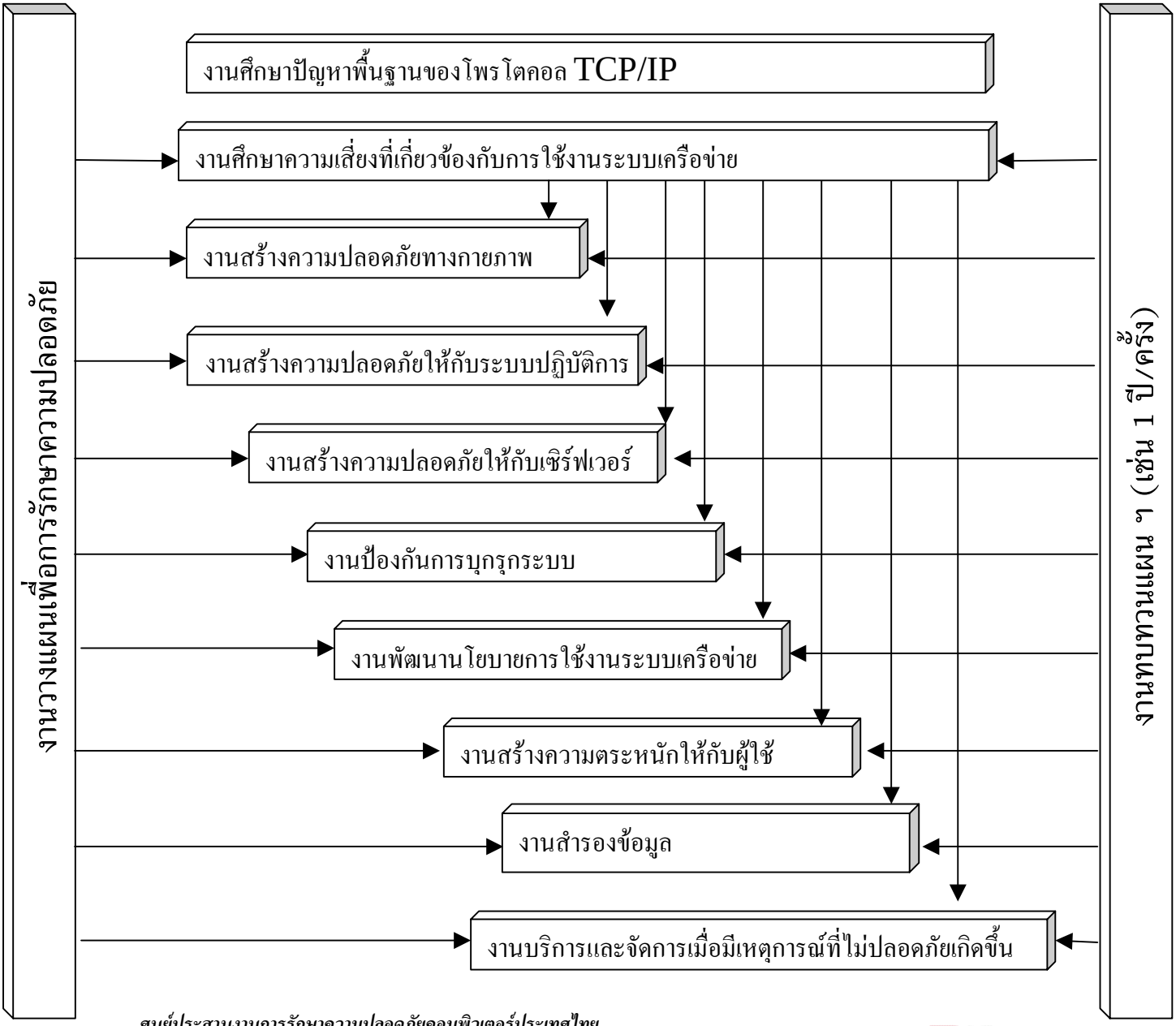
กระบวนการสร้างความปลอดภัยให้กับระบบเครือข่ายสารสนเทศขององค์กร

โดย ดร.บรรจง หะรังษี

บทความนี้มีจุดประสงค์ให้ผู้อ่านทั้งในระดับบริหารและ ผู้ปฏิบัติได้ทราบถึงกระบวนการในการสร้างความปลอดภัยให้กับระบบเครือข่ายสารสนเทศขององค์กร ผู้เขียนมีพื้นฐานเกี่ยวกับ Process Management และ Information Security จึงได้นำพื้นฐานนี้มาเขียนถ่ายทอดในแนว Information Security Process Management คำว่า Process ในภาษาไทยสามารถแปลว่า “งาน” ดังนั้นวลี Information Security Process Management จึงหมายถึงการบริหารงานเพื่อสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ ความมุ่งหวังที่สำคัญของบทความนี้คือเมื่ออ่านจบแล้ว ผู้อ่านจะได้ทราบวิธีการที่อาจกล่าวได้ว่าครบวงจรในการสร้างความปลอดภัยให้กับระบบเครือข่ายสารสนเทศ

งาน(process)ที่เกี่ยวข้องกับการสร้างความปลอดภัยให้กับระบบเครือข่ายโดยพื้นฐานสามารถแสดงได้ดังรูปที่ 1.



ลูกศรในรูปหมายถึงผลของงานซึ่งอยู่ที่ปลายลูกศรมีผลต่องานที่อยู่ที่หัวลูกศร เช่น งานวางแผน (ที่อยู่ในแนวตั้งทางซ้ายมือ) มีผลต่องานทุก ๆ งานที่อยู่ตรงกลาง (ยกเว้นงานศึกษาปัญหาพื้นฐานของโพรโตคอล TCP/IP) งานศึกษาความเสี่ยงและงานทบทวนแผนสร้างความปลอดภัยก็มีผลต่องานทุกงานเช่นเดียวกัน

จากนี้ไปจะเป็นการร้อยเรียงงานต่าง ๆ ที่กล่าวถึงในรูปเข้าด้วยกันเพื่อให้ผู้อ่านได้มองเห็นความสัมพันธ์ของงานเหล่านั้นทั้งหมด

- งานศึกษาปัญหาพื้นฐานของโพรโตคอล TCP/IP ปัญหาความไม่ปลอดภัยเป็นจำนวนมากที่เกิดขึ้นบนระบบเครือข่ายรวมทั้งอินเทอร์เน็ตด้วย มีสาเหตุสำคัญมาจากตัวโพรโตคอลที่ใช้ในการสื่อสารบนเครือข่ายหรือที่เรียกกันว่า TCP/IP (Transmission Control Protocol and Internet Protocol) ดังนั้นผู้วางแผนระบบเครือข่ายควรจะได้เรียนรู้และทำความเข้าใจพื้นฐานนี้เป็นสิ่งแรก
- งานศึกษาความเสี่ยงที่เกี่ยวข้องกับการใช้งานระบบเครือข่าย งานศึกษานี้จะเป็นการศึกษาถึงความเสี่ยงหรือภัยต่าง ๆ ที่สำคัญ ๆ และพบอยู่บ่อย ๆ ทั้งบนระบบเครือข่ายขององค์กรและอินเทอร์เน็ต ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล TCP/IP ด้วย
- งานวางแผนเพื่อสร้างความปลอดภัย งานวางแผนนี้โดยทั่วไปประกอบด้วย
    1) งานศึกษาระบบเครือข่ายปัจจุบัน
    2) งานวิเคราะห์ความเสี่ยงที่มีโอกาสเกิดขึ้นได้จากการใช้งานระบบเครือข่าย
    3) งานออกแบบวิธีการเพื่อลดความเสี่ยงที่พบ
- งานทบทวนแผนเพื่อสร้างความปลอดภัย ภายหลังจากที่ได้มีการนำวิธีการเพื่อลดความเสี่ยงมาใช้งานเป็นระยะเวลาหนึ่ง เช่น 1 ปี องค์กรควรจะได้ทบทวนแผนนี้ใหม่ ทั้งนี้เนื่องจากในช่วงระยะเวลาที่ผ่านมา การนำเทคโนโลยีใหม่มาใช้งาน การอัพเกรดซอฟต์แวร์ เป็นต้น จะทำให้องค์กรรับความเสี่ยงใหม่เข้ามา จึงต้องทำการวิเคราะห์ความเสี่ยงและหาวิธีการแก้ไขเพิ่มเติม จึงเป็นการเข้าสู่กระบวนการขั้นที่ 1, 2, และ 3 ของงานวางแผนเพื่อสร้างความปลอดภัยอีกครั้งหนึ่งนั่นเอง

งานออกแบบวิธีการเพื่อลดความเสี่ยงในขั้นที่ 3 นั้นโดยทั่วไปประกอบไปด้วย

- งานสร้างความปลอดภัยทางกายภาพ ได้แก่ งานควบคุมการเข้าออกอาคารสำนักงาน ห้องคอมพิวเตอร์ ห้องเซิร์ฟเวอร์ หรือห้องที่มีความสำคัญอื่น ๆ งานควบคุมและจำกัดการใช้อุปกรณ์คอมพิวเตอร์ต่าง ๆ
- งานสร้างความปลอดภัยให้กับระบบปฏิบัติการ งานติดตั้งระบบปฏิบัติการให้ทำงานอย่างปลอดภัยถือเป็นพื้นฐานที่สำคัญประการหนึ่งที่ไม่ควรละเลยไม่ว่าเครื่องคอมพิวเตอร์นั้นจะเป็นเครื่องของผู้ใช้ทั่วไปหรือเครื่องเซิร์ฟเวอร์ก็ตาม งานติดตั้งนี้ควรถือเป็นภาคบังคับก่อนที่จะก้าวไปสู่งานสร้างความปลอดภัยให้กับเซิร์ฟเวอร์ อุปมาอุปไมยคล้ายกับหากรากฐานของสิ่งปลูกสร้าง (ระบบปฏิบัติการ) ยังไม่แข็งแกร่งแล้ว การก่อสร้างต่อไป (งานสร้างความปลอดภัยให้กับเซิร์ฟเวอร์) เช่น ก่อสร้างชั้นที่ 1,2 จะไม่สามารถทำได้อย่างปลอดภัย
- งานสร้างความปลอดภัยให้กับเซิร์ฟเวอร์ เมื่อได้ทำการติดตั้งระบบปฏิบัติการอย่างปลอดภัยแล้ว ขั้นต่อไปคืองานติดตั้งและใช้งานเซิร์ฟเวอร์ อาทิ เว็บเซิร์ฟเวอร์(Web Server) เอฟทีพีเซิร์ฟเวอร์(FTP Server) ซีเคียลเชลล์เซิร์ฟเวอร์(Secure Shell Server) ดีเอ็นเอสเซิร์ฟเวอร์(DNS Server) ให้สามารถทำงาน

อย่างปลอดภัย งานสร้างความปลอดภัยนี้จะเกี่ยวข้องกับงานศึกษาเพื่อสร้างความปลอดภัยให้กับเซิร์ฟเวอร์ทุกเครื่องขององค์กร

- งานป้องกันการบุกรุกระบบ งานนี้เป็นงานเสริมสร้างระบบเครือข่ายให้มีความแข็งแกร่งมากยิ่งขึ้น เพื่อให้เซิร์ฟเวอร์หรือเครื่องผู้ใช้ทั่วไปปลอดภัยจากการบุกรุกที่อาจมาจากทางอินเทอร์เน็ต งานป้องกันนี้ประกอบด้วย
    - งานจัดทำไฟร์วอลล์

      งานนี้เป็นงานควบคุมหรือจำกัดการเข้าออกเครือข่ายขององค์กร ซึ่งหมายรวมถึงการป้องกันเพื่อไม่ให้ผู้ที่ไม่มีสิทธิเข้ามาใช้งานเครือข่ายและเซิร์ฟเวอร์ขององค์กร
    - งานจัดทำระบบป้องกันการบุกรุก

      ในกรณีที่ไฟร์วอลล์อนุญาตให้เข้ามาใช้งานได้ เช่น เข้ามาใช้งานเว็บเซิร์ฟเวอร์ขององค์กร สิ่งนี้ไม่ได้หมายความว่าองค์กรจะปลอดภัย 100 เปอร์เซ็นต์ ช่องโหว่ในซอฟต์แวร์ของเว็บเซิร์ฟเวอร์ที่ยังไม่ได้รับการอุดอาจยังมีอยู่และสามารถใช้เป็นช่องทางในการในการบุกรุก งานจัดทำระบบป้องกันการบุกรุกนี้มีจุดประสงค์หลักหนึ่งคือเพื่อลดความเสี่ยงของช่องโหว่ในตัวซอฟต์แวร์
    - งานจัดทำระบบค้นหาจุดอ่อน

      ระบบป้องกันการบุกรุกโดยทั่วไปจะสามารถทำการแจ้งเตือนผู้ดูแลระบบเมื่อตรวจพบความพยายามในการบุกรุก โดยทั่วไประบบนี้จะทำงานอยู่ตลอด 24 ชั่วโมงโดยจะทำการตรวจสอบข้อมูลที่ผ่านเข้าออกเครือข่ายขององค์กรเพื่อดูว่ามีความพยายามที่จะบุกรุกหรือไม่ สำหรับระบบค้นหาจุดอ่อน ความสามารถส่วนหนึ่งที่สำคัญของระบบนี้คือสามารถค้นหาช่องโหว่ในตัวซอฟต์แวร์ซึ่งนับเป็นจุดอ่อนหนึ่ง (เช่นเดียวกับระบบป้องกันการบุกรุก) แต่ระบบนี้โดยปกติจะไม่ได้ทำงานอยู่ตลอด 24 ชั่วโมง และจะมีการนำมาใช้งานตามช่วงระยะเวลาที่กำหนดไว้ เช่น ทุกๆ เดือน รวมทั้งระบบจะไม่ได้ตรวจสอบข้อมูลที่ผ่านเข้าออกเครือข่าย
    - งานตรวจสอบความสมบูรณ์ของไฟล์ในระบบ

      ความพยายามอย่างยิ่งยวดในการป้องกันการบุกรุกระบบไม่ว่าจะด้วยไฟร์วอลล์ ระบบป้องกันการบุกรุก หรือระบบค้นหาจุดอ่อน ก็ตามก็ยังอาจมีโอกาสที่ผู้บุกรุกจะสามารถจู่โจมเข้ามาได้อยู่ดี (เรื่องของความปลอดภัยเป็นเรื่องของการลดความเสี่ยงแต่ไม่สามารถทำให้ความเสี่ยงเป็นศูนย์) อย่างไรก็ตามเมื่อการบุกรุกครั้งหนึ่ง ๆ เกิดขึ้น ผู้บุกรุกมักทิ้งร่องรอยไว้ในระบบที่บุกรุกเข้าไป เช่น การเปลี่ยนแปลงแก้ไขไฟล์ การติดตั้งซอฟต์แวร์ (ไฟล์) เข้าไปในระบบ งานตรวจสอบความสมบูรณ์นี้จะเป็นทางหนึ่งที่จะช่วยให้ผู้ดูแลระบบสามารถทราบถึงการกระทำที่เกิดขึ้นกับไฟล์ในระบบ เช่น ในเครื่องเซิร์ฟเวอร์หนึ่ง ๆ เพื่อจะได้หาทางดำเนินการแก้ไขต่อไป
    - งานป้องกันไวรัส

      การบุกรุกของไวรัสภายในองค์กรอาจจะมาจากการดาวน์โหลดไฟล์ของผู้ใช้ผ่านทางอินเทอร์เน็ตหรือจากทางอี-เมล์ที่ได้รับ โดยทั่วไปไฟร์วอลล์จะอนุญาตการดาวน์โหลดของผู้ใช้ผ่านทางอินเทอร์เน็ต รวมทั้งจะอนุญาตการส่งมอบอี-เมล์จากเมล์เซิร์ฟเวอร์ที่อยู่ภายนอกเข้ามาสู่เมล์เซิร์ฟเวอร์ขององค์กร โดยที่ในทั้งสองกรณีไฟร์วอลล์จะไม่รับรู้ว่ามีไวรัสติดมาด้วยหรือไม่ ดังนั้นงานป้องกันไวรัสจึงเป็นทางเสริมอีกทางหนึ่งที่สำคัญเพื่อป้องกันการบุกรุกจากภายนอกเข้ามาสู่เครือข่ายภายในองค์กร

- งานตรวจสอบปริมาณข้อมูลบนเครือข่าย

  ปริมาณข้อมูลบนเครือข่ายขององค์กรที่สูงมากผิดปกติอาจมีสาเหตุมาจากมีไวรัสกำลังแพร่กระจายอยู่ หรือมีการส่งหรือรับข้อมูลในเครือข่ายขององค์กรเป็นปริมาณสูง ปริมาณข้อมูลในเครือข่ายที่สูงเกินไปนี้จะมีผลทำให้การใช้งานเครือข่ายของพนักงานเป็นไปอย่างล่าช้า ติดขัด หรืออาจถึงขั้นไม่สามารถใช้งานได้เลย ดังนั้นงานตรวจสอบปริมาณข้อมูลนี้ควรจะดำเนินการอย่างสม่ำเสมอเพื่อจะได้รู้ทราบว่ามีความผิดปกติเกิดขึ้นหรือไม่และจะได้ดำเนินการแก้ไขได้อย่างทันท่วงที

- งานเฝ้าดูการทำงานของเซิร์ฟเวอร์

  เซิร์ฟเวอร์ให้บริการส่วนใหญ่ขององค์กรจะให้บริการต่างๆ เช่น เว็บ เอฟทีพี(FTP) ซีเคียลเชลล์(Secure Shell) MySQL เป็นต้น ซึ่งเซิร์ฟเวอร์ให้บริการนี้จะสามารถบันทึกกิจกรรมการเข้าใช้งานของผู้ใช้เพื่อเก็บเอาไว้เป็นหลักฐานยืนยันในภายหลังได้ เช่น วันและเวลาที่เข้าใช้งาน กิจกรรมที่ทำ เป็นต้น ข้อมูลที่บันทึกไว้นี้โดยปกติควรจะได้รับการตรวจสอบอย่างสม่ำเสมอจากผู้ดูแลระบบ (ซึ่งเป็นการเฝ้าดูว่ามีความพยายามที่จะบุกรุกเซิร์ฟเวอร์ขององค์กรหรือไม่) หากพบความผิดปกติ เช่น ความพยายามในการเข้าใช้งานเซิร์ฟเวอร์โดยที่ไม่มีสิทธิ ผู้ดูแลระบบจะได้หาทางแก้ไขต่อไป

- งานอุดช่องโหว่ในตัวซอฟต์แวร์

  ซอฟต์แวร์ที่ใช้งานในระบบเครือข่าย เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์เซิร์ฟเวอร์ต่าง ๆ อาจจะมีช่องโหว่ที่ผู้บุกรุกสามารถใช้ให้เป็นประโยชน์ในการเจาะระบบ ดังนั้นจึงมีความจำเป็นที่จะต้องหาทางอุดช่องโหว่เหล่านี้ ระบบค้นหาจุดอ่อนเป็นวิธีหนึ่งที่สามารถช่วยค้นหา ช่องโหว่ในตัวซอฟต์แวร์ได้ นอกจากนั้นแล้วในปัจจุบันมีซอฟต์แวร์อยู่หลายชนิดที่สามารถช่วยในการอุดช่องโหว่ให้โดยอัติโนมัติ

- งานพัฒนานโยบายการใช้งานระบบเครือข่าย

  งานทางเทคนิคหลายงานที่ได้กล่าวถึงข้างบน ได้แก่ งานสร้างความปลอดภัยให้กับระบบปฏิบัติการและเซิร์ฟเวอร์ งานป้องกันการบุกรุก อาจจะไม่เป็นผลเท่าที่ควร หากผู้ดูแลระบบละเลยการติดตั้งระบบปฏิบัติการหรือเซิร์ฟเวอร์ให้ทำงานอย่างปลอดภัย พนักงานละเลยไม่ติดตั้งซอฟต์แวร์ป้องกันไวรัส พนักงานไม่ทำการสำรองข้อมูลเก็บไว้ ผู้ดูแลระบบไม่เคยตรวจสอบข้อมูลกิจกรรมการเข้าใช้งานเซิร์ฟเวอร์ที่บันทึกไว้ พนักงานขาดการตระหนักถึงภัยของไวรัสที่มีต่อระบบเครือข่ายขององค์กร สิ่งต่าง ๆ เหล่านี้จึงทำให้มีความจำเป็นที่จะต้องจัดทำนโยบายการใช้งานออกมา (เป็นคล้าย ๆ กฎเหล็กที่ต้องปฏิบัติตาม) เพื่อควบคุมพฤติกรรมการใช้งานระบบเครือข่ายของทั้งผู้ดูแลระบบและผู้ใช้งานทั่วไป เพื่อไม่ให้ละเลยหรือปฏิบัติออกนอกลู่นอกทางที่ตนควรกระทำ

- งานสร้างความตระหนักให้กับผู้ใช้

  พฤติกรรมการใช้งานระบบเครือข่าย เช่น การดาวน์โหลดไฟล์โดยไม่มีการตรวจสอบไวรัส การแชร์รหัสผ่าน การแชร์ไฟล์โดยไม่มีรหัสผ่าน การส่งรหัสผ่านทางอีเมล์ หรือพฤติกรรมที่มีความเสี่ยงอื่น ๆ ทั้งหมดนี้สามารถทำให้ระบบเครือข่ายขององค์กรมีความเสี่ยงที่อาจจะถูกบุกรุกหรือได้รับความเสียหายได้ จึงทำให้มีความจำเป็นที่จะต้องจัดกิจกรรมต่าง ๆ เพื่อสร้างความ

ตระหนักให้กับผู้ใช้ เช่น การจัดอบรมเพื่อให้ความรู้ การติดประกาศในที่ ๆ สามารถมองเห็นได้ง่าย เป็นต้น ทั้งนี้เพื่อให้ผู้ใช้มีความระมัดระวังมากยิ่งขึ้นในการใช้งานระบบเครือข่าย

- งานสำรองข้อมูล

  ความเสี่ยงมักเกิดขึ้นได้หลากหลาย เช่น ความเสี่ยงที่เกิดจากฮาร์ดดิสก์เสียหาย ความเสี่ยงที่เกิดจากไวรัสทำลายข้อมูล ความเสี่ยงที่ผู้บุกรุกลบข้อมูลสำคัญทิ้งไป ความเสี่ยงเหล่านี้ล้วนทำให้มีความจำเป็นที่จะต้องสำรองข้อมูลเอาไว้ หากข้อมูลที่ใช้งานเกิดการเสียหาย จะได้นำข้อมูลสำรองมาใช้งานได้

- งานบริหารและจัดการเมื่อมีเหตุการณ์ที่ไม่ปลอดภัยเกิดขึ้น

  เมื่อมีเหตุการณ์บุกรุกเกิดขึ้น เช่น มีไวรัสบนระบบเครือข่าย เครือข่ายถูกบุกรุก ข้อมูลหน้าหลักบนเว็บไซต์ขององค์กรถูกเปลี่ยนแปลง ความพยายามในการบุกรุก ผู้ที่พบเห็นเหตุการณ์ควรจะได้ทราบขั้นตอนปฏิบัติที่จำเป็นเพื่อจะได้รายงานให้ผู้ที่มีอำนาจได้รับทราบเพื่อจะได้หาทางดำเนินการแก้ไขต่อไป งานบริหารและจัดการนี้มีจุดประสงค์สำคัญคือจัดทำขั้นตอนปฏิบัติเพื่อให้ผู้ใช้สามารถรายงานเหตุการณ์ที่พบได้อย่างทันท่วงที