สิ่งที่ผู้บริหารสารสนเทศระดับสูง (CIO) ‘ควรหลีกเลี่ยง’ ในปี 2559

สิ่งที่ผู้บริหารสารสนเทศระดับสูง (CIO) ‘ควรหลีกเลี่ยง’ ในปี 2559

โดยคุณปิยธิดา ตันตระกูล
ผู้จัดการประจำประเทศไทย บริษัทเทรนด์ไมโคร (ประเทศไทย) จำกัด

การรักษาไว้ซึ่งแผนสำรองทางการเงินเป็นสิ่งที่ขาดไม่ได้ โดยเฉพาะอย่างยิ่งเรื่องที่เกี่ยวข้องกับสินทรัพย์ที่สำคัญที่สุดของธุรกิจ

เมื่อย้อนกลับไปในอดีต ตำแหน่งผู้บริหารสารสนเทศระดับสูงหรือซีไอโอ (CIO) เกิดขึ้นครั้งแรกเมื่อ ปี 2523 โดยวิลเลียม ไซนอตต์ ผู้บริหารธนาคารแห่งหนึ่ง เขากล่าวว่า “หน้าที่ของ CIO มีความสำคัญเทียบเท่ากับประธานฝ่ายบริหาร (CEO) และประธานฝ่ายการเงิน (CFO) ถึงแม้ปัจจุบันจะยังไม่มีตำแหน่งนี้ แต่ CIO จะเป็นผู้จำแนกแยกแยะ เก็บรวบรวม และจัดการข้อมูลในรูปแบบของแหล่งทรัพยากรขององค์กร เป็นผู้กำหนดนโยบายด้านสารสนเทศขององค์กร และจัดการดูแลระบบในสำนักงานและที่อื่นๆ ทั้งหมด” แม้ว่าบทบาทหน้าที่ของ CIO ตามที่ไซนอตต์ได้อธิบายไว้จะกลายเป็นจริงในระดับหนึ่งแล้ว แต่จนถึงทุกวันนี้ CIO ก็ยังมีสถานะไม่เท่าเทียมกับ CEO และ CFO อย่างไรก็ตาม สิ่งต่างๆ กำลังเปลี่ยนแปลงไป สืบเนื่องจากเทรนด์ใหม่ๆ เช่น โมบิลิตี้, คลาวด์คอมพิวติ้ง, ซอฟต์แวร์ ดีฟาย ดาต้าเซ็นเตอร์ (SDDC), อินเทอร์เน็ต ออฟ ธิงค์ (IoT), บิ๊กดาต้า และเทคโนโลยีการวิเคราะห์ข้อมูลต่างๆ

องค์กรหลายแห่งเริ่มตระหนักถึงความสำคัญของเรื่องนี้ ดังจะเห็นได้ว่าสถานะของ CIO กำลังเปลี่ยนแปลงอย่างน่าสนใจ กล่าวคือ บริษัทต่างๆ ต้องการ CIO ที่เข้าใจเทคโนโลยีอย่างถ่องแท้ และยังต้องมีความเข้าใจของทุกฝ่ายที่เกี่ยวข้องอย่างลึกซึ้ง ซึ่งรวมถึงลูกค้าด้วย รวมถึงต้องเข้าใจรูปแบบและวิธีการดำเนินธุรกิจของบริษัทของตน บริษัทเหล่านี้ต้องการ CIO ที่สามารถทำหน้าที่ผู้นำในระดับแนวหน้า และสามารถปฏิรูปแผนกเทคโนโลยีสารสนเทศจากหน่วยงานที่ทำหน้าที่ดูแลรักษาฮาร์ดแวร์และซอฟต์แวร์ ให้กลายเป็นผู้ให้บริการที่ขับเคลื่อนการสร้างสรรค์นวัตกรรมทางด้านธุรกิจ นวัตกรรมคือภารกิจใหม่ที่สำคัญของ CIO ทุกคน และถึงเวลาแล้วที่ CIO จะต้องเตรียมพร้อมและลงมือปฏิบัติอย่างจริงจัง

ปีที่ผ่านมาเป็นช่วงเวลาแห่งการทดสอบหลายๆ อย่างที่เกี่ยวกับไซเบอร์ซีเคียวริตี้ มีเรื่องราวมากมายเกี่ยวกับกรณี

ปัญหาข้อมูลรั่วไหลที่เกิดขึ้น โดยหลายๆ กรณีที่เกิดขึ้นเกี่ยวข้องกับบริษัทประกันสุขภาพ (เช่น Anthem และ Premera) และกรณีข้อมูลรั่วไหลครั้งใหญ่ที่เกิดขึ้นกับหน่วยงานที่สำคัญของรัฐบาลกลาง (สำนักงานบริหารจัดการบุคลากรของสหรัฐฯ) ซึ่งข้อมูลลับเกี่ยวกับเจ้าหน้าที่ของรัฐทั้งในอดีตและปัจจุบันเกือบ 22 ล้านคนได้ถูกโจรกรรม พร้อมด้วยข้อมูลทางชีวภาพ (biometric data)ของเจ้าหน้าที่รัฐกว่า 5 ล้านคน

ด้วยเหตุนี้ บทบาทของ CIO จึงมีความสำคัญเพิ่มขึ้นอย่างมาก ทั้งนี้ 91% ขององค์กรด้านสาธารณสุขทั่วโลกประสบปัญหาข้อมูลรั่วไหลอย่างน้อยหนึ่งครั้งในช่วงสองปีที่ผ่านมา นอกจากนั้น ข้อมูลจาก IBM และ Ponemon Institute ระบุว่า มูลค่าความเสียหายโดยเฉลี่ยของกรณีข้อมูลรั่วไหลในปัจจุบันแตะระดับเกือบ 3.8 ล้านเหรียญสหรัฐฯ เพิ่มขึ้น 23 เปอร์เซ็นต์เมื่อเทียบกับปี 2556 ในขณะที่ CIO ทุกคนกำลังจัดเตรียมรายการสิ่งที่ต้องทำในปีใหม่นี้ ควรพิจารณาสิ่งที่ควรหลีกเลี่ยงหรือสิ่งที่ควรระวังเกี่ยวกับกลยุทธ์ด้านไซเบอร์ซีเคียวริตี้ควบคู่กันไปด้วยดังต่อไปนี้

1. อย่าสับสนระหว่างไซเบอร์ อินชัวรันส์ กับ ไซเบอร์ ซีเคียวริตี้: การรักษาไว้ซึ่งแผนสำรองทางการเงินนับเป็นสิ่งที่ขาดไม่ได้ในเรื่องที่เกี่ยวข้องกับสินทรัพย์ที่สำคัญที่สุดของธุรกิจ
ตลาดด้านไซเบอร์ อินชัวรันส์กำลังขยายตัวอย่างต่อเนื่อง เพราะบริษัทต่างๆ เริ่มตระหนักถึงความสำคัญของไซเบอร์ อินชัวรันส์ อย่างไรก็ดี ควรระลึกอยู่เสมอว่าไซเบอร์ อินชัวรันส์
ไม่สามารถปกป้องข้อมูลสำคัญขององค์กรได้ และไซเบอร์ อินชัวรันส์ เป็นเพียงองค์ประกอบเล็กๆ ของกลยุทธ์การรักษาความปลอดภัยทั้งหมดขององค์กรเท่านั้น

2. อย่าละเลยการให้ความรู้แก่ฝ่ายทรัพยากรบุคคลในเรื่องที่เกี่ยวกับแนวทางปฏิบัติทางด้าน
ไซเบอร์ ซีเคียวริตี้ โดยมากแล้วพนักงานมักจะเป็นผู้ก่อให้เกิดจุดอ่อนในโครงสร้างพื้นฐาน
ไซเบอร์ ซีเคียวริตี้ ดังนั้นองค์กรธุรกิจควรจะให้ความรู้แก่พนักงานเกี่ยวกับวิธีการใช้เครื่องมือ อีเมล และอินเทอร์เน็ตอย่างเหมาะสม เพื่อหลีกเลี่ยงการก่อให้เกิดความเสี่ยงต่อเครือข่ายขององค์กร ควรให้การอบรมและจัดเวิร์คช็อปเพื่อให้พนักงานทราบว่าลิงก์ที่มากับอีเมลนั้น ลิงก์ใดคลิกได้ ลิงก์ใดไม่ควรคลิก และมีเว็บไซต์อะไรบ้างที่พนักงานไม่ควรเข้าเยี่ยมชม การให้ความรู้ดังกล่าวเป็นอีกทางหนึ่งที่จะช่วยป้องกันไม่ให้อีเมลหลอกลวงและมัลแวร์เล็ดลอดเข้าสู่เครือข่ายของบริษัทได้

3. อย่าจ่ายค่าไถ่: ก่อนอื่นคุณควรระวังอย่าตกเป็นเหยื่อของมัลแวร์เรียกค่าไถ่ (Ransomware) การให้ความรู้แก่พนักงานและการติดตั้งโซลูชั่นป้องกันมัลแวร์เรียกค่าไถ่อาจช่วยแก้ไขปัญหานี้ได้ในระดับหนึ่ง อย่างไรก็ตาม หากว่าท้ายที่สุดแล้วมีปัญหาเกิดขึ้น ทีมงานที่มีหน้าที่แก้ไขปัญหาจะต้องพร้อมรับมือกับสถานการณ์ดังกล่าว เช่น การแบ็คอัพข้อมูลอย่างเหมาะสมล่วงหน้า ซึ่งจะช่วยให้คุณมั่นใจว่าจะไม่สูญเสียข้อมูลสำคัญ และคุณก็ไม่จำเป็นต้องจ่ายค่าไถ่
ตามคำเรียกร้องของอาชญากรไซเบอร์

พึงระลึกไว้เสมอว่าเมื่อเหยื่อคนใดคนหนึ่งจ่ายเงินค่าไถ่ให้แก่อาชญากรไซเบอร์ นั่นหมายถึงการส่งเสริมให้คนร้าย

โจมตีองค์กรหรือเหยื่อรายอื่นๆ เพิ่มมากขึ้น ดังนั้น ด้วย “ความรับผิดชอบ
ต่อสังคมไซเบอร์” คุณจะต้อง “ปฏิเสธ” การจ่ายเงินค่าไถ่

4. อย่าละเลยแผนรับมือภัยพิบัติของบริษัท: องค์กรหลายแห่งไม่ได้กำหนดกลยุทธ์ที่เหมาะสมเพื่อรับมือกับภัยพิบัติ ขณะที่บางองค์กรมีแผนการรับมือที่หละหลวมและไร้ประสิทธิภาพ
ไม่สามารถใช้งานได้จริงเมื่อเกิดปัญหา หรืออาจทำให้ปัญหาลุกลามมากยิ่งขึ้น โดยเฉพาะ
อย่างยิ่งในกรณีที่ธุรกิจต้องหยุดชะงักเป็นเวลานานจนอาจสร้างความเสียหายร้ายแรงทางการเงิน และทำให้ทั้ง
บริษัทกลายเป็นอัมพาต การรับมือกับกรณีการละเมิดระบบรักษาความปลอดภัยไม่ใช่เพียงแค่การตอบโต้ต่อภัย
คุกคามที่แทรกซึมเข้ามาเท่านั้น แต่จะต้องเป็นแนวทางดำเนินการที่ถูกต้องเหมาะสม ซึ่งองค์กรได้พัฒนาปรับปรุง
อย่างต่อเนื่องและทดสอบการใช้งานจริงเมื่อเกิดปัญหา

ในปี 2559 นี้ CIO จะต้องตรวจสอบให้แน่ใจว่าบริษัทมีแผนรับมือกับภัยพิบัติที่ออกแบบอย่างเหมาะสม รวมถึงการกำหนดกลยุทธ์และการทดสอบการใช้งาน ก่อนที่ปัญหาการเจาะระบบเครือข่ายจะเกิดขึ้นจริง

5. อย่าผ่อนผันเรื่องคุณภาพของโซลูชั่นที่เกี่ยวกับไซเบอร์ ซีเคียวริตี้: เหนือสิ่งอื่นใดคืออย่าลงทุนในเครื่องมือหรือโซลูชั่นที่ไร้ประสิทธิภาพ โดยเฉพาะอย่างยิ่งในกรณีที่มีข้อมูลสำคัญทางธุรกิจเป็นเดิมพัน บริษัทไม่สามารถแบกรับความเสียหายมูลค่ามหาศาลที่อาจเกิดขึ้นจากการเลือกใช้โซลูชั่นที่ไม่เหมาะสม

ระบบคลาวด์และโมบาย คอมพิวติ้ง กำลังขยายขอบเขตของสภาพแวดล้อมไอทีออกไปสู่ภายนอกองค์กร และอินเทอร์เน็ต ออฟ ธิงค์ (IoT) กำลังขยายพื้นที่การโจมตีให้กว้างขวางมากขึ้น แนวโน้ม
ไซเบอร์ซีเคียวริตี้ในปัจจุบันกำลังเปลี่ยนแปลงอย่างรวดเร็ว อย่างไรก็ตาม เรายังมีโอกาสที่จะชนะอยู่บ้าง เพราะ
อาชญากรไซเบอร์ไม่ใช่อัจฉริยะที่ไม่มีใครปราบได้ หากแต่เป็นกลุ่มคนร้ายที่ฉลาดและโจมตี
อย่างเป็นระบบ กุญแจสำคัญสู่ชัยชนะก็คือ การซ้อนกลเพื่อแก้ลำอาชญากรไซเบอร์เหล่านั้น
ด้วยกลยุทธ์ด้านไซเบอร์ ซีเคียวริตี้ที่เหนือกว่า เช่น การเลือกใช้โซลูชั่นที่เหมาะสม การรู้ว่าควรทำและควรหลีกเลี่ยงสิ่งใด การให้ความรู้ต่อพนักงานขององค์กร เป็นต้น

เกี่ยวกับเทรนด์ไมโคร

เทรนด์ไมโคร อินคอร์ปอเรทเต็ด ผู้นำระดับโลกด้านโซลูชั่นความปลอดภัยไซเบอร์ มุ่งมั่นที่จะช่วยให้การแลกเปลี่ยนข้อมูลดิจิทัลในโลกของเราเป็นไปอย่างปลอดภัย เทรนด์ไมโครมีโซลูชั่นที่ให้บริการผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยหลายระดับให้กับดาต้าเซ็นเตอร์, คลาวด์, เน็ตเวิร์ค และเครื่องลูกข่าย ผลิตภัณฑ์และโซลูชั่นทั้งหมดของเทรนด์ไมโครผสานการทำงานร่วมกันเพื่อให้ข้อมูลเชิงลึกเกี่ยวกับการป้องกันภัยคุกคามอย่างชาญฉลาด และสร้างการป้องกันภัยคุกคามที่เกี่ยวโยงกันหลายส่วน ด้วยการควบคุมและแสดงผลแบบรวมศูนย์ ซึ่งช่วยให้สามารถป้องกันภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น

เทรนด์ไมโครมีพนักงานมากกว่า 5,000 คนในกว่า 50 ประเทศ มีผลิตภัณฑ์ โซลูชั่น และความเชี่ยวชาญในการป้องกันภัยคุกคามที่ทันสมัยที่สุดในโลก เราช่วยให้องค์กรต่างๆ เดินทางสู่การใช้งานระบบคลาวด์ได้อย่างปลอดภัย ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.co.th, www.trendmicro.com