รอบ2
ปีงบประมาณ
พ.ศ.2567

สรุปบทเรียนจากการพัฒนาความรู้

หลักสูตร ความเข้าใจการบริหารความเสี่ยง และความปลอดภัยไซเบอร์

จัดทำโดย นายสุพงษ์ ไพชยนต์

ก่อนที่จะอธิบายว่า Cyber Security คืออะไรนั้น ทุกคนคงทราบกันดีว่าในโลกยุคดิจิทัลที่เต็มไปด้วย Big Data หรือข้อมูลข่าวสารจำนวนมหาศาลหลั่งไหลผ่านเครือข่ายอินเทอร์เน็ต องค์กรส่วนใหญ่ต่างก็เลือกใช้อินเทอร์เน็ตเป็นพื้นที่ในการทำงาน ไม่ว่าจะเป็นการเก็บรักษาข้อมูล การสื่อสารภายในองค์กร การเผยแพร่ข้อมูล ฯลฯ แล้วเราจะแน่ใจได้อย่างไรว่าข้อมูลเหล่านั้นมีความปลอดภัยต่อการใช้งาน ด้วยเหตุนี้ทำให้ Cyber Security เข้ามามีบทบาทสำคัญต่อวิถีชีวิตในโลกยุคดิจิทัลเป็นอย่างมาก

Cyber Security

Cyber Security คือเทคโนโลยี หรือกระบวนการ วิธีปฏิบัติที่ถูกออกแบบมาเพื่อปกป้องเครือข่าย, อุปกรณ์, โปรแกรมและข้อมูลจากการถูกโจมตี หรือการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เรียกได้ว่าเป็นระบบความมั่นคงและความปลอดภัยทางไซเบอร์ก็ได้ ซึ่งถือเป็นสิ่งที่สำคัญสำหรับองค์กรต่างๆ ไม่ว่าจะเป็นทั้งในส่วนของภาครัฐ หรือเอกชน เนื่องจากข้อมูลจำนวนมากที่ทางองค์กรเก็บรวบรวมไว้อาจมีที่สำคัญที่ส่งผลกระทบด้านลบกับองค์กรได้หากถูกขโมยเอาข้อมูลออกไป หรือถูกนำมาเปิดเผยได้โดยไม่ได้รับอนุญาตไม่ว่าจะเป็นข้อมูลที่เป็นทรัพย์สินทางปัญญา, ข้อมูลทางการเงินข้อมูลส่วนบุคคล รวมถึงข้อมูลส่วนตัวของลูกค้า ซึ่งในยุคปัจจุบันองค์กรต่างๆ ก็มักจะส่งข้อมูลเหล่านี้กันผ่านอุปกรณ์ต่างๆ และอินเตอร์เน็ต ดังนั้นเพื่อความปลอดภัยบนโลกไซเบอร์ทุกๆ องค์กรจึงจำเป็นต้องมี Cyber Security เพื่อให้กับทำงานมีความปลอดภัย และเป็นไปอย่างมีประสิทธิภาพ

หลักการทำงานของ Cyber Security จะครอบคลุมสิ่งต่างๆ ดังต่อไปนี้

- Network security : เป็นกระบวนการปกป้องเครือข่าย หรือเน็ตเวิร์คจากการถูกโจมตีและการบุกรุกหรือที่เราเคยได้ยินกันว่าการแฮค (Hack) ระบบนั่นเอง
- Application security : แอปพลิเคชั่นจำเป็นต้องการการอัพเดทและการทดสอบอย่างต่อเนื่องเพื่อให้แน่ใจว่ามีปลอดภัยจากการถูกโจมตีจากบุคคลอื่น

- Data security : สิ่งที่อยู่ภายในเครือข่ายและแอปพลิเคชันคือข้อมูล การปกป้องข้อมูล บริษัท และลูกค้าถือเป็นความปลอดภัยอีกขั้นหนึ่ง
- Cloud security : ในปัจจุบันหลายๆ องค์กรนิยมเก็บข้อมูลไว้ใน “คลาวด์” หรือระบบการจัดเก็บข้อมูลแบบออนไลน์ การปกป้องข้อมูลเหล่านั้นถือเป็นความท้าทายอย่างหนึ่ง ที่องค์กรควรให้ความสำคัญ

การปกป้องข้อมูลและ IT systems ของบริษัทถือเป็นสิ่งสำคัญ หากมีระบบการป้องกันที่ไม่ดีพอ หรือละเลยไม่ใช้ความสำคัญ ก็อาจส่งผลทำให้ถูกโจมตีจนได้รับความเสียหาย ส่งผลกระทบต่อการดำเนินการทำงานต่างๆ รวมถึงผลกำไรของบริษัทและความน่าเชื่อถือของบริษัทต่อลูกค้าได้อีกด้วย

Cyber Security Risk

Cyber Security Risk คือแนวโน้มที่จะได้รับผลกระทบจากการหยุดชะงักต่อข้อมูลที่ละเอียดอ่อน การเงิน หรือการดำเนินธุรกิจออนไลน์ รวมถึงการให้บริการบางอย่างที่มีความเกี่ยวข้องต่อการดำเนินธุรกิจและการให้บริการประชาชน โดยทั่วไปความเสี่ยงทางไซเบอร์มีความเกี่ยวข้องกับเหตุการณ์ที่อาจส่งผลให้เกิดการละเมิดข้อมูล การขโมยข้อมูล หรือการทำลายข้อมูลเพื่อให้ไม่สามารถให้บริการได้ ความเสี่ยงทางไซเบอร์นั้นเป็นภัยคุกคามด้านความปลอดภัยต่อการดำเนินงานของธุรกิจและองค์กร ตัวอย่างของความเสี่ยงทางไซเบอร์ ได้แก่

- Ransomware (แรนซัมแวร์) ซึ่งเป็นหนึ่งในมัลแวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูล ไฟล์และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความเชื่อถือในอุตสาหกรรมและองค์กรต่าง ๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูล เพื่อไม่ให้ผู้อื่นสามารถล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์ได้มีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ด้วยการเข้ารหัสข้อมูลของเป้าหมายทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware
- Data leaks (ข้อมูลรั่วไหล) ข้อมูลรั่วไหลเกิดขึ้นเมื่อมีข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ได้ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกโดยอาจบันทึกผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้
- Phishing (ฟิชชิง) คือการโจมตีรูปแบบหนึ่งที่หลอกให้เป้าหมายกรอกข้อมูลส่วนบุคคล ข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลบัตรประชาชน ด้วยวิธีการต่าง ๆ เพื่อให้เป้าหมายส่งข้อมูลนั้นให้กับผู้ไม่หวังดี เช่นการส่งอีเมลหลอกเป้าหมาย “คุณมีการถอนเงินเป็นจำนวนหนึ่ง หากไม่ใช่กรุณาคลิกลิงก์ด้านล่างนี้เพื่อ ยกเลิกการทำรายการ” หรือ “คุณเป็นผู้โชคดีได้รับ iPhone ฟรีเพียงแค่กรอกข้อมูลในนี้” และเมื่อเป้าหมายส่งข้อมูลให้กับผู้ไม่หวังดีแล้วผู้ไม่หวังนำข้อมูลไปดำเนินการเข้าถึงข้อมูลส่วนอื่น ๆ ของเป้าหมาย เช่นข้อมูลการเงิน ข้อมูลรหัสระบบต่าง ๆ ที่เป็นข้อมูลส่วนบุคคล

- Malware (มัลแวร์) หรือ Malicious Software (ซอฟต์แวร์อันตราย) คือซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี เพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมัลแวร์นั้นได้แบ่งออกเป็นหลายประเภท เช่น
- Virus (ไวรัส) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศเป็นอย่างซึ่งโดยมุ่งเน้นในการโจมตีขัดขวางเพื่อไม่ให้ระบบสามารถใช้งานได้
- Worms (เวิร์ม) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารเทศที่มีการเชื่อมต่อผ่านระบบเครือข่ายทั้งภายในและภายนอกโดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงานและขยายตัวส่งต่อภายในระบบเครือข่ายจนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้
- Trojan (โทรจัน) เป็นซอฟต์แวร์ที่มีเป้าหมายการดักจับเปลี่ยนแปลงแก้ไขข้อมูลซึ่งอาจส่งผลต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศหรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้
- Spyware (สปายแวร์) ซอฟต์แวร์ประสงค์ร้ายที่ทำงานอย่างลับๆ บนคอมพิวเตอร์และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล
- Adware (แอดแวร์) คือซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหากับระบบสารสนเทศได้ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัยได้
- Ransomware (แรนซัมแวร์) คือซอฟต์แวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูล ไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูล ไฟล์และเอกสารเพื่อไม่ให้เป้าหมายสามารถใช้งานได้
- Insider threats (ภัยคุกคามจากภายใน) คือภัยคุกคามจากภายในอาจเกิดขึ้นได้กับคนใกล้ชิดภายในองค์กรที่ได้รับอนุญาตในการเข้าถึงข้อมูลที่เป็นความลับซึ่งการเข้าถึงอาจส่งผลเสียต่อข้อมูลหรือระบบที่สำคัญขององค์กรได้ โดยภัยคุกคามชนิดนี้อาจจะเป็นพนักงาน ผู้ขาย ผู้รับเหมา หุ้นส่วนหรือบุคคลที่มีความใกล้ชิด โดยความเสี่ยงและช่องโหว่ทางไซเบอร์นั้นมีวิธีการในการทำงานที่แตกต่างกัน โดยช่องโหว่ถือเป็นจุดอ่อนที่ส่งผลให้เกิดการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาตจากผู้ไม่หวังดีที่อาจก่อให้เกิดความเสี่ยงทางไซเบอร์ภายในระบบสารสนเทศของธุรกิจและองค์กร

การเตรียมความพร้อมสำหรับรับมือเมื่อเกิดเหตุการณ์ภัยพิบัติต่างๆ หรือการมีแผนการที่เรียกว่า Business Continuity Plan (BCP) นั้น จึงเป็นอีกกระบวนการหนึ่งที่จำเป็นที่องค์กรควรจะมีการจัดเตรียมไว้สำหรับใช้ในการบริหารจัดการเมื่อเกิดเหตุการณ์ ทั้งนี้ก็เพื่อที่จะกู้คืนสถานการณ์ให้สามารถกลับมาให้บริการได้อย่างใกล้เคียงกับสถานการณ์ปกติมากที่สุด ภายในระยะเวลาและเงื่อนไขที่องค์กรนั้นๆ ยอมรับได้

Business Continuity Plan (BCP) คืออะไร?

Business Continuity Plan หรือเรียกย่อๆ ว่า BCP คือแผนในการรับมือเหตุการณ์ต่างๆ ที่ธุรกิจอาจต้องหยุดชะงักลง ไม่ว่าจะเป็นเหตุที่ทำให้ธุรกิจหยุดลงเป็นเวลาเพียงไม่กี่ชั่วโมง หรือเป็นเวลาหลายวันก็ตาม และทำให้องค์กรสามารถกลับมาดำเนินธุรกิจต่อเนื่องได้ให้เร็วที่สุด เพื่อให้เกิดความเสียหายต่อลูกค้า, ทรัพย์สิน, ชื่อเสียง และการดำเนินธุรกิจขององค์กรให้น้อยที่สุดนั่นเอง

ใน BCP ของแต่ละองค์กรก็จะมีลำดับความสำคัญของกิจกรรมต่างๆ ที่แตกต่างกันไป เนื่องจากธุรกิจของแต่ละองค์กรแตกต่างกัน ทั้งรูปแบบการดำเนินธุรกิจ, ข้อมูลที่ใช้ในการทำธุรกิจ, ความฉุกเฉินของธุรกิจ, โครงสร้างองค์กร, รูปแบบของอาคารและสถานที่, อำนาจการตัดสินใจภายในองค์กร และอื่นๆ อีกมากมาย ดังนั้นแต่ละองค์กรจึงมีแผนรองรับที่แตกต่างกัน ภายใต้เป้าหมายเดียวกัน คือการบรรเทาความเสียหายของธุรกิจให้ต่ำที่สุดเมื่อเกิดเหตุต่างๆ และกลับมาดำเนินธุรกิจต่อให้ได้รวดเร็วที่สุด

ความคุ้มค่าของการทำ BCP ในองค์กร

เมื่อเกิดภัยพิบัติหรือเหตุฉุกเฉินต่างๆ ขึ้น และองค์กรไม่สามารถรับมือได้อย่างเป็นระบบนั้น ความเสียหายต่างๆ ที่เกิดขึ้นก็ย่อมมีมหาศาล บางกรณีองค์กรอาจโชคดี เพียงแค่กู้ข้อมูลคืนเล็กน้อย และซื้ออุปกรณ์ต่างๆ มาทดแทนก็สามารถดำเนินงานต่อได้ แต่บางกรณีองค์กรอาจโชคร้าย ไม่สามารถดำเนินงานต่อได้จนอาจต้องหยุดกิจการชั่วคราว เพราะข้อมูลและเอกสารสำคัญต่างๆ เสียหายจนไม่อาจกู้คืนได้

ซึ่งในโลกแห่งความเป็นจริง องค์กรไม่สามารถที่จะปล่อยให้ธุรกิจเป็นไปตามโชคชะตาได้ เนื่องจากจะส่งผลกระทบต่อการดำเนินธุรกิจและความไว้วางใจของผู้ใช้บริการหรือลูกค้า ดังนั้น องค์กรจึงต้องมีระบบบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ เพื่อเตรียมความพร้อมในทุกๆ ด้านให้สามารถรองรับเหตุการณ์ภัยพิบัติ

นอกจากนี้การทำ BCP เองยังไม่ได้มีประโยชน์เพียงแค่เมื่อเกิดภัยร้ายหรือเหตุฉุกเฉินเท่านั้น แต่ในขั้นตอนการประเมิน BCP ก็จะทำให้องค์กรได้ทบทวนลำดับความสำคัญของระบบงานต่างๆ และค้นหาจุดอ่อนต่างๆ ทำให้สามารถแก้ไขปัญหา หรือหาหนทางในการบรรเทาปัญหาเหล่านั้นลงไปได้ ในขณะเดียวกันการทำ Compliance ตามมาตรฐานธุรกิจต่างๆ ก็มีข้อกำหนดให้ต้องมีการทำ BCP อยู่ด้วยเช่นกัน ดังนั้นองค์กรที่มี BCP นอกจากจะทำให้ธุรกิจมีความมั่นใจในการดำเนินงานต่อไปมากขึ้นแล้ว ก็ยังทำให้คู่ค้าและลูกค้าเกิดความเชื่อมั่นเพิ่มขึ้นอีกด้วย

แผนต่อเนื่องทางธุรกิจ BCP จึงเป็นแผนที่สำคัญ

ทุกองค์กรมีความเสี่ยงจากภัยพิบัติที่อาจจะเกิดขึ้น รวมถึง

- ภัยธรรมชาติ เช่น พายุทอร์นาโด น้ำท่วมสูง พายุหิมะ แผ่นดินไหว และไฟไหม้
- อุบัติเหตุ
- การก่อวินาศกรรม

- **พลังานน้ำมัน และพลังงานไฟฟ้าหยุดชะงัก**
- **การสื่อสาร การขนส่ง ความปลอดภัย และความล้มเหลวของภาคบริการสาธารณะ**
- **ภัยพิบัติทางสิ่งแวดล้อม เช่น มลพิษและสารเคมีอันตรายที่รั่วไหล**
- **การโจมตีไซเบอร์ และพวกแบล็กแฮกเกอร์**

การสร้างและการบำรุงรักษา BCP ช่วยให้มั่นใจว่าองค์กรมีแหล่งข้อมูลและข้อมูลที่จำเป็นในการบริหารจัดการกับเหตุภาวะฉุกเฉินเหล่านี้

แหล่งที่มา

หลักสูตร : ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยโซเบอร์
บรรยายโดย : ผศ.พิเศษ สันติพัฒน์ อรุณธารี
สถาบัน/หน่วยงาน/ระบบ : มหาวิทยาลัยหอการค้าไทย
รูปแบบหลักสูตร : e-Learning **TDGA**
ช่วงเวลาการฝึกอบรม : ก.ค. 2567