การศึกษาองค์ประกอบของสมรรถนะและแนวโน้มความต้องการของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กร กรณีศึกษา บริษัท มายด์เทอร่า จำกัด

นรินทร์ แสงรุ่ง

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาบริหารธุรกิจมหาบัณฑิต
บัณฑิตวิทยาลัย สาขาการจัดการอุตสาหกรรม
สถาบันเทคโนโลยีไทย - ญี่ปุ่น
ปีการศึกษา 2556

A STUDY OF COMPETENCY AND TREND OF PERSONAL NEED FOR INFORMATION SECURITY PROFESSIONAL A CASE STUDY OF MINDTERRA COMPANY LIMITED

Narin Sangrung

A Term Paper Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Business Administration Program in Industrial Management
Graduate School
Thai - Nichi Institute of Technology
Academic Year 2013

หัวข้อสารนิพนธ์	การศึกษาองค์ประกอบของสมรรถนะและแนวโน้มความต้องการของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กร กรณีศึกษา บริษัท มายด์เทอร่า จำกัด
โดย	นรินทร์ แสงรุ่ง
สาขาวิชา	การจัดการอุตสาหกรรม
อาจารย์ที่ปรึกษาสารนิพนธ์	รองศาสตราจารย์ ดร. ศักดิ์ชัย คิรินทร์ภาณุ

บัณฑิตวิทยาลัย สถาบันเทคโนโลยีไทย-ญี่ปุ่น อนุมัติให้นับสารนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีบัณฑิตวิทยาลัย
(รองศาสตราจารย์ ดร. พิชิต สุขเจริญพงษ์)
วันที่……เดือน……..……พ.ศ……..

คณะกรรมการสอบสารนิพนธ์

..... ประธานกรรมการ
(ดร. กรกฎ เหมสถาปัตย์)

..... กรรมการ
(อาจารย์เกษม ทิพย์ธาราจันทร์)

..... อาจารย์ที่ปรึกษาสารนิพนธ์
(รองศาสตราจารย์ ดร. ศักดิ์ชัย คิรินทร์ภาณุ)

TNI
THAI - NICHI INSTITUTE OF TECHNOLOGY

นรินทร์ แสงรุ่ง : การศึกษาองค์ประกอบของสมรรถนะและแนวโน้มความต้องการของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กร กรณีศึกษา บริษัท มายด์เทอร่า จำกัด. อาจารย์ที่ปรึกษา : รองศาสตราจารย์ ดร. ศักดิ์ชัย คิรินทร์ภาณุ, 69 หน้า.

วัตถุประสงค์ของการศึกษาประกอบด้วยการศึกษาองค์ประกอบของสมรรถนะและแนวโน้มความต้องการของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กร กรณีศึกษา บริษัท มาเทอร่า จำกัด แบบสอบถามเป็นเครื่องมือในการศึกษา โดยการเก็บรวบรวมจากลูกค้าขององค์กรรวม 30 แห่ง ซึ่งผู้ให้ข้อมูลจะเป็นผู้บริหารและผู้เชี่ยวชาญด้าน IT รวม 43 คน จากนั้นนำข้อมูลที่ได้มาวิเคราะห์เป็น 2 ส่วน ความจำเป็นของแต่ละสมรรถนะ โดยการใช้ Likert's Scale แบ่งเป็น 3 ระดับ ได้แก่ สมรรถนะที่มีความจำเป็นมากจะมีระดับคะแนนเฉลี่ย 2.34-3.00 จำเป็น ระดับคะแนนเฉลี่ย 1.67-2.33 และไม่จำเป็น ระดับคะแนนเฉลี่ย 1.00-1.66 และวิเคราะห์แนวโน้มความต้องการของบุคลากรในสายงานนี้ด้วยวิธีการสถิติเชิงพรรณนา

ผลการวิเคราะห์สรุปว่า ในส่วนของคุณลักษณะพื้นฐานมีความจำเป็นกับบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ตัวแปรที่มีความจำเป็นมากของสมรรถนะหลัก ได้แก่ พื้นฐานด้านคอมพิวเตอร์ (2.63) พื้นฐานด้าน Networking และ Internetworking (2.51) พื้นฐานการใช้งานระบบปฏิบัติการเครือข่าย (2.40) และพื้นฐานด้านการจัดการฐานข้อมูล (2.35) ในส่วนของสมรรถนะเฉพาะ ได้แก่ พื้นฐานด้านความปลอดภัยบนระบบปฏิบัติการเครือข่าย (2.40) พื้นฐานด้านการโจมตีบนระบบสารสนเทศ (2.37) และพื้นฐานด้านความปลอดภัยบนระบบปฏิบัติการ (2.37) ในส่วนสุดท้ายคุณลักษณะ ได้แก่ การแก้ปัญหาต่างๆ ได้ (2.47) การคิดวิเคราะห์ได้ (2.44) การให้คำปรึกษาได้ (2.44) การประสานงานที่ดี (2.42) การติดตามงาน (2.42) และความยืดหยุ่นผ่อนปรน (2.40) จากการศึกษาสามารถสรุปได้ว่า การคัดเลือกบุคลากรจะเน้นในการคัดหาคุณลักษณะที่เหมาะสมกับตำแหน่งงานมากกว่าความรู้และทักษะซึ่งสามารถเรียนรู้และสอนจากการทำงานจริงได้ แนวโน้มความต้องการบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ โดยส่วนใหญ่ยังมีความจำเป็นมาก โดยสาเหตุเพื่อป้องกันความเสียหายที่อาจจะเกิดจากการโจมตีของ Hacker และเพื่อป้องกัยความลับหรือข้อมูลสำคัญขององค์กร รวมถึงลดช่องโหว่ที่จะใช้ในการโจมตีหรือสร้างความเสียหายแก่องค์กรได้

บัณฑิตวิทยาลัย ลายมือชื่อนักศึกษา.....

สาขาวิชา การจัดการอุตสาหกรรม ลายมือชื่ออาจารย์ที่ปรึกษา.....

ปีการศึกษา 2556

NARIN SANGRUNG : A STUDY OF COMPETENCY AND TREND OF PERSONAL NEED FOR INFORMATION SECURITY PROFESSIONAL : A CASE STUDY OF MINDTERRA COMPANY LIMITED. ADVISOR : ASSOCIATE PROFESSOR DR. SAKCHAI KIRINPANU, 69 PP.

The objectives were to study competency and trend of personal need for information security professional within the organization of the case study of Mindterra Company Limited. The questionnaire had been used as the tool. The 30 members were major contributors which focused to administrators and IT professionals, totaling 43 respondents. The analysis had been divided as 2 parts. The competency was measured by using Likert Scales which have been divided as three levels : the necessary component is weighted 2.34-3.00, the required component is 1.67-2.33, and the unnecessary component is weighted 1.00-1.66. The trend analysis of personal need was analyzed by using a descriptive analysis.

The analysis concluded that Core Competency Components include basic computer (2.63), basic networking and Internetworking (2.51), basic use network operating systems (2.40) and basic database management (2.35). The Functional Competency Components are basic security system network (2.40), based on attacks on information systems (2.37) and basic security system (2.37). The Attribute Components Include various solutions (2.47), critical thinking (2.44), consultation (2.44), better coordination (2.42), follow-up (2.42) and elastic relaxation of (2.40). The study had been summarized that personnel qualification is focused on screening for the right job because knowledge and skill can be learned and taught from the job. The trend of personal need for information security professional is positive due to the reasons of preventing any damages that may be caused by the onset of a Hacker and protecting confidential or proprietary information of the organization and reducing vulnerability to attack or damage the organization.

Graduate School Student's Signature .....

Field of Study Industrial Management Advisor's Signature .....

Academic Year 2013

กิตติกรรมประกาศ

งานสารนิพนธ์เรื่อง การศึกษาองค์ประกอบของสมรรถนะและแนวโน้มความต้องการของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กร กรณีศึกษา บริษัท มายด์เทอร่า จำกัด สำเร็จลงได้ด้วยความกรุณาของอาจารย์ที่ปรึกษาสารนิพนธ์ คือ รองศาสตราจารย์ ดร. ศักดิ์ชัย คิรินทร์ภาณุ ที่กรุณาให้คำแนะนำในการจัดทำสารนิพนธ์

ขอขอบพระคุณท่านผู้บริหารของบริษัท มายด์เทอร่า จำกัด ที่ให้ความสนับสนุนในการจัดทำสารนิพนธ์ และท้ายที่สุดขอกราบขอบพระคุณ เพื่อนร่วมงานและลูกค้าของบริษัททุกท่านที่กรุณาให้ข้อมูลรวมทั้งสนับสนุนในการทำสารนิพนธ์จนสำเร็จลงด้วยดี

ข้าพเจ้าหวังว่าสารนิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อผู้สนใจ สำหรับเป็นแนวทางในการจัดทำสารนิพนธ์ต่อไป

นรินทร์ แสงุร่ง

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญตาราง (ต่อ)

TNI
THAI - NICHI INSTITUTE OF TECHNOLOGY

สารบัญรูป

สถาบันเทคโนโลยีไทย-ญี่ปุ่น THAI - NICHI INSTITUTE OF TECHNOLOGY TNI

บทที่ 1
บทนำ

ที่มาและความสำคัญของปัญหา

ปัจจุบันประเทศไทยมีการพัฒนาเทคโนโลยีสารสนเทศมาใช้เพื่อเพิ่มความสะดวกในการทำงานที่มีการติดต่อสื่อสารผ่านระบบเครือข่ายที่มีความเร็วสูง แต่จากเทคโนโลยีที่มีการพัฒนาและเพิ่มขึ้นอย่างต่อเนื่อง ทำให้เป็นการเพิ่มช่องทางในการโจมตีของผู้ไม่ประสงค์ดีหรือ Hacker ที่มีวัตถุประสงค์ในการล้วงข้อมูลหรือสร้างความเสียหายแก่ระบบขององค์กร ทำให้บุคลากรในสายงานคอมพิวเตอร์ต้องหันมาเน้นในเรื่องของความปลอดภัยบนระบบสารสนเทศมากยิ่งขึ้น โดยมีการแบ่งสายงานแยกออกต่างหาก ซึ่งเราเรียกบุคลากรกลุ่มนี้ว่า บุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ (Information Security Engineer) ทำให้ผู้ศึกษาสนใจจะการศึกษาองค์ประกอบของสมรรถนะและแนวโน้มความต้องการของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กรของผู้ศึกษาเอง เพื่อนำไปใช้ในการพัฒนารวมถึงศึกษาหาแนวโน้มความต้องการบุคลากรในด้านนี้ขององค์กร

ในองค์กรของผู้ศึกษาที่ใช้กรณีศึกษาเป็นบริษัทผู้ให้บริการทางด้านความปลอดภัยบนระบบสารสนเทศ ซึ่งให้บริการและออกแบบความปลอดภัยให้กับหน่วยงานภาครัฐและเอกชน รวมถึงเป็นที่ปรึกษาด้านความมั่นคงปลอดภัยของข้อมูลด้วย

วัตถุประสงค์การศึกษา

1. ต้องการศึกษาองค์ประกอบของสมรรถนะ (Competency) ของระดับความรู้ความสามารถของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กร
2. ต้องการทราบแนวโน้มความต้องการบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ขององค์กร

ขอบเขตการศึกษา

<u>ประชากร</u>

ประชากรที่ใช้ในการศึกษาองค์ประกอบของสมรรถนะของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ของบุคลากรทางด้านคอมพิวเตอร์ครั้งนี้ คือ บุคลากรด้าน IT ของสถานประกอบที่เป็นลูกค้าของบริษัทที่ผู้ศึกษานั้นสังกัดอยู่ โดยสถานประกอบการของลูกค้าของบริษัททั้งหมดนั้นตั้งอยู่ในเขตกรุงเทพมหานคร

กลุ่มตัวอย่าง

การศึกษาครั้งนี้ เลือกกลุ่มตัวอย่างด้วยวิธีการเลือกกลุ่มตัวอย่างแบบสุ่มจากสถานประกอบการของลูกค้า โดยกลุ่มตัวอย่างนี้ประกอบไปด้วยบุคลากรทางด้านคอมพิวเตอร์โดยจำนวนสถานประกอบการที่จะทำการสุ่มนั้นใช้ Student Distribution (Sample $\geq$ 30) โดยใน 1 สถานประกอบการจะทำการสุ่มบุคลากรด้านคอมพิวเตอร์มา 2 คน ซึ่งประกอบด้วยกลุ่มผู้บริหารที่ทำงานเกี่ยวข้องกับคอมพิวเตอร์โดยตรง และกลุ่มหัวหน้างานหรือผู้เชี่ยวชาญด้าน IT ในองค์กร

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล

ใช้แบบสอบถาม (Questionnaires) ที่สร้างขึ้นโดยอาศัยทฤษฎี เอกสารทางวิชาการ มีลักษณะปลายปิดและเปิด ซึ่งคำถามจะแบ่งเป็น 3 ส่วน คือ

1. ข้อมูลสถานะผู้ให้ข้อมูลสำคัญและสถานประกอบการธุรกิจ
2. ข้อมูลความรู้ (Knowledge) และทักษะ (Skill) ของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ที่ใช้เป็นกรณีศึกษา
3. ข้อมูลแนวโน้มความต้องการบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ขององค์กรที่ใช้เป็นกรณีศึกษา

การวิเคราะห์ข้อมูล

1. ใช้โปรแกรมคอมพิวเตอร์ทางสถิติวิเคราะห์ข้อมูล (Statistical Package for Social Science)
2. สถิติที่ใช้ในการศึกษา โดยใช้สถิติเชิงพรรณนา (Descriptive Statistics) ใช้ในการอธิบายลักษณะต่างๆ ของข้อมูลที่เก็บรวบรวมจากกลุ่มตัวอย่าง เช่น ค่าเฉลี่ย (Average) ค่าร้อยละ (Percentiles) แจกแจงความถี่ (Frequency)

ประโยชน์ที่คาดว่าจะได้รับ

สำหรับประโยชน์ที่คาดว่าจะได้รับจะเป็นประโยชน์ต่อองค์กรภาคธุรกิจซึ่งมีดังนี้

1. องค์กรของผู้ศึกษาได้ทราบถึงความต้องการสมรรถนะของบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ที่ลูกค้าต้องการ
2. องค์กรของผู้ศึกษาได้ทราบถึงความสามารถหลัก (Core Competency) และความสามารถเฉพาะ (Functional Competency) ของบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์

3. องค์กรของผู้ศึกษาได้ทราบแนวโน้มความต้องการบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์

แผนและระยะเวลาในการดำเนินงาน

ตารางที่1 แผนงานและระยะเวลาการดำเนินงาน

ลำดับ	ขั้นตอนการดำเนินการ	ระยะเวลา (เดือน)									
		1	2	3	4	5	6	7	8	9	10
1	ศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง	■	■	■	■						
2	สร้างสมรรถนะที่เกี่ยวข้อง		■	■	■						
3	เก็บข้อมูลปฐมภูมิ				■	■					
4	วิเคราะห์ผล					■	■	■	■		
5	สรุปผลการศึกษา								■	■	
6	จัดทำรูปเล่มสารนิพนธ์									■	■

บทที่ 2
หลักการพื้นฐาน เอกสาร และงานวิจัยที่เกี่ยวข้อง

หลักการพื้นฐาน

การศึกษาองค์ประกอบของสมรรถนะของบุคคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กรเป็นกรณีศึกษา ผู้ศึกษาได้มีการรวบรวมเอกสารและงานวิจัยที่เกี่ยวข้อง โดยอาศัยแนวคิดและทฤษฎีเกี่ยวกับการปฏิบัติงานของบุคลากรทางด้านคอมพิวเตอร์ในสายงานด้านความปลอดภัยบนระบบสารสนเทศ และสมรรถนะตามความหมายต่างๆ จากเอกสารทางวิชาการ และผลงานการวิจัยที่เกี่ยวข้องตามลำดับต่อไปนี้

1. ความเป็นมาของสมรรถนะ
2. แนวคิดที่เกี่ยวข้องกับความหมายของสมรรถนะในประเทศไทย
3. การประยุกต์ใช้ระบบสมรรถนะในต่างประเทศ
4. ความหมาย, องค์ประกอบ, ประเภทและการกำหนดของสมรรถนะ
5. การนำ Competency ไปประยุกต์ใช้
6. เอกสารและงานวิจัยที่เกี่ยวข้อง

ความเป็นมาของสมรรถนะ

จุดกำเนิดของสมรรถนะหรือ Competency เกิดขึ้นในปี ค.ศ. 1970 เมื่อบริษัท McBer ได้รับการติดต่อจาก The US State Department ให้ช่วยเหลือเกี่ยวกับการคัดเลือก Foreign Service Information Officer (FSIOs) หรือ เจ้าหน้าที่ที่ทำหน้าที่เป็นตัวแทนของประเทศสหรัฐอเมริกาในประเทศต่างๆ ทั่วโลก มีหน้าที่เผยแพร่วัฒนธรรมและเรื่องราวของประเทศสหรัฐอเมริกาให้กับคนในประเทศเหล่านั้น ซึ่งในขณะนั้นแทบทั้งหมดของเจ้าหน้าที่เหล่านี้ “เป็นคนผิวขาว” ก่อนหน้านั้น The US State Department คัดเลือกเจ้าหน้าที่ FSIOs ด้วยการใช้แบบทดสอบที่เรียกว่า Foreign Service Officer Exam ซึ่งเป็นแบบทดสอบที่มุ่งทดสอบด้านทักษะ (Skill) ที่เจ้าหน้าที่ระดับสูง (Senior Office) ของหน่วยงานนี้ คิดว่าจำเป็นสำหรับการปฏิบัติงานในตำแหน่งนี้ แต่แบบทดสอบดังกล่าวนี้มีจุดอ่อน คือ

1. เป็นการวัดผลเรื่องวัฒนธรรมของชนชั้นกลางและสูง และยังใช้เกณฑ์ที่สูงมากในการวัดผล ทำให้ชนกลุ่มน้อยในประเทศ (Minority) หรือคนผิวดำไม่มีโอกาสที่จะสอบผ่าน ซึ่งสะท้อนให้เห็นว่า การคัดเลือกพนักงานของหน่วยงานนี้ มีลักษณะของ “การเลือกปฏิบัติ”
2. มีการค้นพบภายหลังว่าคะแนนสอบไม่สัมพันธ์กับผลการปฏิบัติงาน กล่าวคือ ผู้ที่ทำคะแนนสอบได้ดี กลับไม่ได้มีผลการปฏิบัติงานที่ดีตามที่องค์การคาดหวังเสมอไป The US

State Department จึงได้ว่าจ้าง บริษัท McBer ภายใต้การนำของ เดวิด ซี แมคคลีแลนด์ (David, C. McClelland) ให้เข้ามาช่วยแก้ไขปัญหา ดังกล่าวข้างต้น สิ่งที่ เดวิด ซี แมคคลีแลนด์ ได้รับมอบหมายให้ทำ คือ การหาเครื่องมือชนิดใหม่ที่ดีกว่า และสามารถทำนายผลการปฏิบัติงานของเจ้าหน้าที่ FSIOs ได้อย่างแม่นยำแทนแบบทดสอบเก่า ดังนั้น เดวิด ซี แมคคลีแลนด์ จึงเริ่มต้นด้วยกระบวนการดังต่อไปนี้

2.1 ทำการเปรียบเทียบเจ้าหน้าที่ FSIOs ที่มีผลการปฏิบัติงานดี (Superior Performer) กับเจ้าหน้าที่ที่มีผลการปฏิบัติงานตามเกณฑ์เฉลี่ย (Average Performer)

2.2 สร้างเทคนิคการประเมินแบบใหม่ที่เรียกว่า Behavioral Event Interview (BEI) ซึ่งเป็นเทคนิคที่ให้ผู้ทำแบบทดสอบ ตอบคำถาม เกี่ยวกับความสำเร็จสูงสุด 3 เรื่อง และความล้มเหลวสูงสุด 3 เรื่อง เพื่อนำไปสู่สิ่งที่ เดวิด ซี แมคคลีแลนด์ ต้องการค้นหา คือ ผู้ที่มีผลการปฏิบัติงานดี (Superior Performer) มีลักษณะพฤติกรรมอย่างไร

3. วิเคราะห์คะแนนสอบที่ได้จากการทำแบบทดสอบ BEI ของเจ้าหน้าที่ที่มีผลการปฏิบัติงานดี (Superior Performer) และผู้ที่มีผลการปฏิบัติงานตามเกณฑ์เฉลี่ย (Average Performer) เพื่อค้นหาลักษณะของพฤติกรรมที่แตกต่างกันของคน 2 กลุ่มนี้ ซึ่งลักษณะของพฤติกรรมที่ก่อให้เกิดผลการปฏิบัติงานที่ดีหรือ Superior Performance นี้ เดวิด ซี แมคคลีแลนด์ เรียกว่า Competency

เดวิด ซี แมคคลีแลนด์ ได้แสดงแนวคิดของเขาในเรื่อง Competency ไว้ในบทความชื่อ Testing for Competence Rather Than Intelligence ว่า “IQ (ประกอบด้วยความถนัด หรือความเชี่ยวชาญทางวิชาการความรู้และความมุ่งมั่นสู่ความสำเร็จ) ไม่ใช่ตัวชี้วัดที่ดีของผลงานและความสำเร็จโดยรวม แต่ Competency กลับเป็นสิ่งที่สามารถคาดหมาย ความสำเร็จ ในงานได้ดีกว่า” ซึ่งสะท้อนให้เห็นได้อย่างชัดเจนว่า “ผู้ที่ทำงานเก่ง” มิได้หมายถึง “ผู้ที่เรียนเก่ง” แต่ผู้ที่ประสบผลสำเร็จในการทำงานต้องเป็นผู้ที่มีความสามารถในการประยุกต์ใช้หลักการ หรือวิชาการที่มีอยู่ในตัวเองนั้น ก่อให้เกิดประโยชน์ในงานที่ตนทำ จึงจะกล่าวได้ว่า บุคคลผู้นั้นมี Competency จากจุดกำเนิด Competency ดังกล่าวข้างต้นนี้ ทำให้นักการศึกษาและนักวิชาการหลายสำนักได้นำวิธีการของเดวิด ซี แมคคลีแลนด์ มาเป็นแนวทางในการศึกษาเรื่อง Competency ในเวลาต่อมา

แนวคิดที่เกี่ยวข้องกับความหมายของสมรรถนะในประเทศไทย

ในแวดวงการศึกษาและการบริหารของไทย ได้กล่าวถึง คำว่าสมรรถนะไว้นานมาแล้ว กมล สุดประเสริฐ ; และคณะ (อุบลรัตน์ จันทร์เมือง. 2555 ; อ้างอิงจาก กมล สุดประเสริฐ ; และคณะ. 2526) เคยอธิบายไว้ว่า สมรรถนะเป็นคุณสมบัติของคนที่เป็นผลมาจากความรู้ ความเข้าใจ ทักษะ เจตคติ และอุปนิสัยหรือบุคลิกภาพ ซึ่งเป็นผลทำให้เกิดความสามารถในการกระทำพฤติกรรมต่างๆ ที่พึงประสงค์ได้ ซึ่งจะเห็นได้ว่า ไม่แตกต่างจาก

มุมมองเรื่องสมรรถนะในปัจจุบันมากนัก เช่น ณรงค์วิทย์ แสนทอง (2547) นักฝึกอบรมมืออาชีพของไทยที่ได้เสนอว่า สมรรถนะสามารถพิจารณาความหมายออกได้เป็น 2 กลุ่ม คือ กลุ่มแรกมองว่าสมรรถนะเป็นบุคลิกลักษณะของคนที่สะท้อนให้เห็นถึงความรู้ (Knowledge) ทักษะ (Skills) ทัศนคติ (Attitude) ความเชื่อ (Belief) และอุปนิสัย (Trait) และอีกกลุ่มหนึ่งมองว่าเป็นกลุ่มของความรู้ (Knowledge) ทักษะ (Skills) และคุณลักษณะของบุคคล (Attributes) หรือเรียกกันว่า KSAs ซึ่งสะท้อนให้เห็นจากพฤติกรรมในการทำงานที่แสดงออกมาของแต่ละบุคคลที่สามารถวัดและสังเกตเห็นได้

ขณะที่ อาภรณ์ ภู่วิทยพันธุ์ (2547) อธิบายไว้ว่า สมรรถนะ (Competency) เป็นตัวที่กำหนดรายละเอียดของพฤติกรรมการแสดงออก เป็นการตอบคำถามว่า “ทำอย่างไรที่จะทำให้งานที่ได้รับมอบหมายประสบผลสำเร็จ (How)” มากกว่าการตอบคำถามว่า “อะไรเป็นสิ่งที่หัวหน้างานคาดหวังหรือต้องการ (What)” ทั้งนี้การกำหนดความสามารถหรือ Competency นั้นจะแบ่งออกเป็น 3 มุมมอง ได้แก่ KSA ซึ่งมีความหมายที่แตกต่างกันไป กล่าวคือ

(1) ความรู้ (Knowledge) หมายถึง ข้อมูล หรือสิ่งที่ถูกสั่งสมมาจากการศึกษาทั้งในสถาบันการศึกษา สถาบันฝึกอบรม/สัมมนา หรือการศึกษาด้วยตนเอง รวมถึงข้อมูลที่ได้รับจากการสนทนาแลกเปลี่ยนความคิดเห็น และประสบการณ์กับผู้รู้ทั้งในสายวิชาชีพเดียวกัน และต่างสายวิชาชีพ

(2) ทักษะ (Skills) หมายถึง สิ่งที่จะต้องพัฒนาและฝึกฝนให้เกิดขึ้นโดยจะต้องใช้ระยะเวลาเพื่อฝึกปฏิบัติให้เกิดทักษะนั้นขึ้นมา ทั้งนี้ทักษะจะถูกแบ่งออกเป็น 2 ด้าน ได้แก่ ทักษะด้านการบริหาร/จัดการงาน (Management Skills) หรือทักษะในการบริหารควบคุมงาน ซึ่งจะเกี่ยวข้องกับระบบความคิดและการจัดการในการบริหารงานให้มีประสิทธิภาพ เช่น ทักษะในการมีวิสัยทัศน์ทางกลยุทธ์ ซึ่งทักษะดังกล่าวจะแสดงออกถึงการจัดระบบความคิดเพื่อมองไปที่เป้าหมายในอนาคตว่าอยากจะทำ หรือมีความต้องการอะไรในอนาคต และทักษะด้านเทคนิคเฉพาะงาน (Technical Skills) ซึ่งหมายถึง ทักษะที่จำเป็นในการทำงานตามสายงานหรือกลุ่มงานที่แตกต่างกันไป เช่น งานจัดซื้อจะมีหน้าที่ความรับผิดชอบ และลักษณะงานที่แตกต่างไปจากงานผลิต ดังนั้นทักษะที่ต้องการของคนที่ทำงานด้านจัดซื้อได้นั้น จะต้องแตกต่างไปจากงานผลิตเช่นเดียวกัน

(3) คุณลักษณะส่วนบุคคล (Attributes) หมายถึง ความคิด ความรู้สึก เจตคติ ทัศนคติ แรงจูงใจ ความต้องการส่วนบุคคล พบว่า คุณลักษณะส่วนบุคคลนั้นจะเป็นสิ่งที่ติดตัวมา และไม่ค่อยจะเปลี่ยนแปลงไปตามกาลเวลาที่เปลี่ยนไป

ธำรงศักดิ์ คงคาสวัสดิ์ (2548) ได้อธิบายความหมายของสมรรถนะ (Competency) ว่าหมายถึง คุณลักษณะ เช่น ความรู้ ความสามารถ ความชำนาญ ทักษะ ทัศนคติ ความเชื่อ ตลอดจนพฤติกรรมของบุคคลที่จะสามารถปฏิบัติงานให้ประสบความสำเร็จ ขณะที่ รัตนาภรณ์ ศรีพยัคฆ์ (2548) อธิบายว่าสมรรถนะ (Competency) มีความหมายตามพจนานุกรมว่า

ความสามารถ หรือสมรรถนะ ในภาษาอังกฤษมีคำที่มีความหมายคล้ายกันอยู่หลายคำ ได้แก่ Capability, Ability, Proficiency, Expertise, Skill, Fitness, Aptitude โดยสำนักงานคณะกรรมการข้าราชการพลเรือนใช้ภาษาไทยว่า “สมรรถนะ” แต่ในบางองค์กรใช้คำว่า “ความสามารถ” สำหรับ สุกัญญา รัศมีธรรมโชติ (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก สุกัญญา รัศมีธรรมโชติ. 2548) ได้สรุปความหมายของสมรรถนะ (Competency) คือ ความรู้ (Knowledge) ทักษะ (Skills) และคุณลักษณะส่วนบุคคล (Personal Characteristic or Attributes) ที่ทำให้บุคคลนั้นทำงานในความรับผิดชอบของตนได้ดีกว่าผู้อื่น ขณะที่แสงสุรีย์ ทัศนพูนชัย (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก แสงสุรีย์ ทัศนพูนชัย. 2548) ได้ให้คำจำกัดความว่า ความสามารถหรือศักยภาพ หรือสมรรถนะ เป็นคำที่เราคุ้นเคยมานานมีความหมายตรงกับภาษาอังกฤษว่า Competency หมายถึง บุคลิกลักษณะของคนที่สะท้อนให้เห็นถึงความรู้ ทักษะ ทัศนคติ ความเชื่อ และอุปนิสัยของแต่ละบุคคลสามารถวัดหรือสังเกตได้จากพฤติกรรมการทำงานที่แสดงออกมาให้เห็น ซึ่งอาจเกิดได้จากพรสวรรค์ที่มีติดตัวมาตั้งแต่เกิด หรือจากประสบการณ์การทำงาน หรือจากการศึกษาฝึกอบรม ความหมายดังกล่าวนี้ คล้ายกับ ปิยะชัย จันทรวงศ์ไพศาล (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก ปิยะชัย จันทรวงศ์ไพศาล. 2549 : 12) โดยเป็นทักษะ ความรู้ และความสามารถทำงานให้บรรลุตามวัตถุประสงค์และเป้าหมายของงาน

การประยุกต์ใช้ระบบสมรรถนะในต่างประเทศ

แนวคิดเรื่องสมรรถนะของเดวิด ซี แมคคลีแลนด์ ดังกล่าว ได้รับการโต้แย้งจากนักวิชาการด้านจิตวิทยาอุตสาหกรรมจำนวนหนึ่ง เช่น แบเร็ตต์ จี วี ; และ เดพิเน็ต อาร์ แอล (Barrett, G. V. ; and Depinet, R. L. 1991) ในบทความเรื่อง “Reconsideration of Testing for Competence” ซึ่งให้ความเห็นเชิงโต้แย้งกับบทความของเดวิด ซี แมคคลีแลนด์ เรื่อง “Testing for Competence rather than Intelligence” ที่ตีพิมพ์ในปี ค.ศ.1973 โดยนำเสนอทัศนคติด้านลบต่อการวัดความฉลาดทางเชาว์ปัญญาในการทำนายความสำเร็จในการทำงานและมีผลการทำนายที่ด้อยกว่าการวัดสมรรถนะที่เขาได้เสนอไว้ ซึ่งแบเร็ตต์ จี วี ; และ เดพิเน็ต อาร์ แอล ได้ทำการศึกษาวิจัย พบว่า ความสามารถทางเชาว์ปัญญานั้น มีผลต่อความสำเร็จในการทำงาน ในขณะที่ยังไม่มีหลักฐานเชิงประจักษ์ที่บ่งบอกอย่างเด่นชัดว่าสมรรถนะในการทำงานสามารถทำนายผลการปฏิบัติงานได้ และในปัจจุบันนี้ แวดวงวิชาการจิตวิทยาอุตสาหกรรมต่างยอมรับกันว่า ความสามารถทั่วไป (General Cognitive Ability) หรืออาจเรียกอย่างง่ายว่า ความฉลาด สามารถทำนายผลการปฏิบัติงานที่ซับซ้อนได้ดีกว่าการวัดโดยใช้แนวคิดเรื่องสมรรถนะ (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก Hunter ; and Hunter. 1984)

ในทัศนะของสเปนเซอร์ เอ็ม ; และ สเปนเซอร์ เอ็ม เอส (Spencer, M. ; and Spencer, M. S. 1993 : 9-11) สมรรถนะเป็นลักษณะเฉพาะของแต่ละบุคคล (Underlying Characteristic) ที่มีความสัมพันธ์เชิงเหตุและผล (Causal Relationship) จากความมีประสิทธิผลของเกณฑ์ที่ใช้ (Criterion-Reference) และ/หรือการปฏิบัติงานที่ได้ผลสูงสุด (Superior Performance) สมรรถนะในความหมายของสเปนเซอร์ เอ็ม ; และ สเปนเซอร์ เอ็ม เอส นี้ นับได้ว่าไม่แตกต่างไปจากงานของแมคคลีแลนด์โดยมองว่า สมรรถนะมีองค์ประกอบที่สำคัญ 5 ประการ คือ แรงขับ (Motives) คุณลักษณะ (Traits) การรับรู้ตนเอง (Self-Concept) ความรู้ (Knowledge) และทักษะ (Skills) ซึ่งผู้ศึกษาจะขยายรายละเอียดต่อไปในหัวข้อองค์ประกอบของสมรรถนะ

เดล เอ็ม ; และ เฮส เค (Dales, M. ; and Hes, K. 1995 : 80) ได้กล่าวว่า สมรรถนะเป็นการค้นหาสิ่งที่ทำให้เกิดการปฏิบัติงานที่ดีเลิศ (Excellence) หรือการปฏิบัติงานที่เหนือกว่า (Superior Performance) นอกจากนี้ ได้ให้ความหมายสมรรถนะในด้านอาชีพ (Occupational Competence) ว่าหมายถึง ความสามารถ (Ability) ในการทำกิจกรรมต่างๆ ในสายอาชีพเพื่อให้เกิดการปฏิบัติงานเป็นไปตามมาตรฐานที่ถูกคาดหวังไว้ คำว่ามาตรฐาน ในที่นี้คือ องค์ประกอบของความสามารถ (Element of Competence) บวกกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และคำอธิบายขอบเขตงาน (Range Statement) ส่วนนาเกลสมิธ (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก Nagelsmith. 1995) ได้กล่าวถึงสมรรถนะว่า เป็นความสามารถที่จะปฏิบัติกิจกรรมเฉพาะได้ตามเกณฑ์มาตรฐาน โดยมีทักษะ ความรู้ ค่านิยม การคิด และเจตคติ เป็นปัจจัยที่สัมพันธ์กับสมรรถนะสอดคล้องกับแนวคิดของแคทซ์ ; และ กรีน (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก Katz ; and Green. 1992) ซึ่งกล่าวว่า สมรรถนะ หมายถึง ความสามารถในการกระทำสิ่งใดสิ่งหนึ่งที่ระดับความชำนาญ รวมทั้งความรู้ ทักษะ เจตคติ และค่านิยม

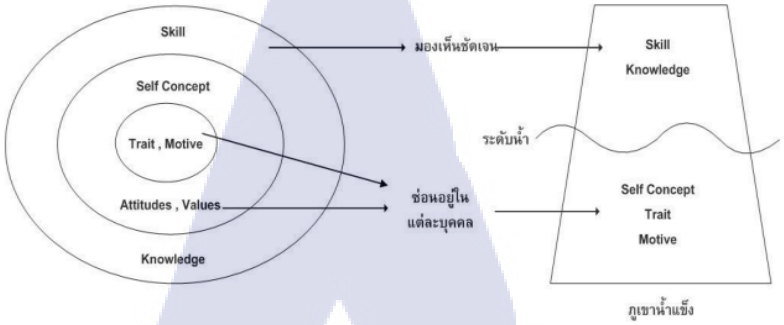
แพร์รี่ (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก Parry. 1998) กล่าวว่า ในการปฏิบัติงานในองค์กรนั้น สมรรถนะมีความเกี่ยวข้องและสัมพันธ์ระหว่างงาน (Work) ผลลัพธ์ (Results) ผลที่ได้จากการทำงาน (Outputs) กับคุณลักษณะของความรู้ (Knowledge) ทักษะ (Skill) และทัศนคติ (Attitude) ในการทำงาน ซึ่งสามารถแสดงออกได้หลายลักษณะด้วยกัน มุมมองที่เกี่ยวกับสมรรถนะอาจจะมีหลากหลายตามค่ายของแนวคิด เช่น ประเทศสหรัฐอเมริกาจะมองสมรรถนะว่า เป็นเสมือนปัจจัยนำเข้า (Input) ที่ได้จากการปฏิบัติงานอันเกิดจากเงื่อนไขที่งานกำหนดขึ้น นอกจากนี้ การกำหนดขอบเขตของสมรรถนะในแต่ละงานจะแตกต่างกันออกไป บางครั้งได้รวมบุคลิกลักษณะ ค่านิยม และรูปแบบบางอย่างไว้ด้วยกันพร้อมกับได้ให้นิยามของสมรรถนะว่าคือ กลุ่มของความรู้ (Knowledge) ทักษะ (Skills) และคุณลักษณะ (Attributes) ที่เกี่ยวข้องกันซึ่งมีผลกระทบต่องานหลักของตำแหน่งงานหนึ่งๆ โดยที่กลุ่มความรู้ ทักษะ และคุณลักษณะดังกล่าวสัมพันธ์กับผลงานของตำแหน่งงาน

นั้นๆ และสามารถวัดผลเปรียบเทียบกับมาตรฐานที่เป็นที่ยอมรับ และเป็นสิ่งที่สามารถเสริมสร้างขึ้นได้โดยการผ่านการฝึกอบรมและการพัฒนา ส่วนเคลมพ์ (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก Klemp. 1999) ผู้เชี่ยวชาญด้านทรัพยากรมนุษย์ได้ให้ความหมายของ สมรรถนะ คือ บุคลิกลักษณะที่อยู่ภายในบุคคลซึ่งมีผลต่อความมีประสิทธิผลหรือผลการทำงานที่เป็นเลิศ นักวิชาการที่ได้เสนอคำอธิบายความหมายของสมรรถนะเช่นเดียวกันอีก ได้แก่ ไรแลท ; และ โลฮาน (Rulatt ; and Lohan) อัลเฮย์ ; และ ออธ (Alhey ; and Orth) และ ชูนโนเวอร์ (Schoonover) (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554)

วิดด์เดทท์ ; และ ฮอลลี่ฟอร์ด (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก Whiddett ; and Hollyforde. 2003) กล่าวว่า สมรรถนะเป็นพฤติกรรมซึ่งบุคคลแสดงออกเมื่อได้ปฏิบัติงานที่เกี่ยวข้องกับคุณลักษณะที่ตนมี และทำให้เกิดผลงานที่มีประสิทธิภาพต่อองค์กร ส่วน อาร์โนลด์ เดอ นาเดลแลค (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก Arnauld de Nadaillac. 2003) สมรรถนะนั้นเป็นสิ่งที่ต้องลงมือปฏิบัติและทำให้เกิดขึ้น กล่าวคือ ความสามารถที่ใช้เพื่อให้เกิดการบรรลุผลและวัตถุประสงค์ต่างๆ ซึ่งเป็นตัว ขับเคลื่อนที่ทำให้เกิดความรู้ (Knowledge) การเรียนรู้ทักษะ (Know-How) และเจตคติ/ลักษณะนิสัยหรือบุคลิกภาพต่างๆ (Attitude) ที่ช่วยให้สามารถเผชิญและแก้ไขสถานการณ์หรือปัญหาต่างๆ ที่เกิดขึ้นได้จริง สำหรับ เดวิด ดี ดูโบอิส ; และ วิลเลียม เจ รอธเวลล์ (สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). 2554 ; อ้างอิงจาก David, D. Dubois ; and William, J. Rothwell. 2004) ได้เสนอไว้ว่า สมรรถนะเป็นคุณลักษณะที่ทุกคนมีและใช้ได้อย่างเหมาะสม เพื่อผลักดันให้ผลการปฏิบัติงานบรรลุตามเป้าหมาย ซึ่งคุณลักษณะเหล่านี้ ได้แก่ ความรู้ ทักษะ บุคลิกภาพ แรงจูงใจทางสังคม ลักษณะนิสัยส่วนบุคคล ตลอดจนรูปแบบความคิดและวิธีการคิด ความรู้สึกและการกระทำ

ความหมายของสมรรถนะ

แนวคิดเกี่ยวกับสมรรถนะเริ่มจากการนำเสนอบทความทางวิชาการของ เดวิด ซี แมคคลีแลนด์ (David, C. McClelland) นักจิตวิทยาแห่งมหาวิทยาลัยฮาววาร์ดเมื่อปี ค.ศ. 1960 ซึ่งกล่าวถึง ความสัมพันธ์ระหว่างคุณลักษณะที่ดีของบุคคล (Excellent Performer) ในองค์การกับระดับทักษะความรู้ ความสามารถ โดยกล่าวว่า การวัด IQ และการทดสอบบุคลิกภาพยังไม่เหมาะสมในการทำนายความสามารถหรือสมรรถนะของบุคคลได้ เพราะไม่ได้สะท้อนความสามารถที่แท้จริงออกมาได้



รูปที่ 1 ความหมายของสมรรถนะตามแนวคิดของ David, C. McClelland

ในปี ค.ศ. 1970 US State Department ได้ติดต่อบริษัท McBer ซึ่งเดวิด ซี แมคคลีแลนด์ เป็นผู้บริหารอยู่ เพื่อให้หาเครื่องมือชนิดใหม่ที่สามารถทำนายผลการปฏิบัติงานของเจ้าหน้าที่ได้อย่างแม่นยำแทนแบบทดสอบเก่า ซึ่งไม่สัมพันธ์กับผลการปฏิบัติงาน เนื่องจากคนได้คะแนนดีแต่ปฏิบัติงานไม่ประสบผลสำเร็จ จึงต้องเปลี่ยนแปลงวิธีการใหม่ เดวิด ซี แมคคลีแลนด์ ได้เผยแพร่แนวคิดและสร้างแบบประเมินแบบใหม่ที่เรียกว่า Behavioral Event Interview (BEI) เป็นเครื่องมือประเมินที่ค้นหาผู้ที่มีผลการปฏิบัติงานดี ซึ่งเดวิด ซี แมคคลีแลนด์ เรียกว่า สมรรถนะ (Competency)

โบยาตซิส อาร์ อี (Boyatizis, R. E. 1982) ได้นิยามคำว่า Competencies เป็นความสามารถในงานหรือเป็นคุณลักษณะที่อยู่ภายในบุคคลที่นำไปสู่การปฏิบัติงานให้เกิดประสิทธิภาพ

แกรี่ แฮเมล ; และ ซี เค พราฮาราด (Gary, Hamel ; and C. K. Prahalad. 1994) ได้นำเสนอแนวคิดที่สำคัญ คือ Core Competencies เป็นความสามารถหลักของธุรกิจ ซึ่งถือว่าในการประกอบธุรกิจนั้นจะต้องมีเนื้อหาสาระหลัก เช่น พื้นฐานความรู้ ทักษะ และความสามารถในการทำงานอะไรได้บ้าง และอยู่ในระดับใด จึงทำงานได้มีประสิทธิภาพสูงสุดตรงตามความต้องการขององค์การ

ในปัจจุบันองค์การของเอกชนชั้นนำได้นำแนวคิดสมรรถนะไปใช้เป็นเครื่องมือในการบริหารงานมากขึ้น และยอมรับว่าเป็นเครื่องมือสมัยใหม่ที่องค์การต้องได้รับความพึงพอใจอยู่ในระดับต้นๆ มีการสำรวจ พบว่า มี 708 บริษัททั่วโลก นำ Core Competency เป็น 1 ใน 25 เครื่องมือที่ได้รับความนิยมเป็นอันดับ 3 รองจาก Coporate Code of Ethics และ Strategic Planning (พสุ เดชะรินทร์. 2546 : 13) แสดงว่า Core Competency จะมีบทบาทสำคัญที่จะเข้าไปช่วยให้งานบริหารประสบความสำเร็จ จึงมีผู้สนใจศึกษาแนวคิดเกี่ยวกับการนำหลักการของสมรรถนะมาปรับให้เพิ่มมากขึ้น

หน่วยงานของรัฐและเอกชนของไทยหลายหน่วยงานได้ให้ความสนใจนำมาใช้ เช่น บริษัท ปูนซีเมนต์ไทย ปตท. และสำนักงานข้าราชการพลเรือน เป็นต้น

สำหรับความหมายของสมรรถนะมีการให้ความหมายไว้หลายอย่าง ดังจะยกตัวอย่างการให้ความหมายของนักวิชาการบางท่าน ดังนี้

สก็อต บี พารี (Scott, B. Parry) นิยามคำว่า สมรรถนะ คือ กลุ่มของความรู้ (Knowledge) ทักษะ (Skills) และคุณลักษณะ (Attributes) ที่เกี่ยวข้องกัน ซึ่งมีผลกระทบต่องานหลักของตำแหน่งงานหนึ่งๆ โดยกลุ่มความรู้ ทักษะ และคุณลักษณะดังกล่าวสัมพันธ์กับผลงานของตำแหน่งงานนั้นๆ และสามารถวัดผลเทียบกับมาตรฐานที่เป็นที่ยอมรับและเป็นสิ่งที่สามารถเสริมสร้างขึ้นได้ โดยผ่านการฝึกอบรมและการพัฒนา (สุกัญญา รัศมีธรรมโชติ. 2547 : 48)

เดวิด ซี แมคคลีแลนด์ กล่าวว่า สมรรถนะ คือ บุคลิกลักษณะที่ซ่อนอยู่ภายในปัจเจกบุคคล ซึ่งสามารถผลักดันให้ปัจเจกบุคคลนั้น สร้างผลการปฏิบัติงานที่ดี หรือตามเกณฑ์ที่กำหนดในงานที่ตนรับผิดชอบ

อานนท์ ศักดิ์รวิชญ์ (2547 : 61) ได้สรุปคำนิยามของสมรรถนะไว้ว่า สมรรถนะ คือ คุณลักษณะของบุคคล ซึ่งได้แก่ ความรู้ ทักษะ ความสามารถ และคุณสมบัติต่างๆ อันได้แก่ ค่านิยม จริยธรรม บุคลิกภาพ คุณลักษณะทางกายภาพ และอื่นๆ ซึ่งจำเป็นและสอดคล้องกับความเหมาะสมกับองค์การ โดยเฉพาะอย่างยิ่งต้องสามารถจำแนกได้ว่าผู้ที่จะประสบความสำเร็จในการทำงานได้ต้องมีคุณลักษณะเด่นๆ อะไร หรือลักษณะสำคัญๆ อะไรบ้าง หรือกล่าวอีกนัยหนึ่งคือ สาเหตุที่ทำงานแล้วไม่ประสบความสำเร็จเพราะขาดคุณลักษณะบางประการคืออะไร เป็นต้น

จากที่กล่าวข้างต้นสรุปได้ว่า สมรรถนะจึงเป็น ความรู้ ทักษะ และคุณลักษณะที่จำเป็นของบุคคลในการทำงานให้ประสบความสำเร็จ มีผลงานได้ตามเกณฑ์หรือมาตรฐานที่กำหนดหรือสูงกว่า

<u>องค์ประกอบของสมรรถนะ</u>

หลักตามแนวคิดของเดวิด ซี แมคคลีแลนด์ มี 5 ส่วน คือ

1. ความรู้ (Knowledge) คือ ความรู้เฉพาะในเรื่องที่ต้องรู้เป็นความรู้ที่เป็นสาระสำคัญ เช่น ความรู้ด้านเครื่องยนต์ เป็นต้น

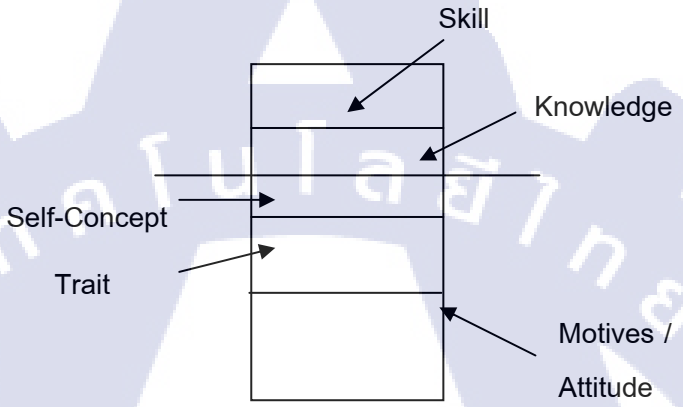
2. ทักษะ (Skill) คือ สิ่งที่ต้องการให้ทำได้อย่างมีประสิทธิภาพ เช่น ทักษะทางคอมพิวเตอร์ ทักษะทางการถ่ายทอดความรู้ เป็นต้น ทักษะที่เกิดได้นั้นมาจากพื้นฐานทางความรู้ และสามารถปฏิบัติได้อย่างแคล่วคล่องว่องไว

3. ความคิดเห็นเกี่ยวกับตนเอง (Self-Concept) คือ เจตคติ ค่านิยม และความคิดเห็นเกี่ยวกับภาพลักษณ์ของตน หรือสิ่งที่บุคคลเชื่อว่าตนเองเป็น เช่น ความมั่นใจในตนเอง เป็นต้น

4. บุคลิกลักษณะประจำตัวของบุคคล (Traits) เป็นสิ่งที่อธิบายถึงบุคคลนั้น เช่น คนที่น่าเชื่อถือและไว้วางใจได้ หรือมีลักษณะเป็นผู้นำ เป็นต้น

5. แรงจูงใจ/เจตคติ (Motives/Attitude) เป็นแรงจูงใจ หรือแรงขับภายใน ซึ่งทำให้บุคคลแสดงพฤติกรรมที่มุ่งไปสู่เป้าหมายหรือมุ่งสู่ความสำเร็จ เป็นต้น

ทั้ง 5 ส่วนดังกล่าวข้างต้นแสดงความสัมพันธ์ในเชิงอธิบายเปรียบเทียบดังภาพ

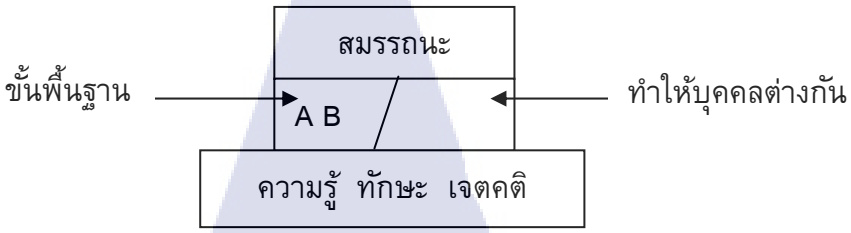


รูปที่ 2 Iceberg Model ของสมรรถนะ

จากรูปที่ 2 พบว่า Skill และ Knowledge อยู่ส่วนบน หมายถึงว่า ทั้ง Skill และ Knowledge สามารถพัฒนาขึ้นได้ไม่ยาก จะโดยวิธีการศึกษาค้นคว้า หรือประสบการณ์ตรงและมีการฝึกฝนจนเกิดความชำนาญ

จากแนวคิดของเดวิด ซี แมคคลีแลนด์นั้น สก็อต บี พารี เห็นควรจะรวมส่วนประกอบที่เป็นความคิดเกี่ยวกับตนเอง คุณลักษณะและแรงจูงใจเข้าเป็นกลุ่มเรียกว่า คุณลักษณะ (Attributes)

ดังนั้น บางครั้งเมื่อพูดถึงองค์ประกอบของสมรรถนะจึงมีเพียง 3 ส่วน คือ ความรู้ ทักษะ คุณลักษณะ ซึ่งตามทัศนะของเดวิด ซี แมคคลีแลนด์ กล่าวว่า สมรรถนะเป็นส่วนประกอบขึ้นมาจากความรู้ ทักษะ และเจตคติ/แรงจูงใจ หรือความรู้ ทักษะ และเจตคติ/แรงจูงใจก่อให้เกิดสมรรถนะ ดังรูปที่ 3 (สุกัญญา รัศมีธรรมโชติ. 2547 : 48)



รูปที่ 3 สมรรถนะเป็นส่วนประกอบที่เกิดขึ้นมาจากความรู้ ทักษะ เจตคติ

จากรูปที่ 3 ความรู้ ทักษะ และเจตคติไม่ใช่สมรรถนะแต่เป็นส่วนหนึ่งที่ทำให้เกิดสมรรถนะดังนั้นความรู้โดดๆ จะไม่เป็นสมรรถนะ แต่ถ้าเป็นความรู้ที่สามารถนำมาใช้ให้เกิดกิจกรรมจนประสบความสำเร็จ ถือว่าเป็นส่วนหนึ่งของสมรรถนะ สมรรถนะในที่นี้จึงหมายถึงพฤติกรรมที่ก่อให้เกิดผลงานสูงสุดนั้น ตัวอย่างเช่น ความรู้ในการขับรถถือว่าเป็นความรู้ แต่ถ้านำความรู้มาทำหน้าที่เป็นผู้สอนขับรถและมีรายได้จากส่วนนี้ ถือว่าเป็นสมรรถนะ

ในทำนองเดียวกันความสามารถในการก่อสร้างบ้านถือว่าเป็นทักษะ แต่ความสามารถในการสร้างบ้านและนำเสนอให้เกิดความแตกต่างจากคู่แข่งได้ถือว่าเป็นสมรรถนะ

หรือในกรณีเจตคติ/แรงจูงใจก็เช่นเดียวกันก็ไม่ใช่สมรรถนะ แต่สิ่งจูงใจให้เกิดพลังทำงานสำเร็จตรงตามเวลาหรือเรียกว่ากำหนด หรือดีกว่ามาตรฐานถือว่าเป็นสมรรถนะ

สมรรถนะตามนัยดังกล่าวข้างต้น สามารถแบ่งออกได้เป็น 2 กลุ่ม คือ

1. สมรรถนะขั้นพื้นฐาน (Threshold Competencies) หมายถึง ความรู้ หรือ ทักษะพื้นฐานที่จำเป็นของบุคคลที่ต้องมีเพื่อให้สามารถที่จะทำงานที่สูงกว่า หรือซับซ้อนกว่าได้ เช่น สมรรถนะในการพูด การเขียน เป็นต้น

2. สมรรถนะที่ทำให้เกิดความแตกต่าง (Differentiating Competencies) หมายถึงปัจจัยที่ทำให้บุคคลมีผลการทำงานที่ดีกว่าหรือสูงกว่ามาตรฐานสูงกว่าคนทั่วไป จึงทำให้เกิดผลสำเร็จที่แตกต่างกัน

<u>ประเภทของสมรรถนะ</u>

สมรรถนะสามารถจำแนกได้เป็น 5 ประเภท คือ

1. สมรรถนะส่วนบุคคล (Personal Competencies)

หมายถึง สมรรถนะที่แต่ละคนมีเป็นความสามารถเฉพาะตัว คนอื่นไม่สามารถลอกเลียนแบบได้ เช่น การต่อสู้ป้องกันตัวของจา พนม นักแสดงชื่อดังในหนังเรื่อง “ต้มยำกุ้ง” ความสามารถของนักดนตรี นักกายกรรม และนักกีฬา เป็นต้น ลักษณะเหล่านี้ยากที่จะเลียนแบบหรือต้องมีความพยายามสูงมาก

2. สมรรถนะเฉพาะงาน (Job Competencies)

หมายถึง สมรรถนะของบุคคลกับการทำงานในตำแหน่งหรือบทบาทเฉพาะตัว เช่น อาชีพนักสำรวจก็ต้องมีความสามารถในการวิเคราะห์ตัวเลข การคิดคำนวณ ความสามารถในการทำบัญชี เป็นต้น

3. สมรรถนะองค์การ (Organization Competencies)

หมายถึง ความสามารถพิเศษเฉพาะองค์การนั้นเท่านั้น เช่น บริษัท เนชั่นแนล (ประเทศไทย) จำกัด เป็นบริษัทที่มีความสามารถในการผลิตเครื่องใช้ไฟฟ้า หรือ บริษัท ฟอร์ด (มอเตอร์) จำกัด มีความสามารถในการผลิตรถยนต์ เป็นต้น หรือ บริษัท ที โอ เอ (ประเทศไทย) จำกัด มีความสามารถในการผลิตสี เป็นต้น

4. สมรรถนะหลัก (Core Competencies)

หมายถึง ความสามารถสำคัญที่บุคคลต้องมีหรือต้องทำเพื่อให้บรรลุผลตามเป้าหมายที่ตั้งไว้ เช่น พนักงานเลขานุการสำนักงานต้องมีสมรรถนะหลัก คือ การใช้คอมพิวเตอร์ได้ ติดต่อประสานงานได้ดี เป็นต้น หรือผู้จัดการบริษัทต้องมีสมรรถนะหลัก คือ การสื่อสาร การวางแผนและการบริหารจัดการ และการทำงานเป็นทีม เป็นต้น

5. สมรรถนะในงาน (Functional Competencies)

หมายถึง ความสามารถของบุคคลที่มีตามหน้าที่ที่รับผิดชอบ ตำแหน่งหน้าที่อาจเหมือนแต่ความสามารถตามหน้าที่ต่างกัน เช่น ข้าราชการตำรวจเหมือนกัน แต่มีความสามารถต่างกัน บางคนมีสมรรถนะทางการสืบสวน สอบสวน บางคนมีสมรรถนะทางปราบปราม เป็นต้น

<u>การวัดสมรรถนะ</u>

การวัดสมรรถนะทำได้ค่อนข้างลำบากจึงอาศัยวิธีการ หรือใช้เครื่องมือบางชนิดเพื่อวัดสมรรถนะของบุคคล ดังนี้

1. ประวัติการทำงานของบุคคลว่าทำอะไรบ้างมีความรู้ ทักษะหรือความสามารถอะไร เคยมีประสบการณ์อะไรมาบ้าง จากประวัติการทำงานทำให้ได้ข้อมูลส่วนบุคคล

2. ผลประเมินการปฏิบัติงาน (Performance Appraisal) ซึ่งจะเป็นข้อมูลเกี่ยวกับการปฏิบัติงานใน 5 ลักษณะ คือ

2.1 ผลการปฏิบัติที่เป็นเนื้องาน (Task Performance) เป็นการทำงานที่ได้เนื้องานแท้ๆ

2.2 ผลงานการปฏิบัติที่ไม่ใช่เนื้องานแต่เป็นบริบทของเนื้องาน (Contextual Performance) ได้แก่ ลักษณะพฤติกรรมของคนปฏิบัติงาน เช่น การมีน้ำใจเสียสละช่วยเหลือคนอื่น เป็นต้น

2.3 ผลการสัมภาษณ์ (Interview) ได้แก่ ข้อมูลที่ได้จากการสัมภาษณ์อาจจะเป็นการสัมภาษณ์แบบมีโครงสร้าง คือ กำหนดคำสัมภาษณ์ไว้แล้วสัมภาษณ์ตามที่กำหนดประเด็น

ไว้กับการสัมภาษณ์แบบแบบไม่มีโครงสร้าง คือ สอบถามตามสถานการณ์คล้ายกับเป็นการพูดคุยกันธรรมดาๆ แต่ผู้สัมภาษณ์จะต้องเตรียมคำถามไว้ในใจ โดยใช้กระบวนการสนทนาให้ผู้ถูกสัมภาษณ์สบายใจให้ข้อมูลที่ตรงกับสภาพจริงมากที่สุด

2.4 ศูนย์ประเมิน (Assessment Center) จะเป็นศูนย์รวมเทคนิคการวัดทางจิตวิทยาหลายๆ อย่างเข้าด้วยกัน รวมทั้งการสนทนากลุ่มแบบไม่มีหัวหน้ากลุ่มรวมอยู่ด้วยในศูนย์นี้

2.5 360 Degree Feedback หมายถึง การประเมินรอบด้าน ได้แก่ การประเมินจากเพื่อนร่วมงาน ผู้บังคับบัญชา ผู้ใต้บังคับบัญชา และลูกค้า เพื่อตรวจสอบความรู้ ทักษะ และคุณลักษณะ

<u>การตรวจสอบสมรรถนะ</u>

การตรวจสอบสมรรถนะว่าพฤติกรรมที่เกิดขึ้นนั้นเป็นสมรรถนะที่ต้องการหรือไม่มีข้อสังเกตดังนี้

1. เป็นพฤติกรรมที่สังเกตได้อธิบายได้
2. สามารถลอกเลียนแบบได้
3. มีผลกระทบต่อความก้าวหน้าขององค์กร
4. เป็นพฤติกรรมที่สามารถนำไปใช้ได้หลายสถานการณ์
5. เป็นพฤติกรรมที่ต้องเกิดขึ้นบ่อยๆ

การนำ Competency ไปประยุกต์ใช้

<u>สมรรถนะหลัก (Core Competency)</u>

สำหรับบุคลากรด้านคอมพิวเตอร์ที่ควรจะมีเป็นหัวข้อในแบบสอบถามโดยนำแนวคิดของ คีนส์ เอ มอร์นัว (Keith, A. Morneau. 2004) ของมหาวิทยาลัย Capella สหรัฐอเมริกา โดยผู้ศึกษาได้นำมาปรับใช้และเพิ่มเติมโดยแบ่งเป็น 3 ส่วน ดังนี้

(1) ความรู้พื้นฐาน (Knowledge)

1. พื้นฐานด้านคอมพิวเตอร์เบื้องต้น
2. พื้นฐานด้าน Networking และ Internetworking
3. พื้นฐานด้าน TCP/IP Protocol
4. พื้นฐานด้านการใช้งาน Internet Service
5. พื้นฐานด้านการจัดการฐานข้อมูล (Database)
6. พื้นฐานในการออกแบบระบบเครือข่าย
7. พื้นฐานการใช้งานระบบปฏิบัติการเครือข่าย (Network Operation System)
8. พื้นฐานการใช้งานระบบปฏิบัติการ (Operation System)

9. พื้นฐานการเขียนโปรแกรมจากภาษาคอมพิวเตอร์ (Programming)
10. พื้นฐานในการออกแบบโปรแกรม
11. พื้นฐานการใช้งานโปรแกรมประยุกต์ต่างๆ
12. พื้นฐานการคำนวณสูตรคณิตศาสตร์ทางคอมพิวเตอร์

(2) ทักษะการทำงาน (Skill) โดยแบ่งออกเป็น 3 ส่วนดังนี้

1. ความสามารถการจัดการระบบคอมพิวเตอร์
   1.1 สามารถ Clone/Backup Hard Disk
   1.2 สามารถติดตั้งระบบปฏิบัติการของคอมพิวเตอร์ต่างๆ ได้ เช่น Windows, Linux เป็นต้น
   1.3 สามารถแก้ไขและซ่อมแซมเครื่องคอมพิวเตอร์
   1.4 สามารถแก้ไขและซ่อมแซมเครื่องคอมพิวเตอร์เซิร์ฟเวอร์
   1.5 การเขียนโปรแกรมด้วยภาษาคอมพิวเตอร์ เช่น C++, C#, Java Script และ Shell Script เป็นต้น
   1.6 ทำการ Install และ Update Drivers ให้กับระบบคอมพิวเตอร์ได้
   1.7 สามารถแก้ไขและซ่อมแซมอุปกรณ์คอมพิวเตอร์อื่นๆ ได้ เช่น Printer, Scanner ,Router , Switch เป็นต้น
   1.8 แก้ไข Registry เพื่อซ่อมแซมระบบคอมพิวเตอร์ได้
   1.9 สามารถ Update โปรแกรมป้องกัน Virus ได้
   1.10 สามารถทำ Cluster & Load Balance ได้
2. ความสามารถด้านการจัดการเครือข่าย
   2.1 การติดตั้งเครือข่ายภายใน (LAN)
   2.2 การติดตั้งเครือข่ายไร้สาย (Wireless Network)
   2.3 การออกแบบระบบเครือข่าย
   2.4 การติดตั้งระบบปฏิบัติการสำหรับเครื่องแม่ข่าย
   2.5 สามารถตรวจสอบการทำงานของ Port/Cable บนระบบเครือข่ายได้
   2.6 สามารถแก้ไขและตั้งค่า VLAN, LAN และ Wireless ได้
   2.7 สามารถแก้ไขและตั้งค่าการเชื่อมต่อระหว่าง Client และ Server หรือ Client และ Network Printer ได้
   2.8 สามารถแก้ไขและตั้งค่าระบบ e-Mail ภายใน Intranet ขององค์กรได้
   2.9 สามารถแก้ไขและตั้งค่า Proxy ของระบบเครือข่ายในองค์กรได้
   2.10 สามารถจัดการระบบ Web Server ขององค์กรได้
3. ความสามารถทางด้านภาษา
   - ภาษาอังกฤษ

(3) คุณลักษณะพื้นฐาน (Underlying Characteristic or Attribute)

1. มีการบริการที่ดี
2. สามารถทำงานเป็นทีมได้
3. มีมนุษยสัมพันธ์กับเพื่อนร่วมงาน
4. มีจริยธรรมในการทำงาน
5. กระตือรือร้นที่จะพัฒนาตนเอง
6. เป็นคนสุภาพเรียบร้อย
7. เป็นคนตรงไปตรงมา
8. มีความมั่นใจในตนเอง

<u>สมรรถนะประจำกลุ่มงานหรือเฉพาะงาน (Functional Competency)</u>

สตีเฟน นอร์ทคัส (Stephen, Northcutt. 2009) ได้กล่าวถึง Functional Competency ของวิศวกรคอมพิวเตอร์ด้านความปลอดภัยไว้ โดยมีการจัดแบ่งหมวดหมู่ไว้ดังนี้

ความรู้พื้นฐาน (Knowledge)

1. Network Operation System หรือระบบปฏิบัติการเครือข่าย
2. Operation System หรือระบบปฏิบัติการ
3. SSL/TLS, CIFS, HTTP/S, DHCP, SMTP, LDAP/S และ DNS
4. VPNs, IPSec และ PKI
5. มาตรฐาน ISO-27000
6. มาตรฐาน COBIT
7. มาตรฐาน ITIL

ทักษะการทำงาน (Skill)

1. วิเคราะห์การความเสี่ยงที่สามารถเกิดขึ้นได้บนระบบคอมพิวเตอร์
2. วิเคราะห์แยกแยะชนิดของการโจมตีที่เกิดขึ้น
3. สามารถแก้ไขการตั้งค่าของระบบคอมพิวเตอร์เพื่อลดความเสียหายกับระบบสารสนเทศได้
4. สามารถสืบหาสาเหตุของความเสียหายที่เกิดขึ้นกับระบบสารสนเทศได้
5. สามารถอธิบายการโจมตีและสาเหตุที่ทำให้เกิดความเสียต่อระบบแก่ผู้ใช้หรือผู้อื่นๆ ได้
6. สามารถแก้ไขและป้องกัน Web Coding ของระบบ Web Server เมื่อเกิดการเปลี่ยนแปลงจากผู้โจมตีได้

คุณลักษณะพื้นฐาน (Underlying Characteristic or Attribute)

ในส่วนของคุณลักษณะพื้นฐาน (Underlying Characteristic or Attribute) ซึ่งได้แนวคิดมาจาก ไบรอัน ดัสเชอร์ (Brian, Dutcher. 2010) ได้กล่าวถึง คุณลักษณะที่จำเป็นสำหรับวิศวกรคอมพิวเตอร์ด้านความปลอดภัยไว้ดังนี้

1. คิดวิเคราะห์ได้
2. มองภาพองค์รวม (การมองการทำงานของทีมรวมถึงระบบสารสนเทศทั้งระบบในองค์กร)
3. เข้าใจผู้อื่น
4. ดำเนินการเชิงรุก
5. มีความถูกต้องของงาน
6. มีความมั่นใจของตนเอง
7. มีความยืดหยุ่นผ่อนปรน
8. มีความเป็นผู้นำ
9. มีการประสานงานที่ดี
10. มีการติดตามงาน
11. แก้ปัญหาต่างๆได้
12. ให้คำปรึกษาได้
13. บริหารการเปลี่ยนแปลงได้

คุณลักษณะพื้นฐาน (Underlying Characteristic or Attribute) โดยมีการปรับปรุงมาจากแนวคิดของ ไบรอัน ดัสเชอร์ (Brian, Dutcher. 2010) ที่ได้กล่าวไว้ก่อนหน้านี้ โดยผู้ศึกษาได้ทำการนำมาปรับใช้ในการสร้างและออกแบบสอบถาม

เอกสารและงานวิจัยที่เกี่ยวข้อง

คลาร่า แอนท์โลวา (Klara, Antlova. 2010) ได้ทำการศึกษาเรื่อง การวางทางสมรรถนะของเทคโนโลยีสารสนทเศภายในกิจการขนาดกลางและขนาดเล็ก โดยใช้วิธีการสัมภาษณ์เจ้าของกิจการหรือผู้จัดการของกิจการขนาดกลางและขนาดเล็ก จำนวน 30 กิจการที่มีการจ้างงานไม่น้อยกว่า 15 ปี โดยมีวัตถุประสงค์เพื่อหาความสำเร็จของกิจการว่ามีส่วนเกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ และการแบ่งบันความรู้ของพนักงานในกิจการ ซึ่งพบว่า กิจการขนาดกลางและขนาดเล็กที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในกิจการบุคลากรต้องมีความรู้ ความเข้าใจในเรื่องเทคโนโลยีสารสนเทศและต้องมีการแบ่งปันความรู้ข้อมูล ข่าวสาร และประสบการณ์ในการทำงาน จึงจะทำให้กิจการประสบความสำเร็จ

มิเชล เจ ทิฟพินส์ ; และ ราวิเพรท เอส โซฮี (Michael, J. Tippins ; and Ravipreet S. Sohi. 2003) ได้ทำการศึกษาเรื่อง สมรรถนะของเทคโนโลยีสารสนเทศกับผลการดำเนินงานขององค์กร : องค์กรได้เรียนรู้ส่วนที่หายไปหรือไม่ โดยการทดสอบความสัมพันธ์ระหว่างเทคโนโลยีสารสนเทศกับผลการดำเนินงานของบริษัท และพัฒนาความเข้าใจว่าทำไมเทคโนโลยีสารสนเทศจึงส่งผลกระทบกับผลการดำเนินงานของบริษัท และพัฒนาความเข้าใจว่าทำไมเทคโนโลยีสารสนเทศจึงส่วผลกระทบกับผลการดำเนินงานของบริษัท ผู้วิจัยได้ทำการวิจัยโดยการส่งแบบสอบถามแก่บริษัทในอุตสาหกรรมผลิตและจำหน่ายเครื่องจักร อุตสาหกรรมเครื่องไฟฟ้าและอะไหล่เครื่องใช้ไฟฟ้า อุตสาหกรรมชิ้นส่วนสำหรับการขนส่ง และอุตสาหกรรมชิ้นส่วนสำหรับเครื่องชั่งและเครื่องคำนวณ จำนวน 524 บริษัท ซึ่งได้รับการตอบกลับจำนวน 271 บริษัท จากวิจัย พบว่า เทคโนโลยีสารสนเทศไม่ส่งผลหกระทบต่อผลการดำเนินงานของบริษัทโดยตรงแต่มีผลในการยกระดับทรัพยากรอื่นภายในองค์กร เช่น การเรียนรู้ภายในองค์กร ซึ่งเป็นการสร้างความได้เปรียบทางการแข่งขัน และนำไปสู่ผลการดำเนินงานที่ดีขึ้นสำหรับบริษัท

เบรนด้า โอลด์ฟิลล์ (Brenda, Oldfield. 2007) ได้ศึกษาวิจัยการแบ่งกลุ่มองค์ความรู้ที่เกี่ยวข้องกับงานด้าน IT Security โดยพัฒนามาเป็น IT Security EBK (Essential Body of Knowledge) ถูกวิจัยขึ้นและเผยแพร่โดยกระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐฯ (United States Department of Homeland Security : DHS) โดยได้อ้างอิงถึงหรือใช้ผลลัพธ์จากเอกสารของกระทรวงกลาโหมสหรัฐหรือ US-DoD ที่ได้เผยแพร่ออกมาก่อนหน้านี้ นั่นคือ DoD-8570.01-M โดย IT Security EBK ฉบับร่างที่ 1 ได้ถูกส่งให้ผู้เชี่ยวชาญที่อยู่ในอุตสาหกรรมที่เกี่ยวข้องได้ทบทวนและให้ข้อคิดเห็นอย่างกว้างขวาง T Security EBK แบ่งมุมมองออกเป็น 3 มิติ ดังนี้

ซึ่งเมื่อนำเอาทั้ง 3 มิติมารวมกันและสรุปความสัมพันธ์ก็จะได้ผลลัพธ์ออกมาดังตารางด้านล่างนี้ ซึ่งเป็นการสรุปภาพรวมให้เห็นว่า ในแต่ละตำแหน่งงาน (Role) ต้องการบุคลากรที่มีความรู้ความสามารถด้านใดบ้าง (Competency Area) และต้องมีขีดความสามารถระดับใดในแต่ละด้านนั้น (Functional Perspective) ดังตารางที่ 2

ตารางที่ 2 IT Security Competency Areas by DHS

IT Security EBK: A Competency and Functional Framework

Functional Perspectives
M - Manage
D - Design
I - Implement
E - Evaluate

IT Security Competency Areas	IT Security Roles																					
	Executive						*Functional*										*Corollary*					
	Chief Information Officer		Information Security Officer			IT Security Compliance Officer		Digital Forensics Professional		IT Systems Operations and Maintenance Professional		IT Security Professional		IT Security Engineer		Physical Security Professional		Privacy Professional		Procurement Professional	
1 Data Security	M		M	D								M	D		D				D		
				E		E				I	E		E		E				E		
2 Digital Forensics			M	D			M	D													
						E	I	E	I												
3 Enterprise Continuity	M		M								D						D				
				F		F			I				F			I					
4 Incident Management	M		M	D							D		D					M	D		
				E		E	I		I	E			E			I		I	E		
5 IT Security Training and Awareness	M		M										D						D		
				E		E						I	E						E		
6 IT Systems Operations and Maintenance								D	M	D					D						
						E	I	E	I	E				I								
7 Network and Telecommunications Security								D	M	D					D						
						E	I		I	E				I								
8 Personnel Security	M		M										D						D		
						E							E				E	I			
9 Physical and Environmental Security	M		M										D			M	D				
				E		E							E			I	E				
10 Procurement	M	D	M	D																M	D
				E		E		E		E							E			I	E
11 Regulatory and Standards Compliance	M		M	D		D												M	D		
		E		E	I	E						I						I	E		
12 Security Risk Management	M		M	D									D					M	D		
		E		E	I	E	I		I			I	E	I		I		I	E		
13 Strategic Security Management	M	D	M	D																	
		E	I	E		E															
14 System and Application Security	M		M												D						
				E		E			I					I	E						

1. Functional Perspective หรือมุมมองในเชิงลักษณะงานโดยแบ่งย่อยออกเป็น 4 ด้าน คือ

1.1 Manage หรือ เชิงบริหาร

1.2 Design หรือ เชิงออกแบบ

1.3 Implement หรือ เชิงปฏิบัติ ลงมือทำ

1.4 Evaluate หรือ เชิงตรวจสอบประเมิน

2. Competencies หรือ การแบ่งกลุ่มองค์ความรู้ที่เกี่ยวข้องกับงานด้าน IT Security ซึ่งแบ่งย่อยออกเป็น 14 ด้าน คือ

2.1 Data Security หรือ การรักษาความปลอดภัยข้อมูล

2.2 Digital Forensics หรือ นิติวิทยาศาสตร์ทางดิจิตอล

2.3 Enterprise Continuity หรือ การบริหารองค์กรอย่างต่อเนื่อง

2.4 Incident Management หรือ การบริหารจัดการเหตุการณ์

2.5 IT Security Training and Awareness หรือ การฝึกอบรมและตระหนักถึงความปลอดภัยข้อมูลสารสนเทศ

2.6 IT System Operations and Maintenance หรือการดำเนินางานและปรับปรุงรักษาระบบความปลอดภัยข้อมูลสารสนเทศ

2.7 Network and Telecommunication Security หรือ การรักษาความปลอดภัยทางเครือข่ายและโทรคมนาคม

2.8 Personnel Security หรือ ความปลอดภัยส่วนบุคคล

2.9 Physical and Environmental Security หรือ การรักษาความปลอดภัยจากทางกายภาพและสิ่งแวดล้อม

2.10 Procurement หรือ การจัดซื้อ/จัดจ้าง

2.11 Regulatory and Standards Compliance หรือ การปฏิบัติตามกฎระเบียบและมาตรฐาน

2.12 Security Risk Management หรือ การบริหารจัดการความเสี่ยงระบบรักษาความปลอดภัยข้อมูล

2.13 Strategic Security Management หรือ การบริหารจัดการกลยุทธ์ในการรักษาความปลอดภัยข้อมูล

2.14 System and Application Security หรือ ระบบความมั่นคงทางระบบงานและระบบความมั่นคงสำหรับโปรแกรมประยุกต์

3. Roles หรือบทบาทหน้าที่หรือตำแหน่งงานในองค์กร ซึ่งแบ่งย่อยออกเป็น 10 บทบาท คือ

3.1 Chief Information Officer หรือ ผู้บริหารสูงสุดด้านสารสนเทศและคอมพิวเตอร์

3.2 Digital Forensics Professional หรือ ผู้เชี่ยนชาญด้านนิติวิทยาศาสตร์ทางดิจิตอล

3.3 Information Security Officer หรือ เจ้าหน้าที่ทางด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ

3.4 IT Security Compliance Officer หรือเจ้าหน้าที่ควบคุมปฏิบัติตามกฎระเบียบข้อบังคับ และกฎหมายตามนโยบายด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ

3.5 IT Security Engineer หรือ วิศวกรด้านการรักษาความปลอดภัยของข้อมูล

3.6 IT Security Professional หรือ ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของข้อมูล

3.7 IT Systems Operations and Maintenance Professional หรือ ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของข้อมูลและการดูแลรักษาระบบระดับปฏิบัติ

3.8 Physical Security Professional หรือ ผู้เชี่ยวชาญด้านความมั่นคงและการป้องกันระบบเชิงกายภาพ

3.9 Privacy Professional หรือ ผู้เชี่ยวชาญด้านการรักษาและป้องกันความเป็นส่วนตัวของระบบสารสนเทศ

3.10 Procurement Professional หรือ ผู้เชี่ยวชาญด้านการจัดซื้อ/จัดจ้าง

อีกงานวิจัยจากองค์การบริหารการบินและอวกาศแห่งชาติ หรือ นาซ่า (National Aeronautics and Space Administration : NASA) ได้จัดทำ Competencies Areas ของ System Engineer ในองค์กร โดยผู้ศึกษาได้ยกเอาหัวข้อ Security, Safety and Mission Assurance มาศึกษาโดยทางนาซ่า ได้จัดทำ Competencies Areas โดยแบ่งออกเป็น 4 Level โดยสรุปเป็นตารางได้ดังนี้

ตารางที่ 3 IT Security : Competency Elements and Descriptions

Level 1	Level 2	Level 3	Level 4
Identify IT Security Requirements, Develop and Implement IT Security Plan			
มีส่วนร่วมในการระบุข้อกำหนดด้านความปลอดภัยไอทีตระหนักถึงการวางแผนการรักษาความปลอดภัยไอที และผลกระทบทางเทคนิคต่อทีมงาน	การจัดการข้อกำหนดสำหรับระบบในแต่ละส่วนย่อย รวมถึงการพัฒนาและการดำเนินงานของไอที แผนการรักษาความปลอดภัยสำหรับระบบในแต่ละส่วนย่อย	การพัฒนาและการดำเนินการตามแผนรักษาความปลอดภัยสำหรับระบบไอทีตามความต้องการของหน่วยงานการรักษาความปลอดภัยสำหรับระบบ IT	การสร้างและออกแบบความต้องการรักษาความปลอดภัยสำหรับระบบ IT เพื่อนำไปสู่การพัฒนาของการรักษาความปลอดภัยด้านไอทีสำหรับองค์กร

กรมโรงงานอุตสาหกรรม (ศส.กรอ.) (2551) ได้มีการวิจัยการแบ่งสมรรถนะพื้นฐานของนักวิชาการคอมพิวเตอร์ (Common Competnecy for IT Professional) เพื่อใช้ในหน่วยงานของ ศส.กรอ. โดยมีการแบ่งไว้ถึง 6 ระดับ ซึ่งครอบคลุมตั้งแต่ผู้ใช้งาน (End User) จนถึงผู้บริหารระดับสูงของสารสนเทศดังตารางดังนี้

ตารางที่ 4 Common Competency for IT Professional

ระดับที่ 0 : ไม่แสดงสมรรถนะด้านนี้อย่างชัดเจน
ระดับที่ 1 : มีความรู้พื้นฐานระบบฐานข้อมูล การสื่อสารข้อมูลและใช้ คำสั่ง SQL ในระดับเบื้องต้น ● ใช้ ผังลำดับการทำงาน (Flow Diagram) ● ใช้โครงสร้างฐานข้อมูล ● ใช้คำสั่ง SQL ระดับเบื้องต้น ● มีความรู้เกี่ยวกับ ระบบ Internet เช่น การสืบค้นข้อมูล และ การส่ง e-Mail ● จัดทำ Web Page โดยใช้ภาษา HTML ● บำรุงรักษาอุปกรณ์ระบบเครือข่าย
ระดับที่ 2 : แสดงสมรรถนะระดับ 1 และออกแบบโครงสร้างฐานข้อมูลขั้นพื้นฐาน เก็บความต้องการ (Requirement) ของผู้ใช้งานวิเคราะห์และออกแบบระบบเบื้องต้นได้ และศึกษาติดตามเทคโนโลยีใหม่ๆ และนำมาประยุกต์ใช้ในหน่วยงาน ● ออกแบบโครงสร้างฐานข้อมูลขั้นพื้นฐาน ● วิเคราะห์และออกแบบระบบงานและฐานข้อมูลเบื้องต้น ● เก็บความต้องการ (Requirement) ของผู้ใช้งาน ● ออกแบบลำดับการทำงาน (Flow Diagram) ได้อย่างมีประสิทธิภาพ ● เป็นผู้ศึกษาและติดตามเทคโนโลยีใหม่ๆ และสามารถนำมาประยุกต์ใช้ในหน่วยงาน
ระดับที่ 3 : แสดงสมรรถนะระดับ 2 และมีความรู้ ความเข้าใจกฎระเบียบ และประกาศต่างๆ ที่เกี่ยวข้องในภารกิจของ ศส.กรอ. จัดทำระบบทะเบียนผู้ใช้ระบบเครือข่ายจัดตั้งทีมงานเพื่อปฏิบัติงานบริหารความปลอดภัย ● มีความรู้ ความเข้าใจกฎระเบียบ และประกาศต่างๆ ที่เกี่ยวข้องในภารกิจของ ศส.กรอ. ● จัดทำระบบทะเบียนผู้ใช้ระบบเครือข่าย ● เรียกใช้ข้อมูลจากระบบฐานข้อมูลอย่างเชี่ยวชาญ ● บริหารทีมงานให้เป็นไปตามเป้าหมาย ● เขียนโปรแกรม Web Application โดยใช้ภาษาต่างๆ เช่น C, VB, JAVA, ASP ● แก้ไขข้อผิดพลาดของโปรแกรมระบบงาน (Debug) ● จัดการด้านความปลอดภัยของระบบและสามารถบำรุงรักษาระบบจราจรในเครือข่าย

ตารางที่ 4 Common Competency for IT Professional (ต่อ)

ระดับที่ 4 : แสดงสมรรถนะระดับ 3 และวิเคราะห์และออกแบบระบบอย่างเชี่ยวชาญ วิเคราะห์ ออกแบบ ติดตั้ง และแก้ไขปัญหาของระบบเครือข่ายท้องถิ่น (LAN) แก้ไขข้อผิดพลาดของโปรแกรมระบบงาน (Debug) เขียนโปรแกรมโนระดับซับซ้อน และจัดการระบบความปลอดภัยในระบบเครือข่าย • ออกแบบระบบฐานข้อมูลอย่างเชี่ยวชาญ • วิเคราะห์ ออกแบบ ติดตั้ง และแก้ไขปัญหาของระบบเครือข่ายท้องถิ่น (LAN) • เขียนโปรแกรม Web Application โดยใช้ภาษาต่างๆ เช่น C, VB, JAVA ในระดับที่ซับซ้อน • จัดการระบบความปลอดภัยในระบบเครือข่าย • วิเคราะห์และออกแบบระบบในระดับสูง
ระดับที่ 5 : แสดงสมรรถนะระดับ 4 และมีความเข้าใจอย่างลึกซึ้งและเชี่ยวชาญใน ระบบสารสนเทศของหน่วยงาน อย่างกว้างขวางหรือสามารถบริหารทรัพยากรของหน่วยงานที่มีอยู่เพื่อน นำมาใช้งานได้อย่างมีประสิทธิภาพ เพื่อพัฒนาระบบการปฏิบัติงานได้อย่างเชี่ยวชาญ • สามารถบูรณาการข้อมูลที่มีอยู่ภายในกับข้อมูลจากภายนอก เพื่อนำผลมาจัดทำรายงาน อันจะเป็นประโยชน์ต่อองค์กรและประชาชนทั่วไป • บริหารงานโครงการ • บริหารระบบสารสนเทศและชี้นำทิศทางขององค์กร • ร่วมกำหนดนโยบายและยุทธศาสตร์เกี่ยวกับการใช้สารสนเทศของ กรอ. • คาดการณ์ปัญหาและความต้องการของผู้ใช้งานที่เกิดขึ้น

สถาบันศึกษามหาสมุทรและชั้นบรรยากาศแห่งชาติของสหรัฐฯ หรือ National Oceanic and Atmospheric Administration (NOAA) (2012) ได้การศึกษาการแบ่งระดับสมรรถนะของบุคลากรภายในสถาบันโดยในหัวข้อ “Information Systems Security” ได้มีการแบ่งระดับไว้ 5 ระดับ ดังตารางต่อไปนี้

ตารางที่ 5 สรุปการแบ่งสมรรถนะของ NOAA

ระดับ 1 : เบื้องต้น	➢ สามารถอธิบายแนวคิดพื้นฐานเพื่อสอดคล้องกับการรับรองความปลอดภัยระบบของข้อมูล
ระดับ 2 : ขั้นพื้นฐาน	➢ สามารถระบุขั้นตอนและงานที่เกี่ยวข้องในการประเมินการรับรองความปลอดภัยระบบสารสนเทศได้ ➢ มีความเข้าใจถึงสาเหตุและการประยุกต์ใช้โปรแกรมเพื่อความปลอดภัยและเครื่องมือที่จะมีส่วนร่วมในขั้นตอนการรับรอง
ระดับ 3 : ขั้นกลาง	➢ มีส่วนร่วมในการประเมินผลของระบบสารสนเทศในการพัฒนาได้รับการรับรองและการรับรองแผน ➢ การใช้เอกสารประกอบการรักษาความปลอดภัยที่เหมาะสมในการพัฒนาด้านความปลอดภัยของระบบ
ระดับ 4 : ขั้นสูง	➢ ประเมินระบบสารสนเทศในการระบุความเสี่ยงที่เหลือเพื่อให้คำแนะนำในการตอบสนองความต้องการการรักษาความปลอดภัยขององค์กรที่เหมาะสม ➢ ความต้องการของระบบได้มีระบุไว้ในแผนรับรองจะรวมอยู่ในกระบวนการวงจรชีวิตของการพัฒนาระบบความปลอดภัย ➢ ดำเนินการกำกับดูแลของกิจกรรมของทีมทดสอบระบบความปลอดภัย
ระดับ 5 : ผู้เชี่ยวชาญ	➢ พัฒนาวิธีการและนโยบายสำหรับการรับรองและการรับรองแผนระบบความปลอดภัยของสารสนเทศทั่วทั้งองค์กร ➢ ดำเนินการทดสอบการป้องกันกับความหลากหลายของการโจมตีและการแก้ปัญหาบนระบบปฏิบัติการฐานข้อมูล ➢ ดำเนินการทดสอบการเจาะระบบ

จอห์น เบอรี่ (John, Berry. 2011) ซึ่งอยู่ในตำแหน่ง CHRO (Chief Human Resource Officer) ของสำนักงานจัดการบุคลากรของประเทศสหรัฐอเมริกา (U. S. Office of Personnel Management : OPM) ได้ศึกษาวิจัยเรื่อง “Competency Model for Cybersecurity” โดยได้สรุปออกมาเป็นตารางดังนี้

ตารางที่ 6 Cybersecurity Competencies for Computer Engineer by John Berry

Core Competency	Functional Competency
ให้ความสนใจกับรายละเอียด	การจัดการการสื่อสารการรักษาความปลอดภัย
ทักษะคอมพิวเตอร์	การจัดการข้อมูล
ความคิดสร้างสรรค์	กลยุทธ์และการวางแผนทรัพยากรสารสนเทศ
บริการลูกค้า	ระบบสารสนเทศ / เครือข่ายการรักษาความปลอดภัย
การตัดสินใจ	การประเมินผลการปฏิบัติงานเทคโนโลยีสารสนเทศ
มีความยืดหยุ่น	การจัดการเครือข่าย
การจัดการข้อมูล	การบริหารโครงการ
ทักษะความสัมพันธ์ระหว่างบุคคล	การวิเคราะห์ความต้องการ
ความเป็นผู้นำ	การบริหารความเสี่ยง
การทำงานเป็นทีม	การพัฒนาซอฟต์แวร์
การสื่อสารในช่องปาก	การทดสอบซอฟต์แวร์และการประเมินผล
พันธมิตร	ระบบบูรณาการ
การวางแผนและการประเมินผล	ระบบการทดสอบและประเมินผล
การแก้ปัญหา	การประเมินช่องโหว่
การจัดการตนเอง	เทคโนโลยีเว็บ
การคิดเชิงกลยุทธ์	

ตารางที่ 7 สรุปผลการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง

สมรรถนะที่เกี่ยวข้อง Information Security Engineer	ผู้ทำการศึกษา									
	Keith, A. Morneau. (2004)	Stephen, Northcutt. (2009)	Brian, Dutcher. (2010)	Klara, Antlova. (2010)	Michael, J. Tippins ; and Ravipreet, S. Sohi. (2003)	Brenda, Oldfield. (2007)	National Aeronautics and Space Administration (NASA) (2010)	National Oceanic and Atmospheric Administration (NOAA) (2012)	ศส.กรอ. (2551)	John, Berry. (2011)
สมรรถนะหลัก (Core Competency)										
พื้นฐานด้านคอมพิวเตอร์เบื้องต้น	X	X	X	X	X	X	X	X	X	X
พื้นฐานด้าน Networking และ Internetworking	X	X	X	X	X	X	X	X	X	X
พื้นฐานด้าน TCP/IP Protocol	X	X			X	X	X	X		
พื้นฐานด้านการจัดการฐานข้อมูล (Database)	X	X	X		X			X	X	X
พื้นฐานในการออกแบบระบบเครือข่าย	X	X	X		X	X	X		X	
พื้นฐานการใช้งานระบบปฏิบัติการเครือข่าย (Network Operation System)	X	X		X	X	X	X	X	X	X
พื้นฐานการใช้งานระบบปฏิบัติการ (Operation System)	X	X		X	X	X	X	X	X	
พื้นฐานการเขียนโปรแกรมจากภาษาคอมพิวเตอร์ (Programming)	X			X		X		X	X	X
พื้นฐานการใช้งานโปรแกรมประยุกต์ต่างๆ	X		X		X	X		X	X	X
ทักษะการ Clone / Backup Hard Disk	X		X	X					X	
ทักษะการติดตั้งระบบปฏิบัติการของคอมพิวเตอร์ต่างๆ ได้ เช่น Windows, Linux เป็นต้น	X		X	X	X	X		X	X	
ทักษะการแก้ไขและซ่อมแซมเครื่องคอมพิวเตอร์	X	X		X	X				X	
ทักษะการแก้ไขและซ่อมแซมเครื่องคอมพิวเตอร์เซิร์ฟเวอร์	X	X		X			X		X	
ทักษะการเขียนโปรแกรมด้วยภาษาคอมพิวเตอร์ เช่น C++, C#, Java Script และ Shell Script เป็นต้น	X			X	X	X		X		
ทักษะการแก้ไขและซ่อมแซมอุปกรณ์คอมพิวเตอร์อื่นๆ ได้เช่น Printer, Scanner, Router, Switch เป็นต้น	X		X				X			
ทักษะการออกแบบระบบเครือข่าย	X		X	X			X	X	X	
ทักษะการติดตั้งระบบปฏิบัติการสำหรับเครื่องแม่ข่าย	X	X	X		X		X	X	X	X
ทักษะการแก้ไขและตั้งค่า VLAN,LAN และ Wireless ได้	X				X	X	X	X	X	
ทักษะการแก้ไขและตั้งค่า Proxy ของระบบเครือข่ายในองค์กรได้	X		X			X				
ทักษะการจัดการระบบ Web Server ขององค์กรได้	X	X		X	X	X	X	X	X	X
ทักษะภาษาอังกฤษ	X	X	X	X	X	X	X	X	X	X

ตารางที่ 7 สรุปผลการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง (ต่อ)

สมรรถนะที่เกี่ยวข้อง Information Security Engineer	ผู้ทำการศึกษา									
	Keith, A. Morneau. (2004)	Stephen, Northcutt. (2009)	Brian, Dutcher. (2010)	Klara, Antlova. (2010)	Michael, J. Tippins ; and Ravipreet, S. Sohi. (2003)	Brenda, Oldfield. (2007)	National Aeronautics and Space Administration (NASA) (2010)	National Oceanic and Atmospheric Administration (NOAA) (2012)	ศส.กรอ. (2551)	John, Berry. (2011)
สมรรถนะเฉพาะ (Functional Competency)										
พื้นฐานด้านการโจมตีบนระบบสารสนเทศ		X	X			X	X	X		X
พื้นฐานด้านความปลอดภัยบน Network Operation System หรือระบบปฏิบัติการเครือข่าย	X	X	X			X				X
พื้นฐานด้านความปลอดภัยบน Operation System หรือระบบปฏิบัติการ	X	X	X				X			X
พื้นฐานด้านโปรโตคอล SSL/TLS, CIFS,HTTP/S,DHCP,SMTP, LDAP/S และ DNS		X	X	X	X	X	X			
พื้นฐานความเข้าใจการทำงานของ VPNs, IPSec และ PKI		X	X	X	X					
พื้นฐานกฎหมาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550		X	X				X			
พื้นฐานด้าน ISO-27000	X	X	X	X	X	X	X	X	X	X
ทักษะการวิเคราะห์การความเสี่ยงที่สามารถเกิดขึ้นได้บนระบบคอมพิวเตอร์		X	X			X		X		X
ทักษะการวิเคราะห์แยกแยะชนิดของการโจมตีที่เกิดขึ้น		X	X			X				X
ทักษะการแก้ไขการตั้งค่าของระบบคอมพิวเตอร์เพื่อลดความเสียหายกับระบบสารสนเทศได้	X	X	X	X	X	X	X	X	X	
ทักษะการสืบหาสาเหตุของความเสียหายที่เกิดขึ้นกับระบบสารสนเทศได้		X	X					X		
ทักษะการใช้งานคำสั่งในระบบปฏิบัติการเครือข่ายต่างๆ (Network Operation System) ได้	X	X	X			X				
ทักษะการใช้งานคำสั่งในระบบปฏิบัติการต่างๆ (Operation System) ได้	X	X	X	X	X		X	X		
ทักษะการออกแบบและวางแผนการป้องกันความเสียหายที่อาจจะเกิดขึ้นกับระบบสารสนเทศได้		X	X			X				X
ทักษะการอธิบายการโจมตีและสาเหตุที่ทำให้เกิดความเสียต่อระบบแก่ผู้ใช้หรือผู้อื่นๆ ได้		X	X			X				X
ทักษะการแก้ไขและป้องกัน Web Coding ของระบบ Web Server เมื่อเกิดการเปลี่ยนแปลงจากผู้โจมตีได้	X	X	X			X	X			X

ตารางที่ 7 สรุปผลการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง (ต่อ)

สมรรถนะที่เกี่ยวข้อง Information Security Engineer	ผู้ทำการศึกษา									
	Keith, A. Morneau. (2004)	Stephen, Northcutt. (2009)	Brian, Dutcher. (2010)	Klara, Antlova. (2010)	Michael, J. Tippins ; and Ravipreet, S. Sohi. (2003)	Brenda, Oldfield. (2007)	National Aeronautics and Space Administration (NASA) (2010)	National Oceanic and Atmospheric Administration (NOAA) (2012)	ศส.กรอ. (2551)	John, Berry. (2011)
คุณลักษณะ (Attribute)										
คิดวิเคราะห์ได้	X	X	X	X	X		X			X
มองภาพองค์รวม	X		X	X			X			
เข้าใจผู้อื่น	X		X							
ดำเนินการเชิงรุก			X		X		X			X
มีความถูกต้องของงาน		X	X	X						X
มีความมั่นใจของตนเอง	X		X		X					
มีความยืดหยุ่นผ่อนปรน			X		X					X
มีความเป็นผู้นำ	X	X	X	X						X
มีศิลปะการสื่อสารจูงใจ			X	X	X					
มีการประสานงานที่ดี			X							X
มีการติดตามงาน	X	X	X	X			X			X
แก้ปัญหาต่างๆ ได้			X				X			X
ให้คำปรึกษาได้	X	X	X		X		X			X
มีการให้อำนาจผู้อื่น			X	X			X			
บริหารการเปลี่ยนแปลงได้	X		X	X	X					

TNI
THAI - NICHI INSTITUTE OF TECHNOLOGY

บทที่ 3
วิธีการดำเนินงานสารนิพนธ์

วิธีการดำเนินงานศึกษา เป็นการศึกษาองค์ประกอบของสมรรถนะของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ โดยศึกษาค้นคว้าจากบุคลากรด้าน IT ของสถานประกอบการทั้งภาครัฐและเอกชน ผู้ศึกษาจึงอาศัยรูปแบบสมรรถนะ (Competency Model) ตามแนวคิดของ เดวิด ซี แมคคลีแลนด์ (David, C. McClelland. 1973) โดยผสมผสานกับแนวคิดใหม่ของ สก็อต บี พารี (Scott, B. Parry. 1992) ที่ดัดแปลงแนวคิดมาจากของ แมคคลีแลนด์ เพื่อศึกษาหาองค์ประกอบของสมรรถนะที่จะใช้ในการทำงานด้านความปลอดภัยบนระบบสารสนเทศของบุคลากรทางด้านคอมพิวเตอร์ โดยแบ่งเป็น 2 สมรรถนะ คือ สมรรถนะหลักของบุคลากร IT ด้านความปลอดภัยบนระบบสารสนเทศ (Core Competencies) และสมรรถนะประจำกลุ่มงานหรือเฉพาะงาน (Functional Competencies)

ในการศึกษาครั้งนี้ ผู้ศึกษาได้ดำเนินตามขั้นตอนดังนี้

1. การกำหนดประชากรและการสุ่มกลุ่มตัวอย่าง
2. การเครื่องมือที่ใช้ในการศึกษา
3. การเก็บรวบรวมข้อมูล
4. การวิเคราะห์ข้อมูล

ประชากรและกลุ่มตัวอย่างที่ใช้ในการศึกษา

ประชากร

ประชากรที่ใช้ในการศึกษาองค์ประกอบของสมรรถนะของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ครั้งนี้ คือ บุคลากรด้าน IT ของสถานประกอบที่เป็นลูกค้าของบริษัทที่ผู้ศึกษานั้นทำงานอยู่ โดยสถานประกอบการของลูกค้าของบริษัททั้งหมดนั้นตั้งอยู่ในเขตกรุงเทพมหานคร

กลุ่มตัวอย่าง

การศึกษาครั้งนี้ เลือกกลุ่มตัวอย่างด้วยวิธีการเลือกกลุ่มตัวอย่างแบบสุ่มจากสถานประกอบการของลูกค้า โดยกลุ่มตัวอย่างนี้ ประกอบไปด้วยบุคลากรทางด้าน IT ในทางตรงทั้งหมดและทางอ้อม โดยจำนวนสถานประกอบการที่จะทำการสุ่มนั้น ใช้หลักของ T-Test หรือ Student Distribution (Sample < 30) โดยใน 1 สถานประกอบการ จะทำการสุ่มบุคลากรด้าน IT มา 2 คน ซึ่งประกอบด้วยกลุ่มผู้บริหารที่ทำงานเกี่ยวข้องกับ IT โดยตรงและกลุ่มหัวหน้างาน

หรือผู้เชี่ยวชาญด้าน IT ในองค์กรจากนั้น นำข้อมูลมาทำสถิติบนโปรแกรม SPSS โดยมีหลักเกณฑ์การเลือกกลุ่มตัวอย่างเพื่อให้ได้ข้อมูลที่เป็นประโยชน์กับการศึกษานี้ มีดังต่อไปนี้

1. เป็นบุคลากรด้านคอมพิวเตอร์ โดยทำงานอยู่ในระดับผู้บริหารระดับกลางหรือหัวหน้างานหรือผู้เชี่ยวชาญ และผู้บริหารระดับสูง โดยต้องได้ตัวอย่างครบทั้ง 2 ระดับ

2. เป็นผู้ใช้งานโดยตรง หรือผู้ให้บริการทางด้าน IT กลุ่มงาน Infrastructure หรือกลุ่มงาน Development Team

3. อายุงานตั้งแต่ 1 ปีขึ้นไป

4. มีความรู้ความเข้าใจขั้นพื้นฐานเกี่ยวกับงานด้าน IT

5. เข้าใจความหมายของสมรรถนะ

6. สถานประกอบการของผู้ให้ข้อมูลสำคัญทั้งหมด ตั้งอยู่ในเขตกรุงเทพมหานครที่ผู้ศึกษาได้ทำการสุ่มจากลูกค้าของบริษัทจำนวนรวม 30 แห่ง มีดังนี้

6.1 บริษัท เอเอเอส ออโต้เซอร์วิส จำกัด
6.2 บริษัท เดอะ คอมมูนิเคชั่น โซลูชั่น จำกัด
6.3 บริษัท เอ็นฟอร์ซซิเคียวริตี้ซิสเต็มส์เอพี จำกัด
6.4 สำนักงานประกันสังคม
6.5 บริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน)
6.6 บริษัท เอดีไอ ไทยแลนด์ จำกัด
6.7 บริษัท คอนทัวร์ จำกัด
6.8 บริษัท เจเอฟบีคิทเช่น จำกัด
6.9 บริษัท สามารถ ไอ-โมบาย จำกัด (มหาชน)
6.10 บริษัท โกลบอล อินส์เทค จำกัด
6.11 บริษัท ซีทีเอช จำกัด (มหาชน)
6.12 บริษัท เซน เทคโนโลยี จำกัด
6.13 บริษัท จี.พี.อะไหล่ จำกัด
6.14 บริษัท เวิร์คพอยท์ เอ็นเทอร์เทนเมนท์ จำกัด (มหาชน)
6.15 บริษัท เอสเอ โลจิสติกส์ เน็ตเวิร์ค จำกัด
6.16 บริษัท ไทยคอม เน็ทเวิร์ค จำกัด
6.17 สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)
6.18 บริษัท วินเนอร์ ออนไลน์ จำกัด
6.19 บริษัท มารูเบนิ จำกัด
6.20 บริษัท ไดกิ้นอินดัสทรีส์ (ประเทศไทย) จำกัด
6.21 บริษัท มินิมอร์ จำกัด
6.22 บริษัทโตโยต้า ทูโช อิเล็กทรอนิกส์ (ไทยแลนด์) จำกัด

6.23 บริษัท โพลี เทเลคอม จำกัด
6.24 บริษัท ฟูจิ ซีร็อกซ์ (ประเทศไทย) จำกัด
6.25 บริษัท กรุงไทยธุรกิจบริการ จำกัด
6.26 บริษัท เอไอ คอมพิวเตอร์ จำกัด
6.27 บริษัท เทเวศประกันภัย จำกัด (มหาชน)
6.28 บริษัท ชไนเดอร์ (ไทยแลนด์) จำกัด
6.29 บมจ. ธนาคารกรุงไทย จำกัด (มหาชน)
6.30 บริษัท มายด์เทอร่า จำกัด

การสร้างเครื่องมือที่ใช้ในการศึกษา

การศึกษาเรื่อง “การศึกษาองค์ประกอบของสมรรถนะของบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์” ผู้ศึกษาจัดทำเครื่องมือในการศึกษาครั้งนี้ เป็นแบบสอบถามเชิงคุณภาพ เป็นการสุ่มตัวอย่างแบบเฉพาะเจาะจง ไปยังกลุ่มผู้บริหารระดับกลางและระดับสูง

<u>ขั้นตอนการสร้างเครื่องมือที่ใช้ในการศึกษา</u>

1. การศึกษาทฤษฎี แนวคิด และงานวิจัยที่เกี่ยวข้อง

2. นำนิยามปฏิบัติการที่กำหนดตามกรอบแนวคิดเพื่อนำมาพัฒนาสร้างแบบสอบถามให้ครอบคลุมตามนิยามปฏิบัติการ โดยใช้หัวข้อสถานภาพของผู้กรอกแบบสอบถาม 1 ส่วน และสมรรถนะ 2 ส่วน รวมเป็น 3 ส่วนดังนี้

2.1 เป็นสถานภาพของผู้กรอกแบบสอบถามเพื่อตรวจสอบว่าตรงตามหลักเกณฑ์ที่ได้ตั้งไว้

2.2 การทำทบทวนวรรณกรรม แล้วสรุปได้ว่า สมรรถนะประกอบไปด้วยสมรรถนะ 2 ส่วน คือ สมรรถนะหลัก (Core Competency) และสมรรถนะประจำกลุ่มงานหรือเฉพาะงาน (Functional Competencies)

2.3 เป็นแนวโน้มความต้องการบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ โดยจะสอบถามในภาพรวมของธุรกิจและอุตสาหกรรมในประเทศไทย และภาพรวมขององค์กรหรือบริษัทของผู้กรอกแบบสอบถาม ซึ่งจะตรงกลับวัตถุประสงค์หลักที่ต้องการทราบแนวโน้มความต้องการบุคลากรที่มีความสามารถทางด้านความปลอดภัยบนระบบสารสนเทศของภาคอุตสาหกรรม และภาคบริการการค้าเชิงพาณิชย์

3. นำแบบสอบถามทำการทดสอบ หรือ Pre-Test กับบุคลากรและคณาจารย์ในสายงาน IT เพื่อใช้ในการปรับปรุงเนื้อหาในแบบสอบถามให้ตรงกับวัตถุประสงค์ในการศึกษา และ

จากนั้นนำแบบสอบถามที่มีการแก้ไขและปรับปรุงแล้วนำไปขอความเห็นของอาจารย์ที่ปรึกษาเพื่อตรวจสอบความเที่ยงตรงและถูกต้องของเนื้อหา

4. ทำการแจกแบบสอบถามตามการสุ่มสถานประกอบการที่เป็นลูกค้าของบริษัทที่ผู้ศึกษาสังกัดอยู่ในงานศึกษานี้ ได้ใช้การสุ่มอย่างเฉพาะเจาะจง (Purposive Sampling) โดยใช้ดุลพินิจของผู้ศึกษา ลักษณะของกลุ่มที่เลือกเป็นไปตามวัตถุประสงค์ของการศึกษา การเลือกกลุ่มตัวอย่างแบบเจาะจงต้องอาศัยความรอบรู้ ความชำนาญและประสบการณ์ในเรื่องนั้นๆ ของผู้ศึกษา การเลือกกลุ่มตัวอย่างแบบนี้มีชื่อเรียกอีกอย่างว่า Judgment Sampling

5. ทำการตรวจสอบข้อมูลภายหลังจากการเก็บรวบรวมข้อมูลได้ครบขนาดตัวอย่างตามวัตถุประสงค์ของการศึกษาแล้ว ผู้ศึกษาจะดำเนินการตรวจสอบข้อมูลแบบสอบถาม โดยตรวจสอบว่าข้อมูลที่ได้มาตรงกันหรือไม่ รวมถึงความสอดคล้องกันของข้อมูล

6. ทำการวิเคราะห์ข้อมูลออกมาในเชิงสถิติแล้วนำมาสรุปผลและแนวโน้มที่ได้จากการศึกษา

การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลนี้ ผู้ศึกษาจะทำการนัดผู้ให้ข้อมูลสำคัญ เพื่อทำการเข้าไปโดยนำแบบสอบถามให้ผู้ให้ข้อมูลสำคัญเป็นรายบุคคล โดยมีการนัดหมายและขออนุญาตเข้าไปและกำหนดวัน เวลาและสถานที่ พร้อมเตรียมเอกสารแบบสอบถามให้พร้อมกับจำนวนคนที่ขอให้กรอกแบบสอบถาม และผู้ศึกษาได้ดำเนินการเก็บรวบรวมข้อมูลด้วยตนเอง เพื่อให้ได้ข้อมูลรายละเอียดข้อเท็จจริง ความคิดเห็น และข้อเสนอแนะของผู้ให้ข้อมูลสำคัญ การเก็บรวบรวมข้อมูลในการศึกษาครั้งนี้ ผู้ศึกษาได้ดำเนินการตามขั้นตอนซึ่งมีรายละเอียดดังต่อไปนี้

1. ผู้ศึกษาเดินทางไปทำการเก็บรวบรวมข้อมูล โดยการสัมภาษณ์เชิงลึกกับกลุ่มตัวอย่างผู้ให้ข้อมูลสำคัญ คือ ผู้บริหารระดับสูง และผู้บริหารระดับกลางหรือหัวหน้างานหรือผู้เชี่ยวชาญ ด้วยตนเอง

2. เมื่อให้กลุ่มตัวอย่างทำการกรอกแบบสอบถามเสร็จเรียบร้อยแล้ว ผู้ศึกษาได้ตรวจสอบความสมบูรณ์ถูกต้องของการทำแบบสอบถาม เพื่อนำมาเป็นข้อมูลในการวิเคราะห์ผลต่อไป

3. นำผลที่ได้ไปวิเคราะห์ข้อมูลในขั้นสุดท้ายต่อไป

การวิเคราะห์ข้อมูล

นำประเด็นที่ได้จากการทำแบบสอบถามมาวิเคราะห์ในเชิงสถิติ สรุปหัวข้อของปัจจัยในด้านต่างๆ ตามขั้นตอนดังนี้

1. ศึกษาข้อมูลแบบสอบถามที่ได้จากผู้ให้ข้อมูลสำคัญและนำมาประมวลผลในรูปแบบสถิติเชิงพรรณนา (Descriptive Statistics)

2. พิจารณาจากประเด็นสำคัญที่ได้จากข้อมูลในแบบสอบถามวิเคราะห์ข้อมูล โดยใช้การวิเคราะห์โดยจำแนกตามชนิดข้อมูล (Typological Analysis) แล้วทำการวิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนา (Descriptive Statistics) ด้วยการแจกแจงความถี่ (Frequency) หาค่าร้อยละ (Percentage)

$$P = \frac{f \times 100}{n}$$

P คือ ร้อยละ
f คือ ความถี่ที่ต้องการเปลี่ยนแปลงเป็นค่าร้อยละ
n คือ จำนวนความถี่ทั้งหมด

และวิเคราะห์โดยหาค่าเฉลี่ย (Mean) ของกลุ่มตัวอย่างที่ตอบแบบสอบถามทั้งหมด

$$\bar{x} = \frac{\sum_{t=0}^{n} X_t}{N}$$

$\bar{x}$ คือ ค่าเฉลี่ย
$\sum_{t=0}^{n} X_t$ คือ ผลรวมของคะแนนทั้งหมด
N คือ ขนาดของกลุ่มตัวอย่างทั้งหมด

3. การใช้มาตรวัดทัศนคติของลิเคอร์ท (Likert's Scale) ในการให้ค่าน้ำหนัก โดยการกำหนดระดับต่างๆ ได้แก่

ความสำคัญหรือมีความจำเป็นมาก มีระดับคะแนนเท่ากับ 3
ความสำคัญหรือมีความจำเป็น มีระดับคะแนนเท่ากับ 2
ความสำคัญหรือไม่มีความจำเป็น มีระดับคะแนนเท่ากับ 1

ตามข้อมูลด้านบน ผู้ศึกษาได้แบ่งช่วงคะแนนออกเป็น 3 ช่วง ตามเกณฑ์การให้คะแนน โดยใช้สูตรคำนวณดังนี้

$$\frac{\text{คะแนนสูงสุด – คะแนนต่ำสุด}}{\text{จำนวนช่วง}} = \frac{3 - 1}{3} = 0.67$$

ส่วนการแปลความหมายค่าเฉลี่ยตาม Likert's Scale ได้ดังนี้

ระดับคะแนนเฉลี่ย 1.00-1.66 คะแนน หมายถึง ระดับความสำคัญหรือไม่มีความจำเป็น

ระดับคะแนนเฉลี่ย 1.67-2.33 คะแนน หมายถึง ระดับความสำคัญหรือมีความจำเป็น

ระดับคะแนนเฉลี่ย 2.34-3.00 คะแนน หมายถึง ระดับความสำคัญหรือมีความจำเป็นมาก

สถาบันเทคโนโลยีไทย-ญี่ปุ่น THAI - NICHI INSTITUTE OF TECHNOLOGY TNI

บทที่ 4
ผลการวิเคราะห์ข้อมูล

จากการศึกษาองค์ประกอบของสมรรถนะของบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กรโดยสอบถามความเห็นจากผู้บริหารและผู้เชี่ยวชาญในสายงานคอมพิวเตอร์จากสถานประกอบการที่เป็นลูกค้าขององค์กร จำนวน 30 แห่ง และจำนวนผู้ให้ข้อมูลคำสัญที่ตอบแบบสอบถามจำนวน 43 คน โดยผู้ศึกษาขอนำเสนอผลการวิเคราะห์ข้อมูลโดยใช้สถิติบรรยายด้วยการแจกแจงความถี่ (Frequency) หาค่าร้อยละ (Percentage) และวิเคราะห์โดยหาค่าเฉลี่ย (Mean) ของกลุ่มตัวอย่างที่ตอบแบบสอบถามทั้งหมด ดังนี้

1. สถานภาพของผู้กรอกแบบสอบถาม
2. สมรรถนะหลัก (Core Competency) และสมรรถนะเฉพาะ (Functional Competency) ของบุคลากรในตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์
3. แนวโน้มความต้องการบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ผลการวิเคราะห์ข้อมูล
4. สรุปผลการวิเคราะห์ข้อมูล

สถานภาพของผู้กรอกแบบสอบถาม

ตารางที่ 8 จำนวนร้อยละของกลุ่มตัวอย่างจำแนกตามเพศ

เพศ	จำนวน	ร้อยละ
ชาย	34	79.07
หญิง	9	20.93

(n = 43)

จากตารางที่ 8 แสดงว่า กลุ่มตัวอย่างส่วนใหญ่เป็นเพศชาย คิดเป็นร้อยละ 79.07 รองลงมาเป็นเพศหญิง โดยคิดเป็นร้อยละ 20.93

ตารางที่ 9 จำนวนร้อยละของกลุ่มตัวอย่างจำแนกตามอายุ

ช่วงอายุ	จำนวน	ร้อยละ
21–30 ปี	14	32.56
31–40 ปี	20	46.51
41–50 ปี	5	11.63
50 ปีขึ้นไป	4	9.30

(n = 43)

จากตารางที่ 9 แสดงว่ากลุ่มตัวอย่างส่วนใหญ่อยู่ในช่วงอายุ 31–40 ปี โดยคิดเป็นร้อยละ 46.51 รองลงมาจะอยู่ในช่วงอายุ 21–30 ปี โดยคิดเป็นร้อยละ 32.56, 41 -50 ปี โดยคิดเป็นร้อยละ 11.63 และ 50 ปีขึ้นไป โดยคิดเป็นร้อยละ 9.30 ตามลำดับ

ตารางที่ 10 จำนวนร้อยละของกลุ่มตัวอย่างจำแนกตามระดับการศึกษา

ระดับการศึกษา	จำนวน	ร้อยละ
ปริญญาตรี	23	53.49
ปริญญาโท	20	46.51
ปริญญาเอก	0	0.0

(n = 43)

จากตารางที่ 10 แสดงว่า กลุ่มตัวอย่างส่วนใหญ่มีระดับการศึกษาอยู่ในระดับปริญญาตรี โดยคิดเป็นร้อยละ 53.49 รองลงมาปริญญาโท โดยคิดเป็นร้อยละ 46.51 ซึ่งตามข้อมูลจะไม่มีกลุ่มตัวอย่างที่อยู่ในระดับปริญญาเอก

ตารางที่ 11 จำนวนร้อยละของกลุ่มตัวอย่างจำแนกตามประเภทสถานประกอบการ

ประเภทสถานประกอบการ	จำนวน	ร้อยละ
ภาครัฐ/รัฐวิสาหกิจ	4	9.30
ภาคเอกชน	39	90.70

(n = 43)

จากตารางที่ 11 แสดงว่า กลุ่มตัวอย่างส่วนใหญ่มาจากสถานประกอบการภาคเอกชน โดยคิดเป็นร้อยละ 90.70 รองลงมาเป็น ภาครัฐ/รัฐวิสาหกิจ โดยคิดเป็นร้อยละ 9.30

ตารางที่ 12 จำนวนร้อยละของกลุ่มตัวอย่างจำแนกตามตำแหน่งงาน

ตำแหน่งงาน	จำนวน	ร้อยละ
ผู้จัดการ/ผู้บริหาร	21	48.84
หัวหน้างาน/ผู้เชี่ยวชาญ	22	51.16

(n = 43)

จากตารางที่ 12 แสดงว่า กลุ่มตัวอย่างส่วนใหญ่จะอยู่ในตำแหน่งหัวหน้างาน/ผู้เชี่ยวชาญ โดยคิดเป็นร้อยละ 51.16 และผู้จัดการ/ผู้บริหาร โดยคิดเป็นร้อยละ 48.84 ตามลำดับ

ตารางที่ 13 จำนวนร้อยละของกลุ่มตัวอย่างจำแนกตามประสบการณ์การทำงาน

ประสบการณ์การทำงาน	จำนวน	ร้อยละ
1-2 ปี	8	18.60
3-4 ปี	10	23.26
5 ปีขึ้นไป	25	58.14

(n = 43)

จากตารางที่ 13 แสดงว่ากลุ่มตัวอย่างโดยส่วนใหญ่มีประสบการณ์การทำงาน 5 ปีขึ้นไป โดยคิดเป็นร้อยละ 58.14 รองลงมา 3-4 ปี โดยคิดเป็นร้อยละ 23.26 และ 1-2 ปี โดยคิดเป็นร้อยละ 18.60 ตามลำดับ

สมรรถนะหลัก (Core Competency) และสมรรถนะเฉพาะ (Functional Competency) ของบุคลากรในตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์

ตารางที่ 14 ค่าเฉลี่ยของความรู้พื้นฐานของสมรรถนะหลัก

ความรู้พื้นฐาน (Knowledge)	จำเป็นมาก	จำเป็น	ไม่จำเป็น	ค่าเฉลี่ย
1. พื้นฐานด้านคอมพิวเตอร์เบื้องต้น	30	10	3	2.63
2. พื้นฐานด้าน Networking และ Internetworking	23	19	1	2.51
3. พื้นฐานการใช้งานระบบปฏิบัติการเครือข่าย (Network Operation System)	19	22	2	2.4
4. พื้นฐานด้านการจัดการฐานข้อมูล (Database)	18	22	3	2.35
5. พื้นฐานด้าน TCP/IP Protocol	17	23	3	2.33
6. พื้นฐานการใช้งานระบบปฏิบัติการ (Operation System)	15	26	2	2.3
7. พื้นฐานในการออกแบบระบบเครือข่าย	18	18	7	2.26
8. พื้นฐานการใช้งานโปรแกรมประยุกต์ต่างๆ	15	21	7	2.19
9. พื้นฐานการเขียนโปรแกรมจากภาษาคอมพิวเตอร์ (Programming)	15	15	13	2.05

จากตารางที่ 14 แสดงว่า ความรู้พื้นฐานที่มีคงวามจำเป็นมากสำหรับบุคลากรด้านคอมพิวเตอร์ที่ต้องมีโดยส่วนใหญ่ต้องมีนั้นประกอบด้วยพื้นฐานด้านคอมพิวเตอร์เบื้องต้น โดยมีค่าเฉลี่ยอยู่ที่ 2.63 รองลงมาเป็น พื้นฐานด้าน Networking และ Internetworking โดยมีค่าเฉลี่ยอยู่ที่ 2.51 และ พื้นฐานการใช้งานระบบปฏิบัติการเครือข่าย(Network Operation System) โดยมีค่าเฉลี่ยอยู่ที่ 2.40 และพื้นฐานด้านการจัดการฐานข้อมูล (Database) โดยมีค่าเฉลี่ยอยู่ที่ 2.35 ตามลำดับอยู่ในเกณฑ์ที่มีความจำเป็นมากโดยเฉพาะความรู้ทางด้าน Network และ Database ต่อมาความรู้พื้นฐานที่อยู่ในเกณฑ์มีความจำเป็นประกอบด้วยพื้นฐานด้าน TCP/IP Protocol โดยมีค่าเฉลี่ยอยู่ที่ 2.33 พื้นฐานการใช้งานระบบปฏิบัติการ (Operation System) โดยมีค่าเฉลี่ยอยู่ที่ 2.30 พื้นฐานในการออกแบบระบบเครือข่ายโดยมีค่าเฉลี่ยอยู่ที่ 2.26 พื้นฐานการใช้งานโปรแกรมประยุกต์ต่างๆ โดยมีค่าเฉลี่ยอยู่ที่ 2.19 และพื้นฐานการเขียนโปรแกรมจากภาษาคอมพิวเตอร์ (Programming) โดยมีค่าเฉลี่ยอยู่ที่ 2.05 ซึ่งหมายความว่า ความรู้พื้นฐาน

เหล่านี้ จำเป็นในการทำงานในบางส่วนงานโดยทั้งหมดนั้นคนที่ทำงานในสายงาน IT Security ไม่จำเป็นต้องรู้ทั้งหมดเลยก็ได้ ในส่วนของโดยความรู้พื้นที่มีการใช้งานอย่างจริงจังที่ผู้ศึกษาได้วิเคราะห์มาส่วนใหญ่จะเป็นในเรื่องของพื้นฐานคอมพิวเตอร์ และ Network ซึ่งในเรื่องของ IT Security จะต้องมีความรู้ด้าน Network มากพอสมควรรวมถึงอุปกรณ์ที่เกี่ยวข้องด้วย

ตารางที่ 15 ค่าเฉลี่ยของความรู้พื้นฐานของสมรรถนะเฉพาะ

ความรู้พื้นฐาน (Knowledge)	จำเป็นมาก	จำเป็น	ไม่จำเป็น	ค่าเฉลี่ย
1. พื้นฐานด้านความปลอดภัยบน Network Operation System หรือระบบปฏิบัติการเครือข่าย	19	22	2	2.4
2. พื้นฐานด้านการโจมตีบนระบบสารสนเทศ	19	21	3	2.37
3. พื้นฐานด้านความปลอดภัยบน Operation System หรือระบบปฏิบัติการ	18	23	2	2.37
4. พื้นฐานกฎหมาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550	18	21	4	2.33
5. พื้นฐานด้าน ISO-27000	22	13	8	2.33
6. พื้นฐานด้านโปรโตคอล SSL/TLS, CIFS, HTTP/S, DHCP, SMTP, LDAP/S และ DNS	16	24	3	2.3
7. พื้นฐานความเข้าใจการทำงานของ VPNs, IPSec และ PKI	16	22	5	2.26

จากตารางที่ 15 แสดงว่า ความรู้พื้นฐานด้านความปลอดภัยบนระบบสารสนเทศที่บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศที่ควรจะมีประกอบด้วยพื้นฐานด้านความปลอดภัยบน Network Operation System โดยมีค่าเฉลี่ยอยู่ที่ 2.40 และ รองลงมาเป็นพื้นฐานด้านความปลอดภัยบน Operation System และระบบปฏิบัติการและพื้นฐานด้านการโจมตีบนระบบสารสนเทศโดยมีค่าเฉลี่ยอยู่ที่ 2.37 รองลงมาเป็นพื้นฐานกฎหมาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550 และ พื้นฐานด้าน ISO-27000 โดยมีค่าเฉลี่ยอยู่ที่ 2.33 ตามลำดับ ซึ่งโดยส่วนใหญ่ “พื้นฐานด้านระบบเครือข่ายหรือ Network จะมีความจำเป็นมากสำหรับบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศเป็นส่วนใหญ่เพราะต้องมีการมองและวิเคราะห์ในภาพรวมของระบบเครือข่ายก่อนที่จะมีการออกแบบหรือแผนในการวางระบบความปลอดภัยให้ระบบ และรองลงมาในส่วนของระบบปฏิบัติการที่จะให้ในการจัดการข้อมูลต่าง ๆ

ในองค์กรก็ต้องมีการศึกษาและหาข้อดีข้อเสียของแต่ละระบบปฏิบัติการจากนั้นทำการปิดการให้บริการในบางส่วนเพื่อลดความเสี่ยง” (Stephen, Northcutt. 2009)

ตารางที่ 16 ค่าเฉลี่ยของทักษะความสามารถการจัดการระบบคอมพิวเตอร์ของสมรรถนะหลัก

ทักษะการทำงาน (Skill)	จำเป็นมาก	จำเป็น	ไม่จำเป็น	ค่าเฉลี่ย
ความสามารถการจัดการระบบคอมพิวเตอร์				
1. สามารถติดตั้งระบบปฏิบัติการของคอมพิวเตอร์ต่างๆ ได้	18	15	10	2.19
2. การเขียนโปรแกรมด้วยภาษาคอมพิวเตอร์	17	12	14	2.07
3. สามารถแก้ไขและซ่อมแซมอุปกรณ์คอมพิวเตอร์อื่นๆ ได้	14	17	12	2.05
4. สามารถแก้ไขและซ่อมแซมเครื่องคอมพิวเตอร์	11	19	13	1.95
5. สามารถแก้ไขและซ่อมแซมเครื่องคอมพิวเตอร์เซิร์ฟเวอร์	11	19	13	1.95
6. สามารถ Clone/ Backup Hard Disk	11	12	20	1.79

จากตารางที่ 16 แสดงว่า ทักษะการทำงานด้านความสามารถการจัดการระบบคอมพิวเตอร์ที่บุคลากรด้านคอมพิวเตอร์ต้องมีประกอบด้วย สามารถติดตั้งระบบปฏิบัติการของคอมพิวเตอร์ต่างๆ ได้โดยมีค่าเฉลี่ยอยู่ที่ 2.19 รองลงมาเป็นการเขียนโปรแกรมด้วยภาษาคอมพิวเตอร์มีค่าเฉลี่ยอยู่ที่ 2.07 ได้ระดับค่าคะแนนเฉลี่ยจัดอยู่ในเกณฑ์มีความจำเป็น หมายความว่าความสามารถติดตั้งระบบปฏิบัติการของคอมพิวเตอร์ต่างๆ การแก้ไขการตั้งค่าต่างๆ ขึ้นอยู่กับลักษณะของงานซึ่งอาจจะมีหรือไม่มีความจำเป็นในบางชนิดงานได้ ซึ่งโดยส่วนใหญ่ทักษะการทำงานในด้านระบบปฏิบัติการไม่มีปัจจัยใดที่มีความจำเป็นมาก โดยมีสาเหตุมาจากลักษณะการทำงานของบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศเพราะการทำงานด้านความปลอดภัยบนระบบสารสนเทศ โดยส่วนใหญ่ “บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศจะเป็นกลุ่มคนที่มีประสบการณ์ทำงานหลายปีจึงอาจจะมองว่าทักษะหรืองานประเภทนี้ไม่จำเป็นต้องทำ และสามารถให้คนอื่นๆ หรือพนักงานใหม่ทำแทนกันได้ หรือบางคนมีการศึกษาและเรียนรู้เน้นไปทางด้านเชิงความปลอดภัยเป็นหลักโดยทักษะการทำงานเหล่านี้อาจแค่เรียนรู้เพื่อเอาประสบการณ์เท่านั้น หรือรู้เพียงแค่บางคำสั่งเพื่อใช้ทำงานเท่านั้น ซึ่งระบบปฏิบัติการอาจจะเน้นไปในด้านความปลอดภัยเพียง

อย่างเดียว” (Stephen, Northcutt. 2009) แต่ในทักษะเหล่านี้มีความจำเป็นมากับงานประเภทสนับสนุนระบบสารสนเทศหรือที่เรียกว่า IT Support มากกว่าสายงาน IT Security ที่จะเน้นไปในเชิงการวิเคราะห์และวางแผนมากกว่า IT Support ที่จะปฏิบัติงานอยู่หน้างานเป็นประจำ จากเหตุที่อ้างของ สตีเฟน นอร์ทคัส ทักษะงานโดยส่วนใหญ่ไม่ค่อยมีความจำเป็นมากสำหรับบุคลากรสาย IT Security นักซึ่งแตกต่างจากของกระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐฯ (United States Department of Homeland Security : DHS) ที่มีการอ้างถึง Competencies ที่มีในส่วนของเรื่อง IT System Operation and Maintenance ด้วยซึ่งอาจจะแตกต่างกันไปตามลักษณะงาน

ตารางที่ 17 ค่าเฉลี่ยของทักษะความสามารถด้านการจัดการเครือข่ายของสมรรถนะหลัก

ทักษะการทำงาน (Skill)	จำเป็นมาก	จำเป็น	ไม่จำเป็น	ค่าเฉลี่ย
ความสามารถด้านการจัดการเครือข่าย				
1. สามารถแก้ไขและตั้งค่า VLAN, LAN และ Wireless ได้	13	22	8	2.12
2. สามารถแก้ไขและตั้งค่า Proxy ของระบบเครือข่ายในองค์กรได้	12	21	10	2.05
3. สามารถจัดการระบบ Web Server ขององค์กรได้	9	25	9	2.00
4. การติดตั้งระบบปฏิบัติการสำหรับเครื่องแม่ข่าย	8	23	12	1.91
5. การออกแบบระบบเครือข่าย	7	23	13	1.86

จากตารางที่ 17 แสดงว่า ทักษะการทำงานด้านความสามารถด้านการจัดการเครือข่ายที่บุคลากรด้านคอมพิวเตอร์ต้องมีโดยส่วนใหญ่ประกอบด้วย สามารถแก้ไขและตั้งค่า VLAN, LAN และ Wireless ได้มีค่าเฉลี่ยอยู่ที่ 2.12 ค่าคะแนนเฉลี่ยอยู่ในการเกณฑ์มีความจำเป็น หมายความว่าลักษณะการทำงานของบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศ โดยส่วนใหญ่ “บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศจะเป็นกลุ่มคนที่มีประสบการณ์ทำงานหลายปีจึงอาจจะมองว่าทักษะหรืองานประเภทนี้ไม่จำเป็นต้องทำ และสามารถให้คนอื่นๆ หรือพนักงานใหม่ทำแทนกันได้ หรือบางคนมีการศึกษาและเรียนรู้เน้นไปทางด้านเชิงความปลอดภัยเป็นหลักโดยทักษะการทำงานเหล่านี้อาจแค่เรียนรู้เพื่อเอาประสบการณ์เท่านั้น หรือรู้เพียงแค่บางคำสั่งเพื่อใช้ทำงานเท่านั้น ซึ่งการ

จัดการเครือข่ายอาจจะเน้นการตั้งค่าต่างๆ เพื่อให้สัมพันธ์กับระบบความปลอดภัยที่มีการออกแบบไว้ให้สอดคล้องกันเพียงแค่นั้น" (Stephen, Northcutt. 2009) การจัดการด้านเครือข่ายเป็นการทำงานในระดับ Physical กับเครื่องอุปกรณ์มากกว่าการร่างหรือออกแบบโครงสร้างระบบเครือข่าย ซึ่งในความเป็นจริงตามที่กระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐฯ (United States Department of Homeland Security : DHS) ได้มีการวาง Competencies Areas ที่เกี่ยวกับการตั้งค่าอุปกรณ์ระบบเครือข่ายต่างๆ ที่บุคลากรในสาย IT Security ควรจะทำเป็น แต่จากค่าเฉลี่ยที่ได้จากแบบสอบถามอาจจะเป็นอีกมุมมองหนึ่งที่ไทยมองไม่เหมือนกับทางอเมริกา

ตารางที่ 18 ค่าเฉลี่ยของทักษะการทำงานของสมรรถนะเฉพาะ

ทักษะการทำงาน (Skill)	จำเป็นมาก	จำเป็น	ไม่จำเป็น	ค่าเฉลี่ย
1. วิเคราะห์การความเสี่ยงที่สามารถเกิดขึ้นได้บนระบบคอมพิวเตอร์	14	27	2	2.28
2. สามารถใช้งานคำสั่งในระบบปฏิบัติการเครือข่ายต่างๆ (Network Operation System) ได้	15	24	4	2.26
3. สามารถแก้ไขการตั้งค่าของระบบคอมพิวเตอร์เพื่อลดความเสียหายกับระบบสารสนเทศได้	13	27	3	2.23
4. สามารถใช้งานคำสั่งใน ระบบปฏิบัติการต่างๆ (Operation System) ได้	14	25	4	2.23
5. สามารถอธิบายการโจมตีและสาเหตุที่ทำให้เกิดความเสียต่อระบบแก่ผู้ใช้หรือผู้อื่นๆ ได้	14	25	4	2.23
6. สามารถสืบหาสาเหตุของความเสียหายที่เกิดขึ้นกับระบบสารสนเทศได้	14	24	5	2.21
7. สามารถออกแบบและวางแผนการป้องกันความเสียหายที่อาจจะเกิดขึ้นกับระบบสารสนเทศได้	13	26	4	2.21
8. สามารถแก้ไขและป้องกัน Web Coding ของระบบ Web Server เมื่อเกิดการเปลี่ยนแปลงจากผู้โจมตีได้	12	24	7	2.12
9. วิเคราะห์แยกแยะชนิดของการโจมตีที่เกิดขึ้น	8	31	4	2.09

จากตารางที่ 18 แสดงว่า ทักษะการทำงานด้านความปลอดภัยบนระบบสารสนเทศที่บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศที่ควรจะมีประกอบด้วย วิเคราะห์การความเสี่ยงที่สามารถเกิดขึ้นได้บนระบบคอมพิวเตอร์โดยมีค่าเฉลี่ยอยู่ที่ 2.28 รองลงมาเป็นสามารถใช้งานคำสั่งในระบบปฏิบัติการเครือข่ายต่างๆ (Network Operation System) ได้โดยมีค่าเฉลี่ยอยู่ที่ 2.26 รองลงมาเป็นความสามารถแก้ไขการตั้งค่าของระบบคอมพิวเตอร์เพื่อลดความเสียหายกับระบบสารสนเทศได้ สามารถใช้งานคำสั่งในระบบปฏิบัติการต่างๆ (Operation System) และสามารถอธิบายการโจมตีและสาเหตุที่ทำให้เกิดความเสียต่อระบบแก่ผู้ใช้หรือผู้อื่นๆ โดยมีค่าเฉลี่ยอยู่ที่ 2.23 ได้ตามลำดับ ซึ่งโดยส่วนใหญ่ทักษะการทำงานต่างๆ จะมีความจำเป็นสำหรับบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศเป็นส่วนใหญ่ แต่จากการสังเกตค่าเฉลี่ยซึ่งมีค่าต่ำกว่า 2.34 ซึ่งอาจวิเคราะห์ได้ว่าทักษะเหล่านี้ มีความจำเป็นแต่ไม่จำเป็นว่าบุคลากรในสายงานนี้จะต้องทำได้ทั้งหมดซึ่ง “ในบางทักษะสามารถเรียนรู้ในหน้างานหรือกับเหตุการณ์การโจมตีที่เกิดขึ้นจริงได้ ซึ่งกรณีนี้อาจจะต้องมีผู้เชี่ยวชาญที่มีประสบการณ์คอยให้คำแนะนำ ซึ่งในบางทักษะอาจจะไม่มีความจำเป็นใน Functional Competencies เลยหากลักษณะงานนั้นๆ ไม่มีความจำเป็นต้องใช้งานทักษะหรือความรู้นั้นๆ” (Stephen, Northcutt. 2009) จากเหตุผลของ สตีเฟน นอร์ทคัส บอกถึงทักษะโดยส่วนมากอาจจะไม่มีความจำเป็นมากสำหรับสายงาน IT Security เลยซึ่งผู้ศึกษามองว่าในการกำหนด Functional Competencies ควรดูลักษณะงานขององค์กรนั้นๆก่อนว่าทักษะใดมีความจำเป็นต้องใช้ในการทำงานในสายงาน IT Security จริงๆ

ตารางที่ 19 ค่าเฉลี่ยของคุณลักษณะพื้นฐาน (Attribute)

คุณลักษณะพื้นฐาน (Attribute)	จำเป็นมาก	จำเป็น	ไม่จำเป็น	ค่าเฉลี่ย
1. แก้ปัญหาต่างๆ ได้	21	21	1	2.47
2. คิดวิเคราะห์ได้	20	22	1	2.44
3. ให้คำปรึกษาได้	20	22	1	2.44
4. มีการประสานงานที่ดี	21	19	3	2.42
5. มีการติดตามงาน	19	23	1	2.42
6. มีความยืดหยุ่นผ่อนปรน	19	22	2	2.4
7. มองภาพองค์รวม	15	27	1	2.33
8. เข้าใจผู้อื่น	16	25	2	2.33
9. มีความถูกต้องของงาน	15	27	1	2.33
10. มีความมั่นใจของตนเอง	13	28	2	2.26
11. มีความเป็นผู้นำ	15	24	4	2.26
12. มีศิลปะการสื่อสารจูงใจ	14	24	5	2.21
13. ดำเนินการเชิงรุก	11	29	3	2.19
14. มีการให้อำนาจผู้อื่น	11	28	4	2.16
15. บริหารการเปลี่ยนแปลงได้	10	30	3	2.16

จากตารางที่ 19 แสดงว่า คุณลักษณะพื้นฐานของบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ที่ควรจะมีโดยส่วนใหญ่ต้องมี คือ สามารถแก้ปัญหาต่างๆ ได้โดยมีค่าเฉลี่ยอยู่ที่ 2.47 รองลงมา คือ คิดวิเคราะห์ได้และให้คำปรึกษาได้โดยมีค่าเฉลี่ยอยู่ที่ 2.44 มีการประสานงานที่ดีและมีการติดตามงานโดยมีค่าเฉลี่ยอยู่ที่ 2.42 ตามลำดับ ซึ่งโดยส่วนใหญ่ทักษะการทำงานต่างๆ จะมีความจำเป็นมากสำหรับบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศที่ต้องมี “คุณลักษณะในการเป็นผู้นำและสามารถแก้ปัญหาที่เกิดขึ้นได้ซึ่งบุคลากรในสายงานนี้จะต้องเจอกับเหตุการไม่คาดคิดอยู่ตลอดเวลา คุณลักษณะที่กล่าวมาจึงมีความจำเป็นในการทำงานเป็นอย่างมาก ซึ่งมักพบได้ทั้ง Core Competencies และ Functional Competencies ทั้งในสายงาน IT Secuirty และสายงาน IT อื่นๆ” (Brian, Dutcher. 2010) จากเอกสารงานวิจัยของ ไบรอัน ดัสเชอร์ ได้ยกคุณลักษณะที่เหมาะสมกับบุคลากรในสายงาน IT มาซึ่งมองเห็นถึงความจำเป็นและให้ความสำคัญไปที่ตัวบุคคลเพราะ Core Competencies และ Functional Competencies นั้น สามารถที่จะเรียนรู้ด้วยตัวเองหรือจากผู้อื่นได้ แต่ในส่วนของคุณลักษณะเป็นสิ่งที่ตัวบุคคลจะต้องสร้างมันขึ้นมาเอง ไบรอัน ดัสเชอร์ จึงให้ความสำคัญกับคุณลักษณะมาเป็นอันดับแรก

ตารางที่ 20 ค่าเฉลี่ยของทักษะความสามารถทางด้านภาษา

	จำเป็นมาก	จำเป็น	ไม่จำเป็น	ค่าเฉลี่ย
ความสามารถทางด้านภาษา				
ภาษาอังกฤษ	36	7	0	2.84
ภาษาญี่ปุ่น	5	10	27	1.48
ภาษาจีน	1	10	31	1.29

จากตารางที่ 20 แสดงว่า ทักษะการทำงานด้านความสามารถทางด้านภาษาที่บุคลากรด้านคอมพิวเตอร์ต้องมีโดยส่วนใหญ่ต้องมีสามารถทางด้านภาษาอังกฤษโดยมีค่าเฉลี่ยอยู่ที่ 2.84 รองลงมาเป็นภาษาญี่ปุ่นและจีน ซึ่งทักษะการทำงานในด้าน “ภาษาอังกฤษจะมีความจำเป็นมากสำหรับบุคลากรด้านคอมพิวเตอร์เป็นส่วนใหญ่ ในส่วนของภาษาตะวันออกกลางหรือในแถบเอเชีย จะยังไม่มีความจำเป็นสำหรับบุคลากรในสายงานนี้” (Michael, J. Tippins ; and Ravipreet, S. Sohi. 2003)

แนวโน้มความต้องการบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์

1. บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศจำเป็นต้องมีประสบการณ์การทำงานก่อนหรือไม่

ตารางที่ 21 บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศจำเป็นต้องมีประสบการณ์การทำงานก่อนหรือไม่

	จำนวน	ร้อยละ
จำเป็น	37	86.05
ไม่จำเป็น	6	13.95

(n=43)

จากตารางที่ 21 แสดงว่า บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศ โดยส่วนใหญ่จำเป็นต้องมีประสบการณ์การทำงานมาก่อนที่จะมาทำงานสายงานนี้ โดยมีค่าเฉลี่ยอยู่ที่ 86.05 ซึ่งโดยส่วนใหญ่บุคลากรในสายงานนี้ต้องมีประสบการณ์ในการทำงานด้านคอมพิวเตอร์พอสมควรและมีความรู้ในหลากหลายสาขา รวมถึงต้องมีประสบการณ์ในการแก้ปัญหาที่เกิดขึ้นกับระบบด้วย

โดยสาเหตุที่ผู้ตอบเลือกไม่จำเป็นมีดังนี้ (ตอบได้มากกว่า 1 คำตอบ)

ตารางที่ 22 สาเหตุที่ผู้ตอบเลือกไม่จำเป็น

ไม่จำเป็น	จำนวน	ร้อยละ
สามารถเรียนรู้และฝึกฝนด้วยตัวเองได้	3	50.00
สามารถหาประสบการณ์ได้จากการทำงานจริง	3	50.00
อื่นๆ	1	16.67

(n=6)

จากตารางที่ 22 สืบเนื่องจากตารางที่ 21 จากกรณีที่บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศไม่จำเป็นต้องมีประสบการณ์การทำงานมาก่อนที่จะมาทำงานสายงานนี้ โดยมีการให้เหตุผลหลักๆ ดังนี้ คือ สามารถเรียนรู้และฝึกฝนด้วยตัวเองได้ โดยคิดเป็นร้อยละ 50.00 รวมถึงสามารถหาประสบการณ์ได้จากการทำงานจริง โดยคิดเป็นร้อยละ 16.67

2. ในภาพรวมขององค์กรหรือบริษัทของท่านมีความคิดเห็นว่าบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศมีความจำเป็นกับองค์กรของท่านหรือไม่อย่างไร

ตารางที่ 23 ในภาพรวมขององค์กรหรือบริษัทของท่านมีความคิดเห็นว่าบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศมีความจำเป็นกับองค์กรของท่านหรือไม่อย่างไร

	จำนวน	ร้อยละ
จำเป็น	36	83.72
ไม่จำเป็น	7	16.28

(n=43)

จากตารางที่ 23 ในภาพรวมขององค์กรหรือบริษัทของท่านมีความคิดเห็นว่าบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศโดยส่วนใหญ่จะมีความจำเป็นกับองค์กรของกลุ่มตัวอย่าง โดยคิดเป็นร้อยละ 83.72

โดยสาเหตุที่กลุ่มตัวอย่างตอบเลือกจำเป็นมีดังนี้ (ตอบได้มากกว่า 1 คำตอบ)

ตารางที่ 24 สาเหตุที่กลุ่มตัวอย่างตอบเลือกจำเป็น

จำเป็น	รวม	ร้อยละ
1. เพื่อป้องกันความลับหรือข้อมูลสำคัญขององค์กร	32	88.89
2. เพื่อป้องกันความเสียหายที่อาจจะเกิดจากการโจมตีของผู้ไม่ประสงค์หรือ Hacker	34	94.44
3. ลดต้นทุนในการจัดจ้าง Outsource	19	52.78
4. ลดการรั่วไหลของข้อมูลขององค์กรในกรณีที่มีการจัดจ้าง Outsource	27	75.00
5. ลดช่องโหว่ที่จะใช้ในการโจมตีหรือสร้างความเสียหายแก่องค์กร	29	80.56
6. ป้องกันการแฝงตัวจากบุคคลภายนอกที่ไม่ใช่คนในองค์กร	20	55.56

(n=36)

จากตารางที่ 24 สืบเนื่องจากตารางที่ 23 จากกรณีที่ในภาพรวมขององค์กรหรือบริษัทของท่านมีความคิดเห็นว่าบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศโดยส่วนใหญ่จะมีความจำเป็นกับองค์กรของกลุ่มตัวอย่างโดยมีการให้เหตุผลหลักๆ คือ เพื่อป้องกันความเสียหายที่อาจจะเกิดจากการโจมตีของผู้ไม่ประสงค์หรือ Hacker โดยคิดเป็นร้อยละ 94.44 รองลงมา เพื่อป้องกันความลับหรือข้อมูลสำคัญขององค์กรโดยคิดเป็นร้อยละ 88.89 ลดช่องโหว่ที่จะใช้ในการโจมตีหรือสร้างความเสียหายแก่องค์กร โดยคิดเป็นร้อยละ 80.56 และลดการรั่วไหลของข้อมูลขององค์กรในกรณีที่มีการจัดจ้าง Outsource โดยคิดเป็นร้อยละ 75.00 ซึ่งเป็นเหตุผลส่วนใหญ่ของกลุ่มตัวอย่างที่จำเป็นต้องมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศไว้ในองค์กร

ตารางที่ 25 หากจำเป็นองค์กรของท่านมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศหรือไม่

	จำนวน	ร้อยละ
มี	29	80.56
ไม่มี	7	19.44

(n=36)

จากตารางที่ 25 สืบเนื่องจากตารางที่ 23 จากกรณีที่ในภาพรวมขององค์กรหรือบริษัทของท่านมีความคิดเห็นว่าบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศ โดยส่วนใหญ่จะมีความจำเป็นกับองค์กรของกลุ่มตัวอย่างนั้น โดยส่วนใหญ่จะมี

บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศอยู่ในองค์กร โดยคิดเป็นร้อยละ 80.56

ตารางที่ 26 จากกรณีที่กลุ่มตัวอย่างตอบเลือกมีจะมีความต้องการเพิ่มบุคลากรในด้านความปลอดภัยบนระบบสารสนเทศหรือไม่

	จำนวน	ร้อยละ
1. ต้องการเพิ่มบุคลากร	7	24.14
2. ไม่มีความต้องการเพิ่มบุคลากร	22	75.86

(n=29)

จากตารางที่ 26 สืบเนื่องจากตารางที่ 25 จากกรณีที่กลุ่มตัวอย่างตอบเลือกมี โดยส่วนใหญ่ไม่มีความต้องการเพิ่มบุคลากรในด้านความปลอดภัยบนระบบสารสนเทศ โดยคิดเป็นร้อยละ 75.86

สาเหตุที่กลุ่มตัวอย่างตอบเลือกไม่มีความต้องการเพิ่มบุคลากรมีเหตุผลดังนี้ (ตอบได้มากกว่า 1 คำตอบ)

ตารางที่ 27 สาเหตุที่กลุ่มตัวอย่างตอบเลือกไม่มีความต้องการเพิ่มบุคลากร

ไม่ต้องการเพิ่มบุคลากร	จำนวน	ร้อยละ
1. ไม่มีงบประมาณในด้านนี้	5	17.24
2. มีกำลังคนที่เพียงพอต่อความต้องการอยู่แล้ว	17	58.62
3. องค์กรยังมีขนาดเล็ก	2	6.90

(n=22)

จากตารางที่ 27 สืบเนื่องจากตารางที่ 25 จากกรณีที่กลุ่มตัวอย่างตอบเลือกมี โดยส่วนใหญ่ไม่มีความต้องการเพิ่มบุคลากรในด้านความปลอดภัยบนระบบสารสนเทศได้ให้เหตุผลหลักๆ โดยส่วนใหญ่แต่ละองค์กรจะมีกำลังคนที่เพียงพอต่อความต้องการอยู่แล้ว โดยคิดเป็นร้อยละ 58.62 รองลงมา บางองค์กรจะไม่มีงบประมาณในด้านนี้ โดยคิดเป็นร้อยละ 17.24

ตารางที่ 28 สาเหตุที่กลุ่มตัวอย่างตอบเลือกไม่มี แล้วในปัจจุบันมีบุคลากรด้านนี้โดยการจัดจ้าง Outsource หรือไม่

	จำนวน	ร้อยละ
มี	6	85.71
ไม่มี	1	14.29

(n=7)

จากตารางที่ 28 สืบเนื่องจากตารางที่ 25 จากกรณีที่กลุ่มตัวอย่างไม่มีความต้องการเพิ่มบุคลากรในด้านความปลอดภัยบนระบบสารสนเทศได้ให้เหตุผลหลักๆ โดยส่วนใหญ่แต่ละองค์กรจะมีการจัดจ้าง Outsource เข้ามาทำงานในองค์กรของตน โดยคิดเป็นร้อยละ 85.71

ในกรณีที่กลุ่มตัวอย่างตอบเลือกไม่มี Outsource มีดังนี้ (ตอบได้มากกว่า 1 คำตอบ)

ตารางที่ 29 ในกรณีที่กลุ่มตัวอย่างตอบเลือกไม่มี Outsource

ไม่มี	จำนวน	ร้อยละ
ยังไม่มีความต้องการบุคลากรในด้านนี้	1	100.00
องค์กรไม่ได้ให้ความสำคัญในด้านนี้	0	0.00
ไม่มีงบประมาณเพียงพอที่จะจัดจ้าง Outsource	0	0.00

(n=1)

จากตารางที่ 29 สืบเนื่องจากตารางที่ 28 จากกรณีที่กลุ่มตัวอย่างไม่มีความต้องการเพิ่มบุคลากรในด้านความปลอดภัยบนระบบสารสนเทศได้ให้เหตุผลหลักๆ และไม่มีการจัดจ้าง Outsource เข้ามาทำงานในองค์กรของตนโดยให้เหตุผลหลักๆ คือ ในองค์กรยังไม่มีความต้องการบุคลากรในด้านนี้ โดยคิดเป็นร้อยละ 100.00

หากในภาพรวมขององค์กรหรือบริษัทของท่านมีความจำเป็นที่ต้องมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศท่านคิดว่าองค์กรหรือบริษัทของท่านควรจะพัฒนาคืออะไรบ้าง (ตอบได้มากกว่า 1 คำตอบ)

ตารางที่ 30 หากในภาพรวมขององค์กรหรือบริษัทของท่านมีความจำเป็นที่ต้องมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศท่านคิดว่าองค์กรหรือบริษัทของท่านควรจะพัฒนา

จำเป็น	จำนวน	ร้อยละ
1. พัฒนาทักษะด้านความปลอดภัยบนระบบสารสนเทศแก่บุคลากรคอมพิวเตอร์ในองค์กร	29	80.56
2. จัดการฝึกอบรมด้านความปลอดภัยบนระบบสารสนเทศทั้งระยะสั้นและระยะยาวแก่บุคลากรคอมพิวเตอร์ในองค์กร	30	83.33
3. มีการศึกษาดูงานด้านความปลอดภัยบนระบบสารสนเทศทั้งในและต่างประเทศ	23	63.89

(n=36)

จากตารางที่ 30 สืบเนื่องจากตารางที่ 23 จากกรณีที่กลุ่มตัวอย่างมีความจำเป็นต้องมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศในองค์กรของตนเอง โดยที่กลุ่มตัวอย่างโดยส่วนใหญ่จะแผนที่จะพัฒนา บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศในองค์กรของตนเอง ดังนี้ คือ จัดการฝึกอบรมด้านความปลอดภัยบนระบบสารสนเทศทั้งระยะสั้นและระยะยาวแก่บุคลากรคอมพิวเตอร์ในองค์กรโดยคิดเป็นร้อยละ 83.33 รองลงมา พัฒนาทักษะด้านความปลอดภัยบนระบบสารสนเทศแก่บุคลากรคอมพิวเตอร์ในองค์กร โดยคิดเป็นร้อยละ 80.56 และมีการศึกษาดูงานด้านความปลอดภัยบนระบบสารสนเทศทั้งในและต่างประเทศ โดยคิดเป็นร้อยละ 63.89 ตามลำดับ

ในกรณีไม่มีความจำเป็นที่ต้องมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศโดยมีเหตุผลดังนี้ (ตอบได้มากกว่า 1 คำตอบ)

ตารางที่ 31 ในกรณีไม่มีความจำเป็นที่ต้องมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศโดยมีเหตุผลดังนี้

ไม่จำเป็น	จำนวน	ร้อยละ
1. มีการจัดจ้าง Outsource	3	42.86
2. ไม่มีข้อมูลที่เป็นความลับหรือข้อมูลที่นำไปแสวงหากำไรได้	7	100.00
3. องค์กรมีขนาดเล็ก จึงยังไม่มีความจำเป็น	1	14.29
4. สามารถให้บุคลากรคอมพิวเตอร์ในสายงานอื่นๆ ทำแทนกันได้	1	14.29

(n=7)

จากตารางที่ 31 สืบเนื่องจากตารางที่ 23 จากกรณีที่กลุ่มตัวอย่างไม่มีความจำเป็นต้องมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศในองค์กรของตนเอง โดยที่กลุ่มตัวอย่างโดยส่วนใหญ่ให้เหตุผลว่าในองค์กรของตนไม่มีข้อมูลที่เป็นความลับหรือข้อมูลที่นำไปแสวงหากำไรได้ โดยคิดเป็นร้อยละ 100 รองลงมา ในบางองค์กรมีการจัดจ้าง Outsource มาทำงานด้านความปลอดภัยบนระบบสารสนเทศ โดยคิดเป็นร้อยละ 42.86 จากการวิเคราะห์อาจจะเกิดจากการที่องค์กรมีขนาดเล็กจึงยังไม่มีความจำเป็นต้องมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศในองค์กรของตนเอง ในบางองค์กรที่ต้องมีการรับรองมาตรฐานด้านความปลอดภัยบนระบบสารสนเทศเลือกที่จะจัดจ้าง Outsource แทนที่จะจัดหามาเป็นพนักงานของตนเองเพราะต้องมาจัดฝึกอบรมเองและเห็นผลช้า ซึ่งมีสิทธิ์ที่จะไม่ประสบความสำเร็จจากการฝึกอบรมเลย

3. <u>ท่านคิดว่ามหาวิทยาลัยหรือสถาบันการศึกษาที่ท่านรู้จักมีการผลิตบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศหรือไม่</u>

ตารางที่ 32 ท่านคิดว่ามหาวิทยาลัยหรือสถาบันการศึกษาที่ท่านรู้จักมีการผลิตบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศหรือไม่

	จำนวน	**ร้อยละ**
มี	9	20.93
ไม่มี	34	79.07

(n=43)

จากตารางที่ 32 โดยส่วนใหญ่จะไม่รู้จักมหาวิทยาลัยหรือสถาบันการศึกษาที่มีการเรียนการสอนหรือผลิตบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศออกมาไม่ค่อยเด่นชัดนักโดยคิดเป็นร้อยละ 79.07 (โดยอ้างจากตารางที่ 30) ที่ผู้ให้ข้อมูลสำคัญได้ให้เหตุผลและให้ความสำคัญกับการพัฒนาบุคลากรทางด้านนี้ในสถาบันอุดมศึกษา แต่อาจจะด้วยสาเหตุที่ว่าในบางมหาวิทยาลัยหรือสถาบันการศึกษา นำวิชาทางด้านความปลอดภัยบนระบบสารสนเทศเป็นเพียงวิชาเลือกในเอกหรือคณะทางด้านคอมพิวเตอร์ และมหาวิทยาลัยหรือสถาบันการศึกษาอาจจะยังไม่มีการพัฒนาบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศอย่างจริงจัง รวมถึงไม่มีการสนับสนุนจากทางภาครัฐและภาคธุรกิจอย่างจริงจัง หรือเล็งเห็นว่าศักยภาพของประเทศไทยยังไม่พร้อม เป็นเหตุให้มีการว่าจ้างผู้ดูแลระบบสารสนเทศด้านความปลอดภัยจากต่างประเทศที่มีการรับรองในระดับสากลมากกว่าที่จะเสี่ยงที่จะจัดหามาเองหรือจัดจ้างบริษัทสัญชาติไทย ซึ่งยังไม่ค่อยมีความน่าเชื่อถือเหมือนกับบริษัทต่างประเทศ

จากการสืบค้น พบว่า วิชาในสายงานความปลอดภัยบนระบบสารสนเทศในมหาวิทยาลัยชั้นนำของประเทศจะถูกบรรจุอยู่ในวิชาเลือกของแต่ละสาขาทั้งในคณะวิศวกรรมศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี คณะเทคโนโลยีสารสนเทศ และสาขาหรือคณะที่เกี่ยวข้องอื่นๆ แต่ยังมีมหาลัยเอกชนบางแห่งที่มีการเปิดสอนในด้านความปลอดภัยโดยจัดเป็นสาขาของคณะในสายงานคอมพิวเตอร์ ได้แก่ มหาเทคโนโลยีมหานคร เปิดสอนหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาความมั่นคงทางระบบสารสนเทศ (Master of Science Program in Information Systems Security) ซึ่งจะเปิดสอนแค่ในระดับปริญญาโท

มหาวิทยาลัยเทคโนโลยีมหานครเป็นมหาวิทยาลัยในประเทศไทยแห่งแรกและแห่งเดียวที่มุ่งเน้นในการสร้างผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ที่ผ่านมาได้ผลิตมหาบัณฑิตที่มีความเชี่ยวชาญออกไปปฏิบัติงานในองค์กรขนาดใหญ่ทั้งภาครัฐและเอกชนเป็นจำนวนมาก ในด้านการวิจัยและพัฒนามหาวิทยาลัยได้มีความร่วมมือทางด้านการวิจัยและพัฒนากับหน่วยงานต่างๆ มากมาย เช่น กองทัพบก สถาบันเทคโนโลยีป้องกันประเทศ บริษัท Cisco Systems Thailand จำกัด ศูนย์เทคโนโลยีคอมพิวเตอร์และอิเล็กทรอนิกส์แห่งชาติ (NECTEC) สถาบันนิติวิทยาศาสตร์ กรมสอบสวนคดีพิเศษ (DSI) ในขณะเดียวกันมหาวิทยาลัยเทคโนโลยีมหานครก็ยังเป็นศูนย์ฝึกอบรมใบรับรองทางด้านความมั่นคงปลอดภัยระบบสารสนเทศเทศชื่อดังอย่าง EC-Council ที่มีใบรับรองทางที่เป็นที่รู้จักและยอมรับจากอุตสาหกรรมอย่างเช่น Certified Ethical Hacker (CEH), Certified Hacking Forensic Investigator (CHFI), EC-Council Certified Secure Programmer (ECSA), EC-Council Certified Security Analyst (ECSA) และ Licensed Penetration Tester (LPT) (ศุภกร กังพิศดาร. 2552)

สรุปสาเหตุสำคัญที่ทำให้วิชาด้าน IT Security ไม่ค่อยมีการเปิดเป็นสาขาหลักในคณะหรือหลักสูตรที่เกี่ยวข้องกับคอมพิวเตอร์นั้น เนื่องจากขาดแคลนบุคลากรที่มีความเชี่ยวชาญในสาขา IT Security รวมถึงเงื่อนไขในการเปิดหลักสูตรที่ต้องมีผู้เชียวชาญหรือคณาจารย์ระดับดุษฎีบัณฑิตอย่างน้อย 3 คน และคณะกรรมการหลักสูตรอีก 2 คน รวมเป็น 5 คน ซึ่งทำให้การเปิดหลักสูตรหรือสาขาที่เกี่ยวข้องกับ IT Security โดยตรงไม่ค่อยมีมากนักในเมืองไทย โดยส่วนใหญ่มักจะถูกระบุอยู่ในวิชาเลือกของคณะหรือหลักสูตรที่เกี่ยวข้องกับคอมพิวเตอร์เท่านั้น และมีเปิดเฉพาะในหลักสูตรปริญญาโทโดยเหตุผลที่ต้องมีประสบการณ์ในการทำงานก่อน

สรุปผลการวิเคราะห์ข้อมูล

1. การศึกษาและวิเคราะห์ผลของข้อมูลสมรรถนะหลัก (Core Competency : C) สมรรถนะเฉพาะ (Functional Competency : F) และคุณลักษณะ (Attribute : A) โดยแบ่งตามค่าเฉลี่ยและความจำเป็น ในแต่ละหัวข้อมีดังนี้

ตารางที่ 33 สมรรถนะที่มีความจำเป็นมาก

สมรรถนะที่มีความจำเป็นมาก	ค่าเฉลี่ย
1. พื้นฐานด้านคอมพิวเตอร์ (C)	2.63
2. พื้นฐานด้าน Networking และ Internetworking (C)	2.51
3. แก้ปัญหาต่างๆ ได้ (A)	2.47
4. คิดวิเคราะห์ได้ (A)	2.44
5. ให้คำปรึกษาได้ (A)	2.44
6. มีการประสานงานที่ดี (A)	2.42
7. มีการติดตามงาน (A)	2.42
8. พื้นฐานการใช้งานระบบปฏิบัติการเครือข่าย (C)	2.40
9. พื้นฐานด้านความปลอดภัยบนระบบปฏิบัติการเครือข่าย (F)	2.40
10. มีความยืดหยุ่นผ่อนปรน (A)	2.40
11. พื้นฐานด้านการโจมตีบนระบบสารสนเทศ (F)	2.37
12. พื้นฐานด้านความปลอดภัยบนระบบปฏิบัติการ (F)	2.37
13. พื้นฐานด้านการจัดการฐานข้อมูล (C)	2.35

จากตารางที่ 33 แสดงให้เห็นว่าถึงสมรรถนะที่มีความจำเป็นมากสำหรับบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ ซึ่งประกอบด้วยพื้นฐานด้านคอมพิวเตอร์ มีค่าเฉลี่ย 2.63 ซึ่งเป็นพื้นฐานที่บุคลากรคอมพิวเตอร์ทุกคนควรจะมี รองลงมาพื้นฐานด้าน Networking และ Internetworking มีค่าเฉลี่ย 2.51 ซึ่งเป็นพื้นฐานสำคัญของบุคลากรสาย IT Security ที่มีการใช้งานพื้นฐานนี้กับการป้องกันความปลอดภัยบนระบบเครือข่ายสารสนเทศ ต่อมาเป็นพื้นฐานการใช้งานระบบปฏิบัติการเครือข่าย มีค่าเฉลี่ย 2.40 โดยบุคลากรสายงานนี้ต้องมีความสามารถทางด้านระบบปฏิบัติการต่างๆ เพื่อที่จะสามารถสนับสนุนระบบเครือข่ายๆ ต่างๆ ได้ สุดท้ายเป็นพื้นฐานด้านการจัดการฐานข้อมูล มีค่าเฉลี่ย 2.35 ซึ่งความรู้ด้านนี้มีความสำคัญในการจัดการบริหารข้อมูลรวมถึงการป้องกันความปลอดภัยของข้อมุลสารสนเทศต่างๆ ด้วย ซึ่งทั้งหมดนี้เป็นสมรรถนะหลักที่มีความจำเป็นมากในบุคลากรสายงาน IT Security ในส่วนของคุณลักษณะได้แก่การแก้ปัญหาต่างๆ ได้ มีค่าเฉลี่ย 2.47 คิดวิเคราะห์ได้ มีค่าเฉลี่ย 2.44 ให้คำปรึกษามีค่าเฉลี่ย 2.44 มีการประสานงานที่ดี มีค่าเฉลี่ย 2.42 มีการติดตามงานมีค่าเฉลี่ย 2.42 และมีความยืดหยุ่นผ่อนปรนมีค่าเฉลี่ย 2.40 จากการสังเกตพบว่า คุณลักษณะต่างๆ มีค่าเฉลี่ยสูงมาก และมีมากกว่าสมรรถนะหลักและเฉพาะนั้น หมายความว่า ในบุคลากรสายงาน IT Security นั้น มีการให้ความสำคัญกับคุณลักษณะในตัวบุคคลมากกว่าความรู้และทักษะ ซึ่งอาจมีสาเหตุมาจากการเรียนรู้งานที่สามารถเรียนรู้ได้จาก

หน้างานและคำแนะนำจากผู้เชี่ยวชาญหรือหัวหน้าที่มีส่วนช่วยในการเสริมความรู้และทักษะให้กับตัวบุคคล แต่ในส่วนของคุณลักษณะเป็นสิ่งที่ตัวบุคคลหรือบุคลากรด้านนี้ ต้องฝึกด้วยตัวเอง ในส่วนของสมรรถนะเฉพาะนั้นประกอบด้วย พื้นฐานด้านความปลอดภัยบนระบบปฏิบัติการเครือข่าย มีค่าเฉลี่ย 2.40 พื้นฐานด้านการโจมตีบนระบบสารสนเทศมีค่าเฉลี่ย 2.37 และพื้นฐานด้านความปลอดภัยบนระบบปฏิบัติการมีค่าเฉลี่ย 2.37 ซึ่งพบได้น้อยในค่าเฉลี่ยที่มีความจำเป็นมากซึ่งประกอบกับเหตุผลในส่วนของคุณลักษณะที่การเรียนรู้ในส่วนของทฤษฎีและทักษะสามารถเรียนรู้เองได้และยังไม่สำคัญเท่ากับคุณลักษณะที่จำเป็นในงานสายนี้

ตารางที่ 34 สมรรถนะที่มีความจำเป็น

สมรรถนะที่มีความจำเป็น	ค่าเฉลี่ย
1. พื้นฐานด้าน TCP/IP Protocol (C)	2.33
2. พื้นฐานกฎหมาย พรบ.คอมพิวเตอร์ พ.ศ.2550 (F)	2.33
3. พื้นฐานด้าน ISO-27000 (F)	2.33
4. มองภาพองค์รวม (A)	2.33
5. เข้าใจผู้อื่น (A)	2.33
6. มีความถูกต้องของงาน (A)	2.33
7. พื้นฐานการใช้งานระบบปฏิบัติการ (C)	2.30
8. พื้นฐานด้านโปรโตคอล SSL/TLS, CIFS, HTTP/S, DHCP, SMTP, LDAP/S และ DNS (F)	2.30

จากตารางที่ 34 แสดงให้เห็นว่าถึงสมรรถนะที่มีความจำเป็นสำหรับบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ซึ่งประกอบด้วย พื้นฐานด้าน TCP/IP Protocol มีค่าเฉลี่ย 2.33 ซึ่งมีส่วนในการเรียนรู้ให้สอดคล้องกับพื้นฐานด้าน Networking และ Internetworking และพื้นฐานด้านการใช้งาน Internet Service (จากตารางที่ 4.30)ที่มีการใช้งาน TCP/IP Protocol ในการตั้งค่าต่าง ๆในระบบเครือข่าย และพื้นฐานการใช้งานระบบปฏิบัติการมีค่าเฉลี่ย 2.30 ซึ่งมีส่วนในการเรียนรู้พื้นฐานด้านความปลอดภัยบนระบบปฏิบัติการ (จากตารางที่ 33) ซึ่งเป็นส่วนของสมรรถนะหลักที่มีความจำเป็นสำหรับบุคลากรสายงานนี้ ต่อในส่วนของสมรรถนะเฉพาะซึ่งประกอบด้วย พื้นฐานกฎหมาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550 มีค่าเฉลี่ย 2.33 พื้นฐานด้าน ISO-27000 มีค่าเฉลี่ย 2.33 และพื้นฐานด้านโปรโตคอล SSL/TLS, CIFS, HTTP/S, DHCP, SMTP, LDAP/S และ DNS มีค่าเฉลี่ย 2.30 ซึ่งในส่วนของข้อกฎหมายและมาตรฐานเป็นสิ่งจำเป็นในการบริหารงานข้อมูลสารสนเทศและความปลอดภัยของข้อมูลสารสนเทศ ซึ่งสิ่งที่จำเป็นในการทำงานทั้งในสายงาน IT ปกติและ IT Security ต่อมาในส่วนของคุณลักษณะประกอบด้วย มองภาพองค์รวม เข้าใจผู้อื่นและ

ความถูกต้องของงาน โดยมีค่าเฉลี่ย 2.33 เท่ากัน ซึ่งเป็นคุณลักษณะที่จำเป็นในการทำงานไม่ว่าในงานด้าน IT หรือ IT Security ก็ตามก็ต้องมีการมองภาพองค์รวมหรือการมองทั้งองค์กรในเชิงสารสนเทศ รวมถึงการสื่อสารกับผู้อื่นที่มีเกี่ยวข้องไปถึงการให้คำแนะนำและการสอนงานต่างๆ ทั้งนี้ที่สำคัญ คือ ความถูกต้องของงานซึ่งจะขึ้นอยู่กับความสามารถของแต่ละบุคคลจะมีความรอบคอบมากน้อยแค่ไหน ซึ่งคุณลักษณะเหล่านี้เป็นสิ่งที่บุคลากรในสายงาน IT จะต้องทำให้ได้

ในส่วนที่มีความจำเป็นแต่มีค่าเฉลี่ยอยู่ต่ำสุดเลยในส่วนใหญ่จะอยู่ในส่วนของสมรรถนะหลักประกอบด้วย พื้นฐานการออกแบบโปรแกรมมีค่าเฉลี่ย 1.88 การออกแบบระบบเครือข่ายมีค่าเฉลี่ย 1.86,ความสามารถในการทำ Cluster และ Load Balance ได้มีค่าเฉลี่ย 1.84 และ สามารถ Clone/Backup Hard Disk มีค่าเฉลี่ย 1.79 ซึ่งมีสาเหตุมาจากเนื้องานและทักษะส่วนใหญ่จะไปในทางนักเขียนโปรแกรม (Programmer) และเจ้าหน้าที่สนับสนุนด้านคอมพิวเตอร์ (IT Support/IT Helpdesk) ซึ่งอาจจะจำเป็นหรือไม่จำเป็นเลยสำหรับบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ ซึ่งอาจจะขึ้นอยู่กับงานที่ทำมีความเกี่ยวข้องกับทักษะที่ว่ามา ว่าจะต้องใช้ในการทำงานจริงหรือไม่

2. การศึกษาแนวโน้มความต้องการบุคลากรมีความสามารถทางด้านความปลอดภัยบนระบบสารสนเทศทั้งในระดับองค์กรและระดับประเทศยังคงมีความต้องการเป็นส่วนใหญ่ เนื่องมาจากเทคโนโลยีใหม่ที่มีการเพิ่มจำนวนขึ้นอย่างต่อเนื่อง ประกอบกับความรวดเร็วในการสื่อสารทำให้ พบว่า มีช่องโหว่เกิดขึ้นใหม่ทุกๆ นาที รวมถึงผลกระทบที่เกิดขึ้นส่งผลร้ายถึงความเชื่อมั่นขององค์กรเอง รวมถึงภาพลักษณ์ของประเทศได้เลยทีเดียว จึงทำให้บุคลากรสายงานนี้ยังมีความต้องการเป็นจำนวนมากไม่ว่าจะเป็นการรับบุคลากรเข้ามาทำงานในองค์กรหรือการจัดจ้างมาจากทาง Outsource เอง ซึ่งก็มีบางส่วนที่ยังคงไม่มีความต้องบุคลการในสายงานนี้อย่างจริงจัง เนื่องจากขนาดขององค์กรและความสำคัญของข้อมูลที่องค์กรมียังไม่ใช่เป้าหมายในการโจมตีของผู้ไม่ประสงค์ดีหรือ Hacker และบางองค์กรยังคงมีการจัดจ้าง Outsource มาทำงานแทนบ้างในบางกรณีที่องค์กรมีข้อผูกมัดกับตัวบทกฎหมายหรือมาตรฐานที่ต้องได้รับการยอมรับจากลูกค้า เพื่อรักษาความเชื่อมั่นขององค์กรเพียงเท่านั้น

3. ในส่วนของคุณลักษณะพื้นฐาน (Attribute) มีความจำเป็นกับบุคลากรผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์รวมถึงบุคลากรคอมพิวเตอร์ที่เกี่ยวข้อง ซึ่งคุณลักษณะทั้งหมดนั้นขึ้นอยู่กับตัวบุคคลเองว่าจะสามารถทำได้หรือไม่ ซึ่งต่างจากความรู้ทฤษฎี และทักษะที่สามารถเรียนรู้ได้จากผู้เชี่ยวชาญหรือจากหน้างานได้เลย และมีหนังสือที่สามารถเข้าไปหาอ่านหาความรู้เพิ่มเติมได้ จึงสรุปว่าคุณลักษณะพื้นฐานต่างๆ ต้องแล้วแต่การพัฒนาของแต่ละคน แล้วจึงนำมาประกอบการตัดสินใจในการเลื่อนระดับหรือเลื่อนตำแหน่งว่าบุคคลดังกล่าวมีคุณลักษณะที่พร้อมในระดับหรือตำแหน่งงานที่สูงขึ้นหรือไม่ ประกอบกับความรู้ความสามารถที่พร้อมไปทำงานในระดับที่มีทั้งความเสี่ยงและความยากมากขึ้นหรือไม่

บรรณานุกรม

บรรณานุกรม

กรมโรงงานอุตสาหกรรม (ศส.กรอ.). (2551). **สมรรถนะพื้นฐานของนักวิชาการคอมพิวเตอร์ (Common Competency for IT Professional)**. สืบค้นเมื่อ 13 กุมภาพันธ์ 2557, จาก http://www2.diw.go.th/Policy/news/Competency/Functional%20Competency/Specific%20Competency/ด้านสารสนเทศ.pdf

ณรงค์วิทย์ แสนทอง. (2547). **มารู้จัก COMPETENCY กันเถอะ**. กรุงเทพฯ : เอช อาร์ เซ็นเตอร์.

ธำรงศักดิ์ คงคาสวัสดิ์. (2548). **เริ่มต้นอย่างไร เมื่อนำ Competency มาใช้ในองค์กร**. กรุงเทพฯ : สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น).

บุญเสริม วีสกุล. (2517). **สถิติตอนที่ 1 วิธีเก็บและประมวลผลข้อมูล**. กรุงเทพฯ : ไทยวัฒนาพาณิช.

พสุ เดชะรินทร์. (2546). **กลยุทธ์ใหม่ในการจัดการ**. กรุงเทพ ฯ : ฮาซันพริ้นติ้ง.

มหาวิทยาลัยราชภัฏพระนคร. (ม.ป.ป.). **สมรรถนะของบุคลากรมหาวิทยาลัยราชภัฏพระนคร**. สืบค้นเมื่อ 1 กุมภาพันธ์ 2557, จาก http://www.pnru.ac.th/offi/person/upload-files/uploaded/joy/1.สมรรถนะและระดับสมรรถนะ.pdf

รัตนาภรณ์ ศรีพยัคฆ์. (2548). **การปรับใช้สมรรถนะในการบริหารทรัพยากรมนุษย์**. นนทบุรี : สำนักงานข้าราชการพลเรือน.

ศุภกร กังพิศดาร. (2552). **Security is All Around**. สืบค้นเมื่อ 13 กุมภาพันธ์ 2557, จาก http://www.it.mut.ac.th/about/170-security

สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น). (2554). **ความหมายของสมรรถนะ**. สืบค้นเมื่อ 1 กุมภาพันธ์ 2557, จาก http://www.tpa.or.th/writer/read_this_book_topic.php?passTo=c63d4f3d1df7691d2c964ebd1731eb54&pageid=2&bookID=1288&read=true&count=true

สุกัญญา รัศมีธรรมโชติ. (2547). **Competency : เครื่องมือการบริหารที่ปฏิเสธไม่ได้**. กรุงเทพ ฯ : สถาบันเพิ่มผลผลิตแห่งชาติ.

อานนท์ ศักดิ์วรวิชญ์. (2547). **แนวคิดเรื่องสมรรถนะ Competency : เรื่องเก่าที่เรายังหลงทาง**. กรุงเทพ ฯ : จุฬาลงกรณ์มหาวิทยาลัย.

อาภรณ์ ภู่วิทยพันธุ์. (2547). **Career Development in Practice**. กรุงเทพ ฯ : เอช อาร์ เซ็นเตอร์.

อุบลรัตน์ จันทร์เมือง. (2555). **การพัฒนาสมรรถนะของบุคลากรวิทยาลัยการอาชีพวังสะพุง**. เลย : วิทยาลัยการอาชีพวังสะพุง.

Barrett, G. V. ; and Depinet, R. L. (1991, October). A Reconsideration of Testing for Competence rather than for Intelligence. **American Psychologist**. 46(10) : 1,012-1,024.

Boyatizis, R. E. (1982). **The Competent Manager**. New York : McGraw-Hill.

Brenda, Oldfield. (2007). **Competency and Functional Framework for IT Security Workforce Development**. Washington, DC : United States Department of Homeland Security.

Brian, Dutcher. (2010). **Determining the Role of the IA/Security Engineer**. Vermont : Norwich University.

Dales, M. ; and Hes, K. (1995). **Creating Training Miracles**. Sydney : Prentice Hall.

David, C. McClelland. (1973). Testing for Competence rather than for Intelligence. **American Psychologist**. 28(1) : 1-14.

Gary, Hamel ; and C. K. Prahalad. (1994). **Competing for the Future**. Boston : Harvard Business Press.

John, Berry. (2011). **Competency Model for Cybersecurity**. Washington, DC : United States Office of Personnel Management.

Keith, A. Morneau. (2004). **Designing an Information Security Program as a Core Competency of Network Technologists**. Minnesota : University of Capella.

Klara, Antlova. (2010). ICT Competencies and Knowledge Alignment in Small and Medium Enterprises. **Information and Communication Technologies for the Advanced Enterprise**. 1(1) : 125-138.

Michael, J. Tippins. (1999). **Information Management Within the Distribution Channel : The Effects of Information Technology and Customer Learning on Channel Performance Outcomes**. Nebraska : The University of Nebraska-Lincoln.

Michael, J. Tippins ; and Ravipreet, S. Sohi. (2003). IT Competency and Firm Performance : Is Organizational Learning A Missing Link?. **Strategic Management Journal**. 24(8) : 745-761.

Mitrani, A. ; Dalziel, M. ; and Fitt, D. (1992). **Competency Based Human Resource Management : Value Driven Strategies for Recruitment, Development, and Reward**. London : McGraw-Hill.

National Aeronautics and Space Administration. (2010). **NASA's System Engineer Competencies**. Retrieved January 18, 2014, from http://www.nasa.gov/pdf/303747main_Systems_Engineering_Competencies.pdf

National Oceanic and Atmospheric Administration. (2012). **IT Security Competency Model**. Retrieved January 23, 2014, from http://www.wfm.noaa.gov/SHCM/compet_model/IT_SecurityCompetencyModel.pdf

Scott, B. Parry. (1992). **Evaluating the Impact If Training**. Alexxandria : American Society for Training and Development.

Spencer, M. ; and Spencer, M. S. (1993). **Competence at Work : Models for Superiors Performance**. New York : John Wiley and Sons.

Stephen, Northcutt. (2009). **Varied Paths Taken to Information Security Competency**. Retrieved January 15, 2014, from http://www.sans.edu/research/management-laboratory/article/path-to-infosec

ภาคผนวก

ภาคผนวก ก.

แบบสอบถามที่ใช้ในการศึกษา

แบบสอบถาม

เรื่องที่ศึกษา : การศึกษาองค์ประกอบของสมรรถนะของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภายในองค์กร กรณีศึกษา บริษัท มายด์เทอร่า จำกัด

ส่วนที่ 1 สถานภาพของผู้กรอกแบบสอบถาม

1.1 เพศ ☐ชาย ☐หญิง

1.2 อายุ ☐21 – 30 ปี ☐31 – 40 ปี ☐41 – 50 ปี ☐50ปีขึ้นไป

1.3 ระดับการศึกษา ☐ ปริญญาตรี ☐ปริญญาโท ☐ปริญญาเอก

1.4 สถานประกอบการ

☐ ภาครัฐ/รัฐวิสาหกิจ (โปรดระบุชื่อหน่วยงานหรือบริษัท)_____

☐ ภาคเอกชน (โปรดระบุชื่อบริษัท)_____

(โปรดระบุประเภทธุรกิจ)_____

1.5 ตำแหน่งงาน ☐ผู้จัดการ/ผู้บริหาร ☐หัวหน้างาน/ผู้เชี่ยวชาญ

1.6 ประสบการณ์การทำงาน ☐1 – 2 ปี ☐3 – 4 ปี ☐5 ปีขึ้นไป

ส่วนที่ 2 สมรรถนะหลักของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ภาย (Core Competency)

2.1 ความรู้พื้นฐาน (Knowledge)	**จำเป็นมาก**	**จำเป็น**	**ไม่จำเป็น**
2.1.1 พื้นฐานด้านคอมพิวเตอร์เบื้องต้น			
2.1.2 พื้นฐานด้าน Networking และ Internetworking			
2.1.3 พื้นฐานด้าน TCP/IP Protocol			
2.1.4 พื้นฐานด้านการจัดการฐานข้อมูล (Database)			
2.1.5 พื้นฐานในการออกแบบระบบเครือข่าย			
2.1.6 พื้นฐานการใช้งานระบบปฏิบัติการเครือข่าย (Network Operation System)			
2.1.7 พื้นฐานการใช้งานระบบปฏิบัติการ (Operation System)			
2.1.8 พื้นฐานการเขียนโปรแกรมจากภาษาคอมพิวเตอร์ (Programming)			
2.1.9 พื้นฐานการใช้งานโปรแกรมประยุกต์ต่างๆ			
2.1.10 อื่นๆ (โปรดระบุ)_____			

2.2 ทักษะการทำงาน (Skill)	จำเป็นมาก	จำเป็น	ไม่จำเป็น
ความสามารถการจัดการระบบคอมพิวเตอร์			
2.2.1 สามารถ Clone/ Backup Hard Disk			
2.2.2 สามารถติดตั้งระบบปฏิบัติการของคอมพิวเตอร์ต่างๆ ได้ เช่น Windows, Linux เป็นต้น			
2.2.3 สามารถแก้ไขและซ่อมแซมเครื่องคอมพิวเตอร์			
2.2.4 สามารถแก้ไขและซ่อมแซมเครื่องคอมพิวเตอร์เซิร์ฟเวอร์			
2.2.5 การเขียนโปรแกรมด้วยภาษาคอมพิวเตอร์ เช่น C++, C#, Java Script และ Shell Script เป็นต้น			
2.2.6 สามารถแก้ไขและซ่อมแซมอุปกรณ์คอมพิวเตอร์อื่นๆ ได้ เช่น Printer, Scanner, Router, Switch เป็นต้น			
2.2.7 อื่นๆ (โปรดระบุ)_____			
ความสามารถด้านการจัดการเครือข่าย			
2.2.8 การออกแบบระบบเครือข่าย			
2.2.9 การติดตั้งระบบปฏิบัติการสำหรับเครื่องแม่ข่าย			
2.2.10 สามารถแก้ไขและตั้งค่า VLAN, LAN และ Wireless ได้			
2.2.11 สามารถแก้ไขและตั้งค่า Proxy ของระบบเครือข่ายในองค์กรได้			
2.2.12 สามารถจัดการระบบ Web Server ขององค์กรได้			
2.2.13 อื่นๆ (โปรดระบุ)_____			
ความสามารถทางด้านภาษา			
2.2.14 ภาษาอังกฤษ			
2.2.15 ภาษาอื่นๆ (โปรดระบุ)_____			

ส่วนที่ 3 สมรรถนะเฉพาะของบุคลากรตำแหน่งผู้เชี่ยวชาญระบบรักษาความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ (Functional Competency)

3.1 ความรู้พื้นฐาน (Knowledge)	**จำเป็นมาก**	**จำเป็น**	**ไม่จำเป็น**
3.1.1 พื้นฐานด้านการโจมตีบนระบบสารสนเทศ			
3.1.2 พื้นฐานด้านความปลอดภัยบน Network Operation System หรือระบบปฏิบัติการเครือข่าย			
3.1.3 พื้นฐานด้านความปลอดภัยบน Operation System หรือระบบปฏิบัติการ			
3.1.4 พื้นฐานด้านโปรโตคอล SSL/TLS, CIFS, HTTP/S, DHCP, SMTP, LDAP/S และ DNS			
3.1.5 พื้นฐานความเข้าใจการทำงานของ VPNs, IPSec และ PKI			
3.1.6 พื้นฐานกฎหมาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550			
3.1.7 พื้นฐานด้าน ISO-27000			
3.1.8 อื่นๆ (โปรดระบุ)_____			
3.2 ทักษะการทำงาน (Skill)	**จำเป็นมาก**	**จำเป็น**	**ไม่จำเป็น**
3.2.1 วิเคราะห์การความเสี่ยงที่สามารถเกิดขึ้นได้บนระบบคอมพิวเตอร์			
3.2.2 วิเคราะห์แยกแยะชนิดของการโจมตีที่เกิดขึ้น			
3.2.3 สามารถแก้ไขการตั้งค่าของระบบคอมพิวเตอร์เพื่อลดความเสียหายกับระบบสารสนเทศได้			
3.2.4 สามารถสืบหาสาเหตุของความเสียหายที่เกิดขึ้นกับระบบสารสนเทศได้			
3.2.5 สามารถใช้งานคำสั่งในระบบปฏิบัติการเครือข่ายต่างๆ (Network Operation System) ได้			
3.2.6 สามารถใช้งานคำสั่งในระบบปฏิบัติการต่างๆ (Operation System) ได้			
3.2.7 สามารถออกแบบและวางแผนการป้องกันความเสียหายที่อาจจะเกิดขึ้นกับระบบสารสนเทศได้			
3.2.8 สามารถอธิบายการโจมตีและสาเหตุที่ทำให้เกิดความเสียต่อระบบแก่ผู้ใช้หรือผู้อื่นๆ ได้			
3.2.9 สามารถแก้ไขและป้องกัน Web Coding ของระบบ Web Server เมื่อเกิดการเปลี่ยนแปลงจากผู้โจมตีได้			
3.2.10 อื่นๆ (โปรดระบุ)_____			

3.3 คุณลักษณะพื้นฐาน (Attribute)	จำเป็นมาก	จำเป็น	ไม่จำเป็น
3.3.1 คิดวิเคราะห์ได้			
3.3.2 มองภาพองค์รวม			
3.3.3 เข้าใจผู้อื่น			
3.3.4 ดำเนินการเชิงรุก			
3.3.5 มีความถูกต้องของงาน			
3.3.6 มีความมั่นใจของตนเอง			
3.3.7 มีความยืดหยุ่นผ่อนปรน			
3.3.8 มีความเป็นผู้นำ			
3.3.9 มีศิลปะการสื่อสารจูงใจ			
3.3.10 มีการประสานงานที่ดี			
3.3.11 มีการติดตามงาน			
3.3.12 แก้ปัญหาต่างๆ ได้			
3.3.13 ให้คำปรึกษาได้			
3.3.14 มีการให้อำนาจผู้อื่น			
3.3.15 บริหารการเปลี่ยนแปลงได้			
3.3.16 อื่นๆ (โปรดระบุ)_____			

3.4 บุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศจำเป็นต้องมีประสบการณ์การทำงานก่อนหรือไม่

☐ จำเป็น (โปรดระบุประสบการณ์การทำงานอย่างน้อย_____ปี)

☐ ไม่จำเป็น เพราะเหตุใด (สามารถเลือกได้มากกว่า 1 ตัวเลือก)

- ○ สามารถเรียนรู้และฝึกฝนด้วยตัวเองได้
- ○ สามารถหาประสบการณ์ได้จากการทำงานจริง
- ○ อื่นๆ (โปรดระบุ)_____

_____

ส่วนที่ 4 แนวโน้มความต้องการบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศ

4.1 ในภาพรวมขององค์กรหรือบริษัทของท่านมีความคิดเห็นว่าบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศมีความจำเป็นกับองค์กรของท่านหรือไม่อย่างไร

☐ **จำเป็นเพราะเหตุใด (สามารถเลือกได้มากกว่า 1 ตัวเลือก)**

- ○ เพื่อป้องกันความลับหรือข้อมูลสำคัญขององค์กร
- ○ เพื่อป้องกันความเสียหายที่อาจจะเกิดจากการโจมตีของผู้ไม่ประสงค์หรือ Hacker
- ○ ลดต้นทุนในการจัดจ้าง Outsource
- ○ ลดการรั่วไหลของข้อมูลขององค์กรในกรณีที่มีการจัดจ้าง Outsource
- ○ ลดช่องโหว่ที่จะใช้ในการโจมตีหรือสร้างความเสียหายแก่องค์กร
- ○ ป้องกันการแฝงตัวจากบุคคลภายนอกที่ไม่ใช่คนในองค์กร
- ○ อื่นๆ (โปรดระบุ) _____
  _____

หากจำเป็น องค์กรของท่านมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศหรือไม่

- ○ มี (โปรดระบุจำนวน_____คน) แล้วท่านมีความคิดที่จะเพิ่มบุคลากรด้านนี้หรือไม่
  - ☐ ต้องการเพิ่มบุคลากร (โปรดระบุจำนวน_____คนโดยประมาณ)
  - ☐ ไม่ต้องการเพิ่มบุคลากรเพราะเหตุใด (สามารถเลือกได้มากกว่า 1 ตัวเลือก)
    - Δ ไม่มีงบประมาณในด้านนี้
    - Δ มีกำลังคนที่เพียงพอต่อความต้องการอยู่แล้ว
    - Δ องค์กรยังมีขนาดเล็ก
    - Δ อื่นๆ(โปรดระบุ)_____
      _____
- ○ ไม่มี แล้วในปัจจุบันมีบุคลากรด้านนี้โดยการจัดจ้าง Outsource หรือไม่
  - ☐ มี (โปรดระบุจำนวน_____คน)
  - ☐ ไม่มี เพราะเหตุใด (สามารถเลือกได้มากกว่า 1 ตัวเลือก)
    - Δ ยังไม่มีความต้องการบุคลากรในด้านนี้
    - Δ องค์กรไม่ได้ให้ความสำคัญในด้านนี้
    - Δ ไม่มีงบประมาณเพียงพอที่จะจัดจ้าง Outsource
    - Δ อื่นๆ(โปรดระบุ)_____
      _____

หากในภาพรวมขององค์กรหรือบริษัทของท่านมีความจำเป็นที่ต้องมีบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศ ท่านคิดว่าองค์กรหรือบริษัทของท่านควรจะพัฒนาคืออะไรบ้าง (เลือกได้มากกว่า 1 ข้อ)

- ○ พัฒนาทักษะด้านความปลอดภัยบนระบบสารสนเทศแก่บุคลากรคอมพิวเตอร์ในองค์กร
- ○ จัดการฝึกอบรมด้านความปลอดภัยบนระบบสารสนเทศทั้งระยะสั้นและระยะยาวแก่บุคลากรคอมพิวเตอร์ในองค์กร
- ○ มีการศึกษาดูงานด้านความปลอดภัยบนระบบสารสนเทศทั้งในและต่างประเทศ
- ○ อื่นๆ (โปรดระบุ)_____
  _____

☐ **ไม่จำเป็น เพราะเหตุใด (สามารถเลือกได้มากกว่า 1 ตัวเลือก)**

- ○ มีการจัดจ้าง Outsource
- ○ ไม่มีข้อมูลที่เป็นความลับหรือข้อมูลที่นำไปแสวงหากำไรได้
- ○ องค์กรมีขนาดเล็ก จึงยังไม่มีความจำเป็น
- ○ องค์กรมีการใช้งานระบบคอมพิวเตอร์น้อยมาก
- ○ สามารถให้บุคลากรคอมพิวเตอร์ในสายงานอื่นๆทำแทนกันได้
- ○ ไม่มีงบประมาณในด้านนี้อย่างจริงจัง
- ○ อื่นๆ (โปรดระบุ)_____
  _____

4.2 ท่านคิดว่ามหาวิทยาลัยหรือสถาบันการศึกษาที่ท่านรู้จักมีการผลิตบุคลากรคอมพิวเตอร์ในด้านความปลอดภัยบนระบบสารสนเทศหรือไม่

☐ มี (โปรดระบุชื่อมหาวิทยาลัยหรือสถาบันการศึกษาที่ท่านรู้จักอย่างน้อย 1 ตัวอย่างหรือมากกว่านั้น)

_____
_____
_____

☐ ไม่มี