แบบสอบถามการวิจัย เลขที่แบบสอบถาม.....

เรื่อง "ความสามารถสำหรับสร้างความคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม"

คำชี้แจง

แบบสอบถามนี้ได้จัดทำขึ้นเพื่อสอบถามความคิดเห็นในประเด็นของ **ความสามารถสำหรับสร้างความคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทาน เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม** ผู้วิจัยจึงใคร่ขอความร่วมมือในการตอบแบบสอบถาม โดยอนุเคราะห์ให้ข้อมูลหรือแสดงความคิดเห็นที่ตรงกับความเป็นจริง ความรู้สึก หรือความคิดเห็นของท่านมากที่สุด ข้อมูลที่ได้จะนำไปใช้ประกอบการศึกษาและจะใช้เพื่อประโยชน์ด้านวิชาการเท่านั้น ผู้วิจัยขอรับรองว่าข้อมูลที่ได้จากแบบสอบถามจะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายกับท่านหรือผู้ที่เกี่ยวข้องแต่ประการใด ข้อคำถามในแบบสอบถาม แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลทั่วไปขององค์กรท่าน

ส่วนที่ 2 ข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัทท่าน

ส่วนที่ 3 ความคิดเห็นเกี่ยวกับความสามารถสำหรับสร้างความคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทาน

ส่วนที่ 4 ความคิดเห็นเกี่ยวกับความร่วมมือกันของโซ่อุปทาน

ส่วนที่ 5 ความคิดเห็นเกี่ยวกับปัญหาภัยคุกคามทางไซเบอร์

ส่วนที่ 6 ความคิดเห็นเกี่ยวกับการจัดการเสี่ยงทางไซเบอร์ของโซ่อุปทาน

ส่วนที่ 7 ข้อมูลสภาพการดำเนินงานที่เกี่ยวข้องกับการจัดการความต่อเนื่องทางธุรกิจ

ใน **ส่วนที่ 1** และ **2** โปรดพิจารณาข้อคำถาม แล้วทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับข้อเท็จจริงของท่าน สำหรับ **ส่วนที่ 3 - 7** ขอให้ท่านพิจารณาข้อคำถาม แล้วทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับความคิดเห็นหรือความรู้สึกของท่านมากที่สุดเพียงช่องเดียว โดยแบ่งระดับคำตอบเป็น 5 ระดับ ดังนี้

5	หมายถึง	ระดับมากที่สุด
4	หมายถึง	ระดับมาก
3	หมายถึง	ระดับปานกลาง
2	หมายถึง	ระดับน้อย
1	หมายถึง	ระดับน้อยที่สุด

ผู้วิจัย

นายนริส อุไรพันธ์ E-mail: naris080515@yahoo.com โทรศัพท์ : 062-807-5550

นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาการวิชาจัดการโลจิสติกส์และโซ่อุปทาน

วิทยาลัยโลจิสติกส์และซัพพลายเชน มหาวิทยาลัยศรีปทุม

นิยามศัพท์ที่ใช้ในการวิจัย

1. ไซเบอร์ (Cyber) มีความหมายว่าเกี่ยวข้องกับคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ หรืออินเทอร์เน็ต หรือความเป็นจริงเสมือน (Virtual Reality) เช่น ไซเบอร์สเปซ (Cyberspace) หมายถึง สภาพแวดล้อมสมมติในเครือข่ายอินเทอร์เน็ต
2. ตัวแบบวุฒิภาวะความสามารถ (Capability Maturity Model) หมายถึง เป็นต้นแบบของการวัดวุฒิภาวะความสามารถในการทำงาน ความสำเร็จในการทำงานใด ๆ ในอนาคตของบริษัทหรือหน่วยงาน ขึ้นอยู่กับระดับวุฒิภาวะความสามารถในการทำงานของบริษัทหรือหน่วยงานนั้นในทำนองเดียวกันวุฒิภาวะความสามารถของบริษัทหรือหน่วยงานนั้น ก็ขึ้นอยู่กับผลการทำงานในอดีตของบริษัทหรือหน่วยงานนั้น
3. ความคืนสภาพได้ (Resilience) หมายถึง ความสามารถ (Capacity) ในการตอบสนองต่อการหยุดชะงักใดๆ ที่ไม่คาดคิดได้ ตัวอย่างเช่น การเกิดการโจมตีจากผู้ก่อการร้าย หรือ ภัยพิบัติจากธรรมชาติ โดยสามารถที่จะกลับคืน หรือฟื้นตัวเข้าสู่สภาวะปกติได้เหมือนก่อนที่มีการหยุดชะงัก หรือเข้าสู่สภาวะใหม่ที่ดีกว่า
4. โซ่อุปทานไซเบอร์ (Cyber-Supply Chain) หมายถึง โซอุปทานที่บริษัทหรือองค์กร รวมทั้งคู่ค้าที่มาทำธุรกิจได้มีการทำธุรกรรมร่วมกันบนทางคอมพิวเตอร์ด้วยการสื่อสารทางด้านอินเทอร์เน็ต โดยมีเป้าหมายอย่างเดียวกัน ที่จะนำไปสู่ทีมที่มีประสิทธิภาพ รวดเร็ว และน่าเชื่อถือ ทำให้ได้เปรียบคู่แข่งขัน

คำชี้แจงส่วนที่ 1 : ข้อมูลทั่วไปขององค์กรท่าน

กรุณาอ่านข้อความแล้วใส่เครื่องหมาย ☑ หน้าคำตอบที่ท่านเลือก ซึ่งตรงกับความเป็นจริงขององค์กรท่านมากที่สุด

1. ธุรกิจของท่านเป็นประเภทใด
   - ☐ ภาคการค้า
   - ☐ ภาคการบริการ
   - ☐ ภาคการผลิต
   - ☐ ภาคธุรกิจเกษตร

2. ระยะเวลาที่ท่านดำเนินการกิจการ
   - ☐ น้อยกว่า 1 ปี
   - ☐ 1 - 3 ปี
   - ☐ 4 - 9 ปี
   - ☐ 10 ปี ขึ้นไป
   - ☐ อื่น ๆ _____

3. จำนวนพนักงานในองค์กร
   - ☐ 1 - 5 คน
   - ☐ 6 - 10 คน
   - ☐ 11 - 50 คน
   - ☐ 51 - 100 คน
   - ☐ 101 - 199 คน
   - ☐ 200 คนขึ้นไป

4. ขอบเขตระดับตลาดที่ธุรกิจของท่านให้การบริการ
   - ☐ ระดับภูมิภาค
   - ☐ ระดับประเทศ
   - ☐ ระดับนานาชาติ
   - ☐ อื่น ๆ _____

5. ตำแหน่งของผู้ตอบแบบสอบถาม
   - ☐ กรรมการผู้จัดการ/รองกรรมการผู้จัดการ
   - ☐ ผู้อำนวยการฝ่าย/รองผู้อำนวยการฝ่าย
   - ☐ ผู้จัดการแผนก/รองผู้จัดการแผนก
   - ☐ หัวหน้าแผนก/รองหัวหน้าแผนก
   - ☐ พนักงาน/เจ้าหน้าที่ปฏิบัติการ
   - ☐ พนักงาน/เจ้าหน้าที่สนับสนุนปฏิบัติการ
   - ☐ อื่น ๆ (โปรดระบุ) _____

6. สัดส่วนของพนักงานของท่านที่มีพื้นฐานความรู้ทางด้านเทคโนโลยีสารสนเทศหรือไอที
   - ☐ น้อยกว่า 50%
   - ☐ 51 - 60%
   - ☐ 61 - 70%
   - ☐ 71 - 80%
   - ☐ มากกว่า 80%
   - ☐ ไม่มีพนักงานที่มีความรู้ทางด้านไอทีเลย
   - ☐ อื่น ๆ _____

คำชี้แจงส่วนที่ 2 : ข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัทท่าน

ขอความกรุณาท่านพิจารณาข้อความในหัวข้อต่อไปนี้แล้วใส่เครื่องหมาย ☑ หน้าคำตอบที่ท่านเลือก ซึ่งตรงกับความเป็นจริงขององค์กรท่านมากที่สุด

1. องค์กรของท่านได้รายงานหรือแจ้งเตือนพนักงานว่าได้ตกเป็นเหยื่อจากการโจมตีทางไซเบอร์แล้วหรือไม่
   - ☐ ใช่ ได้รายงานทุกครั้งที่พบ
   - ☐ ใช่ แต่น้อยมาก
   - ☐ ได้แจ้งเป็นบางครั้ง
   - ☐ ไม่เคยได้แจ้งเลย
   - ☐ อื่น ๆ _____

2. บริษัทของท่านมีแผนฉุกเฉินในการรับมือต่อเหตุการณ์การโจมตีทางไซเบอร์หรือไม่
   - ☐ มี
   - ☐ ไม่มี
   - ☐ กำลังดำเนินการภายใต้แผนฉุกเฉินนี้อยู่
   - ☐ อื่น ๆ _____

3. บริษัทของท่านมีการใช้งานอย่างเข้มงวด เกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอยู่แล้ว หรือไม่
   - ☐ มี
   - ☐ มีเป็นบางครั้ง
   - ☐ ไม่มี
   - ☐ ไม่ทราบ
   - ☐ อื่น ๆ _____

4. บริษัทของท่านมีการทบทวน เกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศอยู่แล้ว หรือไม่
   - ☐ มี
   - ☐ มีเป็นบางครั้ง
   - ☐ ไม่มี
   - ☐ ไม่ทราบ
   - ☐ อื่น ๆ _____

5. ระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่องค์กรใช้อยู่ในปัจจุบัน (ตอบได้มากกว่า 1 ข้อ)
   - ☐ โปรแกรมป้องกันไวรัส (Anti-virus Software)
   - ☐ ไฟร์วอลล์ (Firewall)
   - ☐ Application-level Firewall
   - ☐ ระบบเครือข่ายเสมือน (VPN : Virtual Private Network)
   - ☐ โปรแกรมป้องกันสปายแวร์ (Anti-spyware Software)
   - ☐ ระบบตรวจจับการบุกรุก (Instruction Detection Systems)
   - ☐ ระบบป้องกันการบุกรุก (Instruction Prevention Systems)
   - ☐ การเข้ารหัสข้อมูลที่สื่อสารระหว่างเครื่องคอมพิวเตอร์หรืออุปกรณ์เน็ตเวิร์ค (Encryption for Data Transit)
   - ☐ การเข้ารหัสข้อมูลที่ถูกเก็บในอุปกรณ์เก็บข้อมูล (Encryption for Data in Storage)
   - ☐ โปรแกรมการจัดการลงบันทึกเข้าออก (Log Management Software)
   - ☐ เครื่องมือสืบสวนด้านนิติวิทยาศาสตร์สำหรับระบบคอมพิวเตอร์ (Forensics Tools)
   - ☐ ระบบรักษาความมั่นคงปลอดภัยเครือข่ายไร้สาย (Specialized Wireless Security System)
   - ☐ ระบบรักษาความมั่นคงปลอดภัยเครื่องลูกข่าย/ระบบควบคุมการเข้าใช้เครือข่าย (Endpoint Security Client Software/NAC)
   - ☐ ระบบยืนยันตัวผู้ใช้ด้วยชีวมิติ (Biometrics)
   - ☐ อื่น ๆ _____

6. รูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ (ตอบได้มากกว่า 1 ข้อ)
   - ☐ ตรวจสอบความมั่นคงปลอดภัยโดยบุคลากรภายในองค์กร (Security Audits by Internal Staff)
   - ☐ ทดสอบหาความบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรโดยบุคลากรภายในองค์กร (Penetration Testing by Internal Staff)
   - ☐ ตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยองค์กรภายนอก (Security Audits by External Organization)
   - ☐ ตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยเครื่องมืออัตโนมัติ (Automated Tools)
   - ☐ ตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยโปรแกรมเฝ้าติดตามผ่านเว็บไซต์ (Web Activity Monitoring Software)
   - ☐ อื่น ๆ _____

7. นโยบายความมั่นคงปลอดภัยไซเบอร์อะไรบ้างที่บริษัทของท่านได้ดำเนินการอยู่ในขณะนี้ (ตอบได้มากกว่า 1 ข้อ)
   - ☐ มีแผนพัฒนาความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ
   - ☐ มีการจ้างบริษัทจากภายนอกในการจัดการเรื่องความมั่นคงปลอดภัยทางคอมพิวเตอร์

☐ มีแผนการประเมินความเสี่ยง/ช่องโหว่ทางด้านเทคโนโลยีสารสนเทศ
☐ มีการเช่าศูนย์ที่ให้บริการในการตรวจสอบคอมพิวเตอร์/เครือข่าย
☐ มีเอกสารมาตรฐานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์อย่างเป็นทางการ
☐ มีการฝึกอบรมบุคลากรให้รับรู้ถึงกระบวนการการรักษาความมั่นคงปลอดภัย
☐ มีการเก็บรักษาสื่อ อุปกรณ์ในการสำรองข้อมูล
☐ มีการควบคุมเกี่ยวกับซอฟต์แวร์ที่มีการละเมิดลิขสิทธิ์
☐ มีการจัดการสื่อทางคอมพิวเตอร์ที่สามารถถอดได้ (ตัวอย่างเช่น USB)
☐ มีมาตรการในการรักษาความมั่นคงปลอดภัยสำหรับการนำเอาอุปกรณ์ส่วนตัวมาใช้
☐ มีมาตรฐานความมั่นคงปลอดภัยสำหรับการใช้งานการประมวลผลแบบคลาวด์
☐ ไม่ทราบว่ามีหรือไม่
☐ ไม่มีตามหัวข้อข้างบน
☐ อื่น ๆ _____

คำชี้แจงส่วนที่ 3 : ความคิดเห็นเกี่ยวกับข้อมูลสภาพการดำเนินงานที่แท้จริงเกี่ยวกับความร่วมมือกันของโซ่อุปทาน

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
1. การแบ่งปันข้อมูลร่วมกัน (Information Sharing)					
1.1 บริษัทมีกระบวนการในการแบ่งปันข้อมูลระหว่างบริษัทอื่น ๆ ในโซ่อุปทาน					
1.2 กระบวนการในการแบ่งปันข้อมูลระหว่างบริษัทอื่น ๆ ในโซ่อุปทานที่มีอยู่นั้น เป็นกระบวนการที่มีประสิทธิภาพ					
1.3 บริษัทได้มีการแบ่งปันข้อมูลด้านกลยุทธ์ให้กับทั้งลูกค้าและผู้จำหน่าย					
1.4 การดำเนินการในเรื่องของการแบ่งปันข้อมูลที่ผ่านมาทำให้เกิดประโยชน์ต่อบริษัทเป็นอย่างมาก					
1.5 การแบ่งปันข้อมูลระหว่างบริษัทอื่น ๆ ในโซ่อุปทานเป็นผลทำให้เกิดความร่วมมือกันในโซ่อุปทาน					

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
2. ความไว้ใจ (Trust)					
2.1 คู่ค้าที่มีอยู่ในโซ่อุปทานที่มีอยู่มีความซื่อสัตย์ในการติดต่อเพื่อทำธุรกิจกับบริษัทของท่าน					
2.2 คู่ค้าที่อยู่ในโซ่อุปทานมีการป้องกันความลับของลูกค้าที่ได้รับจากบริษัทของท่าน					
2.3 คู่ค้าที่อยู่ในโซ่อุปทานได้ให้ข้อมูลที่ถูกต้องกับบริษัทของท่านเสมอ					
2.4 คู่ค้าที่อยู่ในโซ่อุปทานของท่านเต็มใจที่จะให้ความช่วยเหลือและสนับสนุนกับบริษัทของท่านโดยไม่มีข้อยกเว้น					
2.5 เมื่อบริษัทของท่านประสบต่อปัญหาใด ๆ และแจ้งไปยังคู่ค้าที่อยู่ในโซ่อุปทานคู่ค้าเหล่านั้นจะปฏิบัติต่อบริษัทของท่านด้วยความเข้าใจ					
3. ความร่วมมือกันในการสื่อสาร (Collaborative Communication)					
3.1 บริษัทของท่านและคู่ค้าในโซ่อุปทาน มีการจัดการประชุมร่วมกันอย่างสม่ำเสมอ					
3.2 บริษัทของท่านและคู่ค้าในโซ่อุปทาน มีการสื่อสารกันแบบเปิดและแบบสองทางอยู่แล้ว					
3.3 บริษัทของท่านและคู่ค้าในโซ่อุปทาน มีการสื่อสารทั้งที่เป็นทางการและไม่เป็นทางการ					
3.4 บริษัทของท่านและคู่ค้าในโซ่อุปทาน มีช่องทางในการสื่อสารกันอยู่หลายช่องทาง					
3.5 บริษัทของท่านและคู่ค้าในโซ่อุปทาน มีการประสานงานระหว่างกันโดยส่วนใหญ่จะใช้การสื่อสารทางด้านข้อความระหว่างกัน					
4. การสร้างความรู้ร่วมกัน (Knowledge Sharing)					
4.1 บริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าในโซ่อุปทานที่เกี่ยวกับกลยุทธ์ในการดำเนินการร่วมกันเพื่อความสำเร็จที่จะเกิดขึ้นในระยะยาว					

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
4.2 บริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าในโซ่อุปทานในการแลกเปลี่ยนแนวความคิดใหม่ๆ เพื่อความสัมพันธ์ที่ดีต่อกันในระยะยาว					
4.3 บริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าในโซ่อุปทาน เกี่ยวกับการพัฒนาโอกาสทางด้านนวัตกรรม โดยเฉพาะในเรื่องที่เกี่ยวข้องกับการจัดการความเสี่ยงและความไม่แน่นอนทางด้านธุรกิจที่จะเกิดขึ้น					

คำชี้แจงส่วนที่ 4 : ความคิดเห็นเกี่ยวกับข้อมูลสภาพการดำเนินงานที่แท้จริงเกี่ยวกับปัญหาภัยคุกคามไซเบอร์

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
1. แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (External Motivation of Cyber Attacks)					
1.1 ผู้บุกรุกเข้าสู่เครือข่ายมีวัตถุประสงค์ในการทดสอบขีดความสามารถของตนเอง หรือต้องการท้าทายโดยการเจาะระบบให้สำเร็จ					
1.2 ความรุนแรงขององค์กรอาชญากรรมที่มุ่งกระทำต่อธุรกรรมทางการเงินและทรัพย์สินทางปัญญาของวิสาหกิจ					
1.3 การโจมตีทางไซเบอร์ที่เกิดขึ้นกับวิสาหกิจมักจะมีสาเหตุมาจากการความแตกต่างทางด้านอุดมการณ์และการเมือง					
1.4 นโยบายทางภาครัฐส่งผลให้เกิดการโจมตีทางไซเบอร์ที่มีต่อบริษัทท่าน					
2. ช่องโหว่ของดำเนินงานภายใน (Internal Organizational Vulnerabilities)					
2.1 กลยุทธ์ นโยบาย และมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบันของบริษัทท่านเป็นผลทำให้เกิดการโจมตีทางไซเบอร์					
2.2 การดำเนินการและยึดมั่นในกลยุทธ์และมาตรฐานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัทท่านจะส่งผลให้เกิดการโจมตีทางไซเบอร์นั้นลดลง					
2.3 การอบรมพนักงานรวมไปถึงการทำให้พนักงานได้ตะหนักถึงภัยคุกคามทางไซเบอร์จะทำให้การโจมตีทางไซเบอร์นั้นลดลงได้					

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
2.4 การที่มีโครงสร้างพื้นฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่อ่อนแอในบริษัทของท่านจะส่งผลให้เกิดการโจมตีทางไซเบอร์ที่มากขึ้น					
2.5 ความสามารถในการพัฒนาทักษะความสามารถบุคลากรในบริษัทของท่านจะส่งต่อการจัดการความปลอดภัยในโลกไซเบอร์ให้มีประสิทธิภาพมากขึ้น					
3. การรับมือต่อภัยคุกคามไซเบอร์ (Threats Coping)					
3.1 บริษัทของท่านมีการกำหนดนโยบาย (Policy) ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ไว้อย่างชัดเจนในการเพื่อใช้ในการรับมือต่อภัยคุกคามไซเบอร์					
3.2 บริษัทของท่านมีความชัดเจนในการบูรณาการในการกำหนดโครงสร้าง (Organization) การจัดหน่วยและการบรรจุบุคคลที่มีคุณลักษณะพิเศษและมีความเชี่ยวชาญเฉพาะด้าน มีมาตรฐานการปฏิบัติงาน และเป็นแบบอย่างที่ดีในด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์					
3.3 บริษัทของท่านมีการกำหนดกรอบการดำเนินงาน (Frame work) อย่างเป็นระบบแบบแผนที่ชัดเจนและสามารถปฏิบัติได้ในการรับมือกับภัยคุกคามด้านไซเบอร์ขององค์กร					
3.4 บริษัทของท่านมีการประเมินผลการปฏิบัติขององค์กรทั้งการประเมินภายในด้วยตนเอง และการประเมินจากภายนอก เพื่อติดตามความก้าวหน้า ปัญหาข้อขัดข้อง ข้อจำกัดอุปสรรคต่างๆ เพื่อหาทางแก้ไขปัญหาและอุปสรรคแต่เนิ่นๆ สำหรับการรับมือกับภัยคุกคามด้านไซเบอร์					

คำชี้แจงส่วนที่ 5 : ความคิดเห็นเกี่ยวกับ ข้อมูลสภาพการดำเนินงานที่แท้จริงเกี่ยวกับการจัดการ ความเสี่ยงทางไซเบอร์ของโซ่อุปทาน

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
1. ด้านบุคลากร (People)					
1.1 บุคลากรของบริษัทท่านมีความสามารถและความชำนาญและความเชี่ยวชาญต่อการจัดการความเสี่ยงอยู่ในระดับสูง					
1.2 บุคลากรของบริษัทของท่านมีความตระหนักถึงการจัดการความเสี่ยงเป็นอย่างดี					
1.3 บุคลากรในตำแหน่งผู้จัดการของบริษัทท่านมีความรู้ความชำนาญต่อการจัดการความเสี่ยงเป็นอย่างดี					
1.4 บริษัทของท่านมีการจัดการความเสี่ยงด้วยการสนับสนุนให้พนักงานทำงานร่วมกันเป็นทีม					
1.5 บริษัทของท่านมีนโยบายให้พนักงานสร้างความสัมพันธ์ที่ดีไม่ว่าจะเป็นทั้งลูกค้า ผู้จำหน่าย รวมไปถึงคู่ค้าต่าง ๆ					
2. ด้านกระบวนการ (Process)					
2.1 บริษัทของท่านได้มีการดำเนินการในเรื่องของการติดตั้งโปรแกรมป้องกันไวรัสไว้แล้ว					
2.2 บริษัทของท่านมีระบบรักษาความปลอดภัยของข้อมูลในการที่จะรักษาข้อมูลต่าง ๆ ที่สำคัญของบริษัทของท่าน					
2.3 บริษัทของท่านมีการจัดการในเรื่องของระบบเครือข่ายในการป้องการการเข้ามาโจมตีจากผู้ไม่หวังดี					
2.4 บริษัทของท่านมีระบบในการจัดการบัญชีรายชื่อผู้เข้าใช้งานในระบบต่าง ๆ โดยการสร้างกฎเกณฑ์ในการตั้งค่าไว้อย่างมีประสิทธิภาพ					
2.5 ภัยคุกคามทางไซเบอร์ในปัจจุบันนี้ ทำให้เกิดผลเสียต่อระบบเครือข่ายคอมพิวเตอร์ของท่านอย่างมาก					

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
2.6 บริษัทของท่านมีทรัพยากร และความสามารถในการรักษาความปลอดภัย ที่จะรับมือต่อการโจมตีที่เกิดจากภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ					
2.7 ข้อมูลที่สำคัญ ของบริษัทท่านได้รับการจัดการต่อการรับมือจากการโจมตีที่เกิดจากภัยคุกคามทางไซเบอร์ไว้อย่างมีประสิทธิภาพ					
2.8 ปัจจุบันบริษัทของท่านได้รับผลประโยชน์จากการดำเนินการในด้านการจัดการความเสี่ยงที่มาจากการโจมตีทางไซเบอร์					
3. ด้านเทคโนโลยี (Technology)					
3.1 โครงสร้างพื้นฐานอันประกอบไปด้วย สถาปัตยกรรมของระบบ ผู้ใช้งานระบบ รวมไปถึงผู้ให้บริการจากภายนอก ได้รับการจัดการเพื่อรับมือจากการโจมตีที่เกิดจากภัยคุกคามทางไซเบอร์ไว้อย่างมีประสิทธิภาพ					
3.2 ท่านไม่สามารถเข้าถึงเครื่องมือทางด้านเทคโนโลยีที่สามารถสนับสนุนการทำงานของท่านได้ เมื่อท่านประสบกับปัญหาภัยคุกคามทางไซเบอร์					
3.3 ท่านมีความเชื่อมั่นต่อเทคโนโลยีในการรักษาความปลอดภัย เมื่อบริษัทของท่านได้ประสบกับปัญหาภัยคุกคามทางไซเบอร์ นั่นหมายความว่า ปัญหาภัยคุกคามดังกล่าวจะไม่ส่งผลกระทบต่องานของท่าน					
3.4 บริษัทของท่านมักจะหาวิธีการใหม่ๆ ในการรักษาความปลอดภัยจากการโจมตีทางไซเบอร์มาใช้เองโดยไม่ได้ทำการปรึกษาจากที่ปรึกษาจากภายนอกเลย					

คำชี้แจงส่วนที่ 6 : ความคิดเห็นเกี่ยวกับข้อมูลสภาพการดำเนินงานที่แท้จริงเกี่ยวกับความสามารถ สำหรับสร้างความคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทาน

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
1. ความคล่องตัว (Agility)					
1.1 บริษัทของท่านสามารถที่จะทำการตรวจจับถึงภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ภายในบริษัทของท่านด้วยความรวดเร็ว					
1.2 บริษัทของท่านสามารถที่จะทำการตัดสินใจกระทำการใดๆ เมื่อพบกับภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่างๆ ภายในบริษัทของท่านด้วยความรวดเร็ว					
1.3 บริษัทของท่านสามารถที่ตอบสนองต่อภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ภายในบริษัทของท่านด้วยความรวดเร็ว					
1.4 บริษัทของท่านสามารถที่ปรับเปลี่ยนวิธีการในการดำเนินธุรกรรมต่างๆ ภายในบริษัทได้อย่างรวดเร็ว เมื่อเผชิญกับภัยคุกคามที่เข้ามาโจมตีการทำงานในบริษัทของท่าน					
2. ความทนทาน (Robust)					
2.1 บริษัทของท่าน สามารถที่จะกลับเข้าสู่สภาวะปกติได้อย่างรวดเร็วเมื่อถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก					
2.2 บริษัทของท่าน สามารถที่จะปรับเปลี่ยนกระบวนการไปสู่สภาวะการทำงานใหม่ๆ หลังจากการถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก					
2.3 บริษัทของท่านได้เตรียมความพร้อมเกี่ยวกับการจัดการทางการเงินไว้เป็นอย่างดี ต่อการถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก					
2.4 บริษัทของท่าน สามารถที่จะดำเนินธุรกรรมกับคู่ค้าในโซ่อุปทานต่อไปได้ แม้จะถูกโจมตีจากภัยคุกคามที่ทำให้การดำเนินงานเกิดการชะงัก					
2.5 บริษัทของท่าน สามารถที่จะรักษา ควบคุม หน้าที่ต่าง ๆ ในโซ่					

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
อุปทาน หลังจากที่ถูกโจมตีจากภัยคุกคาม ที่ทำให้การดำเนินงานเกิดการชะงัก					
2.6 บริษัทของท่าน สามารถที่จะดึงเอาความรู้ ความหมายต่างๆ ที่เป็นประโยชน์อันเกิดจากการถูกโจมตีจากภัยคุกคาม เพื่อนำมาเป็นข้อมูลในการแก้ปัญหาอาจถูกโจมตีในครั้งต่อไป					

คำชี้แจงส่วนที่ 7 : ข้อมูลสภาพการดำเนินงานที่แท้จริงเกี่ยวกับการจัดการความต่อเนื่องทางธุรกิจ

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
1. แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)					
1.1 แผนความต่อเนื่องทางธุรกิจสามารถทำให้บริษัทรวมไปถึงผู้ถือหุ้นมีความเข้าในถึงระดับของความเสี่ยงที่สามารถทำให้กิจการดำเนินต่อไปได้					
1.2 แผนความต่อเนื่องทางธุรกิจสามารถนำมาใช้จัดการธุรกรรมต่าง ๆ ในโซ่อุปทานได้อย่างมีประสิทธิภาพ					
1.3 แผนความต่อเนื่องทางธุรกิจสามารถสร้างความเชื่อถือให้กับผู้ถือหุ้นที่มีต่อบริษัทได้					
1.4 แผนความต่อเนื่องทางธุรกิจสามารถที่ทำให้เกิดแผนในการบริหารธุรกิจ และจะสามารถช่วยป้องกันทรัพย์สินของบริษัท รวมไปถึงข้อมูลที่สำคัญของบริษัท พร้อมทั้งยังสามารถที่จะฟื้นฟูปัญหาที่เกิดขึ้นให้กลับมาทำงานได้อย่างมีประสิทธิภาพตามเดิม					
1.5 แผนความต่อเนื่องทางธุรกิจทำให้เกิดความสามารถทางการแข่งขันได้					
2. แผนกู้คืนภัยพิบัติ (Disaster Recovery Plan)					
2.1 แผนกู้คืนภัยพิบัติได้เข้ามาจัดการเกี่ยวกับเครื่องมือ อุปกรณ์ ที่จะนำมาใช้แก้ปัญหาเมื่อเกิดภัยพิบัติได้อย่างมีประสิทธิภาพ					
2.2 แผนกู้คืนภัยพิบัติทำให้มีการจัดการเกี่ยวกับระบบการจัดการเครือข่าย					

ข้อคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
ในบริษัทได้อย่างมีประสิทธิภาพ					
2.3 แผนกู้คืนภัยพิบัติทำให้สามารถประหยัดค่าใช้จ่ายในการกู้คืนระบบเนื่องจากมีการทำแผนการปฏิบัติรองรับไว้แล้ว					
2.4 การมีโซลูชั่นในการกู้คืนระบบสามารถช่วยในการรักษาชื่อเสียงของบริษัทของท่านกับลูกค้าและคู่ค้าได้					
2.5 การมีโซลูชั่นในการกู้คืนระบบสามารถช่วยให้มั่นใจได้ว่า บริษัทของท่านจะปฏิบัติตามกฎระเบียบของอุตสาหกรรมได้					
3. การจัดการวิกฤต (Crisis Management)					
3.1 การจัดการวิกฤตทำให้เกิดความเชื่อมั่นในสายตาของคู่ค้าในโซ่อุปทาน ต่อปัญหาทางด้านความเสี่ยงที่บริษัทของท่านกำลังประสบอยู่					
3.2 การจัดการวิกฤต ยิ่งดำเนินการได้เร็วมากแค่ไหน ยิ่งมีผลต่อชื่อเสียงของบริษัทมากขึ้นเท่านั้น					
3.3 การจัดการวิกฤต ทำให้คู่ค้าในโซ่อุปทานเห็นได้ว่า บริษัทของท่านมีความเป็นมืออาชีพในการบริหาร					
4. การจัดการเหตุฉุกเฉิน (Emergency Management)					
4.1 บริษัทของท่านมีการเตรียมการสำหรับการป้องกัน (Prevent) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ					
4.2 บริษัทของท่านมีการเตรียมพร้อมรับมือ (Preparedness) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ					
4.3 บริษัทของท่านมีแผนในการตอบสนอง (Response) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ					
4.4 บริษัทของท่านมีแผนสำหรับการฟื้นฟูแก้ไข (Recovery) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ					

ข้อเสนอแนะอื่นๆ ……..……...……...

……...……

……..…….....

ขอกราบขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการตอบแบบสอบถาม