แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในองค์กร

Information Security Policies and Practices in the Organization

สรวิศ บุญมี และสุคนธ์ทิพย์ คำจันทร์

บทคัดย่อ

บทความนี้นำเสนอแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เป็นประโยชน์ต่อองค์กรทั่วไปในการนำไปปรับใช้ซึ่งครอบคลุมถึงการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ระบบสำรองของสารสนเทศจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินและและประเมินความเสี่ยงด้านสารสนเทศรวมถึงแนวทางใหม่ในการฝึกบุคลากรเพื่อซ้อมรับมือภัยทางไซเบอร์ (Cyber Drill) และการเตรียมความพร้อมรับความเสียหายทางไซเบอร์ (Cyber Resilience)

คำสำคัญ: ความมั่นคงปลอดภัยด้านสารสนเทศ, แนวนโยบายและแนวปฏิบัติ, การซ้อมรับมือภัยทางไซเบอร์, การเตรียมความพร้อมรับความเสียหายทางไซเบอร์

Abstract

This paper presents the policies and practices in the field of information security in order to benefit the organization in general to adopt such as information access control, backup, emergency plan and risk assessment. This paper also included new approaches in training staff to rehearse against the Cyber-attack (Cyber Drill) and prepare to survive after a successful attack (Cyber Resilience).

Keyword: information security, policy and practice, cyber drill, cyber resilience

ความนำ

ในการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศในองค์กรนั้นมีองค์ประกอบที่ควรคำนึงถึง3 ประการคือ กระบวนการ บุคลากร และเทคโนโลยี (Schneier, 2013) ซึ่งหากละเลยองค์ประกอบใดก็อาจจะไม่ประสบความสำเร็จ เช่น หากมีการจัดหาเทคโนโลยีมาแต่ไม่ให้ความสำคัญกับบุคลากร หรือกระบวนการก็อาจเกิดปัญหาในการขาดคนบำรุงรักษา หรือสับสนในวิธีการแก้ปัญหาได้ องค์กรจึงควรเริ่มโดยการวางแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจากนั้นควรประกาศรวมถึงการให้ความรู้ มีการฝึกบุคลากรเพื่อซ้อมรับมือภัยทางไซเบอร์ (Cyber Drill) และควรเพิ่มแผนการเตรียมความพร้อมรับความเสียหายทางไซเบอร์ (Cyber Resilience) ด้วย เพื่อให้สามารถกลับมาดำเนินการได้ตามปกติได้โดยเร็วแม้จะถูกโจมตีสำเร็จทำให้เกิดความเสียหายไปแล้ว

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์กรควรจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยควรประกอบด้วยเนื้อหาดังต่อไปนี้

1. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

2. จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

หน่วยงานควรจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงาน โดยจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของหน่วยงาน จากนั้นจึงประกาศนโยบายและข้อปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องทั้งหมดทราบไม่ว่าเป็นผู้บริหาร ฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ใช้ เพื่อให้สามารถเข้าถึงเข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้ นอกจากนี้ควรต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน รวมทั้งควรทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ควรมีเนื้อหาอย่างน้อยครอบคลุมดังต่อไปนี้

1. ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อยดังนี้

1.1. มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

1.2 ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานนั้น ๆ

1.3 ควรกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับ ชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

2. ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึง สารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนด ด้านความมั่นคงปลอดภัย

3. ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตร การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยควรมีเนื้อหาอย่างน้อย ดังนี้

1.2. สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

1.3. การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

1.4. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

1.5. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

1.6. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

4. ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

1.7. การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

1.8. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

1.9. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

5. ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

5.1 การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

5.2 การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

5.3 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

5.4 การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

5.5 การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

5.6 การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

6. ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)เพื่อป้องกันการเข้าถึง

ระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

6.1 การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

6.2 การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication)ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

6.3 การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

6.4 การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

6.5 เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

6.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

7. ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

7.1 การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์ ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

7.2 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

7.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

7.4 การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

8. หน่วยงานที่มีระบบสารสนเทศควรจัดทำระบบสำรองตามแนวทางต่อไปนี้

8.1 ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

8.2 ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

8.3 ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบ

สารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

8.4 ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

8.5 สำหรับความถี่ของการปฏิบัติในแต่ละข้อควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

9. จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยต้องมีเนื้อหาอย่างน้อย ดังนี้

9.1 จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง

9.2 ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก(external auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

10. กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

การเตรียมความพร้อมของผู้ใช้ระบบสารสนเทศ

นอกจากกระบวนการข้างต้นแล้ว ผู้ใช้ระบบถือเป็นอีกองค์ประกอบสำคัญ และเป็นจุดอ่อนที่ถูกโจมตีจากการคุกคามทางไซเบอร์อยู่เสมอถึงแม้จะมีกระบวนการป้องกันแล้ว การเตรียมความพร้อมของผู้ใช้ระบบสารสนเทศและการให้ความรู้ด้านภัยสารสนเทศจึงเป็นเรื่องจำเป็นที่องค์กรต้องทำเป็นประจำทุกปี เช่นเดียวกับการซ้อมหนีไฟ องค์กรจึงควรทำการซ้อมรับมือภัยทางไซเบอร์(Cyber Drill)เพื่อให้ผู้ใช้คอมพิวเตอร์ในองค์กรตลอดจนผู้บริหารทั้งระดับกลางและระดับสูงได้ตระหนักรู้และสร้างประสบการณ์ในการรับมือกับภัยคุกคามอย่างได้ผลในทางปฏิบัติส่งผลให้มีความพร้อมต่อภัยทางไซเบอร์ต่างๆที่จะเกิดขึ้น (ปริญญา หอมเอนก, 2558)

การฝึกซ้อมควรจำลองสถานการณ์การคุกคามที่พบได้ทั่วไป และไม่ควรแจ้งล่วงหน้าว่าจะมีการฝึกซ้อม เช่น การทำฟิชชิง (Phishing) ส่งอีเมลหลอกลวงให้ผู้ใช้เปิดเผยข้อมูลสำคัญอย่างชื่อบัญชีและรหัสผ่าน ควรมีการเก็บสถิติผู้ที่หลงเชื่อไว้ จากนั้นอาจจะจัดให้มีการให้ความรู้ด้านภัยสารสนเทศ แล้วจึงทำการฝึกซ้อมซ้ำเพื่อเปรียบเทียบและวัดผลในการให้ความรู้

การเตรียมความพร้อมรับความเสียหายทางไซเบอร์ (Cyber Resilience)

กลไกในการป้องกันการโจมตีจากแฮกเกอร์และผู้ไม่หวังดีโดยใช้มัลแวร์เป็นเครื่องมือตั้งแต่อดีตมานั้นไม่สามารถแก้ปัญหามัลแวร์ได้ 100% ยกตัวอย่างเช่น ทุกวันนี้ยังมีการโจมตีแบบ APT (Advanced Persistent Threat) และ Ransomware อยู่โดยตลอดเวลา โดยจะเห็นได้จากข่าวที่มีบริษัทใหญ่ๆถูกเจาะระบบอยู่เป็นประจำ เช่น Home Depot, Target Supermarket และ Sony Pictures

จากแนวความคิดในการแก้ปัญหาความมั่นคงปลอดภัยไซเบอร์แบบP-D-R Model โดย P คือ Protect D คือ Detect และ R คือ Response (ป้องกัน ตรวจจับ และ

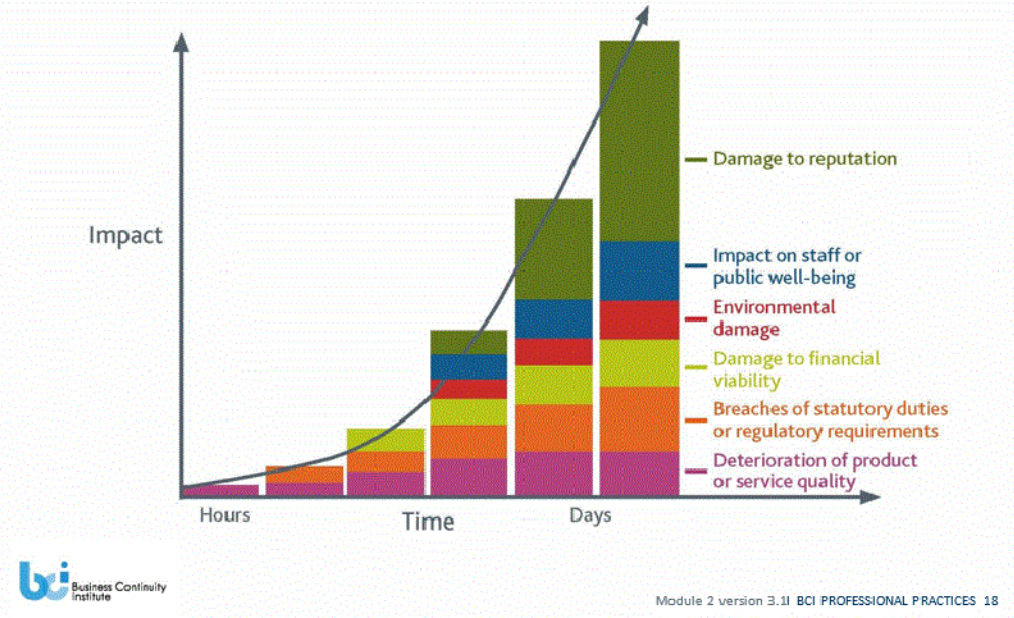
ตอบสนอง) ที่ผ่านมาเชื่อว่าการป้องกัน (P) คือ การแก้ปัญหาที่ดีที่สุด นั่นคือ

Pt > (Dt + Rt) โดย t = time (เวลา)

ซึ่งมีความหมายว่า ถ้าเวลาในการป้องกันมากกว่าเวลาในการตรวจจับและเวลาในการตอบสนององค์กรจะสามารถคงสภาวะที่ยังมีความมั่นคงปลอดภัยไว้ได้ แต่ถ้าเวลาในการป้องกันน้อยกว่าเวลาในการตรวจจับและเวลาในการตอบสนอง ระบบขององค์กรก็จะไม่ปลอดภัยอีกต่อไป แต่โดยทั่วไปในปัจจุบันมักพบว่า

Pt << (Dt + Rt)

หมายถึงเวลาในการตรวจจับและตอบสนองมีมากกว่าเวลาในการป้องกันเป็นอย่างมากดังนั้นจึงควรหันมาเปลี่ยนจากการทุ่มเททรัพยากรไปที่ “P”มาเป็นการให้ความสำคัญที่ “D”และ “R”มากขึ้น ถ้าต้องการให้ระบบขององค์กรมั่นคงปลอดภัยควรพยายามลดเวลาในการตรวจจับลง (Dt) และลดเวลาในการตอบสนองลง (Rt) ด้วยเช่นกัน โดยหากองค์กรมีแผนบริหารความต่อเนื่อง (Business Continuity Plan--BCP) อยู่แล้วควรให้ครอบคลุมถึงทรัพยากรสารสนเทศด้วย เพื่อที่ว่าหากเกิดการโจมตีสำเร็จ องค์กรจะสามารถแก้ไขความผิดพลาด และกลับมาดำเนินการตามปกติได้อย่างเร็วที่สุด ยกตัวอย่างเช่น การใช้เทคโนโลยีในการตรวจจับความผิดปกติในระบบแบบ Real-Timeตลอดจนระบบป้องกันที่สามารถปิดช่องทางของแฮกเกอร์ได้ในเวลาที่กำหนดซึ่งยิ่งใช้เวลาน้อยเท่าไรก็จะลดความเสียหายได้มากเท่านั้นดังภาพ 1



ภาพ 1 Business Impact and Time

บทสรุป

ถึงแม้องค์กรจะต้องเตรียมการรักษาความมั่งคงปลอดภัยด้านสารสนเทศทั้งในด้านกระบวนการ บุคลากร และเทคโนโลยีอย่างครบถ้วนแล้ว แต่สิ่งที่ต้องคำนึงถึงเพิ่มเติมในปัจจุบันคือการเตรียมพร้อมกับเหตุการณ์ไม่พึงประสงค์อยู่ตลอดเวลาเช่น การตรวจจับความผิดปกติในระบบแบบ Real-Timeตลอดจนระบบป้องกันที่สามารถปิดช่องทางของแฮกเกอร์ได้ในเวลาที่กำหนดซึ่งจะช่วยทำให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรมีประสิทธิผลมากขึ้น และสามารถทำให้องค์กรมี Cyber Resilience และ Business Resilience ในที่สุด

เอกสารอ้างอิง

เขมณัฏฐ์ อำนวยวรชัย. (2558). การพัฒนาทรัพยากรการเรียนรู้ทางสถิติผ่านเว็บไซต์เพื่อส่งเสริมการเรียนรู้ที่เน้นผู้เรียนเป็นสำคัญ. *วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชีย ฉบับวิทยาศาสตร์และเทคโนโลยี*, *9*(1), 204-212.

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553. (2553, 23 มิถุนายน). ราชกิจจานุเบกษา. เล่ม 127 ตอนพิเศษ 78ง., หน้า 131-138.

ปริญญา หอมเอนก. (2558). Paradigm shift in cybersecurity from “Time-based Security” to “Responsive Security”. ค้นจาก http://www.acisonline.net/

Itgovernance. (2015). Cyber Resilience. Retrieved from http://www.itgovernance.co.uk/cyber-resilience.aspx