รู้จักกับ Cybersecurity Framework เพิ่มแรงขับเคลื่อนในการทำ Digital Transformation

“อินเทอร์เน็ต” ชื่อนี้ไม่มีใครไม่รู้จัก อินเทอร์เน็ตเป็นหนึ่งในแรงขับเคลื่อนสำคัญสำหรับการพัฒนาความเจริญเติบโตทางเศรษฐกิจของทุกประเทศทั่วโลก อินเทอร์เน็ตกลายเป็นเวทีสำหรับการแลกเปลี่ยนความคิดเห็นของประชาชนในหลายประเทศทั่วโลก และยังเป็นช่องทางการล้วงข้อมูลโดยอาชญากรไซเบอร์ ซึ่งในยุคดิจิทัลที่หลายองค์กรเริ่มทำ Digital Transformation ก็มีการเก็บข้อมูล รวบรวมข้อมูลต่าง ๆ นำมาวิเคราะห์การตลาด ทั้งข้อมูลในอดีต ปัจจุบัน สามารถนำมาคาดการณ์ความเป็นไปในอนาคตได้ ดังนั้น ข้อมูลก็เหมือนสินทรัพย์ที่จำเป็นต้องมีการรักษาความปลอดภัย เพื่อป้องกันการรั่วไหลของข้อมูล อันนำไปสู่ความเสียหายตามมาได้ ทำให้คนทั่วโลกวิตกกังวลกับภัยคุกคามด้านไซเบอร์เป็นอย่างมาก

ที่มาของ NIST Cybersecurity Framework

ปัญหาด้านภัยคุกคามทางไซเบอร์ต้องได้รับการแก้ไขอย่างจริงจัง ต้องมีการวางแผนการดำเนินการอย่างเป็นระบบเพื่อบริหารจัดการความเสี่ยงดังกล่าวได้อย่างมีประสิทธิภาพและเดินหน้าการทำ Digital Transformation ได้อย่างราบรื่น ทางรัฐบาลของประเทศสหรัฐอเมริกาได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (NIST) ทำการพัฒนากรอบการดำเนินงาน ที่เรียกว่า NIST Cybersecurity Framework เพื่อปรับปรุงความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐานในการปฏิบัติที่ดีที่สุด ซึ่งครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กร และ เทคโนโลยี เพื่อบริหารความเสี่ยงทางไซเบอร์ ที่มีผลกระทบกับหน่วยงานโครงสร้างพื้นฐานสำคัญได้อย่างเหมาะสม ไม่ใช่แค่สหรัฐอเมริกาเท่านั้นที่ใช้ NIST Cybersecurity Framework เท่านั้น ยังแพร่หลายไปทั่วโลก รวมถึงประเทศไทย ในหลาย ๆ องค์กรเริ่มนำ Framework นี้ไปประยุกต์ใช้รับมือกับภัยคุกคามทางไซเบอร์

หัวใจสำคัญของ Framework แบ่งออกเป็น 5 ฟังก์ชันหลัก คือ

การระบุ (Identify)

การระบุและศึกษาทำความเข้าใจบริบทต่าง ๆ ทรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงความปลอดภัยที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ

การป้องกัน (Protect)

เป็นการวางแผนมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร เพื่อป้องกันระบบขององค์กรเหมาะสมสำหรับการบริหารโครงสร้างพื้นฐานสำคัญ ครอบคลุมการฝึกอบรมและการสร้างความตระหนัก มาตรการควบคุมการเข้าถึงข้อมูล มาตรการด้านความมั่นคงและความปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติตลอดจนเทคโนโลยีที่ใช้

การตรวจจับ (Detect)

การกำหนดขั้นตอนและดำเนินการกระบวนการต่าง ๆ เพื่อตรวจหาสถานการณ์ที่ผิดปกติด้านความปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจ และติดตามอย่างต่อเนื่อง

การตอบสนอง (Respond)

เป็นการกำหนดขั้นตอนและดำเนินการ เพื่อรับมือกับสถานการณ์ผิดปกติด้านความปลอดภัยทางไซเบอร์ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

การคืนสภาพ (Recover)

เป็นการกำหนดขั้นตอนและดำเนินการกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง และสามารถฟื้นฟูระบบให้กลับมาเป็นเหมือนเดิมได้

ดังนั้น การใช้ NIST Cybersecurity Framework ก็ถือเป็นการทำ Digital Transformation ได้เช่นกัน เพราะข้อมูลคือหัวใจหลักในการทำ Digital Transformation ข้อมูลจึงต้องได้รับการปกป้องให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ เพื่อไม่ให้ความเสียหายเกิดขึ้นได้ เมื่อองค์กรสามารถใช้ทั้ง 5 ฟังก์ชัน ได้อย่างเหมาะสม โดยกำหนดผลลัพธ์ที่ต้องการ และกรอบปฏิบัติสำหรับการดำเนินงานเพื่อวัตถุประสงค์ของแต่ละอุตสาหกรรมหรือโครงสร้างพื้นฐาน จะช่วยให้องค์กรเข้าใจ และจัดทำโครงงานและระบบด้าน Cyber Security ได้อย่างมีประสิทธิภาพมากขึ้น หากใครสนใจอาชีพ Cyber Security สามารถตามไปอ่านได้ที่นี่ คลิก

อ้างอิง :

https://www.catcyfence.com/it-security/article/nist-cybersecurity-framework/

https://www.mindphp.com/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD/73-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/5194-nist-cybersecurity-framework.html