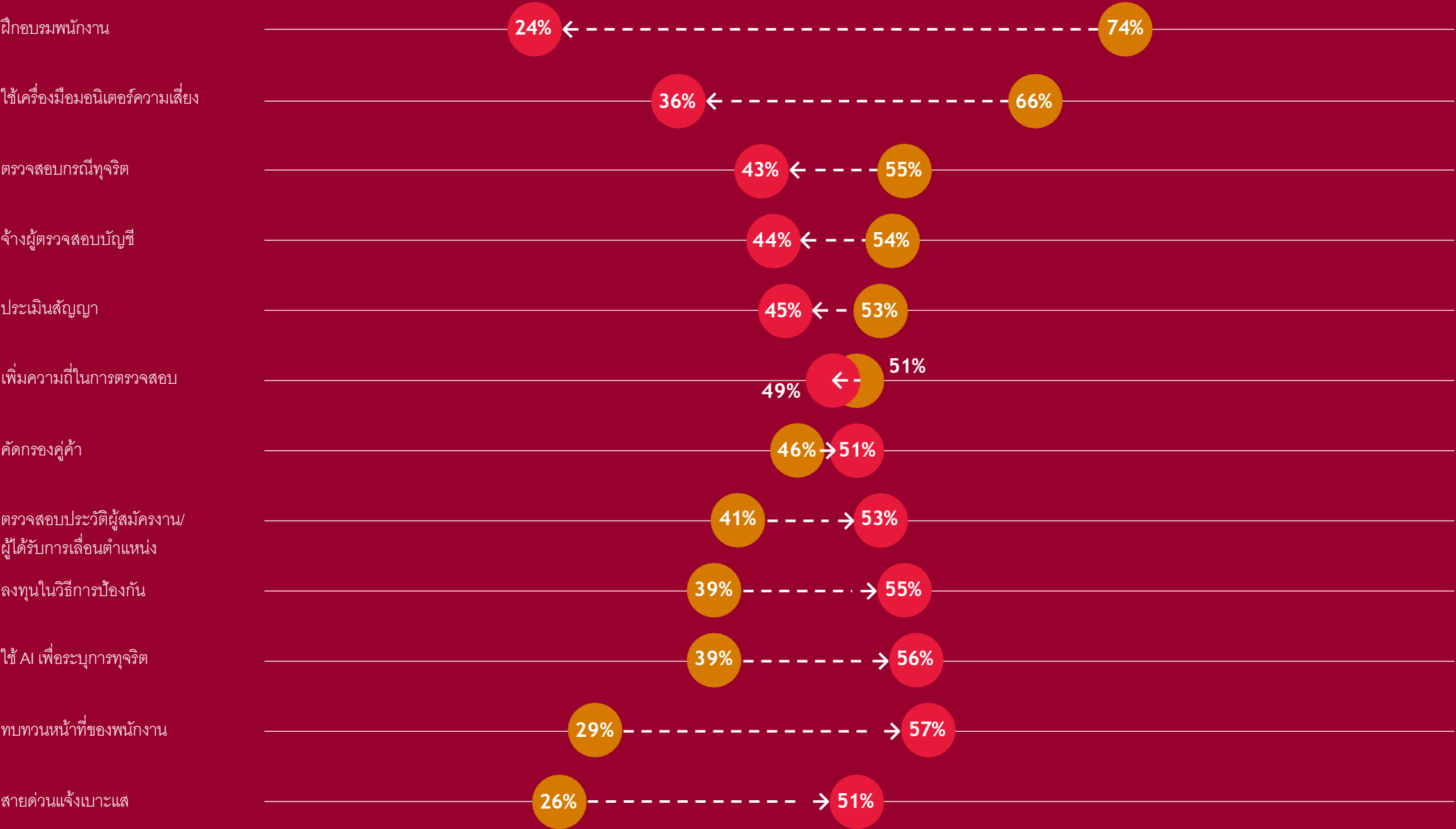
ปัจจุบัน บริษัทต่าง ๆ ได้ใช้มาตรการหลักหลายอย่างเพื่อรับมือกับการฉ้อโกง โดย 74% ให้ความสำคัญกับการฝึกอบรมพนักงาน (Staff Training) 66% ลงทุนใน เครื่องมือตรวจสอบความเสี่ยง (Risk-Monitoring Tools) 55% ดำเนินการ ตรวจสอบการฉ้อโกง (Fraud Checks) สิ่งที่น่ากังวลคือ เมื่อถูกถามถึงสิ่งที่พวกเขาจะให้ความสำคัญเป็นอันดับแรกในอีกสองปีข้างหน้า มีผู้ตอบแบบสอบถามเพียง 24% เท่านั้น ที่ระบุว่า การฝึกอบรมพนักงานยังคงเป็นสิ่งสำคัญอันดับต้น ๆ

Pomerantz กล่าวว่า: "มีความ เข้าใจผิด ที่ว่า การฝึกอบรมพนักงานเป็นสิ่งที่ต้องทำ เพียงแค่ครั้งเดียวก็เพียงพอแล้ว "



การรับมือกับการทุจริต: การฝึกอบรมพนักงานและการลงทุนในเครื่องมือตรวจสอบคือสิ่งที่เราต้องให้ความสำคัญและดำเนินการทันทีในวันนี้

● การดำเนินการในปัจจุบัน ● การดำเนินการในอีก 2 ปีข้างหน้า



"การฝึกอบรมไม่ใช่สิ่งที่ทำครั้งเดียวจบ ต้องมีการทบทวนและเสริมความรู้อยู่เสมอ เพราะพนักงานที่ได้รับการฝึกเมื่อ 3 ปีที่แล้ว อาจมีถึงหนึ่งในสามที่ลาออกไปแล้ว"

อย่างไรก็ตาม ธุรกิจอาจ มองข้ามโอกาสสำคัญในการตรวจจับการทุจริตภายในองค์กรเพราะมีเพียง 26% เท่านั้นที่ระบุว่า "การติดตั้งสายด่วนแจ้งเบาะแส (Whistleblower hotline)" เป็นหนึ่งในแนวทางต่อสู้กับการทุจริต ถือว่าเป็น กลยุทธ์ที่มีคะแนนต่ำที่สุดในการสำรวจ ซึ่งน่าสนใจ เพราะข้อมูลจาก ACFE (Association of Certified Fraud Examiners)ระบุว่า 43% ของการทุจริตถูกตรวจพบจากการแจ้งเบาะแส ไม่ใช่จากการตรวจสอบหรือระบบ

อย่างไรก็ตาม Glenn Pomerantz ให้ความเห็นว่า "สถิตินี้อาจไม่ใช่เรื่องผิดปกติ เพราะหลายองค์กรอาจ 'มีระบบแจ้งเบาะแสที่ใช้งานได้แล้ว' จึงไม่ได้มองว่าเป็นสิ่งใหม่ที่ต้องทำเพิ่มเติม" ■

ข้อมูลเชิงลึก

## ขจัดความเข้าใจผิดเพื่อบริหารความเสี่ยงการทุจริต

### Glenn Pomerantz

Partner, Global Head of Forensics, BDO USA

“การตรวจสอบประวัติของพนักงานใหม่ถือเป็นหนึ่งในกระบวนการควบคุมความเสี่ยงภายในองค์กร ไม่ว่าจะเป็นการตรวจสอบประวัติส่วนตัว หรือการเช็คข้อมูลจากผู้ว่าจ้างเดิม

แต่ในหลายกรณี การตรวจสอบเหล่านี้กลับไม่เข้มงวดพอ และมักละเลยการอ้างอิงจากผู้ว่าจ้างเดิม ซึ่งตอกย้ำให้เห็นถึงความสำคัญของการ ‘ตรวจสอบให้ครบถ้วน’ ก่อนจ้างงาน”

ผมเห็นว่าองค์กรต่าง ๆ อยู่บน ‘แนวทาง’ ที่แตกต่างกัน บางแห่งก็แค่ทำตามเช็คลิสต์และติ๊กถูกลงในช่องของการตรวจสอบประวัติเพื่อให้ผ่านตามข้อกำหนดด้านการปฏิบัติตามกฎระเบียบข้อบังคับ (compliance) ในขณะที่บางองค์กรตรวจสอบอย่างละเอียด โดยเฉพาะกับพนักงานในตำแหน่งที่ต้องได้รับความไว้วางใจ

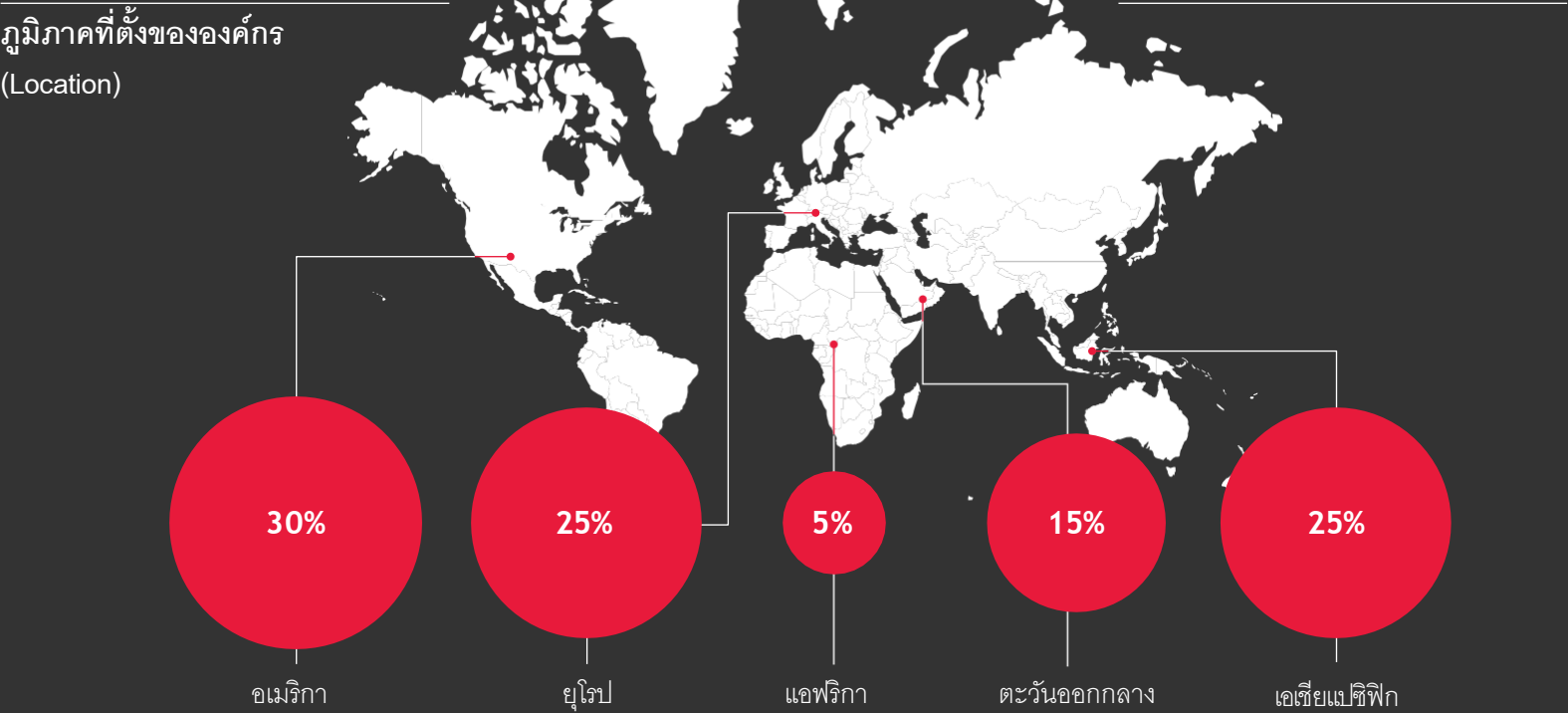
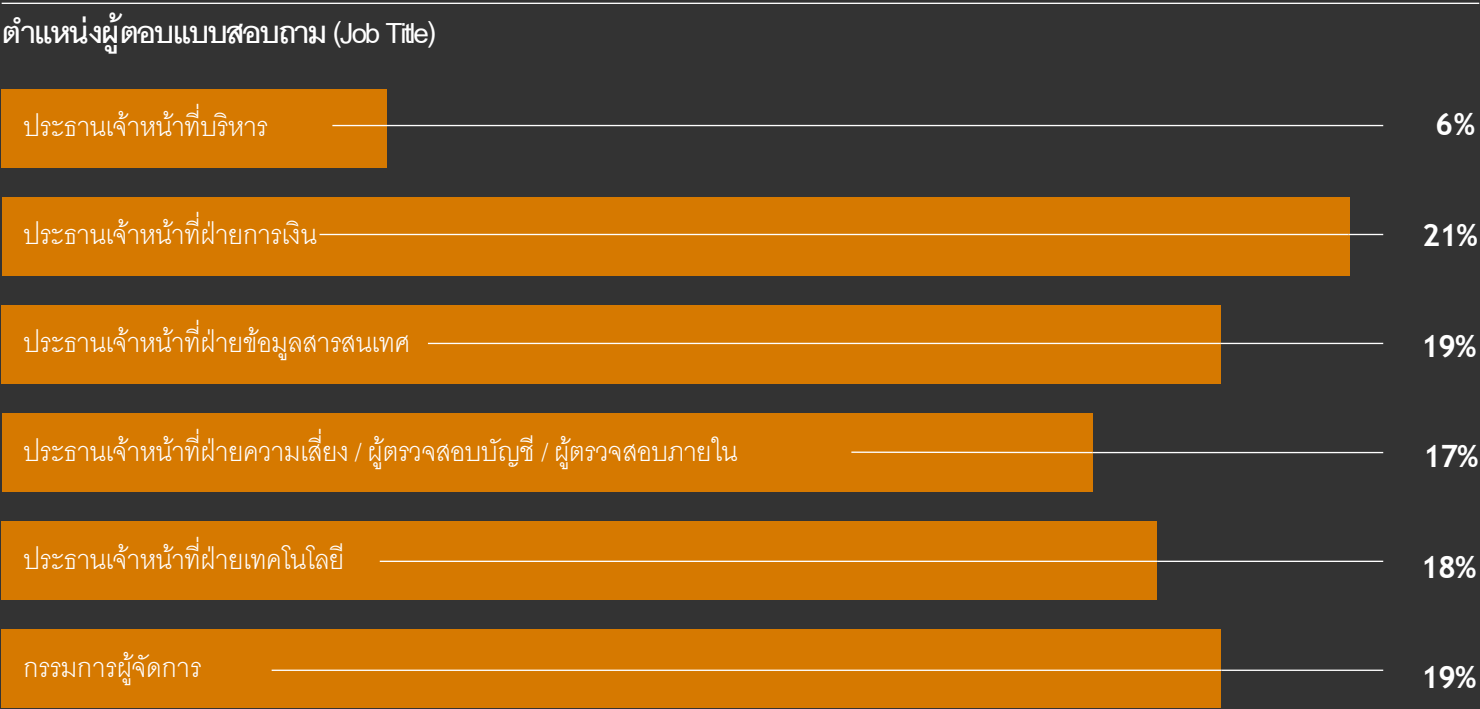
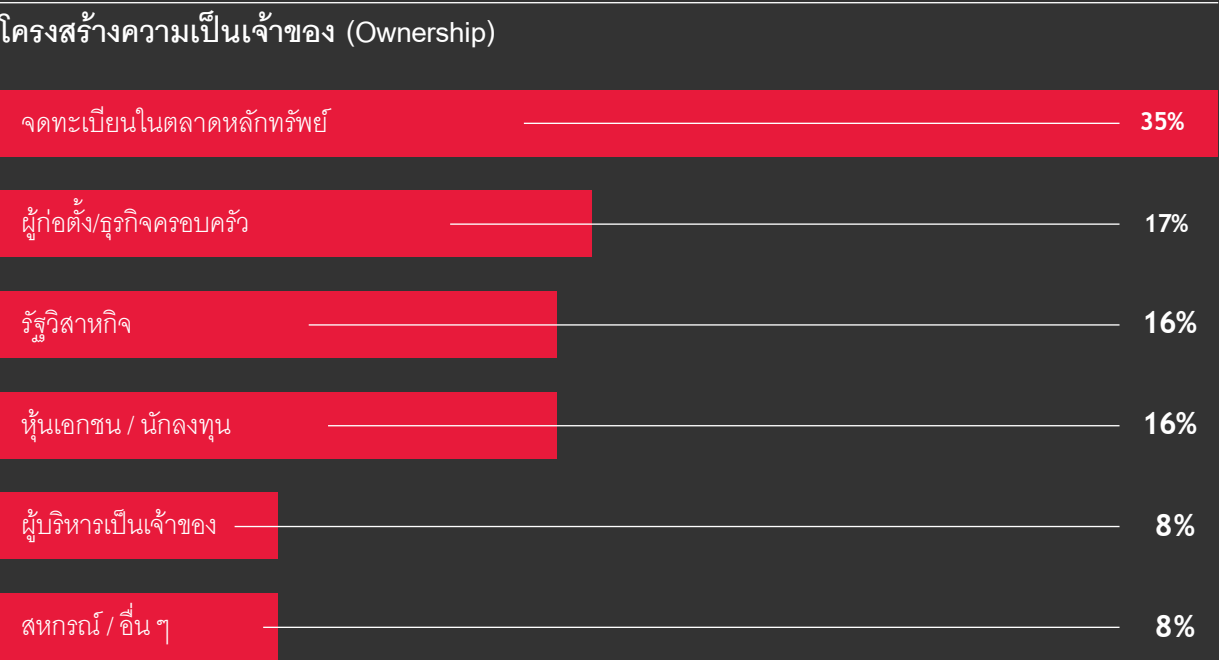
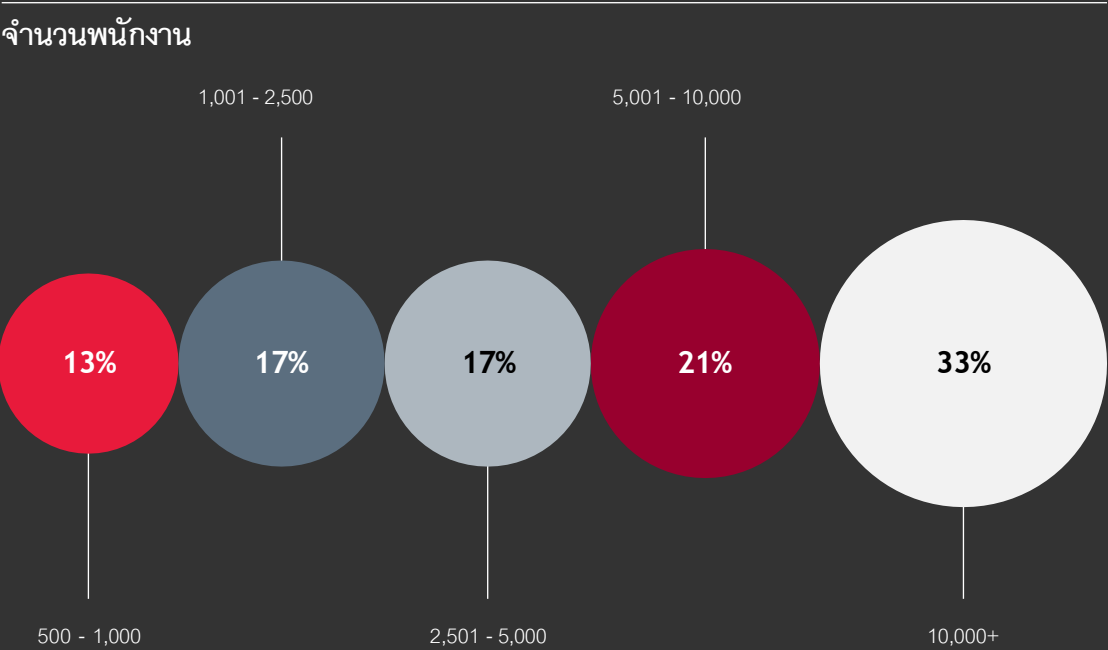
ข้อเสนอแนะของฉันคือ ให้คุณลองโทรศัพท์ไปคุยกับอดีตนายจ้างของผู้สมัครดูคุณอาจพบว่า ประมาณ 50% ของพวกเขายินดีพูดคุยด้วย และ 90% ของกลุ่มที่คุยด้วยนั้น จะให้ข้อมูลเชิงลึกแบบไม่เป็นทางการ (Off the Record) ซึ่งสามารถช่วยให้คุณ ตัดสินใจจ้างงานได้อย่างมีข้อมูลและรอบด้านมากยิ่งขึ้น” ■

“ผมเห็นว่าองค์กรต่าง ๆ มีแนวทางที่หลากหลาย บางแห่งเพียงแค่ทำตามเช็คลิสต์และติ๊กถูกในช่องของการตรวจสอบประวัติเพื่อให้ผ่านตามข้อกำหนดด้านการปฏิบัติตามกฎระเบียบข้อบังคับ (compliance) ในขณะที่บางแห่งดำเนินการตรวจสอบอย่างเข้มงวดกับพนักงานที่อยู่ในตำแหน่งซึ่งต้องได้รับความไว้วางใจ”

# ระเบียบวิธีวิจัยและข้อมูล ประชากรกลุ่มตัวอย่าง

BDO และ alan. agency ได้ทำการสำรวจผู้บริหารระดับสูงจำนวน 500 คน (รวมถึง CEO, CFO, CRO, CTO และผู้บริหารระดับสูงอื่นๆ) จากธุรกิจหลากหลายอุตสาหกรรมทั่วโลก ได้แก่ บริการทางการเงินพลังงานและสาธารณูปโภคการดูแลสุขภาพและวิทยาศาสตร์ชีวภาพการผลิตกองทุน Private Equityและอุตสาหกรรมอื่นๆ โดยทุกองค์กรที่เข้าร่วมการสำรวจมีพนักงานอย่างน้อย 500 คนรายได้ต่อปีขั้นต่ำ 100 ล้านดอลลาร์สหรัฐ

การเก็บข้อมูลภาคสนามดำเนินการโดย iResearch Consulting Groupระหว่างวันที่ 24 มกราคม ถึง 17 กุมภาพันธ์ 2568



FOR MORE INFORMATION:

KOEN CLAESENS

Global Head of Risk Advisory Services, BDO Belgium

[koen.claessens@bdo.be](mailto:koen.claessens@bdo.be)

The BDO network (referred to as the 'BDO network') is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision with the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium. Each of the BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

Copyright © June 2025 BDO LLP. All rights reserved. Published in the UK.

[www.bdo.global](http://www.bdo.global)

