แนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศ 2019

วิชย์ศุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

6. การควบรวม และซื้อกิจการ

มูลค่าของการควบรวม และเข้าซื้อกิจการสูงถึง 4 ล้านล้านดอลลาร์ในปี 2018 แสดงให้เห็นถึงการรวมกันของธุรกิจ และการผสานกระบวนการ รวมถึงระบบเทคโนโลยีสารสนเทศระหว่างองค์การที่เกิดขึ้นจำนวนมาก ถึงแม้ว่าในหลายๆ กรณีอาจมีวิธีการที่เหมาะสมซึ่งประเมินแล้วว่าไร้ความเสี่ยงด้านความปลอดภัยในโลกไซเบอร์ แต่ก็ไม่ได้หมายความว่าการควบรวมกิจการดังกล่าว จะมีแนวทางด้านความปลอดภัยทางไซเบอร์เป็นไปในทิศทางเดียวกัน แต่จะมุ่งให้ความสำคัญที่แผนการควบรวมกิจการในส่วนอื่นๆ มากกว่า องค์การจึงจำเป็นต้องประสานแนวทางการรักษาความปลอดภัยไซเบอร์ร่วมกัน และยกขึ้นมาเป็นเรื่องสำคัญที่ต้องดำเนินการ เพราะปัจจุบันปฏิเสธไม่ได้เลยว่าจะต้องอาศัยเทคโนโลยีสารสนเทศในการขับเคลื่อนองค์การเป็นหลัก

7. กฎ ระเบียบ ข้อบังคับ

กฎ ระเบียบ ข้อบังคับ และมาตรฐานที่เพิ่มขึ้นที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ได้รับการออกแบบมาเพื่อปกป้องลูกค้า ความเร็วของการออกกฎระเบียบไซเบอร์ และบังคับใช้ภายในองค์การนั้นเพิ่มขึ้นตั้งแต่ปี 2018 โดยหลายองค์การกำหนดขั้นตอนสำหรับจัดการความเสี่ยงในการปฏิบัติงานตามกฎระเบียบที่เพิ่มขึ้น อย่างไรก็ตาม กฎระเบียบ และการปฏิบัติตามกฎระเบียบนั้น เป็นเพียงส่วนการควบคุม และป้องกันจากภายในเท่านั้น องค์การจะต้องสร้างความสมดุลให้กับกฎระเบียบใหม่ และการพัฒนากลไกการป้องกันภัยคุกคามทางไซเบอร์ในด้านอื่นๆ ควบคู่กันไปด้วย

8. คณะกรรมการบริหาร

การกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ ยังคงเป็นประเด็นสำคัญให้คณะกรรมการบริหารต้องตัดสินใจดำเนินการใน

เรื่องต่างๆ ที่เกี่ยวข้อง ความเสี่ยงส่วนบุคคลที่เพิ่มขึ้นทำให้คณะกรรมการบริหารต้องขยายขอบเขตการบริหารจัดการอย่างต่อเนื่อง โดยต้องเปลี่ยนแนวคิดจากการกำหนดนโยบายเพื่อป้องกันเป็นการกำหนดนโยบายหรือวางแผนเชิงรุกมากขึ้น

จากรายงานข้างต้น Aon ในฐานะขององค์การที่ปรึกษาได้สะท้อนผลการวิเคราะห์ออกมา ในมุมที่มองมาจากภายในองค์การในลักษณะของประเด็นความเสี่ยงที่องค์การต้องเตรียมพร้อมเพื่อรับมือกับภัยไซเบอร์ซึ่งเริ่มคืบคลานเข้ามาเป็นส่วนหนึ่งของกิจวัตรประจำวันส่วนบุคคลของบุคลากร ทั้งจากการดำเนินกิจกรรมส่วนตัวที่เกี่ยวพัน และเชื่อมต่อกับเทคโนโลยีอยู่เกือบตลอดเวลา และการปฏิบัติงานให้กับองค์การที่เกี่ยวข้องกับการเชื่อมต่อกับเทคโนโลยีเช่นกัน จนเหมือนกับผสานเป็นเรื่องเดียวกัน ส่งผลต่อพฤติกรรมของบุคลากร ทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้นควบคุมได้ยากมากขึ้นเป็นลำดับ ถือว่าเป็นโจทย์ยากที่องค์การต้องเผชิญในช่วงนี้ผมขอเรียกว่า “การเปลี่ยนผ่านพฤติกรรมไซเบอร์” ของบุคลากร จนกว่าจะมีการผสานชีวิตส่วนตัวกับการทำงานที่ลงตัวมากขึ้น และเหมาะสม

รายงานฉบับต่อมาคือ Risk in Focus 2019 report ของสมาพันธ์สถาบันตรวจสอบภายในแห่งยุโรป (ECIIA) ซึ่งเป็นบทวิเคราะห์ที่สำรวจจากองค์การชั้นนำ และได้รับการยอมรับติด 1 ใน 5 รายงานผลการวิเคราะห์ที่ได้รับการยอมรับในระดับโลก โดย ECIIA กล่าวว่า ค่าใช้จ่ายทั่วโลกที่เกิดจากอาชญากรรมไซเบอร์ จะเพิ่มขึ้นเป็น 6 ล้านล้านดอลลาร์ในช่วงระหว่างปี 2015 ถึงปี 2021 แสดงให้เห็นถึงภัยคุกคามที่มีความซับซ้อนมากขึ้น และกระทบกับองค์การในทุกอุตสาหกรรม หลายองค์การใช้ประโยชน์จากการทดสอบการเจาะระบบ และข้อมูลอย่างมีจริยธรรม (White hack) ซึ่งดำเนินการด้วยองค์การ และบุคลากรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยเพื่อประเมินให้แน่ใจว่า ระบบขององค์การนั้นได้มาตรฐานและปลอดภัย

รายงาน Risk in Focus 2019 report ของ ECIIA กล่าวถึงประเด็นด้านความปลอดภัยไซเบอร์โดยสรุป ดังนี้

■ ความเสี่ยงที่เกิดจาก Cloud เพิ่มมากขึ้น

ความเสี่ยงด้านความปลอดภัยทางไซเบอร์นั้นเพิ่มขึ้นตามการใช้บริการบนระบบ Cloud โดย Microsoft ได้รายงานว่ามีการโจมตีบัญชีลูกค้า Cloud-Azure เพิ่มขึ้นถึงสี่เท่าในปี 2017 ถึงแม้ว่าเทคโนโลยี และความปลอดภัยของ ระบบ Cloud นั้น จะสามารถทนทานต่อการโจมตีทางไซเบอร์ได้เป็นอย่างดี แต่ทว่าการโจรกรรมข้อมูลส่วนใหญ่เกิดจากรหัสผ่านที่คาดเดาได้ง่าย ตามมาด้วยการโจมตีในรูปแบบการสร้างข้อมูลลวง (Phishing) และการฝ่าฝืนข้อกำหนดการให้บริการของบุคคลที่สาม ซึ่ง ECIIA แนะนำว่าองค์การควรประเมินว่าในการย้ายข้อมูล และระบบจากสภาพแวดล้อมเดิม

เพื่อไปให้บริการบนระบบทรัพยากรสารสนเทศที่เข้มแข็งขึ้นนั้น ได้พิจารณาเรื่องความปลอดภัยของผู้ให้บริการเป็นหลักหรือไม่ มีระบบที่สามารถจะตรวจจับการละเมิดที่อาจเกิดขึ้นได้หรือไม่ รวมถึงการทำให้แน่ใจว่าคู่ค้า และพันธมิตรทางธุรกิจมีวิธีการและระบบที่มีประสิทธิภาพที่เท่าเทียมกันในการรักษาความปลอดภัยทางไซเบอร์หรือไม่

■ กฎเกณฑ์การปกป้องข้อมูลที่มีความสอดคล้องกัน

ภายใต้กฎเกณฑ์การคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป (GDPR) ทั้งตัวควบคุมข้อมูล และตัวประมวลผลข้อมูลจะต้องรับผิดชอบร่วมกัน และรับผิดชอบต่อความเสียหายที่เกิดจากการฝ่าฝืนข้อมูล ผลที่ตามมาอาจรุนแรง นอกเหนือจากค่าปรับที่ลงโทษสูงถึง 20 ล้านยูโร สหภาพยุโรปสามารถสั่งให้ยุติการดำเนินธุรกิจเพื่อป้องกันการประมวลผลข้อมูลเพิ่มเติมที่จะก่อให้เกิดความเสียหาย ทำให้ลดมูลค่าของความสูญเสียได้อย่างมีนัยสำคัญ

นอกจากนี้ภายในเดือนพฤษภาคม 2018 จีนได้เผยแพร่คำแนะนำโดยละเอียดเกี่ยวกับการปฏิบัติตามกฎหมายความปลอดภัยทางไซเบอร์ของตนเองซึ่งมีผลบังคับใช้มาตั้งแต่ปี 2016 องค์การใดๆ ที่จัดการกับข้อมูลส่วนบุคคลของประชาชนชาวจีน จะต้องดำเนินการตามกฎระเบียบดังกล่าว ในสหรัฐอเมริกาองค์การที่ต้องการเปิดเผยข้อมูลที่ถูกคุ้มครองด้วยสหภาพยุโรปจะต้องได้รับการรับรองภายใต้โครงการคุ้มครองความเป็นส่วนตัวของ EU-US

อย่างไรก็ตามก็ยังมีเรื่องอื้อฉาวในสภาพยุโรปซึ่งส่งผลต่อชื่อเสียงขององค์การจำนวนมากซึ่งถูกเปิดเผยผ่านสื่อสาธารณะในช่วง 12 เดือนที่ผ่านมาเกี่ยวกับการโจรกรรมหรือการใช้ข้อมูลส่วนบุคคลในทางที่ผิด ทำให้เกิดปัญหามากมายต่อผู้บริโภค โดย 27% ขององค์การธุรกิจในสหภาพยุโรปรายงานว่าสามารถปฏิบัติตามกฎระเบียบใหม่ได้ภายในหนึ่งเดือนหลังจากมีผลบังคับใช้ และอีก 93% คาดว่าจะแก้ไขปัญหานี้ได้ภายในปี 2019 ทำให้เห็นว่าการปฏิบัติตามมาตรฐานข้อมูลระหว่างประเทศนั้นเป็นเรื่องของทั้งระเบียบ และชื่อเสียงซึ่งมีความสำคัญต่อองค์การอย่างมาก และต้องดำเนินการให้มีความสอดคล้องกับกฎเกณฑ์ที่เกี่ยวข้องของแต่ละประเทศให้เป็นสากล

อ่านต่อฉบับหน้า