การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์

บทบาทของแนวป้องกัน 3 ชั้น

The Institute of Internal Auditors | Global

สารบัญ

บทสรุปสำหรับผู้บริหาร

องค์กรทุกประเภทกำลังเสี่ยงต่อภัยคุกคามทางไซเบอร์มากขึ้น เนื่องจากองค์กรพึ่งพาการใช้คอมพิวเตอร์ เครือข่าย โปรแกรม และระบบงาน/แอพพลิเคชัน สื่อสังคมออนไลน์ และข้อมูล ที่เพิ่มมากขึ้นเรื่อยๆ การละเมิดด้านความปลอดภัยสามารถส่งผลกระทบเชิงลบต่อองค์กรและลูกค้าขององค์กรทั้งในด้านการเงินและชื่อเสียง การเชื่อมต่อกันได้ทั่วโลกและการเข้าถึงสารสนเทศโดยผู้ใช้งานภายนอกองค์กรเพิ่มความเสี่ยงมากไปกว่าที่เคยมีมาในอดีตซึ่งได้รับการจัดการด้วยวิธีการควบคุมทั่วไป (General Control) และการควบคุมระบบงาน (Application Control) การพึ่งพาขององค์กรต่อระบบสารสนเทศและการพัฒนาเทคโนโลยีใหม่ๆ ทำให้การประเมินการควบคุมทั่วไปและการควบคุมระบบงานแบบดั้งเดิมนั้นไม่เพียงพอที่จะให้ความเชื่อมั่นด้านความมั่นคงปลอดภัยทางไซเบอร์ได้

ความมั่นคงปลอดภัยทางไซเบอร์จะหมายถึงเทคโนโลยี กระบวนการ และวิธีปฏิบัติที่ได้รับการออกแบบให้ปกป้องสินทรัพย์ที่เกี่ยวกับสารสนเทศขององค์กร (คอมพิวเตอร์ เครือข่าย โปรแกรม และข้อมูล) จากการเข้าถึงโดยไม่ได้รับอนุญาต ความถี่และความรุนแรงของการโจมตีทางไซเบอร์ที่กำลังเพิ่มขึ้นเรื่อยๆ ทำให้การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ดีขึ้นเป็นสิ่งจำเป็น

หน่วยงานตรวจสอบภายในมีบทบาทที่สำคัญยิ่ง ในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร โดยพิจารณาว่า:

- ใครที่มีสิทธิเข้าถึงสารสนเทศที่มีคุณค่ามากที่สุดขององค์กรได้?
- สินทรัพย์ใดที่น่าจะเป็นเป้าหมายที่จะถูกโจมตีทางไซเบอร์ได้มากที่สุด
- ระบบใดที่จะเกิดความเสียหายที่มีนัยสำคัญมากที่สุดหากมีช่องโหว่
- ข้อมูลใดถ้ามีผู้ซึ่งไม่ได้รับอนุญาตได้รับไปแล้ว จะทำให้เกิดการสูญเสียด้านการเงินและความสามารถในการแข่งขัน เกิดปัญหาที่เกี่ยวข้องทางกฎหมายตามมา หรือเสียชื่อเสียงขององค์กร
- ผู้บริหารมีการเตรียมตัวเพื่อตอบสนองได้ในเวลาที่เหมาะสม หากเกิดเหตุการณ์ซึ่งเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ขึ้น แล้วหรือไม่

แนวปฏิบัตินี้จะพูดคุยถึงบทบาทของหน่วยงานตรวจสอบภายในที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งรวมถึง:

- บทบาท CAE (Chief Auditing Executives - CAE) ที่เกี่ยวข้องกับการให้ความเชื่อมั่น การกำกับดูแล ความเสี่ยง และภัยคุกคามทางไซเบอร์
- การประเมินความเสี่ยงตามธรรมชาติ (Inherent Risks) และภัยคุกคาม (Threats)
- บทบาทและภาระหน้าที่ของแนวป้องกันชั้นแรก ชั้นที่สอง และชั้นที่สาม ที่เกี่ยวข้องกับการบริหารความเสี่ยง การควบคุม และการกำกับดูแล
- ช่องว่างของการให้ความเชื่อมั่นอาจเกิดขึ้นที่ใดได้บ้าง
- ภาระหน้าที่ในการรายงานของหน่วยงานตรวจสอบภายใน

นอกจากนี้แล้ว แนวปฏิบัติฉบับนี้ได้สำรวจถึงความเสี่ยงที่เกิดขึ้นใหม่ๆ และภัยคุกคามทั่วไปที่แนวป้องกันทั้ง 3 ชั้นได้เผชิญ และนำแนวทางอย่างตรงไปตรงมาในการประเมินความเสี่ยงและวิธีการควบคุมด้านความมั่นคงปลอดภัยทางไซเบอร์

บทนำและนัยสำคัญทางธุรกิจ

ผู้ตรวจสอบภายในจำเป็นต้องมีวิธีการให้ความเชื่อมั่นที่เป็นปัจจุบันสำหรับการให้ความเชื่อมั่นเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ แม้ว่าการประเมินวิธีการควบคุมทั่วไปสำหรับด้าน IT (IT General Control) จะมีประโยชน์ก็ตาม แต่ก็ยังไม่เพียงพอในการให้ความเชื่อมั่นด้านความมั่นคงปลอดภัยทางไซเบอร์ เพราะว่าการควบคุมทั่วไปด้าน IT เหล่านั้นไม่เหมาะสมทั้งในด้านกาลเวลาและความสมบูรณ์ วัตถุประสงค์พื้นฐานในการตรวจสอบภายใน เช่น ความสมบูรณ์ ความถูกต้อง และการให้สิทธิยังคงมีความเกี่ยวข้องอยู่ อย่างไรก็ตาม ปัจจัยใหม่ๆ ที่เกิดขึ้นจำนวนมากกำลังขับเคลื่อนให้มีความจำเป็นที่จะต้องมีแนวทางการตรวจสอบภายในที่เป็นปัจจุบันเพื่อให้ได้ข้อสรุปในการยืนยันถึงความมั่นคงปลอดภัยทางไซเบอร์ที่มีคุณค่า

การเพิ่มขึ้นอย่างรวดเร็วของเทคโนโลยีในวันนี้ ทำให้เกิดการเข้าถึงสารสนเทศขององค์กรจากผู้ใช้งานมากยิ่งขึ้นกว่าแต่ก่อน บุคคลที่สามได้รับสิทธิการเข้าถึงระบบสารสนเทศองค์กรมากขึ้นโดยผ่านห่วงโซ่อุปทาน ลูกค้า และผู้ให้บริการ ข้อมูลที่มีความหลากหลายมากขึ้นก็พร้อมใช้งานได้ทันทีเนื่องจากองค์กรหลายๆ แห่งมักจัดเก็บสารสนเทศที่อ่อนไหวและเป็นความลับจำนวนมากไว้ในโครงสร้างพื้นฐานเสมือนจริง (Virtualized Infrastructure) ที่สามารถเข้าถึงได้โดยผ่านการประมวลผลแบบคลาวด์ (Cloud Computing)

ปัจจัยอื่นที่ส่งผลกระทบต่อแนวทางการตรวจสอบภายในคือ การเพิ่มขึ้นของจำนวนอุปกรณ์ที่สามารถเชื่อมต่อและมีส่วนในการแลกเปลี่ยนข้อมูลอยู่เสมอ (เป็นที่รู้จักกันในนาม “อินเทอร์เน็ตในทุกสิ่ง” หรือ“Internet of Things”) เมื่อองค์กรต่างๆ อยู่ในยุคโลกาภิวัฒน์ (Globalize) และเวบขององค์กรที่เกี่ยวกับพนักงาน ลูกค้า และผู้ให้บริการซึ่งเป็นบุคคลที่สามได้ขยายออกไป ความคาดหวังที่จะเข้าถึงสารสนเทศขององค์กรได้อย่างสม่ำเสมอก็มีเพิ่มขึ้นอีกด้วย คนรุ่นใหม่ที่เกิดมาในยุคดิจิทัล (Digital Natives)[1] คาดหวังที่จะเข้าถึงข้อมูลแบบเรียลไทม์ (Real-time Access) ได้จากทุกๆ ที่

ภัยคุกคามที่ไม่คาดคิดอาจเกิดขึ้นมาได้จาก ความสัมพันธ์ที่ไม่เป็นมิตรระดับโลก (Hostile global relationships) กลุ่มแฮกเกอร์ที่ร่วมกันกระทำความผิด (Organized Hackers) บุคคลภายในองค์กร (Insiders) รวมถึงซอฟต์แวร์และบริการที่ไม่ได้มาตรฐาน ระเบียบพิธีการ (protocol) ด้านความมั่นคงปลอดภัยทางไซเบอร์อาจซับซ้อนมากขึ้น ในขณะที่ข้อกำหนดและมาตรฐานของทางการเกี่ยวกับการเปิดเผยเหตุการณ์หรือ

[1] คำว่า “digital native” ได้ถูกใช้ในปี 2544 ในบทความเรื่อง “Digital Natives Digital Immigrants” โดยที่ปรึกษาทางการศึกษาและผู้เขียน ชื่อ Marc Prensky ใช้กล่าวถึง คนในรุ่นที่เติบโตมากับการใช้ภาษาดิจิทัลของ คอมพิวเตอร์ วีดีโอเกม สื่อสังคม และสิ่งอื่นๆ ที่คล้ายกัน

การละเมิดด้านความมั่นคงปลอดภัยทางไซเบอร์ยังคงเพิ่มมากขึ้นเรื่อยๆ ความสำคัญของการตรวจพบและสื่อสารเหตุการณ์ความเสี่ยงภายในเวลาที่กำหนดไว้ มีน้ำหนักมากกว่าคุณค่าในเชิงป้องกันของวิธีการควบคุมทั่วไปด้าน IT ที่เป็นแบบดั้งเดิมและอยู่รอบๆ

เพื่อตอบสนองกับความเสี่ยงใหม่ๆ ที่เกิดขึ้น CAE ทั้งหลายได้เผชิญกับความท้าทายในการให้ความมั่นใจว่าผู้บริหารได้นำวิธีการควบคุมเชิงป้องกันและตรวจพบมาใช้งาน CAE ต้องสร้างแนวทางการตรวจสอบภายในที่ชัดเจนเพื่อประเมินความเสี่ยงและความสามารถในการตอบสนองของผู้บริหารด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมุ่งเน้นถึงเวลาตอบสนองที่สั้นขึ้น CAE ควรที่จะใช้ประโยชน์จากความเชี่ยวชาญของผู้ที่อยู่ในแนวป้องกันชั้นที่หนึ่งและชั้นที่สอง เพื่อที่จะได้ข้อมูลที่เป็นปัจจุบันเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์

ความเสี่ยงที่สำคัญและภัยคุกคามที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

ความมั่นคงปลอดภัยทางไซเบอร์เกี่ยวข้องกับระบบที่สนับสนุนวัตถุประสงค์ขององค์กรที่เกี่ยวกับประสิทธิผลและประสิทธิภาพของการดำเนินงาน ความน่าเชื่อถือของรายงานภายในและภายนอก และการปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่บังคับใช้ องค์กรมักจะออกแบบ และนำเอาวิธีการควบคุมด้านความมั่นคงปลอดภัยทางไซเบอร์มาใช้ทั่วทั้งองค์กรเพื่อปกป้องความถูกต้องสมบูรณ์ (Integrity) ความลับ (Confidentiality) และความพร้อมใช้ (Availability) ของสารสนเทศ

การโจมตีทางไซเบอร์ยังคงดำเนินต่อไปด้วยเหตุผลหลายประการซึ่งได้แก่ การทุจริตด้านการเงิน การขโมยข้อมูล หรือใช้ข้อมูลในทางที่ผิด สาเหตุที่เกิดจากนักเคลื่อนไหว (Activist Causes) ต้องการทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้ และต้องการทำลายโครงสร้างพื้นฐานและบริการที่สำคัญของรัฐบาลหรือองค์กร แหล่งที่มาของภัยคุกคามทางไซเบอร์โดยทั่วไปทั้ง 5 แหล่ง ได้แสดงไว้ในตารางที่ 1

ตารางที่ 1: แหล่งที่มาของภัยคุกคามทางไซเบอร์ทั่วไป 5 แหล่ง

- ประเทศ-รัฐ
- อาชญากรรมในโลกไซเบอร์
- แฮกเกอร์นักเคลื่อนไหว (Hacktivists) บุคคลที่ใช้ระบบคอมพิวเตอร์ในการโจมตีเป้าหมาย เพื่อแสดงความคิดเห็นในทางสังคมหรือการเมือง
- บุคคลภายในองค์กรและผู้ให้บริการ ผู้พัฒนาผลิตภัณฑ์และบริการที่ไม่ได้มาตรฐาน

เพื่อความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับองค์กร เป็นเรื่องสำคัญที่จะต้องระบุว่าสารสนเทศอะไรที่มีค่าต่อบุคคลภายนอก หรือทำให้เกิดการหยุดชะงักที่มีนัยสำคัญถ้าหากมันไม่พร้อมใช้งานหรือเกิดความเสียหายขึ้น นอกจากนี้แล้ว เป็นสิ่งสำคัญที่จะต้องระบุว่าสารสนเทศอะไรที่จะส่งผลให้เกิดความเสียหายด้านการเงินและการแข่งขัน หรือชื่อเสียงขององค์กร ถ้าบุคคลอื่นได้มันไป หรือถูกนำไปเปิดเผยต่อสาธารณะชน

ตัวอย่างของสารสนเทศที่ควรนำมาพิจารณา ประกอบด้วย ข้อมูลลูกค้าและพนักงาน สินทรัพย์ทางปัญญา ห่วงโซ่อุปาทาน คุณภาพและความปลอดภัยของผลิตภัณฑ์ เงื่อนไขในสัญญาและการกำหนดราคา การวางแผนเชิงกลยุทธ์ และข้อมูลด้านการเงิน

อุตสาหกรรมที่องค์กรดำเนินธุรกิจอยู่ก่อให้เกิดบริบทที่สำคัญในการระบุภัยคามทางไซเบอร์ ตัวอย่างเช่น ผู้ค้าปลีกอาจเน้นที่การปกป้องข้อมูลลูกค้าและทำให้มั่นใจว่าการบริการลูกค้าจะไม่หยุดชะงัก ทรัพย์สินทาง

ปัญญาอาจเป็นเรื่องที่ต้องเป็นกังวลที่สำคัญอย่างหนึ่งสำหรับองค์กรที่เป็นศูนย์กลางด้านวิจัยและพัฒนา ผู้ผลิตอาจเน้นเรื่องของความน่าเชื่อถือและประสิทธิภาพของระบบการผลิตและห่วงโซ่อุปาทาน รวมทั้งคุณภาพและความปลอดภัยของผลิตภัณฑ์ บริษัทที่ให้บริการทางวิชาชีพอาจจะต้องระวังมากที่สุดในเรื่องสารสนเทศในทางการค้าซึ่งละเอียดอ่อนที่มีอยู่ในสัญญาและโมเดลต้นทุนทางการเงิน (Financial Costing Models.)

แนวป้องกันสามชั้น: บทบาทและภาระหน้าที่

สมาคมผู้ตรวจสอบภายใน (IIA) ได้ออกเอกสารแสดงจุดยืน (Position Paper) ซึ่งแสดงถึงแนวทางปฏิบัติที่เป็นเลิศเพื่อปรับปรุงประสิทธิผลและประสิทธิภาพของหน่วยงานซึ่งทำหน้าที่เกี่ยวกับความเสี่ยงและการควบคุมภายในองค์กรที่ชื่อว่า “แนวป้องกัน 3 ชั้นสำหรับการบริหารความเสี่ยงและการควบคุมที่มีประสิทธิผล” ตีพิมพ์เมื่อมกราคม 2556 ขั้นตอนที่สำคัญยิ่งในการประเมินบทบาทหน่วยงานตรวจสอบภายในที่เกี่ยวกับเรื่องความมั่นคงปลอดภัยทางไซเบอร์ ก็คือการทำให้มั่นใจได้ว่า แนวป้องกันทั้ง 3 ชั้น ได้มีการแบ่งแยกหน้าที่กันอย่างเหมาะสมและดำเนินการได้อย่างมีประสิทธิผล ยิ่งไปกว่านั้น ระเบียบพิธีการ (protocol) ในการยกระดับปัญหาควรจะได้รับการกำหนดขึ้นมาเพื่อระบุบทบาทและภาระหน้าที่ที่เกี่ยวข้องในการระบุและยกระดับการจัดการความเสี่ยงที่สูงเกินไปจากระดับความเสี่ยงที่องค์กรยอมรับได้ ซึ่งหมายถึงระดับความเสี่ยงที่องค์กรเต็มใจจะยอมรับ

ในฐานะที่เป็นแนวป้องกันชั้นแรก ผู้บริหารเป็นเจ้าของและบริหารข้อมูล กระบวนการ ความเสี่ยง และวิธีการควบคุม สำหรับเรื่องความมั่นคงปลอดภัยทางไซเบอร์นั้นมักตกเป็นหน้าที่ของผู้ดูแลระบบและบุคคลอื่นที่ได้รับมอบหมายให้ดูแลความปลอดภัยของสินทรัพย์ขององค์กร กิจกรรมทั่วไปของแนวป้องกันชั้นแรกมีอยู่ในตารางที่ 2 หน้า 10

แนวป้องกันชั้นที่สองประกอบด้วยหน่วยงานที่ดูแลเรื่องความเสี่ยง การควบคุม และหน่วยงานที่กำกับดูแลการปฏิบัติตามกฎระเบียบซึ่งมีภาระหน้าที่ในการทำให้มั่นใจได้ว่า กระบวนการและวิธีการควบคุมของแนวป้องกันชั้นแรกยังมีคงมีอยู่และดำเนินการได้อย่างมีประสิทธิผล หน่วยงานงานเหล่านี้อาจรวมถึงกลุ่มคนต่างๆ ที่มีภาระหน้าที่ในการทำให้มั่นใจว่า การบริหารความเสี่ยง และการเฝ้าระวังความเสี่ยงและภัยคุกคามในโลกความมั่นคงปลอดภัยทางไซเบอร์มีประสิทธิผล หน้าที่งานทั่วไปที่ดำเนินการโดยแนวป้องกันชั้นที่สองได้แสดงไว้ในตารางที่ 3 หน้า 13

ในฐานะที่เป็นแนวป้องกันชั้นที่สาม หน่วยงานตรวจสอบภายในจะให้ความเชื่อมั่นด้วยความเป็นอิสระและเที่ยงธรรมแก่ผู้บริหารระดับสูงและคณะกรรมการในเรื่องการกำกับดูแล การบริหารความเสี่ยง และวิธีการควบคุม การให้ความเชื่อมั่นนี้รวมถึง การประเมินประสิทธิผลของกิจกรรมต่างๆ ในภาพรวมที่ดำเนินการโดยแนวป้องกันชั้นแรกและชั้นที่สองในการบริหารและบรรเทาความเสี่ยงและภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ กิจกรรมทั่วๆ ไปที่ดำเนินการโดยแนวป้องกันชั้นที่สามได้แสดงให้เห็นคร่าวๆ ในตารางที่ 4 หน้า 17

เจ้าของและกิจกรรมที่สำคัญของแนวป้องกันชั้นที่หนึ่ง (First Line of Defense)

แนวป้องกันชั้นแรกประกอบด้วยผู้จัดการด้านปฏิบัติการซึ่งเป็นเจ้าของและบริหารความเสี่ยงและวิธีการควบคุม และนำเอาวิธีการแก้ไขมาใช้ปฏิบัติเพื่อจัดการแก้ไขข้อบกพร่องของกระบวนการและการควบคุม องค์กรอาจกำหนดให้มีตำแหน่งต่างๆ ได้ แต่ต้องให้มีความตระหนักเรื่องความมั่นคงปลอดภัยทางไซเบอร์ไว้ในจิตใจ

หัวหน้างานด้านเทคโนโลยี (Chief technology officer - CTO) โดยทั่วไป มักจะรับผิดชอบในการให้ความรู้และทิศทางเกี่ยวกับเทคโนโลยีที่มีอยู่เพื่อขับเคลื่อนพันธกิจองค์กรและบ่อยครั้งก็จะมีภาระหน้าที่ในการปกป้องทรัพย์สินทางปัญญาขององค์กรด้วย ภาระหน้าที่ของ CTO อาจรวมถึงการทำให้มั่นใจได้ว่า องค์กรมีการเตรียมตัวสำหรับระยะต่อไปของพัฒนาการทางเทคโนโลยีที่จะช่วยให้เกิดความได้เปรียบทางการแข่งขัน การเปลี่ยนแปลงทางกลยุทธ์ และนวัตกรรม

องค์กรอาจว่าจ้างหัวหน้างานด้านความมั่นคงปลอดภัย (Chief Security Officer - CSO) หัวหน้างานด้านความมั่นคงปลอดภัยสารสนเทศ (Chief information security officer - CISO) หรือบุคคลอื่นใดให้มีภาระหน้าที่เกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

CSO หรือ CISO ในฐานะที่เป็นเสาหลักสำคัญในการระบุและทำความเข้าถึงภัยคุกคามทางไซเบอร์ จะสร้างและนำกลยุทธ์ความมั่นคงปลอดภัยทางไซเบอร์มาปรับใช้ และบังคับใช้นโยบายและวิธีปฏิบัติ พวกเขามักจะรับบทบาทผู้นำในการพัฒนาโครงการ (Programs) การกำกับดูแล เพื่อพิสูจน์ว่าสินทรัพย์ขององค์กรและข้อมูลของผู้มีส่วนได้เสียได้รับการปกป้องอย่างเหมาะสม

หัวหน้างานด้านสารสนเทศ (Chief Information Officer - CIO) อาจได้รับการว่าจ้างให้ทำหน้าที่ในการขับเคลื่อนความได้เปรียบทางการแข่งขัน และการเปลี่ยนแปลงทางกลยุทธ์ตลอดทั่วทั้งองค์กร CIO สามารถรับภาระหน้าที่ในการพัฒนาโครงการความมั่นคงปลอดภัยทางไซเบอร์ การดำเนินการโครงการฝึกอบรมด้านความมั่นคงปลอดภัยทั่วองค์กร และพัฒนานโยบายความมั่นคงปลอดภัยทางไซเบอร์

CTO CSO CISO และ CIO ทำงานร่วมกับประธานเจ้าหน้าที่บริหาร (CEO) และผู้บริหารระดับสูงท่านอื่นๆ ในการต่อสู้กับอาชญากรรมทางไซเบอร์และการโจมตีทางไซเบอร์ที่เกี่ยวข้อง ถ้าหน่วยงานอื่นในองค์กรมีภาระหน้าที่ที่เกี่ยวกับเทคโนโลยีของตนเอง หน่วยงานเหล่านี้ก็ต้องทำหน้าที่ในการออกแบบและนำวิธีการควบคุมที่เหมาะสมมาใช้เพื่อให้เกิดความมั่นคงปลอดภัยในเทคโนโลยีและข้อมูลของพวกเขา พร้อมทั้งประสานงานกับหน่วยงานอื่นที่ทำหน้าที่ประเมินความเสี่ยงภายในองค์กร

ตารางที่ 2: กิจกรรมทั่วไปของแนวป้องกันชั้นแรก

- บริหารงานเกี่ยวกับวิธีปฏิบัติ อบรม และทดสอบด้านความมั่นคงปลอดภัย
- คงไว้ซึ่งการตั้งค่าอุปกรณ์ด้านความมั่นคงปลอดภัย ซอฟต์แวร์ที่มีความเป็นปัจจุบัน และการปรับปรุงซอฟต์แวร์ในส่วนที่ค้นพบว่ามีจุดอ่อน (Security Patch)
- นำระบบตรวจจับการบุกรุกมาปรับใช้งานและดำเนินการทดสอบการเจาะระบบ
- จัดตั้งค่า (Configure) เครือข่ายอย่างมั่นคงปลอดภัยเพื่อให้บริหารและปกป้องกระแสข้อมูลจราจรเครือข่าย(Network traffic flow)ได้อย่างเพียงพอ
- จัดทำทะเบียนสินทรัพย์สารสนเทศ อุปกรณ์ด้านเทคโนโลยี และซอฟต์แวร์ที่เกี่ยวข้อง
- นำแผนงาน (Programs) การปกป้องและป้องกันความเสียหายข้อมูลมาปรับใช้ด้วยการเฝ้าติดตามดูแลที่เกี่ยวข้อง
- จำกัดบทบาทการเข้าถึงเพื่อให้มีสิทธิการใช้งานให้น้อยที่สุด
- เข้ารหัสข้อมูลเมื่อมีความเป็นไปได้ที่จะทำ
- นำการบริหารช่องโหว่มาใช้ด้วยการตรวจกวาด (Scan)แบบภายในและภายนอก
- สรรหาและรักษาผู้ที่มีความสามารถซึ่งมีวุฒิบัตรด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ

เมื่อองค์กรไม่ได้มีขนาดใหญ่พอที่จะสนับสนุนให้มีตำแหน่งต่างๆ ดังกล่าวข้างต้นได้ แนวทางที่ใช้กันอยู่ทั่วไปก็คือ จัดให้มีการรวมตัวกันของผู้จัดการด้านธุรกิจและเทคโนโลยีสารสนเทศผู้ซึ่งมีส่วนได้เสียในการตอบโต้ความเสี่ยงที่มีต่อความปลอดภัยทางไซเบอร์ที่เกี่ยวข้อง ภาระหน้าที่ที่กล่าวมาก่อนหน้านี้อาจได้รับการดูแลโดยบุคลากรเพียงหนึ่งคนหรือมากกว่านั้นที่อยู่ในแนวป้องกันชั้นแรก โดยให้อำนาจที่เหมาะสมในการดำเนินการกับความเสี่ยงที่เกี่ยวข้อง

วิธีการควบคุมภัยคุกคามทางไซเบอร์โดยทั่วไป (Common Cyber Threat Controls)

เนื่องจากภัยคุกคามทางไซเบอร์ได้ถูกออกแบบมาเพื่อทำให้ระบบล่ม หรือเพื่อเก็บ/จับข้อมูล (Capture Data) ภัยคุกคามจึงมักเกิดในที่ซึ่งจัดเก็บข้อมูลสำคัญไว้ อันได้แก่ ศูนย์ข้อมูล (Data Centers) เครือข่ายภายในสภาพแวดล้อมที่ได้เก็บข้อมูลไว้ภายนอก (Externally hosted environments) และแม้กระทั่งแพล็ทฟอร์มเพื่อความต่อเนื่องทางธุรกิจ (Business continuity platforms) ไม่ว่าการโจมตีจะเกิดขึ้นที่ไหนก็ตาม ผลลัพธ์สุดท้ายอาจรวมถึง การละเมิดกฎหมายระเบียบข้อบังคับ ถูกปรับ เสื่อมเสียชื่อเสียง และสูญเสียรายได้

ข้อมูลที่มีความอ่อนไหวและข้อมูลที่เป็นความลับสามารถถูกจัดระดับชั้นและถูกจัดเก็บไว้ภายใน ภายนอก หรือทั้งภายในและภายนอก องค์กรส่วนใหญ่พึ่งพาเทคโนโลยีเช่น การตั้งค่าที่ปลอดภัย (secure configuration) ไฟร์วอลล์ (Firewalls) และการควบคุมการเข้าถึงซึ่งนับเป็นแนวป้องกันชั้นแรก อย่างไรก็ตาม การโจมตีเฉพาะ (Dedicated Attack) เมื่อ Firewall ทำงานหนักเกินไป ผู้โจมตีอาจเข้าถึงและอาจนำรายการที่ไม่ได้รับอนุญาตไปประมวลผลได้

เพื่อลดความเสี่ยงในการโจมตีที่เข้าถึงไฟร์วอลล์ แนวป้องกันชั้นแรกจะดำเนินการเชิงป้องกันที่ขอบเขตของเครือข่าย (perimeter of the network) มันเป็นกระบวนการที่ท้าทายซึ่งเกี่ยวข้องกับการจำกัดการเข้าถึงและปิดกั้นการจราจรของข้อมูลที่ไม่ได้รับอนุญาต (Unauthorized traffic) วิธีการควบคุมเชิงตรวจพบ เช่น การเฝ้าติดตามประเมินผล ควรได้รับการจัดตั้งขึ้นเพื่อเฝ้าระวังช่องโหว่ที่เคยพบเห็นมาก่อนโดยอาศัยข้อมูลที่ได้มาเกี่ยวกับผลิตภัณฑ์ซอฟต์แวร์ องค์กร และเว็บไซต์ประสงค์ร้าย

หลายๆ องค์กรมีการสร้างบัญชีขาวสำหรับแทรฟิก (traffic) ที่ดี และบัญชีดำสำหรับแทรฟิกที่ถูกปิดกั้น อย่างไรก็ตาม การเฝ้าติดตามอย่างมีประสิทธิภาพและมีการปรับปรุงอยู่บ่อยๆ เป็นสิ่งสำคัญ เพราะการรับส่งข้อมูลในเครือข่ายมีลักษณะเปลี่ยนแปลงได้ง่าย ถ้าผู้โจมตีสามารถเข้าถึงระบบได้แล้ว ขั้นตอนต่อไปของการโจมตีคือการพยายามได้สิทธิเป็นผู้ดูแลระบบ (Administrative privileges) และปกปิดร่องรอยของการโจมตี

เมื่อข้อมูลได้ถูกจัดเก็บไว้ภายนอกองค์กร มันเป็นเรื่องที่สำคัญมากสำหรับองค์กรที่จะมั่นใจได้ว่า ผู้ให้บริการมีการบริหารความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสม ขั้นตอนแรกที่สำคัญของแนวป้องกันชั้นแรกคือการทำสัญญาที่เข้มงวดโดยกำหนดให้มี รายงานการควบคุมขององค์กรที่ให้บริการ (service organization control -- SOC) เงื่อนไขเกี่ยวกับสิทธิในการเข้าตรวจสอบ สัญญาระดับของการให้บริการ (service level agreements --SLAs) และ/หรือ งานที่เกี่ยวกับการตรวจความมั่นคงปลอดภัยทางไซเบอร์โดยละเอียด นอกจากนั้น ควรระบุความคาดหวังเกี่ยวกับการรายงาน เพื่อกำหนดวิธีการป้องกันที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศไว้ด้วย

หลังจากใช้ความระมัดระวังอย่างเหมาะสมและมีการเจรจาต่อรองและลงนามแล้ว ผู้บริหารควรพิจารณาให้มีการดูแลและกำกับผู้ขาย (Vendor) ด้วยการเฝ้าติดตามประเมินผลและการรายงานตัวชี้วัดที่สำคัญเพื่อให้มั่นใจในการปฏิบัติตามสัญญาระดับการให้บริการ (SLAs) ถ้าผู้ขายไม่สามารถทำตามข้อกำหนดในสัญญา ผู้บริหารควรขอใช้สิทธิในการเข้าตรวจสอบ เรียกร้องให้มีการแก้ไขในสิ่งที่เป็นกังวลให้เสร็จภายในเวลาที่เหมาะสม บังคับใช้การคิดค่าปรับ และพิจารณาแผนในการเปลี่ยนไปใช้บริการของผู้ขายรายอื่นหากจำเป็น

ผู้บริหารต้องตื่นตัวต่อรูปแบบการโจมตีที่เกี่ยวกับวิศวกรรมทางสังคม (social engineering) ซึ่งรวมถึง อีเมล์หลอกลวง (Phishing e-Mail) และ โทรศัพท์ที่ประสงค์ร้าย โดยการปลอมตัวเป็นองค์กรหรือบุคคลที่ถูกต้องตามกฎหมายที่ต้องการข้อมูลหรือการกระทำบางอย่าง ผู้โจมตีจะโน้มน้าวบุคคลที่ได้รับอนุญาตให้แบ่งปันข้อมูลที่มีความอ่อนไหว ให้การรับรองระบบของผู้โจมตี (Provide System Credential) คลิกลิงค์ที่นำไปสู่เว็บไซต์หลอกลวง หรือกระทำการติดตั้งซอฟต์แวร์ประสงค์ร้ายบนเครื่องคอมพิวเตอร์ของเหยื่อ ซอฟต์แวร์ประสงค์ร้ายมีความซับซ้อนมากขึ้นเรื่อยๆ และเล็งเป้าไปที่วัตถุประสงค์หรือเครือข่ายที่เฉพาะเจาะจงมากขึ้นๆ ทันทีที่มันได้รับการติดตั้ง มันสามารถทำซ้ำตัวเองกระจายไปทั่วเครือข่ายขององค์กร ทำให้ระบบและความพร้อมใช้หยุดชะงัก ขโมยข้อมูล และผู้โจมตีจะดำเนินการขั้นสูงขึ้นไปเพื่อการทุจริต

ซอฟต์แวร์ประสงค์ร้ายก้าวหน้าขึ้นด้วยการใช้ประโยชน์จากการขาดความตระหนักรู้ ดังนั้น การเตือนบุคลากรอยู่บ่อยๆ ให้ระวังอีเมล์ที่น่าสงสัยหรือไม่ปกติ การร้องขอที่ไม่เคยปรากฏมาก่อน โทรศัพท์ หรือกิจกรรมของระบบ เป็นสิ่งที่สำคัญ การอบรมจะช่วยให้บุคลากรรับรู้ได้ถึงการสื่อสารที่ปลอมมา และเพื่อที่จะรายงานเหตุการณ์เหล่านั้นอย่างรวดเร็วเพื่อไปทำการค้นคว้า การยกระดับปัญหา และการหาทางแก้ไขปัญหา บทเรียนที่ได้รับ (Lesson Learned) และความรู้ที่ได้รับจากองค์กรอื่นในอุตสาหกรรมเดียวกัน จะถูกนำมาใช้เป็นประโยชน์ในการฝึกอบรม การสร้างความตระหนักรู้ และการนำมาตรการเชิงป้องกันอื่นๆ มาใช้เพิ่มเติมได้

เจ้าของและกิจกรรมที่สำคัญของแนวป้องกันชั้นที่สอง (Second Line of Defense)

แนวป้องกันชั้นที่สองมักจะประกอบด้วยหน่วยงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายระเบียบข้อบังคับ ซึ่งมีบทบาทหลักสำคัญในการออกแบบโครงการ และสถานะเกี่ยวกับความมั่นคงปลอดภัยขององค์กร

แนวป้องกันชั้นที่สองมีภาระหน้าที่เกี่ยวกับ:

- การประเมินความเสี่ยงและความเสียหายที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ และตัดสินว่าสอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้หรือไม่
- การเฝ้าระวังความเสี่ยงปัจจุบันและที่เกิดขึ้นใหม่ และการเปลี่ยนแปลงในกฎหมายระเบียบข้อบังคับ
- ทำงานร่วมกับหน่วยงานที่อยู่ในแนวป้องกันชั้นแรกเพื่อให้มั่นใจว่า การออกแบบวิธีการควบคุมมีความเหมาะสม

ตารางที่ 3: กิจกรรมโดยทั่วไปของแนวป้องกันชั้นที่สอง

- ออกแบบนโยบาย อบรมและทดสอบความมั่นคงปลอดภัยทางไซเบอร์
- ดำเนินการประเมินความเสี่ยงทางไซเบอร์
- รวบรวมอัจฉริยะภัยคุกคามทางไซเบอร์
- จัดประเภทข้อมูลและออกแบบบทบาทการเข้าถึงแบบให้สิทธิน้อยที่สุด
- เฝ้าระวังเหตุการณ์ ตัวชี้วัดความเสี่ยงที่สำคัญและการแก้ไข
- สรรหาและรักษาไว้ซึ่งผู้ที่มีความสามารถที่ได้รับวุฒิบัตรความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ประเมินความสัมพันธ์ของบุคคลภายนอก ผู้สนับสนุนปัจจัยการผลิต และผู้ให้บริการ
- วางแผน/ทดสอบความต่อเนื่องทางธุรกิจ และการมีส่วนร่วมในกิจกรรมและการทดสอบการกู้คืนความหายนะ

ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์มีพลังให้เกิดความเปลี่ยนแปลงอย่างเห็นได้ชัดมากกว่าความเสี่ยงแบบดั้งเดิมโดยส่วนใหญ่ และทำให้จำเป็นต้องตอบสนองในเวลาที่เหมาะสม ในขณะที่ความเสี่ยงและสิ่งที่เปิดรับความเสี่ยงขององค์กรเปลี่ยนแปลงไป แนวป้องกันชั้นที่สองก็มีความสำคัญยิ่งในการขับเคลื่อนการกำกับดูแล การดูแลให้มีการเตรียมการและการรักษาความมั่นคงปลอดภัยที่เพียงพอให้แก่องค์กรเพื่อตอบสนองต่อสภาพแวดล้อมของภัยคุกคามที่พัฒนาขึ้นเรื่อยๆ

การละเมิดความมั่นคงปลอดภัยอาจนำไปสู่การเปลี่ยนแปลงระดับความเสี่ยงที่องค์กรยอมรับได้ และกฎหมายและระเบียบข้อบังคับของรัฐบาล

แนวปฏิบัติ (Practice Guide) ของสมาคมผู้ตรวจสอบภายใน (IIA) เรื่อง “งานตรวจสอบภายในและแนวป้องกันชั้นที่สอง (Internal Audit and the Second Line of Defense)” ได้ระบุว่า การดูแลและออกแบบนโยบาย มาตรฐาน และการกำหนดขีดจำกัด (limits) เป็นหลักสำคัญของแนวป้องกันชั้นที่สอง ตัวอย่างเช่น ควรกำหนดความคาดหวังและแนวทางที่ชัดเจนโดยตั้งบนพื้นฐานของชั้นความเสี่ยงของช่องโหว่ (vulnerability risk tiers) ซึ่งรวมถึง อัตราการไม่ปฏิบัติตามกฎระเบียบข้อบังคับที่ยอมรับได้ เพื่อให้แนวทางในการซ่อมแซม (patching) โครงสร้างพื้นฐานที่สำคัญก่อนที่จะยกระดับปัญหาไปยังผู้บริหารระดับสูง

แนวป้องกันชั้นที่สองควรทำงานร่วมกับแนวป้องกันชั้นแรกและชั้นที่สามอย่างใกล้ชิด เพื่อสร้างความตระหนักอย่างได้ผลให้กับคณะกรรมการหรือองค์คณะที่ทำหน้าที่กำกับดูแล และเพื่อให้มั่นใจว่าการรายงานเกี่ยวกับความเสี่ยงและวิธีการควบคุมด้านความมั่นคงปลอดภัยทางไซเบอร์มีความเพียงพอและเป็นปัจจุบัน เนื่องจากแนวป้องกันชั้นที่สองทำหน้าที่และรายงานการประเมินความเสี่ยงของพวกเขา พวกเขาควรจะคงลำดับความสำคัญในเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้มาเป็นลำดับแรกเสมอ นอกจากนี้ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์แบบเฉพาะ (Dedicated Cybersecurity) ควรจะต้องมีการดำเนินการ โดยขึ้นอยู่กับอุตสาหกรรมและประเภทขององค์กร

บทบาทของแนวป้องกันชั้นที่สองควรมีความชัดเจน ตัวอย่างเช่น ต้องทำความเข้าใจในบทบาทที่เกี่ยวกับการปฏิบัติตามกฎระเบียบข้อบังคับที่เกี่ยวกับ IT ซึ่งต้องมีบทบาทในเหตุการณ์ความเสี่ยงอย่างคล่องแคล่วว่องไวและรีบด่วน การทำความเข้าใจนี้ต้องทำก่อนที่จะเกิดเหตุการณ์จริงขึ้น ตัวชี้วัดความเสี่ยงที่สำคัญพร้อมกับขีดคั่นขั้นต่ำ (threshold) ตามที่ได้ตกลงกัน สามารถใช้เป็นเครื่องมือที่มีประโยชน์ในการเฝ้าติดตามดูแล กำกับดูแล และรายงาน

องค์กรจะใช้ประโยชน์จากผู้ขาย (vendor) และผู้จัดหา (suppliers) หลักในกระบวนการที่สำคัญ แนวป้องกันชั้นที่สองอาจจำเป็นต้องประเมินความสัมพันธ์กับผู้ให้บริการซึ่งเป็นกลุ่มบุคคลที่สามเหล่านี้เกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากผู้ให้บริการอาจเข้าถึงข้อมูลที่อ่อนไหวและได้รับการจัดชั้นว่าเป็นความลับได้โดยผ่านการเชื่อมต่อเครือข่ายโดยตรงหรือโดยวิธีการอื่นในการโอนข้อมูล ควรมีการสอบทานเงื่อนไขที่เกี่ยวกับการควบคุมทางเทคนิคและสัญญา และเป็นสิ่งสำคัญยิ่งที่ผู้ให้บริการจะต้องจัดให้มีการให้ความเชื่อมั่นเป็นระยะๆ ด้วยการรายงานเกี่ยวกับวิธีการควบคุมความมั่นคงปลอดภัยทางไซเบอร์อย่างเพียงพอตามที่ได้ตกลงกันไว้

แนวป้องกันชั้นที่สองมีภาระหน้าที่ที่จะทำให้มั่นใจได้ว่า ผู้บริหารมีการกำกับดูแลผู้ขายซึ่งได้ถูกว่าจ้างมาในเรื่องที่เกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ การกำกับดูแลดังกล่าวโดยทั่วไปจะรวมถึงการ

ได้รับรายงานและการสอบทานรายงานเกี่ยวกับการควบคุม การติดตามประเมินผลกิจกรรมการควบคุมต่างๆ และการยกระดับปัญหาความเสี่ยงไปยังองค์คณะที่ทำหน้าที่กำกับดูแลภายในองค์กร เช่น คณะอนุกรรมการดูแลความเสี่ยงจากผู้ให้บริการ เมื่อผู้ให้บริการปฏิบัติไม่สอดคล้องกับความคาดหวัง หรือไม่เป็นไปตามระดับสัญญาการให้บริการ (SLAs)

ปัญหาที่ซ่อนอยู่ของแนวป้องกันชั้นที่หนึ่งและชั้นที่สอง

ปัญหาหรืออันตรายที่ซ่อนอยู่มักจะเกิดขึ้นเมื่อการเฝ้าระวังและการดูแลไม่ได้อยู่เป็นส่วนหนึ่งในระเบียบพิธีการ (protocol) ของความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง ภัยคุกคามและช่องโหว่ใหม่ๆ ยังคงเกิดขึ้นทุกๆ วัน การขาดซึ่งการอบรม การให้ความรู้ และการเฝ้าติดตามดูแลเป็นประจำอย่างจริงจังจะทำให้มีการโจมตีและภัยคุกคามเกิดขึ้นต่อองค์กรและการบุกรุกระบบและข้อมูลที่สำคัญได้

เพื่อเป็นการบรรเทาความเสี่ยงนี้ หลายๆ องค์กรได้จัดตั้งคณะอนุกรรมการด้านความมั่นคงปลอดภัยทางไซเบอร์ ที่มี CSO CISO และ/หรือหัวหน้างานด้านความลับส่วนบุคคล (chief privacy officer) เป็นผู้นำ ซึ่งจะมีการพบปะพูดคุยกันเป็นระยะๆ กับผู้มีส่วนได้เสียในโครงสร้างพื้นฐาน เครือข่าย และทีมงานความมั่นคงปลอดภัยทางไซเบอร์ รวมไปถึงผู้บริหารที่เกี่ยวข้องกับการบริหารความเสี่ยงและการปฏิบัติตามกฎระเบียบข้อบังคับด้านเทคโนโลยีสารสนเทศ วัตถุประหลักประการหนึ่งของคณะอนุกรรมการชุดนี้ก็คือ การทำความเข้าใจในสินทรัพย์ที่สำคัญขององค์กร การประเมินความเสี่ยง โอกาสที่จะเกิดภัยคุกคาม ผลกระทบที่อาจเกิดขึ้น และวิธีการควบคุมที่มีอยู่ซึ่งนำมาใช้ปกป้องสินทรัพย์เหล่านี้จากการโจมตีด้านความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างเพียงพอ คณะอนุกรรมการยังมีการหารือกันในภัยคุกคามที่เกิดขึ้นใหม่ๆ และมาตรการที่เกี่ยวข้องซึ่งรวมถึง ผลลัพธ์การทดสอบเจาะระบบครั้งล่าสุด ซึ่งได้ทดสอบประสิทธิผลของการปกป้องความมั่นคงปลอดภัยทางไซเบอร์ด้วยการเลียนแบบการกระทำของผู้โจมตีในชีวิตจริง[2]

[2] ISCA “ภาคอภิธานศัพท์ ISACA” 69. 2015 http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (เข้าดูเมื่อ 20 มิถุนายน 2559) สงวนลิขสิทธิ์ในการนำมาใช้ต้องได้รับการอนุญาต

ปัญหาที่ซ่อนอยู่อื่นๆ รวมถึงการขาดซึ่ง:

- การระบุแนวป้องกันที่ชัดเจน ซึ่งต้องทำหน้าที่ร่วมกันอย่างใกล้ชิดเพื่อให้ความมั่นใจว่าความเสี่ยงที่สำคัญได้ถูกระบุและจัดการอย่างมีประสิทธิภาพและประสิทธิผล
- การมีส่วนร่วมและการสนับสนุนของผู้บริหารเพื่อให้มั่นใจว่ากลยุทธ์ความมั่นคงปลอดภัยทางไซเบอร์ได้รับความใส่ใจและสนใจอย่างเพียงพอ
- การตอบสนองในเวลาที่เหมาะสมและการวิเคราะห์สาเหตุที่แท้จริงหลังเกิดเหตุการณ์
- การกำหนดระเบียบพิธีการและภาระหน้าที่ ในการตอบสนองต่อเหตุการณ์ที่ลุกลามเพิ่มขึ้น
- กลุ่มทักษะที่จำเป็น
- สารสนเทศและความรู้เกี่ยวกับอุตสาหกรรมเพื่อระบุความเสี่ยงที่เกิดขึ้นใหม่ๆ แบบเชิงรุก
- การลงทุนหรือจัดงบประมาณด้านเวลา เงิน และทรัพยากรที่เพียงพอต่อการริเริ่มโครงการด้านความมั่นคงปลอดภัยทางไซเบอร์ ประกอบด้วยการบำรุงรักษาและการซ่อมแซมจุดบกพร่องของโปรแกรมคอมพิวเตอร์ (Patching) เป็นประจำ

บทบาทของหน่วยงานตรวจสอบภายในในฐานะที่เป็นแนวป้องกันชั้นที่สาม (Third Line of Defense)

ในขณะที่การกำกับดูแลเป็นภาระหน้าที่หลักของคณะกรรมการและผู้บริหารระดับสูงขององค์กร การประเมินการกำกับดูแลเป็นบทบาทหลักของหน่วยงานตรวจสอบภายใน มาตรฐาน IIA ที่ 2110.A2[3] กำหนดให้หน่วยงานตรวจสอบภายในต้องทำการประเมินว่าการกำกับดูแลเทคโนโลยีสารสนเทศขององค์กรสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่

หน่วยงานตรวจสอบภายในในฐานะที่เป็นแนวป้องกันชั้นที่สามมีบทบาทที่สำคัญในการประสานงานกับแนวป้องกันชั้นที่สอง โดยเฉพาะอย่างยิ่งกับหน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ หน่วยงานตรวจสอบภายในอาจให้คำปรึกษาที่เกี่ยวกับ:

[3] กรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (The International Professional Practices Framework (IPPF) Altamonte Springs: The Institute of Internal Auditors, Inc., 2013), 30.

- ความสัมพันธ์ระหว่างความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และความเสี่ยงเกี่ยวกับองค์กร
- การจัดลำดับความสำคัญของกิจกรรมการตอบสนองความเสี่ยงและวิธีการควบคุม
- การตรวจสอบการบรรเทาความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ในทุกแง่มุมที่เกี่ยวข้องขององค์กร เช่น สิทธิการเข้าถึงขั้นพิเศษ การออกแบบเครือข่าย การบริหารผู้ขาย การเฝ้าติดตาม ประเมินผล และอื่นๆ
- การให้ความเชื่อมั่นในกิจกรรมการแก้ไขต่างๆ
- การสร้างความตระหนักด้านความเสี่ยงให้มากขึ้น และประสานงานกับหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะอย่างยิ่งในองค์กรซึ่งหน่วยงานที่เป็นแนวป้องกันชั้นที่แรกและชั้นที่สองขององค์กรยังพัฒนาไม่เต็มที่
- การพิสูจน์เพื่อยืนยันถึงความสมเหตุสมผลว่า การรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ถูกรวมอยู่ในแผนความต่อเนื่องทางธุรกิจและการดำเนินการทดสอบการกู้คืนภัยพิบัติขององค์กรแล้ว

ตารางที่ 4: กิจกรรมทั่วไปของแนวป้องกันชั้นที่สาม

- จัดให้มีการประเมินอย่างต่อเนื่องที่เป็นอิสระเกี่ยวกับการป้องกันและตรวจจับมาตรการ
- ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
- ประเมินสินทรัพย์สารสนเทศของผู้ใช้งานที่มีสิทธิการเข้าถึงสูงสำหรับการตั้งค่าความมั่นคงปลอดภัยที่เป็นมาตรฐาน เว็บไซต์ที่น่าสงสัย ซอฟต์แวร์ประสงค์ร้าย และการจารกรรมข้อมูล
- ดำเนินการตรวจสอบสถานะการณ์ติดตามของการฟื้นฟู
- ดำเนินการประเมินความเสี่ยงทางไซเบอร์ขององค์กรที่ให้บริการ บุคคลภายนอก และผู้สนับสนุนปัจจัยการผลิต (บันทึก : แนวป้องกันชั้นที่ 1 และชั้นที่สองแบ่งบันภาระหน้าที่อย่างต่อเนื่อง)

ในฐานะที่เป็นส่วนหนึ่งของการประเมินความมีประสิทธิผลของกระบวนการบริหารความเสี่ยงตามที่กำหนดไว้ในมาตรฐาน IIA ที่ 2120 เรื่อง การบริหารความเสี่ยง บทบาทของหน่วยงานตรวจสอบภายใน ก็คือการประเมินความเสี่ยงและวิธีการควบคุมด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นอิสระ เพื่อให้มั่นใจได้ว่าสอดคล้องกับความเสี่ยงขององค์กร ประเด็นนี้เกี่ยวข้องกับการสอบทานความเพียงพอของการทำงานของแนวป้องกันชั้นที่สองที่เกี่ยวกับกรอบโครงสร้าง มาตรฐาน การประเมินความเสี่ยง และการกำกับดูแล

นอกจากนั้น หน่วยงานตรวจสอบภายในยังต้องประเมินประสิทธิผลของวิธีการควบคุมในแนวป้องกันชั้นแรก เป็นเรื่องสำคัญที่พึงระลึกว่า วิธีการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศเป็นพื้นฐานแต่ก็ไม่ได้ให้คำตอบ

แบบเบ็ดเสร็จในการบรรเทาความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ความซับซ้อนของความมั่นคงปลอดภัยทางไซเบอร์ทำให้ต้องเพิ่มเติมชั้นของวิธีการควบคุมต่างๆ ขึ้น เช่น การเฝ้าระวังความเสี่ยง วิธีการที่ตรวจพบการใช้ประโยชน์จากจุดอ่อนหรือช่องโหว่ของระบบได้ในขณะเกิดเหตุ และการดำเนินการแก้ไขโดยทันที

เนื่องจากการให้ความเชื่อมั่นที่ตั้งอยู่บนพื้นฐานของการประเมินแบบดั้งเดิมและแยกกันประเมินนั้น ไม่สามารถก้าวทันความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ กลยุทธ์การให้ความเชื่อมั่นแบบใหม่ๆ จึงเป็นที่ต้องการ มีการใช้เทคนิคการตรวจสอบอย่างต่อเนื่อง (continuous auditing techniques) มากขึ้นเรื่อยๆ ในการประเมินการเปลี่ยนแปลงการตั้งค่าเพื่อความมั่นคงปลอดภัย (security configurations) ความผิดปกติที่เกิดจากความเสี่ยงที่เกิดขึ้นใหม่ๆ และแนวโน้มต่างๆ ระยะเวลาการตอบสนอง และกิจกรรมการดำเนินการแก้ไข

เพื่อเป็นการเพิ่มคุณค่าของหน่วยงานตรวจสอบภายใน CAE ควรมีวิสัยทัศน์ที่จะมองหานวัตกรรมในการให้ความเชื่อมั่นอย่างต่อเนื่องโดยผ่านทางการประเมินในขณะที่งานดำเนินไป ซึ่งจะทำให้มีการสื่อสารในเชิงคาดการณ์ล่วงหน้าถึงความเสี่ยงที่เกิดขึ้นใหม่ๆ โดยสื่อสารได้ในเวลาที่เหมาะสม แนวทางการตรวจสอบเทคโนโลยีระดับโลก (GTAG) เรื่อง “การประสานการตรวจสอบอย่างต่อเนื่องและการเฝ้าติดตามประเมินผลอย่างต่อเนื่องเพื่อให้ความเชื่อมั่นอย่างต่อเนื่อง” ได้ให้ความชัดเจนในการสร้างกลยุทธ์สำหรับการดำเนินการประเมินอย่างต่อเนื่องโดยประสานงานกับหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎระเบียบ (Compliance functions) ในแนวป้องกันชั้นที่สอง

ตามแนวปฏิบัติ (Practice Guide) เรื่อง “การพึ่งพาผู้ให้ความเชื่อมั่นรายอื่นโดยหน่วยงานตรวจสอบภายใน" หน่วยงานตรวจสอบภายในสามารถพึ่งพาแนวป้องกันชั้นที่สองได้ถ้าผู้ตรวจสอบภายในได้มีการตรวจหรือสอบยันงานใดงานหนึ่งซ้ำและได้ข้อสรุปออกมาเช่นเดียวกัน ตัวอย่างเช่น แทนที่จะทำการทดสอบการเจาะระบบซึ่งได้ทำเสร็จไปแล้วโดยหน่วยงานบริหารความเสี่ยงด้าน IT ซ้ำอีก ผู้ตรวจสอบภายในสามารถสอบทานรายละเอียดของการทดสอบ (ซึ่งรวมถึงขอบเขตของการทดสอบด้วย) และตัดสินใจว่าจะเชื่อมั่นในผลลัพธ์หรือไม่ ถ้าเป็นไปได้ ผู้ตรวจสอบภายในควรจะเข้าร่วมสังเกตการณ์และสัมภาษณ์ทีมงานด้านเทคนิคที่ทำงานนั้น ใช้ประโยชน์จากผลลัพธ์และบทเรียนที่ได้รับ เพื่อนำมารวมอยู่ในวิธีการตรวจสอบภายในด้านความมั่นคงปลอดภัยทางไซเบอร์ในอนาคต

หน่วยงานตรวจสอบภายในควรหารือและสร้างความคาดหวังที่ชัดเจนเกี่ยวกับผู้ให้บริการภายนอกร่วมกับแนวป้องกันชั้นแรกและชั้นที่สอง ขึ้นอยู่กับขอบเขตการให้บริการ ผู้ให้บริการภายนอกสามารถจัดให้มีการเฝ้าระวัง

ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง โดยเฉพาะเรื่องของการประมวลผลแบบคลาวด์ที่ขับเคลื่อนให้ความต้องการในโครงสร้างพื้นฐานของแหล่งเก็บข้อมูล (hosted infrastructure) มีเพิ่มมากขึ้น ในการใช้เทคโนโลยีเฝ้าติดตามดูแลอย่างต่อเนื่อง ผู้ให้บริการมีการพัฒนาความสามารถในการจัดให้มีวิธีการที่ประหยัดแก่ผู้บริหารในการวัดความเสี่ยงทางไซเบอร์ได้อย่างทันท่วงทีและใช้เวลาการตอบสนองที่สั้นลง อย่างไรก็ตาม บริการประเภทเหล่านี้ไม่ใช่แหล่งของการให้ความเชื่อมั่นหลัก และองค์กรผู้ใช้งานส่วนใหญ่แทบจะไม่เคยมีใครร้องขอให้ผู้ให้บริการทำการเฝ้าติดตามอย่างต่อเนื่อง

10 คำถามที่ CAE พึงพิจารณาในการประเมินการกำกับดูแลขององค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

1. ผู้บริหารระดับสูงและองค์คณะที่ทำหน้าที่กำกับดูแล (คณะกรรมการตรวจสอบ คณะกรรมการบริษัท เป็นต้น) ตระหนักถึงความเสี่ยงที่สำคัญซึ่งเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ความริเริ่มดำเนินการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ได้รับการสนับสนุนและมีการให้ลำดับความสำคัญที่เพียงพอหรือไม่?
2. ผู้บริหารได้ดำเนินการประเมินความเสี่ยงเพื่อระบุสินทรัพย์ที่มีเสี่ยงต่อภัยคุกคามทางไซเบอร์ หรือการละเมิดความมั่นคงปลอดภัย รวมทั้งได้มีการประเมินผลกระทบที่อาจเกิดขึ้น (ทางด้านการเงินและไม่ใช่ด้านการเงิน) หรือไม่?
3. แนวป้องกันชั้นที่หนึ่งและชั้นที่สองได้ร่วมมือกันกับองค์กรอื่นๆ ในอุตสาหกรรมเดียวกัน (เช่น การประชุมสัมมนา การประชุมการแสดงความคิดเห็นในเครือข่าย (Networking Forums) และการออกอากาศทางเว็บ (Webcasts)) เพื่อติดตามข่าวสารเกี่ยวกับความเสี่ยงใหม่ๆ หรือที่เพิ่งเกิดขึ้นใหม่ จุดอ่อนโดยทั่วไป และการละเมิดความมั่นคงปลอดภัยทางไซเบอร์หรือไม่?
4. มีนโยบายและวิธีปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์อยู่หรือไม่ และพนักงานและผู้รับเหมาได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์เป็นระยะๆ หรือไม่?
5. กระบวนการด้าน IT ได้รับการออกแบบและใช้งานอยู่ เพื่อตรวจจับภัยคุกคามทางไซเบอร์หรือไม่ ผู้บริหารมีวิธีการควบคุมด้วยการเฝ้าติดตามประเมินผลอย่างเพียงพอหรือไม่?
6. มีกลไกการให้ข้อมูลตอบกลับทำงานอยู่ เพื่อให้ความเข้าใจแก่คณะกรรมการและผู้บริหารระดับสูงอย่างลึกซึ้งถึงสถานะของโครงการต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรหรือไม่?

7. ผู้บริหารกำหนดให้มีสายด่วนหรือวิธีปฏิบัติในกรณีฉุกเฉินที่มีประสิทธิผลเมื่อเกิดเหตุการณ์โจมตีหรือภัยคุกคามทางไซเบอร์หรือไม่ และสิ่งเหล่านี้ได้มีการสื่อสารไปยังพนักงาน ผู้รับเหมา และผู้ให้บริการหรือไม่?
8. หน่วยงานตรวจสอบภายในมีความสามารถในการประเมินกระบวนการและวิธีการควบคุมต่างๆ เพื่อบรรเทาภัยคุกคามทางไซเบอร์ หรือ CAE จำเป็นต้องพิจารณาการใช้ทรัพยากรที่เป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์เพิ่มเติม?
9. องค์กรได้จัดทำและเก็บรักษารายการผู้ให้บริการจากภายนอกที่มีสิทธิเข้าถึงระบบ ซึ่งรวมถึงผู้ให้บริการทั้งหลายที่เก็บข้อมูลไว้ภายนอกองค์กร (เช่น ผู้ให้บริการด้านเทคโนโลยีสารสนเทศ ผู้ให้บริการจัดเก็บข้อมูลบนคลาวด์ ผู้ประมวลผลการชำระเงิน) หรือไม่? ได้มีการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์อย่างอิสระเพื่อประเมินประสิทธิผลของวิธีการควบคุมขององค์กรที่ให้บริการซึ่งเป็นส่วนหนึ่งของโครงการการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์หรือไม่?
10. ตรวจสอบภายในระบุถึงภัยคุกคามทางไซเบอร์ที่พบเห็นโดยทั่วไปที่องค์กรเผชิญอยู่อย่างเพียงพอหรือไม่ (เช่น ประเทศ-รัฐอาชญากรรมทางไซเบอร์ ระบบสื่อสังคมออนไลน์ ซอฟต์แวร์ประสงค์ร้าย) และรวมสิ่งเหล่านี้เข้าไว้ในการประเมินความเสี่ยงและกระบวนการวางแผนของการตรวจสอบภายใน

ตารางที่ 5: สัญญาณเตือนภัยช่องว่างการกำกับดูแลที่อาจเกิดขึ้น

- โครงสร้างการกำกับดูแลที่แยกออกจากกันและแตกต่างกัน
- กลยุทธ์ที่ไม่สมบูรณ์
- ความล่าช้าของความพยายามด้านความมั่นคงปลอดภัยทางไซเบอร์
- การตัดหรือลดงบประมาณ
- การตัดสินใจที่ไม่ชัดเจนเกี่ยวกับการบังคับให้มีความรับผิดชอบในหน้าที่

คำถามทั้ง 10 ข้อนี้เน้นให้เห็นความจำเป็นที่ต้องมีการกำกับดูแลที่แข็งแกร่ง ซึ่งไม่เพียงแต่ที่ผู้บริหารระดับสูงเท่านั้น แต่หมายถึงทั่วทั้งองค์กร หากได้คำตอบซึ่งเป็นที่น่าพึงพอใจสอดคล้องกันทั่วทั้งองค์กร นั่นหมายถึงว่าองค์กรน่าจะมีการกำกับดูแลที่ดีที่อยู่แล้ว

การใช้คำถามข้างต้น CAE จะสามารถเริ่มการระบุสัญญาณเตือนภัย (red flags) ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ CAE อาจประเมินว่า แนวป้องกันชั้นที่สองได้มีการดำเนินการตามกลยุทธ์หรือไม่ และแนวป้องกันชั้นแรกได้ถูกจัดวางตำแหน่งให้ระบุและตอบสนองต่อความเสี่ยงรวมทั้งดำเนินการแก้ไขทันที

หรือไม่? มาตรการที่ครอบอยู่คือโครงสร้างการกำกับดูแล ตารางที่ 5 แสดงรายการสัญญาณเตือนภัยว่ามีช่องว่างของการกำกับดูแลที่อาจเกิดขึ้น

CAE มีบทบาทที่จะต้องตีความคำตอบในเบื้องต้นจากคำถามเริ่มต้นเหล่านี้ และเริ่มกระบวนการระบุบริเวณที่อยู่ภายใต้ภัยคุกคามโดยใช้แนวทางที่ตั้งอยู่บนพื้นฐานความเสี่ยงที่เป็นระบบระเบียบ การใช้วิจารณญาณอย่างมืออาชีพของ CAE จะมีบทบาทอย่างมากในการทำความเข้าใจอย่างถ่องแท้เกี่ยวกับความสัมพันธ์ระหว่างภัยคุกคามกับความมั่นคงปลอดภัยทางไซเบอร์

มันเป็นสิ่งสำคัญที่จะระลึกว่า โครงสร้างการกำกับดูแลของผู้บริหารระดับสูงอาจส่งผลกระทบต่อลักษณะของการรับรู้สัญญาณเตือนภัยเหล่านี้ ดังนั้น วิจารณญาณอย่างมืออาชีพของ CAE และแนวทางการตรวจสอบโดยอาศัยความเสี่ยงเป็นพื้นฐาน จะช่วยให้เกิดการสื่อสารที่มีประสิทธิผลถึงสัญญาณเตือนภัยเหล่านี้ เพื่อที่จะประเมินว่าผู้บริหารมีวิธีการควบคุมเพื่อบรรเทาภัยคุกคามอยู่แล้วหรือไม่

สัญญาณเตือนภัยทั่วไปอาจส่งสัญญาณอาการของการกำกับดูแลที่อ่อนแอ ได้แก่ การขาดกลยุทธ์สำหรับโครงการด้านความมั่นคงปลอดภัยทางไซเบอร์และความริเริ่มต่างๆ ที่เกี่ยวข้อง และ/หรือ ความล่าช้าในการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยมาเป็นเวลาหลายปี การตัดงบประมาณของหน่วยงานความมั่นคงปลอดภัยอย่างมีนัยสำคัญ อาจเป็นสิ่งที่ยืนยันว่าควรได้รับความสนใจ ถ้าหน่วยงานความมั่นคงปลอดภัยสารสนเทศไม่มีปฏิกิริยา และไม่เต็มใจ หรือไม่สามารถขับเคลื่อนความรับผิดชอบร่วมกับผู้บริหารเกี่ยวกับวิธีการควบคุมทางไซเบอร์ที่จำเป็นแล้ว อาจจำเป็นที่จะต้องเพิ่มความตระหนักให้แก่ผู้บริหารและแรงสนับสนุนจากผู้บริหารที่มีต่อหน่วยงาน

ของเขตการตรวจสอบภายในและการทำงานร่วมกัน

การกำหนดขอบเขตความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นการดำเนินการที่ต้องพึ่งพาซึ่งกันและกัน โดยต้องมีการวางแผนร่วมกันกับหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎระเบียบในแนวป้องกันชั้นที่สอง การวางแผนการตรวจสอบจะมีประสิทธิผลมากที่สุดเมื่อมีการบูรณาการร่วมกับหน่วยงานที่กำกับดูแลการปฏิบัติตามกฎระเบียบผู้ซึ่งมีความเข้าใจลึกซึ้งในการจัดลำดับความสำคัญของผลกระทบทางธุรกิจ และบูรณาการร่วมกับผู้ที่ผู้ตรวจสอบสามารถทำงานร่วมกันได้ทั้งในระหว่างและหลังการตรวจสอบภายใน

CAE ควรกำหนดว่าแผนการตรวจสอบภายในได้ครอบคลุมอะไรบ้าง และควรบันทึกถึงบริเวณที่การให้ความเชื่อมั่นอาจจะยังไม่ได้ครอบคลุมถึงในปัจจุบัน เพื่อให้สอดคล้องตามมาตรฐาน IIA ที่ 2050 เรื่อง การประสานงาน ความครอบคลุมความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมนั้นจะต้องเกิดจากการทำงานร่วมกันกับแนวป้องกันชั้นแรกและชั้นที่สองเพื่อที่จะมั่นใจได้ว่า หน่วยงานตรวจสอบภายในได้ระบุสารสนเทศซึ่งมีความสำคัญมากที่สุดต่อองค์กร ในการจัดลำดับความสำคัญสูงสุดให้แก่สารสนเทศที่สำคัญมากที่สุดนั้น หน่วยงานตรวจสอบภายในควรทำงานร่วมกับเจ้าของข้อมูลที่เกี่ยวข้อง (ซึ่งรวมถึง ผู้บริหารข้อมูลองค์กร) ประเมินกระบวนการให้สิทธิ และระบุว่าใครบ้างที่ได้รับสิทธิในการเข้าถึงข้อมูลภายในบริบทที่เกี่ยวกับความสำคัญของข้อมูล

ต่อมา หน่วยงานตรวจสอบภายในควรร่วมกับผู้บริหารด้านปฏิบัติการเพื่อระบุระบบและเทคโนโลยีที่เอื้อต่อเส้นทางในการเข้าถึงเพื่อดูสารสนเทศที่สำคัญ (เช่น ข้อมูลพนักงาน สารสนเทศที่สามารถระบุตัวบุคคลได้ หมายเลขบัตรเครดิตลูกค้า ประวัติการสั่งซื้อจากผู้ขาย). การทำงานร่วมกับผู้บริหารด้านปฏิบัติการจะช่วยให้มั่นใจได้ว่า องค์ประกอบต่างๆ ที่เกี่ยวข้องกับช่องโหว่ด้านความมั่นคงปลอดภัยทางไซเบอร์ได้รับการเฝ้าติดตามอย่างต่อเนื่อง ตรวจสอบภายในควรพิจารณากำหนดขนาดของขอบเขตของการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์โดยตั้งอยู่บนพื้นฐานของผู้ที่มีสิทธิเข้าถึงสารสนเทศที่สำคัญ และประเมินเทคโนโลยีที่เกี่ยวข้องกับเส้นทางการเข้าถึงของพวกเขาเหล่านั้น

คำถามต่อไปนี้จะช่วยอำนวยความสะดวกให้แก่กระบวนการระบุสารสนเทศที่สำคัญ :

- สารสนเทศใดที่คิดว่ามีความสำคัญและทำไม?
- อะไรคือคุณค่าของข้อมูล (สำหรับผู้ทุจริต คู่แข่งขัน อื่นๆ)?
- ที่ซึ่งสารสนเทศมีการเข้าถึง ประมวลผล และจัดเก็บ คือที่ใด?
- สารสนเทศถูกส่ง (transmitted) อย่างไร?

- ความเข้มงวดหลังจากการให้สิทธิและยกเลิกสิทธิการเข้าถึง มีมากน้อยเพียงใด?
- ระดับของการเข้าถึงได้รับการกำหนดตามบทบาท และบทบาทใดที่ได้รับการเข้าถึงในระดับที่เป็นผู้ดูแลระบบ (Administrative Access)?
- สิทธิการเข้าถึงได้มีการมอบหมาย อนุมัติ เฝ้าติดตาม และยกเลิกอย่างไร?
- สารสนเทศได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต ดีเพียงใด?
- ประเภทการทดสอบใดที่ได้ดำเนินการไปแล้ว (การเจาะระบบ การเข้าถึง การตามรอยการเปลี่ยนแปลง อื่นๆ)?
- มีการเฝ้าระวังความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ สำหรับผู้ซึ่งตามหน้าที่แล้วมีสิทธิการเข้าถึงสารสนเทศที่สำคัญ อย่างไร

ถ้าการจัดทำเอกสารแผนความต่อเนื่องทางธุรกิจและการกู้คืนจากความหายนะยังไม่เสร็จเรียบร้อย ผู้บริหารควรพิจารณาดำเนินการวิเคราะห์ผลกระทบทางธุรกิจ เพื่อจัดกลุ่ม จัดลำดับความสำคัญ และจัดทำเอกสารเกี่ยวกับประชากรของระบบ ข้อมูล ทรัพยากรที่สำคัญ CAE สามารถใช้ผลลัพธ์จากการวิเคราะห์ผลกระทบทางธุรกิจนี้ให้เกิดประโยชน์ เพื่อที่จะตัดสินว่า แผนการตรวจสอบภายในได้ครอบคลุมระบบที่มีสารสนเทศที่สำคัญอย่างเพียงพอแล้วหรือไม่ และแล้ว CAE ก็สามารถเปิดเผยต่อคณะกรรมการ เกี่ยวกับบริเวณที่อาจจะให้ความเชื่อมั่นในปัจจุบัน หรือยังจะไม่ให้ความเชื่อมั่น และแผนในการจัดให้มีความครอบคลุมถึง

แนวทางหนึ่งในการประเมินความเสี่ยงและวิธีการควบคุมความมั่นคงปลอดภัยทางไซเบอร์

6 องค์ประกอบของกรอบโครงสร้างที่มีความพึ่งพาซึ่งกันและกัน ตามที่แสดงอยู่ข้างล่างนี้ สามารถนำมาใช้ในการประเมินการออกแบบและประสิทธิผลในทางการดำเนินงานของวิธีการควบคุมและกำกับดูแลความมั่นคงปลอดภัยของผู้บริหาร เนื่องจากความบกพร่องที่มีในขององค์ประกอบใดๆ จะส่งผลกระทบต่อประสิทธิผลของความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมได้ การประเมินว่าแต่ละองค์ประกอบได้รับการออกแบบและมีการทำงานร่วมกับองค์ประกอบอื่นอย่างไร จะให้พื้นฐานแก่ CAE ในการที่จะตัดสินว่า องค์กรได้เตรียมการในการระบุความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ดีเพียงใด ถ้าองค์ประกอบไม่ได้รับการออกแบบหรือทำงานร่วมกันได้ไม่ค่อยดี องค์กรก็เตรียมการได้ไม่ดีพอที่จะระบุภัยคุกคามทางไซเบอร์และความเสี่ยงที่เกิดขึ้นใหม่ได้

กรอบโครงสร้างการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์

องค์ประกอบที่ 1: การกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์

หน่วยงานตรวจสอบภายในควรทำความเข้าใจในการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร มาตรฐาน ของ IIA ที่ 2100 เรื่อง ลักษณะของงาน กำหนดให้หน่วยงานตรวจสอบภายในประเมินและมีส่วนช่วยในการปรับปรุงกระบวนการ การกำกับดูแล การบริหารความเสี่ยง และการควบคุมให้ดีขึ้น การกำกับดูแลอาจหมายรวมถึง การให้ความชัดเจนในบทบาทและภาระหน้าที่ การกำหนดความรับผิดชอบ การยอมรับกล

ยุทธ์สำหรับหลายๆ ปี และการจัดลำดับความสำคัญของแผนปฏิบัติการที่รวมเอาความร่วมมือเชิงกลยุทธ์ของผู้มีส่วนได้เสียหลายๆ ฝ่ายไว้

การกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ที่เข้มแข็งขึ้นอยู่กับ :

- การทำงานร่วมกันและการรวบรวมความรอบรู้และความเชี่ยวชาญด้านความเสี่ยงที่มีต่อความมั่นคงปลอดภัยทางไซเบอร์ บนพื้นฐานของภัยคุกคามที่อาจส่งผลกระทบต่อองค์กร
- กำหนดระดับความเสี่ยงที่ยอมรับได้และช่วงความเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้
- การวางแผนความต่อเนื่องทางธุรกิจและการกู้คืนจากความหายนะ ในกรณีที่เกิดการหยุดชะงัก
- การตอบสนองต่อการละเมิดความมั่นคงปลอดภัยทางไซเบอร์อย่างทันท่วงที
- การสร้างวัฒนธรรมที่ตระหนักในความเสี่ยงและภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์

หลักฐานของการกำกับดูแลที่มีประสิทธิผล แสดงให้เห็นได้จาก การมีนโยบายที่กำหนดไว้อย่างชัดเจน เครื่องมือที่เกี่ยวข้อง ทีมงานที่เพียงพอ และการฝึกอบรมเป็นอย่างดี

ผู้มีส่วนได้เสียจำนวนมากที่มีมุมมองต่างกันจะทำให้คุณภาพของการกำกับดูแลแข็งแกร่งขึ้น คณะอนุกรรมการที่ทำหน้าที่กำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์มักจะรวมถึง ผู้บริหารระดับสูงและตัวแทนจากแนวป้องกันชั้นแรก ชั้นที่สอง และชั้นที่สาม เจ้าของเทคโนโลยีและกระบวนการ และผู้มีส่วนได้เสียภายนอกที่สำคัญที่อาจเป็นไปได้เช่น ผู้จำหน่าย ลูกค้า ผู้ให้บริการ และกลุ่มผู้ที่ทำอาชีพเดียวกัน

ทีมงานที่ทำหน้าที่ตอบสนองต่อเหตุการณ์จะรายงานประเภทการละเมิดที่องค์กรเผชิญอยู่ไปยังผู้บริหารและคณะกรรมการอย่างสม่ำเสมอ เพื่อให้ความเข้าใจอย่างลึกซึ้งมากขึ้นเกี่ยวกับช่องว่างที่ยังไม่เป็นที่รู้จักมาก่อนหน้านี้ ผู้บริหารก็จะสามารถติดตามประเด็นปัญหาซึ่งได้ถูกระบุมาแล้วโดยผ่านการกระบวนแก้ไข

องค์ประกอบที่ 2: ทะเบียนสินทรัพย์สารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศควรจัดทำทะเบียนสินทรัพย์สารสนเทศทั้งหมดให้เป็นปัจจุบันและกำหนดลำดับความสำคัญของสินทรัพย์ที่จำเป็นต่อการทำให้วัตถุประสงค์องค์กรเดินหน้าและการดำเนินการที่ยั่งยืน เพื่อให้บรรลุเป้าหมายเชิงกลยุทธ์และความริเริ่มใหม่ๆ ในทางกลยุทธ์ขององค์กร สินทรัพย์เหล่านี้จำต้องมีมากกว่าการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศแบบดั้งเดิมและการประเมินผลเป็นระยะ วิธีการควบคุมเชิงป้องกันและเชิงตรวจพบที่ได้รับการออกแบบมาให้ปกป้องสินทรัพย์ที่มีค่านั้น จำเป็นต้องได้รับการเฝ้าติดตามอย่างต่อเนื่องเพื่อให้มั่นใจได้ว่า ยังคงทำงานต่อเนื่องได้อย่างมีประสิทธิผล

ในการประเมินสินทรัพย์สารสนเทศขององค์กร มีสิ่งที่ควรพิจารณาดังต่อไปนี้:

- ข้อมูล
  - ประเภท (เช่น รายการธุรกรรม การตั้งค่าทาง IT (IT Configuration) ข้อมูลที่ไม่มีโครงสร้าง)
  - การจัดอันดับ (ช่วยให้เป็นมาตรฐาน และลำดับความสำคัญ)
  - สิ่งแวดล้อม (เช่น คลังข้อมูล ฐานข้อมูลที่สำคัญ)
- ที่เก็บข้อมูลของสินทรัพย์ด้านเทคโนโลยีในโครงสร้างพื้นฐาน
  - เครื่องแม่ข่าย (Servers)
  - อุปกรณ์เครือข่าย (Network Device)
  - หน่วยจัดเก็บข้อมูล (Storage)
  - อุปกรณ์ผู้ใช้งาน (End-user devices) (เช่น คอมพิวเตอร์แบบพกพา (Laptops) อุปกรณ์แบบพกพา (Mobile Devices))
- ระบบงาน/แอพพลิเคชัน (Applications)
- ความสัมพันธ์ภายนอก (External Relationships)
  - สภาพแวดล้อมที่ระบบ/ข้อมูลได้ถูกจัดเก็บไว้กับกลุ่มบุคคลที่สาม (Third-party hosted environments)
  - การแบ่งปันแฟ้มข้อมูลกับองค์กรภายนอก (เช่น ผู้จัดจำหน่าย หน่วยงานกำกับดูแล รัฐบาล)

ความสามารถในการระบุว่าซอฟต์แวร์ใดและอุปกรณ์ใดที่กำลังมีปฏิสัมพันธ์กันบนเครือข่ายเป็นพื้นฐานที่จะสามารถป้องกันภัยคุกคามทางไซเบอร์ได้ องค์กรจะไม่สามารถปกป้องการโจมตีเครือข่ายบนอุปกรณ์และซอฟต์แวร์ที่ไม่รู้จักได้ องค์กรที่อนุญาตให้พนักงานนำอุปกรณ์ของตนเองมาใช้งานจะประสบกับปริมาณและความหลากหลายของอุปกรณ์และซอฟต์แวร์เป็นจำนวนมากที่เข้าถึงข้อมูลโดยผ่านเครือข่ายองค์กร การควบคุมอุปกรณ์ที่พนักงานเป็นเจ้าของและควบคุมการเชื่อมต่อไปยังเครือข่ายเป็นเรื่องสำคัญที่ผู้บริหารควรให้ความสนใจ มีพนักงานเป็นจำนวนมากขึ้นที่จำเป็นต้องเข้าถึงสารสนเทศขององค์กรได้มากขึ้นตลอดเวลา ความสามารถในการตรวจจับ พิสูจน์ตัวตน และการจัดทำทะเบียนอุปกรณ์ที่ไม่รู้จักจะช่วยองค์กรในการแกะรอย เฝ้าระวัง และวัดการเปลี่ยนแปลงต่างๆ ในอุปกรณ์เหล่านั้น เพื่อให้มั่นใจได้ว่ากลยุทธ์ความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมมีประสิทธิผล

องค์ประกอบที่ 3: การตั้งค่าความปลอดภัยที่เป็นมาตรฐาน

ซอฟต์แวร์ที่บริหารการตั้งค่าแบบอัตโนมัติในลักษณะรวมศูนย์สามารถถูกนำมาใช้ในการกำหนดและรักษาค่าขั้นต่ำ (baselines) ของอุปกรณ์ ระบบปฏิบัติการ และซอฟต์แวร์ระบบงาน/แอพพลิเคชันได้ การใช้ซอฟต์แวร์บริหารจะมีประสิทธิผลมากกว่าการบริหารระบบด้วยมือหรือในลักษณะที่ไม่มีมาตรฐาน หน่วยงานความมั่นคงปลอดภัยสารสนเทศและหน่วยงานตรวจสอบภายในควรสอบทานค่าขั้นต่ำเพื่อให้มั่นใจว่า จะสามารถประเมินสภาพแวดล้อมได้อย่างถูกต้องโดยอยู่บนพื้นฐานของความเสี่ยงได้ (เช่น ในสภาพแวดล้อมที่ต้องเผชิญกับเว็บภายนอก อาจจำเป็นต้องมีมาตรการปกป้องเพิ่มเติม) กระบวนการในการปิดช่องโหว่ (Patches) ที่จำเป็น รวมถึงการปรับปรุงซอฟต์แวร์และฮาร์ดแวร์ เป็นสิ่งจำเป็นเพื่อให้มั่นใจได้ว่า การตั้งค่าการรักษาความมั่นคงปลอดภัยยังคงมีความเป็นปัจจุบันเมื่อมีข้อมูลเกี่ยวกับภัยคุกคามใหม่ๆ อยู่ในอุตสาหกรรม

องค์ประกอบที่ 4: การบริหารการเข้าถึงสารสนเทศ

ผู้บริหารควรพิจารณาการนำวิธีการควบคุมเชิงป้องกันมาใช้ เช่น การมีกระบวนการอนุมัติและให้สิทธิในการเข้าถึงแก่ผู้ใช้งานตามบทบาทในงาน ยิ่งไปกว่านั้น กระบวนการในการตรวจจับเมื่อพนักงานมีการโยกย้ายภายในองค์กรจะช่วยให้มั่นใจได้ว่า สิทธิการเข้าถึงของผู้ใช้งานคนนั้นได้ถูกปรับเปลี่ยนและเป็นไปตามบทบาทในงานใหม่ หน่วยงานตรวจสอบภายในอาจทำการสอบทานการเข้าถึงข้อมูลและระบบที่สำคัญของผู้ใช้งานเพื่อยืนยันว่าระดับของสิทธิการเข้าถึงเหมาะสมกับบทบาทหน้าที่งานในปัจจุบัน

สิทธิการเข้าถึงของผู้ดูแลระบบที่มีสิทธิการใช้งานระดับสูงมีความสำคัญอย่างมาก ผู้ใช้งานที่สามารถเข้าถึงและปล่อยข้อมูลได้เป็นเรื่องที่เสี่ยงต่อความมั่นคงปลอดภัยทางไซเบอร์มากที่สุด การเปิดเผยรหัสผ่านของพวกเขาโดยไม่เจตนา หรือการโหลดซอฟต์แวร์ประสงค์ร้ายที่เป็นผลมาจากความพยายามหลอกลวง ผู้ใช้งานจะสามารถหลบเลี่ยงชั้นของวิธีการควบคุมของระบบที่ได้รับการออกแบบมาเพื่อให้ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตได้ ผู้ที่มีสิทธิการเข้าถึงมีอยู่ทั้งภายในและภายนอกองค์กร ดังนั้นองค์กรควรให้ความสนใจในพนักงาน ผู้ให้คำปรึกษา และผู้ขาย ที่เข้าถึงข้อมูลสำคัญได้ไม่ว่าข้อมูลนั้นจะถูกจัดเก็บไว้ภายในหรือภายนอกองค์กรก็ตาม การตรวจสอบกิจกรรมการควบคุมเชิงป้องกันในการให้และยกเลิกสิทธิการเข้าถึง และประเมินความน่าสงสัยและพฤติกรรมผู้ใช้งานที่มีสิทธิการใช้งานสูง ถือเป็นมาตรการสำคัญที่จะทำให้โครงการด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรมีประสิทธิผล

องค์ประกอบที่ 5: การตอบสนองและการฟื้นฟูอย่างรวดเร็ว

ความสามารถขององค์กรในการสื่อสารและแก้ไขเหตุการณ์ความเสี่ยงได้โดยทันที จะชี้ให้เห็นถึงประสิทธิผลและระดับความสมบูรณ์หรือวุฒิภาวะ (maturity) ของโครงการได้ โครงการที่มีวุฒิภาวะแล้วจะสามารถทำให้เวลาในการจัดการความเสี่ยงสั้นลงได้อย่างต่อเนื่อง บทบาทหนึ่งของแนวป้องกันชั้นที่สองคือ:

- สื่อสารความเสี่ยงที่มีสาระสำคัญ
- ทำการแก้ไข
- แกะรอยประเด็นปัญหาที่ได้ระบุมาแล้ว เพื่อหาทางแก้ปัญหา
- ดูแนวโน้มและรายงานการแก้ปัญหาให้ทั่วทั้งองค์กร

องค์ประกอบที่ 6: การติดตามดูแลอย่างต่อเนื่อง

ในฐานะที่เป็นองค์ประกอบสุดท้ายของกรอบโครงสร้าง เมื่อทำการตรวจสอบในแต่ละ 5 องค์ประกอบที่กล่าวมาข้างต้นอย่างต่อเนื่อง จะช่วยในการตัดสินว่าความเสี่ยงได้รับการจัดการอย่างไร และการแก้ไขดำเนินการได้ดีเพียงใด แนวทางการประเมินที่มีประสิทธิผลต้องมีมากกว่า การทำสำรวจรายการที่ต้องปฏิบัติตาม (Checklist adherence surveys) ซึ่งทำเป็นกิจวัตร แนวป้องกันชั้นที่สองได้รับการคาดหวังว่าจะนำกลยุทธ์ในการเฝ้าติดตามมาใช้ปฏิบัติ ซึ่งกลยุทธ์นั้นได้ถูกออกแบบมาเพื่อสร้างการเปลี่ยนแปลงทางพฤติกรรมที่รวมถึง:

- การประเมินระดับการเข้าถึงและการสแกน (scanning) ที่เกี่ยวกับการเฝ้าติดตามดูผู้ที่เข้าถึงข้อมูลที่มีความอ่อนไหว เพื่อวัดความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ สำหรับกลุ่มผู้ใช้งานส่วนหนึ่งที่ปฏิบัติงานในกระบวนการที่มีความสำคัญ จะเป็นการดีถ้าจะพัฒนาหนทางที่เป็นระบบในการค้นหาช่องโหว่ที่มีอยู่ในสินทรัพย์ทาง IT ทั้งหลาย การตั้งค่าความมั่นคงปลอดภัยเว็บไซต์ที่มีปัญหา กรณีซอฟต์แวร์ประสงค์ร้าย และการจารกรรมข้อมูล
- การประเมินช่องโหว่: การสแกนระบบอย่างสม่ำเสมอมีความสำคัญยิ่งในการระบุช่องโหว่ภายในสภาพแวดล้อม ทันทีที่ระบุช่องโหว่ จัดกลุ่มช่องโหว่ (เช่น วิกฤต รุนแรง ปานกลาง) และจัดการ (เช่น จัดการกับช่องโหว่ทั้งหมดในระบบที่มีความเสี่ยงสูงภายใน 30 วัน) เริ่มทำกิจกรรมการแก้ไขเพื่อจัดการกับช่องโหว่ตามที่ได้ระบุมา
- การเผชิญกับระบบภายนอกมักจะก่อให้เกิดความเสี่ยงสูงที่สุดต่อองค์กร และควรได้รับการจัดลำดับให้ความสำคัญในระดับสูง อย่างไรก็ตาม กิจกรรมการแก้ไขเป็นสิ่งที่ดีที่สุดแต่ไม่ได้จำกัดแค่ในการเผชิญกับสภาพแวดล้อมภายนอกเท่านั้น ทรัพยากรของแนวป้องกันชั้นแรกและชั้นที่สองสามารถ

ทำงานได้ทั่วองค์กรเพื่อกำหนดและเห็นชอบในสัญญาระดับการให้บริการ (SLAs) และตรวจสอบภายในสามารถช่วยโดยการประเมินว่า ผู้บริหารกำลังปฏิบัติตาม SLA ที่กำหนดไว้หรือไม่

- การประเมินความเสี่ยงและการเฝ้าติดตามประเมินผลบุคคลภายนอก: โครงการต่างๆ จะสามารถช่วยในการประเมินความเสี่ยงที่เกี่ยวกับผู้ขาย (vendor) ที่เป็นกลุ่มบุคคลที่สาม และระดับความเสี่ยงต่อความมั่นคงปลอดภัยขององค์กรโดยอยู่บนพื้นฐานของบริการที่ให้แก่องค์กร ตัวอย่างเช่น ถ้าผู้ขายจัดเก็บข้อมูลที่สำคัญขององค์กร ผู้บริหารควรพิจารณาให้มีการกำหนดโครงการการดูแลในเรื่องต่างๆ เช่น:
    - การเฝ้าติดตามประเมินผล SLAs อย่างแข็งขัน
    - การเปลี่ยนแปลงการตั้งค่าความมั่นคงปลอดภัยของสารสนเทศ
    - ผลลัพธ์จากงานที่ได้รับมอบหมายในการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นอิสระ
    - การรายงานเพื่อรับประกันการควบคุมการทำงานภายในองค์กร (Service organization controls -- SOC)
    - การประเมินช่องโหว่และทดสอบการเจาะระบบ
    - วิธีปฏิบัติในการยกระดับปัญหาไปยังผู้บริหารของผู้ขาย
    - การทำการประเมินค่าขั้นต่ำ (Baseline) เพื่อตรวจสอบวิธีการควบคุมความมั่นคงปลอดภัยที่สำคัญ
    - การประเมินอย่างต่อเนื่องซึ่งวิเคราะห์สถาปัตยกรรมทางเทคนิคและวิธีการควบคุมที่มีอยู่เพื่อปกป้องข้อมูลองค์กร
    - การเฝ้าติดตามทรัพยากรของกลุ่มบุคคลที่สามที่เข้าถึงเครือข่ายและระบบขององค์กร เพื่อมั่นใจได้ว่า ทรัพยากรเหล่านี้ไม่ได้กำลังทำกิจกรรมที่ไม่เหมาะสม หรือทำให้องค์กรเกิดความเสี่ยงจากการเข้าถึงนี้โดยไม่จำเป็น
- การทดสอบการเจาะระบบ: แนวป้องกันชั้นที่สองอาจดำเนินการทดสอบเจาะระบบหรือช่องโหว่ที่เคยพบเห็นมาก่อนเพื่อประเมินวิธีการควบคุมทางเทคนิคในเชิงป้องกัน รวมทั้ง ความสามารถของผู้บริหารในการตรวจจับและตอบโต้การโจมตี การทดสอบการเจาะระบบควรรวมถึงการทดสอบองค์ประกอบที่ไม่ต้องประกาศให้ทราบ เพื่อให้การประเมินความสามารถและความพร้อมในการตอบสนองสถานการณ์การโจมตีทางไซเบอร์ในโลกแห่งความเป็นจริงมีความน่าเชื่อถือและความเที่ยงธรรมมากยิ่งขึ้น อย่างไรก็ตาม ขอบเขตในการทดสอบควรมีความสมเหตุสมผล ไม่รบกวนการดำเนินงาน และได้รับการอนุมัติล่วงหน้าโดยผู้นำที่เกี่ยวข้อง ตัวอย่างเช่น การทดสอบการจำลอง

สถานการณ์ทางธุรกิจเมื่อมีการโจมตีแบบให้ปฏิเสธการให้บริการ (denial-of-service attack) ซึ่งรบกวนเครือข่ายแบบประสงค์ร้าย ควรมีการประสานงานกับผู้นำของหน่วยงานก่อนเพื่อมิให้รบกวนการดำเนินงานตามปกติ

- ซอฟต์แวร์ประสงค์ร้าย: เนื่องจากช่องโหว่อาจจะถูกค้นพบหลังจากอุปกรณ์หรือผลิตภัณฑ์ซอฟต์แวร์ได้ส่งถึงลูกค้าแล้ว ควรมีกระบวนการเพื่อตรวจสแกนอุปกรณ์และผลิตภัณฑ์อย่างสม่ำเสมอ ระบุช่องโหว่ และทำการปิดช่องโหว่ตามลำดับความสำคัญ (เช่น สินทรัพย์ที่สำคัญจะต้องได้รับการปิดช่องโหว่เป็นลำดับแรก) บางระบบและการปิดช่องโหว่อาจตกอยู่ต่ำกว่าเกณฑ์ระดับความเสี่ยงที่ตั้งไว้ (Risk Threshold) ดังนั้น จึงควรเฝ้าติดตามและรายงาน โดยไม่ต้องดำเนินการอย่างใดต่อไป
- การเฝ้าติดตามและตอบสนองเหตุการณ์: การผสมผสานระหว่างกระบวนการการเฝ้าติดตามและตอบสนองเหตุการณ์นี้ จะช่วยให้องค์กรตรวจจับ ตอบสนอง แก้ไข กู้คืน และรายงานต่อผู้บริหารในกรณีที่มีการละเมิด เทคโนโลยีบันทึกเหตุการณ์ (Logging) และการเฝ้าระวัง (Monitoring) รวมถึงทีมงานตอบสนองที่ได้รับการอบรมมาเป็นอย่างดี เป็นสิ่งสำคัญที่จะให้ความมั่นใจได้ว่าวิธีการควบคุมเหล่านี้บรรลุวัตถุประสงค์ได้ตามที่ต้องการ

ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับอุตสาหกรรมที่เกิดขึ้นใหม่ รวมทั้งเหตุการณ์ที่องค์กรหรือองค์กรอื่นในอุตสาหกรรมเดียวกันได้ประสบมา ทำให้เกิดความจำเป็นที่จะต้องปรับเปลี่ยนกลยุทธ์การเฝ้าติดตามอย่างต่อเนื่องได้ตลอดเวลา

ภาคผนวก ง แสดงรายการแต่ละองค์ประกอบของกรอบโครงสร้างนี้ และกิจกรรมทางการบริหาร ซึ่งรวมถึงการเฝ้าติดตามประเมินผลอย่างต่อเนื่อง ซึ่งหน่วยงานตรวจสอบภายในอาจจะต้องการใช้พิจารณาในการให้บริการตรวจสอบและการให้ความเชื่อมั่นอย่างต่อเนื่อง

บทบาทของ CAE ในการรายงานการให้ความเชื่อมั่นต่อคณะกรรมการบริหารและองค์คณะที่ทำหน้าที่กำกับดูแลอื่น

เนื่องจากสภาพแวดล้อมของความเสี่ยงได้มีการพัฒนาขึ้นและมีการใช้บริการแบบคลาวด์ อุปกรณ์แบบพกพาและสื่อสังคมออนไลน์กันมากขึ้น ดังนั้น ภัยคุกคามทางไซเบอร์ก็มีเพิ่มขึ้น CAE ควรหารือเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้ขององค์กรร่วมกับผู้บริหารระดับสูงและคณะกรรมการเป็นประจำ CAE ควรพบผู้นำหรือคณะอนุกรรมด้านการบริหารความเสี่ยงและภัยคุกคามขององค์กรอย่างสม่ำเสมอ เพื่อจัดลำดับความสำคัญของความเสี่ยงและภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อมั่นใจว่าทรัพยากรได้ถูกจัดสรรไปยังเรื่องที่มีความสำคัญมากที่สุด ดังนั้น จึงเป็นเรื่องสำคัญที่ผู้บริหารจะต้องระบุและพัฒนากลยุทธ์ในการระบุสินทรัพย์ระบบสารสนเทศและข้อมูลที่มีความสำคัญอย่างยิ่งยวดต่อองค์กร และเพื่อให้ CAE ได้สอบยันร่วมกับผู้บริหารระดับสูงและคณะกรรมการ

คณะกรรมการและผู้บริหารระดับสูงคาดหวัง CAE ในการให้ความเชื่อมั่นด้านการบริหารความเสี่ยงและการควบคุม ซึ่งรวมถึง ประสิทธิผลโดยภาพรวมของกิจกรรมที่ได้กระทำโดยแนวป้องกันชั้นแรกและชั้นที่สองในการบริหารและบรรเทาความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ คณะกรรมการจำเป็นต้องเข้าใจในสินทรัพย์ระบบสารสนเทศและข้อมูลที่ซึ่งมีความสำคัญอย่างยิ่งยวดต่อองค์กรของพวกเขา และได้รับความเชื่อมั่นจาก CIO CISO CSO CTO และ CAE เกี่ยวกับการนำวิธีการควบคุมมาใช้ในการป้องกัน ตรวจจับและบรรเทาความเสี่ยงด้านไซเบอร์ให้อยู่ในช่วงความเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้

CAE ควรให้ความมั่นใจว่า คณะกรรมการจะรู้เท่าทันภัยคุกคามด้านไซเบอร์ที่มีลักษณะเฉพาะทางธุรกิจและผลกระทบซึ่งเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์อาจมีต่อองค์กร คณะกรรมการและผู้บริหารระดับสูงอาจได้รับประโยชน์จากการมีส่วนร่วมในการอบรมเพื่อสร้างความความตระหนักรู้และการให้ความรู้ต่างๆ เพื่อที่จะได้ทำความเข้าใจในข้อมูลความเสี่ยง (Profile) ด้านภัยคุกคามทางไซเบอร์ขององค์กร ความตระหนักรู้ที่มีเพิ่มขึ้นอย่างต่อเนื่องจะทำให้คณะกรรมการอยู่ในสถานะที่มีความรู้ที่ดีขึ้นซึ่งจำเป็นต่อการพิสูจน์ว่าองค์กรมีโครงสร้างการกำกับดูแลที่เหมาะสม เพื่อใช้ป้องกันและเฝ้าติดตามระบบและข้อมูลที่มีความสำคัญต่อองค์กร หัวข้อความมั่นคงปลอดภัยทางไซเบอร์เชิงเทคนิคซึ่งได้รับการแปลให้เป็นข้อมูลที่มีความหมายจะช่วยให้คณะกรรมการสามารถปฏิบัติหน้าที่ในการกำกับดูแลและเฝ้าติดตามสภาพแวดล้อมทางไซเบอร์และความเสี่ยงที่เกี่ยวข้องได้ตลอดเวลา

การสื่อสารที่มีประสิทธิผลระหว่างแนวป้องกันทั้ง 3 ชั้นและคณะกรรมการเป็นสิ่งสำคัญยิ่ง การจัดให้มีการสื่อสารเป็นระยะๆ จะช่วยให้มั่นใจได้ว่า คณะกรรมการจะได้รับข้อมูลที่เกี่ยวข้องในการปฏิบัติหน้าที่ในบทบาทการกำกับดูแลการควบคุมภายในได้อย่างมีประสิทธิผล คณะกรรมการยังคาดหวังให้ CAE ให้ความเชื่อมั่นว่าผู้บริหารมีกลยุทธ์และแผนในการแจ้งเตือนคณะกรรมการ เจ้าหน้าที่ผู้บังคับใช้กฎหมาย ลูกค้า และสาธารณะชน ในกรณีที่เกิดเหตุการณ์การละเมิดอย่างร้ายแรงขึ้น ควรมีการกำหนดระเบียบพิธีการปฏิบัติสำหรับการยกระดับและการสื่อสาร และสอบทานโดยคณะกรรมการ เพื่อที่จะเชื่อมั่นได้ว่า มีการแจ้งเตือนในเวลาที่เหมาะสมเมื่อมีการละเมิดเกิดขึ้น

แผนกลยุทธ์และการสื่อสารควรจัดทำไว้เป็นเอกสารและสอบทานโดยคณะกรรมการ พร้อมทั้งกำหนดบทบาทและภาระหน้าที่ไว้อย่างชัดเจนในกรณีที่เกิดการใช้ประโยชน์จากจุดอ่อนหรือช่องโหว่ด้านความมั่นคงปลอดภัยทางไซเบอร์ซึ่งทำให้เกิดการหยุดชะงัก แผนจำเป็นต้องได้รับการทดสอบ และร่างจดหมาย/การแถลงข่าวที่อาจจะเกิดขึ้นต้องได้รับการสอบทานโดยที่ปรึกษาทางกฎหมายล่วงหน้าก่อน กลยุทธ์การตอบสนองและการแก้ไขสถานการณ์ที่มีความครอบคลุมและวางแผนมาเป็นอย่างดี จะช่วยลดผลกระทบต่อองค์กรและรักษาไว้ซึ่งความไว้วางใจและความเชื่อมั่นของลูกค้าและผู้มีส่วนได้เสียอื่นๆ เมื่อเกิดเหตุละเมิดขึ้น

ภาคผนวก ก มาตรฐานหลักการตรวจสอบภายในสากล

ในส่วนต่อไปนี้ ได้คัดเลือกมาจาก *มาตรฐานสากลการปฏิบัติงานวิชาชีพตรวจสอบภายใน (มาตรฐาน)* ของสมาคมผู้ตรวจสอบภายใน (IIA) เฉพาะที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

มาตรฐาน 1210 - ความชำนาญ

ผู้ตรวจสอบภายในต้องมีความรู้ ทักษะ และความสามารถอื่นๆ ที่จำเป็นต่อการปฏิบัติหน้าที่ที่ได้รับมอบหมาย หน่วยงานตรวจสอบภายในโดยรวมแล้วต้องมีหรือได้รับ ความรู้ ทักษะ และความสามารถอื่นๆ ที่จำเป็นต้องนำมาใช้ในการปฏิบัติงานตามหน้าที่ของหน่วยงานนั้น

> 1210.A3 – ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมหลักของเทคโนโลยีสารสนเทศ รวมทั้งเทคนิคการตรวจสอบด้วยเทคโนโลยีสารสนเทศ เพื่อให้ปฏิบัติงานที่ได้รับมอบหมายได้ อย่างไรก็ตาม ใช่ว่าผู้ตรวจสอบภายในทุกคนที่จำเป็นต้องมีความเชี่ยวชาญเทียบเท่ากับผู้ตรวจสอบภายในที่รับผิดชอบงานตรวจสอบเทคโนโลยีสารสนเทศโดยตรง

มาตรฐาน 2050 –การประสานงานและการพึ่งพาผลงานของผู้อื่น

หัวหน้าหน่วยงานตรวจสอบภายในควรแลกเปลี่ยนข้อมูล ประสานงาน และพิจารณาใช้ผลงานของผู้ให้บริหารด้านกรให้ความเชื่อมั่นและให้คำปรึกษาจากภายในและภายนอกองค์กรรายอื่นๆ เพื่อให้เกิดความมั่นใจในความครอบคลุมอย่างเหมาะสม และเพื่อให้การปฏิบัติงานซ้ำซ้อนกันน้อยที่สุด

มาตรฐาน 2110 – การกำกับดูแล

หน่วยงานตรวจสอบภายในต้องประเมินและให้คำแนะนำที่เหมาะสม เพื่อปรับปรุงกระบวนการกำกับดูแลขององค์กร เพื่อ

- การเสริมสร้างความมีจริยธรรมและคุณค่าที่เหมาะสมภายในองค์กร
- การทำให้เชื่อมั่นได้ในเรื่องการบริหารผลการปฏิบัติงานขององค์กรและความรับผิดชอบในผลของงานที่มีประสิทธิภาพ
- การสื่อสารเกี่ยวกับความเสี่ยงและการควบคุมไปยังส่วนงานต่างๆ ที่เหมาะสมภายในองค์กร
- การประสานกิจกรรมและสื่อสารข้อมูลระหว่างคณะกรรมการ ผู้สอบบัญชี ผู้ตรวจสอบภายใน ผู้ให้ความเชื่อมั่นอื่นๆ และผู้บริหารขององค์กร

2110.A2 – หน่วยงานตรวจสอบภายในต้องประเมินว่าการกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กรสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่

มาตรฐาน 2120 – การบริหารความเสี่ยง

หน่วยงานตรวจสอบภายในต้องประเมินความมีประสิทธิผลและมีส่วนช่วยในการปรับปรุงกระบวนการบริหารความเสี่ยง

ภาคผนวก ข ข้อแนะนำการตรวจสอบภายในสากลที่เกี่ยวข้อง

แนวปฏิบัติ (Practice Guide) เรื่อง "การบริหารความต่อเนื่องทางธุรกิจ – การบริหารภาวะวิกฤต (Business Continuity Management – Crisis Management)"

แนวปฏิบัติ (Practice Guide) เรื่อง "การตรวจสอบความเสี่ยงด้านข้อมูลส่วนบุคคล – พิมพ์ครั้งที่ 2 (Auditing Privacy Risks, 2nd Edition)"

GTAG เรื่อง "วิธีการควบคุมการบริหารการเปลี่ยนแปลงและปิดช่องโหว่: สิ่งที่สำคัญยิ่งต่อความสำเร็จองค์กร พิมพ์ครั้งที่ 2 (Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition)"

GTAG เรื่อง "การบริหารการตรวจสอบเทคโนโลยีสารสนเทศ พิมพ์ครั้งที่ 2 (Management of IT Auditing, 2nd Edition)"

GTAG เรื่อง "การว่าจ้างผู้ให้บริการด้านเทคโนโลยีสารสนเทศจากภายนอก พิมพ์ครั้งที่ 2 (Information Technology Outsourcing, 2nd Edition)"

GTAG เรื่อง "การบริหารการระบุตัวตนและการเข้าถึง (Identity and Access Management)"

GTAG เรื่อง "การพัฒนาแผนการตรวจสอบเทคโนโลยีสารสนเทศ (Developing the IT Audit Plan)"

GTAG เรื่อง "การกำกับดูแลความมั่นคงปลอดภัยของสารสนเทศ (Information Security Governance)"

GTAG เรื่อง "การตรวจสอบการกำกับดูแลเทคโนโลยีสารสนเทศ (Auditing IT Governance)"

หนังสือแสดงจุดยืน (Position Paper) เรื่อง "แนวป้องกัน 3 ชั้นสำหรับการบริหารความเสี่ยงและการควบคุมที่มีประสิทธิผล" (The Three Lines of Defense in Effective Risk Management and Control)

ภาคผนวก ค นิยามแนวคิดหลัก

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity): การปกป้องสินทรัพย์สารสนเทศโดยจัดการกับภัยคุกคามที่มีต่อสารสนเทศที่ถูกประมวลผล จัดเก็บ และส่งต่อโดยระบบสารสนเทศในระหว่างเครือข่าย[4]

ภัยคุกคามทางไซเบอร์ (Cyber Threat): บุคคลซึ่งพยายามเข้าถึงอุปกรณ์ระบบควบคุม และ/หรือเครือข่าย โดยใช้เส้นทางการสื่อสารโดยไม่ได้รับอนุญาต การเข้าถึงนี้อาจมาจากภายในองค์กรโดยผู้ใช้งานที่น่าเชื่อถือ หรือมาจากสถานที่ห่างไกลโดยบุคคลที่ไม่รู้จักโดยมาทางอินเทอร์เน็ต ภัยคุกคามที่มีต่อระบบการควบคุมอาจจะมาจากแหล่งต่างๆ ซึ่งรวมถึง รัฐบาลที่ไม่เป็นมิตร กลุ่มผู้ก่อการร้าย พนักงานที่โกรธแค้น ผู้บุกรุกที่ประสงค์ร้าย[5]

แฮกเกอร์นักเคลื่อนไหว(Hacktivists): กลุ่มแฮกเกอร์ที่ก่อให้เกิดภัยทางไซเบอร์ได้ในระดับปานกลางซึ่งดำเนินการโจมตีแยกไปต่างหากแต่ทำความเสียหายได้ กลุ่มแฮกเกอร์นักเคลื่อนไหวระหว่างประเทศนี้มักจะต้องการเบี่ยงเบนความคิดเห็นหรือโฆษณาชวนเชื่อมากกว่าที่จะต้องการทำลายโครงสร้างพื้นฐาน เป้าหมายของพวกนี้ก็คือ เพื่อสนับสนุนประเด็นในทางการเมือง เป้าหมายรองลงมาคือ การโฆษณาชวนเชื่อและก่อให้เกิดความเสียหายเพื่อสร้างชื่อเสียงในทางลบ[6]

ความมั่นคงปลอดภัยของสารสนเทศ (Information Security):จะให้ความมั่นใจว่า สารสนเทศภายในองค์กรจะได้รับการป้องกันไม่ให้มี การเปิดเผยข้อมูลแก่ผู้ใช้งานที่ไม่ได้รับอนุญาต (การรักษาความลับ -- confidentiality) การแก้ไขที่ไม่เหมาะสม (ความถูกต้องสมบูรณ์ -- integrity) การไม่สามารถเข้าถึงได้เมื่อต้องการ (ความพร้อมใช้ -- availability)[7]

---

[4] ISACA, “ISACA Glossary of Terms,” 29. 2558 http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (เข้าดูเมื่อ 20 มิถุนายน 2559).สงวนลิขสิทธิ์ ใช้โดยได้รับอนุญาต

[5] Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, “Cyber Threat Source Descriptions.” https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions (เข้าดูเมื่อ 20 มิถุนายน 2559)

[6] Ibid. https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#hack (เข้าดูเมื่อ 20 มิถุนายน 2559)

[7] ISACA, “ISACA Glossary of Terms,” 49. 2558. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (เข้าดูเมื่อ 20 มิถุนายน 2559). สงวนลิขสิทธิ์ ใช้โดยได้รับอนุญาต

ซอฟต์แวร์ประสงค์ร้าย (Malware): ซอฟต์แวร์ประสงค์ร้ายที่ได้ถูกออกแบบมาเพื่อ แทรกซึม ทำลาย หรือได้รับข้อมูลจากระบบคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากเจ้าของ[8]

การปิดช่องโหว่ (Patch):การแก้ไขความผิดพลาดและช่องโหว่ของการเขียนซอฟต์แวร์[9]

อีเมล์หลอกลวง (Phishing): เป็นการโจมตีทางจดหมายอิเล็กทรอนิกส์ประเภทหนึ่ง (email) ที่พยายามโน้มน้าวใจผู้ใช้งานว่า ผู้ส่งจดหมายเป็นคนที่มีตัวตนจริง แต่มีเจตนาที่จะได้ข้อมูลเพื่อนำไปใช้โจมตีแบบวิศวกรรมทางสังคม[10]

สถานะความมั่นคงปลอดภัย (Security posture): สถานะความมั่นคงปลอดภัยของ เครือข่าย สารสนเทศ และระบบขององค์กรที่อยู่บนพื้นฐานของทรัพยากรที่ใช้ในการให้ความเชื่อมั่นในสารสนเทศ (Information Assurance--IA resources) (เช่น บุคลากร อุปกรณ์ ซอฟต์แวร์ นโยบาย) และความสามารถที่นำมาใช้ในการบริหารแนวป้องกันขององค์กรและตอบโต้เมื่อสถานการณ์เปลี่ยนแปลงไป[11]

---

[8] Ibid., 59.

[9] Ibid., 69.

[10] Ibid., 70.

[11] Richard Kissel, Editor, “Glossary of Key Information Security Terms, NSISTIR 7298, Revision 2,” 179. 2558 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (เข้าดูเมื่อ 5 กรกฎาคม 2559)

ภาคผนวก ง ข้อควรพิจารณาในการตรวจสอบภายในด้านความมั่นคงปลอดภัยทางไซเบอร์

องค์ประกอบต่อไปนี้ (ซึ่งจัดตามกิจกรรมซึ่งได้อธิบายมาแล้วในแนวปฏิบัติฉบับนี้) ทำหน้าที่ร่วมกันเพื่อดำเนินการเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ นอกจากนี้ ยังได้รวมข้อพิจารณาในการเฝ้าติดตามประสิทธิผลของการปฏิบัติงานไว้ด้วย:

องค์ประกอบที่ 1: การกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์

- เป้าหมายเชิงกลยุทธ์พร้อมกับผู้มีส่วนได้เสียที่ต้องรับผิดรับชอบ และบทบาท ภาระหน้าที่ที่ชัดเจน
- สายการรายงานที่ช่วยส่งเสริมอำนาจตามภาระหน้าที่และวัตถุประสงค์ที่เหมาะสม
- มีความเชี่ยวชาญในการใช้เครื่องมือด้านความมั่นคงปลอดภัย และบังคับใช้นโยบาย
- องค์ประกอบของวิธีปฏิบัติ ประกอบด้วย
    - การกำหนดและสื่อสารถึงระดับความเสี่ยงที่ยอมรับได้
    - กำหนดนโยบายความมั่นคงปลอดภัยทางไซเบอร์
    - ดำเนินการประเมินความเสี่ยงและเฝ้าติดตามบนพื้นฐานของเหตุผลและวิธีการที่มีความสม่ำเสมอ
    - การอบรมและการจัดกำลังคนเข้าทำงานเพื่อนำกลยุทธ์การเฝ้าติดตามความมั่นคงปลอดภัยมาปรับใช้เพื่อสร้างความยั่งยืนเมื่อต้องการขององค์กรมีการเปลี่ยนแปลง
    - กำหนดให้มีการตรวจสอบอย่างเป็นอิสระในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ที่บุคคลภายนอกเป็นผู้ผลิต หรือขายสินค้า หรือให้บริการเฉพาะอย่าง
- การสื่อสารอย่างต่อเนื่อง มาตรวัด การรายงาน และการแกะรอยการกระทำการ
- การบริหารเหตุการณ์ผิดปกติ (Incident Management)
- การวางแผนความต่อเนื่องทางธุรกิจที่เกี่ยวกับสถานการณ์จำลองด้านความมั่นคงปลอดภัยทางไซเบอร์
- ความชัดเจนและการมีส่วนร่วมของผู้บริหารระดับสูงและคณะกรรมการ

องค์ประกอบที่ 2: การจัดทำทะเบียนสินทรัพย์สารสนเทศ

- **รายการทะเบียนข้อมูล** (Inventory of data): ผู้บริหารจะระบุและจัดกลุ่มประเภทและสถานที่ของข้อมูลสำคัญและอ่อนไหว ไม่ว่าจะเก็บที่ภายในหรือภายนอกองค์กรก็ตาม
- **รายการทะเบียนอุปกรณ์ที่ได้รับอนุญาตและไม่ได้รับอนุญาต**: อุปกรณ์ที่ได้รับอนุญาตให้เข้าถึงเครือข่าย (การจัดทำทะเบียน การติดตาม และการแก้ไข) และอุปกรณ์ซึ่งไม่ได้รับอนุญาตที่ตรวจพบจะถูกลบออกไป
    - เฝ้าติดตามจำนวนอุปกรณ์ที่ไม่ได้รับอนุญาตบนเครือข่ายองค์กร และระยะเวลาเฉลี่ยที่ใช้ในการลบอุปกรณ์ที่ไม่ได้รับอนุญาตออกไปจากเครือข่าย
    - ตามรอยร้อยละของระบบบนเครือข่ายองค์กรที่ไม่ได้มีการพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงเครือข่ายองค์กร
    - จัดทำรายการทะเบียนอุปกรณ์เครือข่าย เครื่องแม่ข่าย และอุปกรณ์ผู้ใช้งานให้เป็นปัจจุบันเสมอ
- **รายการทะเบียนซอฟต์แวร์ที่ได้รับอนุญาตและไม่ได้รับอนุญาต**: ทำให้มั่นใจว่าซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นที่ถูกติดตั้ง/สั่งให้ทำงานบนเครือข่าย (จัดทำทะเบียน ตามรอย และแก้ไข) และเชื่อมั่นได้ว่ามีการป้องกันซอฟต์แวร์ที่ไม่ได้รับอนุญาตไม่ให้ได้รับการติดตั้ง ถ้าตรวจพบซอฟต์แวร์ที่ไม่ได้รับอนุญาตควรลบออกในเวลาที่เหมาะสม
    - จำนวนรายการซอฟต์แวร์ที่ไม่ได้รับอนุญาตในเครือข่ายและเวลาเฉลี่ยที่ถูกใช้ในการลบซอฟต์แวร์ที่ไม่ได้รับอนุญาตออกจากเครือข่าย
    - ร้อยละของระบบขององค์กรที่ไม่ได้ใช้งานซอฟต์แวร์บัญชีขาว/บัญชีดำ
    - จำนวนซอฟต์แวร์แอพพลิเคชันที่ถูกบล็อคโดยซอฟต์แวร์บัญชีขาว/บัญชีดำขององค์กร
    - ร้อยละของระบบที่ได้รับการเพิ่มความแข็งแกร่งให้แก่ระบบ (Hardened Systems)

องค์ประกอบที่ 3: การตั้งค่าความมั่นคงปลอดภัยที่เป็นมาตรฐาน

- **การตั้งค่าความมั่นคงปลอดภัยสำหรับอุปกรณ์และซอฟต์แวร์บนอุปกรณ์พกพา คอมพิวเตอร์พกพา เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องแม่ข่าย**: สร้าง นำมาใช้งาน และบริหารจัดการอย่างว่องไว (ตามรอย รายงาน แก้ไข) การตั้งค่าความมั่นคงปลอดภัย
    - ร้อยละของระบบขององค์กรที่ไม่ได้รับการตั้งค่าตามมาตรฐานการตั้งค่าที่ได้รับอนุมัติ

- ร้อยละของระบบขององค์กรที่มีการตั้งค่าความมั่นคงปลอดภัยที่ไม่ได้ถูกบังคับใช้โดยเทคนิคของระบบบริหารการตั้งค่า
- ร้อยละของระบบขององค์กรที่ยังไม่ได้รับการปิดช่องโหว่ด้านความมั่นคงปลอดภัยให้เป็นปัจจุบันด้วยซอฟต์แวร์ระบบปฏิบัติการล่าสุดที่มีอยู่
- ร้อยละของระบบขององค์กรที่ยังไม่ได้รับการปิดช่องโหว่ด้านความมั่นคงปลอดภัยให้เป็นปัจจุบัน ด้วยแอพพลิเคชันซอฟต์แวร์ทางธุรกิจล่าสุดที่มีอยู่

- **การตั้งค่าความมั่นคงปลอดภัยสำหรับอุปกรณ์เครือข่าย เช่น ไฟร์วอลล์ เราเตอร์ และสวิตช์**: สร้าง นำมาใช้งาน และบริหารจัดการอย่างว่องไว (ตามรอย รายงาน แก้ไข) การตั้งค่าความมั่นคงปลอดภัย
  - ปริมาณและความถี่ของการเปลี่ยนแปลงการตั้งค่าระบบเครือข่าย
  - ระยะเวลาเฉลี่ยในการแจ้งเตือนผู้ดูแลระบบขององค์กรให้ทราบถึงการเปลี่ยนแปลงการตั้งค่าโดยไม่ได้รับอนุญาต และระยะเวลาเฉลี่ยในการบล้อค/กักกัน การเปลี่ยนแปลงบนเครือข่าย

องค์ประกอบที่ 4: การบริหารการเข้าถึงสารสนเทศ

- **การควบคุมการใช้สิทธิของผู้ดูแลระบบ**: เฝ้าติดตามการใช้ การแต่งตั้ง และการตั้งค่าของสิทธิการใช้งานที่เป็นของผู้ดูแลระบบในคอมพิวเตอร์ เครือข่าย และระบบงาน/แอพพลิเคชัน
- **การเฝ้าติดตามและควบคุมบัญชีผู้ใช้งาน**: บริหารวงจรชีวิตของบัญชีผู้ใช้งานระบบและระบบงาน/แอพพลิเคชัน (การสร้าง การใช้งาน บัญชีที่ไม่เคลื่อนไหว และการลบ)
- **การควบคุมการเข้าถึงโดยตั้งอยู่บนพื้นฐานของ "ความจำเป็นที่ต้องทราบ"** (the need to know): ตามรอย ควบคุม ป้องกัน และแก้ไข การเข้าถึงสินทรัพย์ที่สำคัญให้มีความปลอดภัย (เช่น สารสนเทศ ทรัพยากร ระบบ)
- **ประชากรผู้ใช้งาน**: กระบวนการเข้าถึงของผู้ใช้งานต้องคำนึงถึงทุกคนที่มีสิทธิเข้าถึงข้อมูลที่สำคัญได้ ซึ่งรวมถึงผู้ใช้งานทั้งภายในและภายนอกองค์กร องค์กรส่วนใหญ่จะมีพนักงาน ที่ปรึกษา และผู้ขาย ซึ่งเข้าถึงข้อมูลได้จากภายในและจากภายนอก รวมถึงกลุ่มบุคคลที่สามเมื่อมีการโอนข้อมูลออกไปให้

องค์ประกอบที่ 5: การตอบสนองและการแก้ไขโดยทันที

- การปรับปรุงโครงการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ให้ดีขึ้นอย่างต่อเนื่อง เริ่มจากการให้ข้อเสนอแนะและดำเนินการให้เสร็จสมบูรณ์ภายในเวลาที่เหมาะสม
- ประเมินช่องโหว่ วิเคราะห์ข้อมูลเกี่ยวกับภัยคุกคาม และระบุช่องว่างที่มี
- วัดผลการปฏิบัติงานและเปรียบเทียบกับเกณฑ์เทียบเคียงในอุตสาหกรรมเดียวกัน (Industry Benchmark) และองค์กรอื่นในอุตสาหกรรมเดียวกัน
- กำหนดความรู้ ทักษะ และความสามารถที่เฉพาะเจาะจงซึ่งจำเป็นต่อการสนับสนุนโครงการ
- ต่อไปนี้เป็นรายการตัวอย่างของเกณฑ์วัดบางเกณฑ์:
    - ปริมาณและร้อยละของการแก้ไขที่มีความยั่งยืน แยกตามสถานที่ตั้ง/ฝ่ายงาน/พนักงาน
    - จำนวนช่องโหว่ด้านเทคโนโลยีสารสนเทศและข้อยกเว้นของนโยบายแยกตามสถานที่ตั้ง/ฝ่ายงาน/พนักงาน
    - ค่าคะแนนการปฏิบัติตามแพลทฟอร์ม (Platform compliance scores) แยกตามสถานที่ตั้ง/ฝ่ายงาน

องค์ประกอบที่ 6: การเฝ้าติดตามอย่างต่อเนื่อง

- **การป้องกันซอฟต์แวร์ประสงค์ร้าย** (Malware defense): ควบคุมการติดตั้ง การแพร่กระจาย การสั่งให้รหัสซอฟต์แวร์ประสงค์ร้าย (Malicious code) ทำงาน มีการปรับปรุงมาตรการป้องกันโดยเร็ว รวบรวมข้อมูล ดำเนินการแก้ไข
- **การจำกัดและการควบคุมพอร์ตของเครือข่าย ระเบียบพิธีการที่ใช้ในการสื่อสาร และเครื่องแม่ข่ายของเครือข่าย** (Limitation and control of network ports, protocols and server): ตามรอย ควบคุม และแก้ไขการใช้พอร์ตในแรปฏิบัติงาน ระเบียบพิธีการที่ใช้ในการสื่อสาร และบริการที่ให้แก่อุปกรณ์ในเครือข่าย
- **ความมั่นคงปลอดภัยของซอฟต์แวร์ระบบงาน/แอพพลิเคชั่น** (Application Software Security): ป้องกัน ตรวจจับ และแก้ไขจุดอ่อนด้านความปลอดภัยของซอฟต์แวร์ ทั้งที่พัฒนาขึ้นเองภายในองค์กรและที่จัดซื้อ/จัดหามาใช้ทั้งหมด

- **การควบคุมการเข้าถึงแบบไร้สาย** (Wireless access control): ตามรอย ควบคุม และแก้ไขการใช้เครือข่ายแบบไร้สาย (Wireless LANs) จุดเข้าถึง (Access Point) และระบบลูกข่ายแบบไร้สาย (Wireless client systems)
- **การปกป้องเขตแดน** (Boundary defense): ตรวจจับ ป้องกัน และ แก้ไข เส้นทางของเครือข่ายที่กำลังส่งต่อข้อมูลที่เครือข่ายมีระดับความน่าเชื่อถือที่ต่างกัน
- **การทดสอบการเจาะระบบ การทดสอบอีเมล์หลอกลวง และ การดำเนินการโดยทีมฉุกเฉิน** (Penetration tests, Phishing tests, and red team exercises): ทดสอบความแข็งแกร่งของแนวป้องกันขององค์กร (เทคโนโลยี กระบวนการ และคน) ในภาพรวม
- **การบำรุงรักษา การเฝ้าติดตาม และการวิเคราะห์เหตุการณ์การเปลี่ยนแปลง**(Maintenance, monitoring and analysis of change events): รวบรวม จัดการ และวิเคราะห์เหตุการณ์ (events) และกรณีต่างๆ (Incidents) ที่มีการเปลี่ยนแปลง ซึ่งจะสามารถช่วยในการตรวจจับ ทำความเข้าใจ หรือกู้คืนสภาพจากการถูกโจมตีได้ รวมถึงการวิเคราะห์จากระบบที่ตรวจจับการบุกรุก (intrusion detection systems -- IDS) และทะเบียนบันทึก (Log) กิจกรรมของผู้ใช้งานที่มีสิทธิสูง
- **การปกป้องข้อมูล/การป้องกันข้อมูลสูญหาย** (Data protection/data loss prevention): ป้องกัน/บรรเทาผลกระทบจากการถูกจารกรรมข้อมูล เพื่อให้มั่นใจได้ในเรื่อง ความเป็นส่วนตัว/ความสมบูรณ์ถูกต้องของข้อมูล การนำเครื่องมือมาช่วย ตามสมควร

ผู้เขียน/ผู้สนับสนุนข้อมูล

Bradley C. Ames CRMA CISA

Forrest R. foster CISA

Caroline Glunn CIA CISA

Mike Lynn CRMA

Dean Nakama

Tim Penrose CIA CISA

Sajay Rai CISM

เกี่ยวกับสมาคม

สมาคมผู้ตรวจสอบภายใน (IIA) เป็นหน่วยงานด้านการตรวจสอบภายในที่ได้รับการยอมรับอย่างกว้างขวางในการเป็นผู้ให้การสนับสนุน ผู้ให้ความรู้ และผู้กำหนดมาตรฐาน แนวทางปฏิบัติต่างๆ และวุฒิบัตรรับรองคุณวุฒิต่างๆ ที่เกี่ยวข้องกับวิชาชีพตรวจสอบภายใน สมาคมก่อตั้งขึ้นในปีพ.ศ. 2484 ในปัจจุบัน IIA ได้ให้บริการสมาชิกมากกว่า 185,000 คน จากมากกว่า 170 ประเทศและดินแดน สำนักงานใหญ่ของสมาคมตั้งอยู่ที่เลคแมรี่ (Lake Mary) มลรัฐฟลอริดา สหรัฐอเมริกา สำหรับข้อมูลเพิ่มเติมโปรดเยี่ยมชม www.globaliia.org หรือ www.theiia.org

เกี่ยวกับแนวทางเสริม (Supplemental Guidance)

แนวทางเสริมเป็นส่วนหนึ่งของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (IPPF) ของ IIA และให้แนวทางเพิ่มเติม (ไม่บังคับ) สำหรับการปฏิบัติกิจกรรมต่างๆ ของหน่วยงานตรวจสอบภายใน โดยที่แนวทางเสริมสนับสนุน*มาตรฐาน* **แนวทางเสริม**จึงไม่ได้ต้องการที่จะเชื่อมโยงโดยตรงกับความสำเร็จในการปฏิบัติให้สอดคล้องกับ*มาตรฐาน* แต่มีวัตถุประสงค์เพื่อพูดถึงประเด็นเฉพาะ รวมทั้งประเด็นบางประเด็นของบางภาคส่วน กับมีกระบวนการและวิธีการโดยรายละเอียดใส่ไว้ให้ด้วย แนวทางนี้ได้รับการรับรองโดย IIA โดยผ่านกระบวนการสอบทานและการอนุมัติอย่างเป็นทางการมาแล้ว

แนวปฏิบัติ (Practice Guides)

แนวปฏิบัติเป็นรูปแบบหนึ่งของแนวทางเสริม (Supplemental Guidance) ที่ให้แนวทางสำหรับการดำเนินกิจกรรมตรวจสอบภายในโดยละเอียด ซึ่งรวมถึงรายละเอียดของกระบวนการและวิธีการต่างๆ เช่น เครื่องมือและเทคนิค โปรแกรม และขั้นตอนทีละขั้น รวมถึงตัวอย่างผลงานที่ส่งมอบ ในฐานะที่แนวปฏิบัติถือเป็นส่วนหนึ่งของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (IPPF) จึงเพียงแค่แนะนำให้ปฏิบัติสอดคล้องกับแนวปฏิบัติ (แต่ไม่บังคับ) แนวปฏิบัติได้รับการรับรองโดย IIA โดยผ่านกระบวนการสอบทานและการอนุมัติอย่างเป็นทางการมาแล้ว

แนวการตรวจสอบเทคโนโลยีสารสนเทศระดับโลก (Global Technologies Audit Guide--GTAG) เป็นรูปแบบหนึ่งของแนวปฏิบัติที่เขียนขึ้นโดยใช้ภาษาธุรกิจที่ตรงไปตรงมา เพื่อกล่าวถึงประเด็นต่างๆ ที่เกี่ยวข้องกับการบริหาร การควบคุม หรือความปลอดภัยที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศภายใน ในช่วงเวลาที่เหมาะสม

สำหรับเอกสารแนะนำแนวทางอื่นๆ ที่จัดทำและรับรองโดยสมาคมผู้ตรวจสอบภายใน ท่านสามารถเยี่ยมชมเว็บไซต์ของเราได้ที่ www.globaliia.org/standards-guidance หรือ www.theiia.org/guidance

ข้อความปฏิเสธความรับผิดชอบ

IIA ตีพิมพ์เอกสารนี้เพื่อจุดประสงค์ในการให้ข้อมูลและเพื่อการศึกษาเท่านั้น และไม่ได้มีวัตถุประสงค์เพื่อให้คำตอบที่ชัดเจนที่สุดสำหรับสถานการณ์เฉพาะแต่ละสถานการณ์ ดังนั้น จึงมีวัตถุประสงค์เพียงเพื่อใช้เป็นแนวทางในการปฏิบัติงานเท่านั้น IIA จึงใคร่แนะนำให้ท่านขอคำปรึกษาจากผู้เชี่ยวชาญอิสระซึ่งมีความรู้เกี่ยวข้องโดยตรงกับสถานการณ์เฉพาะนั้นๆ IIA จะไม่รับผิดชอบใดๆ ต่อการที่ผู้ใดก็ตามเชื่อและอาศัยคำแนะนำนี้แต่เพียงอย่างเดียว

ลิขสิทธิ์

16 กันยายน 2559