รายงานมาตรฐานบุคลากร IT

เสนอ

ดร.ครรชิต มาลัยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชา Managing Information Technology

(214552)

ประจำภาคการศึกษาที่ 1/2547

สมาชิกกลุ่ม

1) นายครองเขตต์ เขื่อนธรรม	รหัส 4565412
2) นายธารธรรม อุประวงศา	รหัส 4665418
3) นายนฤทธิ์ ตรงเนตรปัญญา	รหัส 4665422
4) นายพรชัย ภัควันต์	รหัส 4665430
5) นายวุฒิเลิศ รุ่งฉาย	รหัส 4665442
6) นายเวนิช ทองโสม	รหัส 4665443
7) นายสยาม กาญจนสาย	รหัส 4665449
8) นายอนะพิชา นวะมะรัตน	รหัส 4665459

สารบัญ

1. มาตรฐานบุคลากร IT

บุคลากรทาง IT คือบุคคลที่เกี่ยวข้องในการกำหนดแนวคิดหรือดำเนินการทางด้าน IT (Information Technology) ได้แก่

- CIO (Chief of Information Officer)
- Software development (System analyst, Implementation (coding))
- IT Security (Preventing, monitoring and protecting)
- IT Support (Consulting, Solving)
- IT Trainer
- IT Certificate

บุคคลเหล่านี้ก็ต้องมีความรู้ความสามารถทางด้านนี้ดีพอที่จะทำให้งานในหน้าที่บรรลุเป้าหมาย ในแง่ของความเป็นมาตรฐานของความรู้ความสามารถของบุคคลากรเหล่านี้อาจจะไม่สามารถระบุให้ชัดแจ้งได้ เพราะในแต่ละองค์กรก็อาจจะต้องการความรู้ความสามารถทาง IT แตกต่างกันออกไป ขึ้นอยู่กับรูปแบบของการดำเนินธุรกิจ หรือชนิดของธุรกิจนั้นๆ อย่างเช่น องค์กรที่ทำธุรกิจที่ไม่ได้มีผลิตภัณฑ์เกี่ยวข้องกับ IT (เช่นบริษัทผลิตอาหารสัตว์) อาจจะต้องการบุคลากร IT เพื่อสนับสนุนการปฏิบัติงานทางธุรกิจ หรือเป็น Back office เท่านั้น จะต่างจากบริษัทที่ประกอบการทางด้าน IT โดยตรงที่ต้องการบุคลากรที่มีความรู้ความสามารถที่จะสร้างผลิตภัณฑ์ทางด้าน IT ได้นอกเหนือไปจากงานการสนับสนุน

ทั้งนี้ทั้งนั้น ไม่ว่าจะเป็นธุรกิจแบบใดในปัจจุบัน ก็ต้องมีส่วนงานทางด้าน IT ที่เหมือนๆกันอยู่คืองานสนับสนุนธุรกิจหรือ Back office

ในที่นี้จึงจะกล่าวถึงในภาพรวมของความรู้ความสามารถของบุคลากรที่พึงจะมีเพื่อให้บริษัทหรือองค์กรบรรลุเป้าหมาย

2. Chief Information Officer (CIO)

ด้วยแรงผลักดันทางด้านการตลาด, ด้วยเรื่องของโลกาภิวัฒน์, และลูกค้ามีความต้องการเพิ่มมากขึ้นอยู่ตลอดเวลา เป็นเหตุให้องค์กรขนาดใหญ่ของโลกได้รับรู้ว่า เทคโนโลยีนั้นต้องเล่นกันแบบรวมกันเป็นหนึ่งเดียว, มีบทบาทสำคัญที่จะทำให้ฝ่ายบริหารบรรลุวัตถุประสงค์หลักทางธุรกิจ และในท้ายที่สุดคือ ช่วยให้บรรลุวิสัยทัศน์ขององค์กร

อย่างไรก็ตาม การลงทุนทางด้านเทคโนโลยี แล้วไม่ได้ใช้มันเต็มศักยภาพ ก็จะเป็นความสูญเสีย (wasteful) และขาดความรับผิดชอบ (irresponsible) ซึ่งมักจะแสดงให้เห็นถึงความล้มเหลวในระดับพื้นฐานของการบริหารจัดการภายในองค์กร

ในการลงทุนแต่ละครั้ง บ่อยครั้งเกิดขึ้นโดยที่ CIO (Chief Information Officer) ไม่ได้รับการพิจารณาให้มีส่วนร่วมในการพูดคุยถึงยุทธศาสตร์ และองค์กรทางด้าน IT (IT Organization) เองก็ไม่ได้ถูกพิจารณาให้มีส่วนร่วมเป็นหนึ่งในยุทธศาสตร์ทางธุรกิจ CIO ที่มีความสามารถในการเชื่อมเทคโนโลยีเข้ากับเป้าหมายของธุรกิจ จะเป็นผู้ที่ได้รับสนใจและมีความน่าเชื่อถือจากผู้นำในหน่วยธุรกิจต่างๆ และเป็นหัวหน้าทีมของบริษัท องค์กรทางด้าน IT นั้นต้องการที่จะถูกผูกรวมเข้ากับธุรกิจเพื่อทำให้เกิดมูลค่าที่แท้จริง ต้องได้รับการสนับสนุนจากบริษัท และหัวหน้าหน่วยธุรกิจต่างๆ จาก CEO และผู้ที่อยู่ในคณะผู้บริหารระดับสูง

บทบาทของ CIO จะมีความสลับซับซ้อนมากขึ้น ในปี 1970 ถึง 1980 นั้น CIO จะเป็นหัวหน้าในงานการจัดการข้อมูล (data processing) ของบริษัท วันนี้ CIO จะก้าวขึ้นไปเป็นหัวหน้าหน่วยงานทางธุรกิจ ที่มีความรับผิดชอบในหลายๆกรณี ทั้งในเรื่องการดูแลรักษาโครงสร้างพื้นฐานของเทคโนโลยีและโครงข่ายสื่อสาร ด้วยการ upgrading, installing, และอบรมผู้ใช้เกี่ยวกับการใช้โปรแกรมระบบช่วยตัดสินใจทางธุรกิจ (business decision support software) และเรื่องของการเช่าหรือซื้อชิ้นส่วนใหม่ๆสำหรับระบบคอมพิวเตอร์หรือระบบสื่อสาร งบประมาณของ CIO ที่ใช้ในเรื่องของคน, การบำรุงรักษา, การจัดซื้อ, โครงการใหม่ๆ, การจัดหาที่ปรึกษา, หรือการ Outsourcing อาจจะวิ่งไปถึงหลักร้อยหรือล้านดอลลาร์ได้

การเปลี่ยนแปลงบทบาทของ CIO ที่เห็นนี้ CIO ต้องมีทักษะอะไรบ้าง? อะไรคือสิ่งที่ CIO ต้องรับผิดชอบเป็นอันดับแรก? CIO จะต้องนั่งตรงจุดไหนที่สัมพันธ์กันกับหัวหน้าส่วนงานอื่นๆ? และสุดท้าย CEO ต้องทำอะไรเพื่อพัฒนาและทะนุถนอม CIO?

- ในทางอุดมคติแล้ว, ผู้นำบริษัทควรมอง CIO เป็นบุคลากรที่คุณค่าที่อยู่ในทีมของผู้บริหาร ที่เป็นผู้ให้ความเห็นหรือแสดงให้เห็นว่าเทคโนโลยีนั้นจะช่วยให้บริษัทบรรลุวิสัยทัศน์ และวัตถุประสงค์ของธุรกิจได้อย่างไร แต่งานของ CEO นั้นจะเป็นเรื่องของการใช้เหตุผลในการเลือกใช้เทคโนโลยีให้เกิดผลกระทบทางบวกแก่วิสัยทัศน์ของบริษัท

- CIO ควรมีโอกาสที่จะได้นั่งในแถวหน้าของงานการวางแผนทางยุทธศาสตร์ของธุรกิจ และให้ความเห็นถึงบทบาทของเทคโนโลยี แต่ CIO ไม่ควรที่จะเสนอการตัดสินใจในขั้นสุดท้ายเกี่ยวกับการลงทุนทางด้านเทคโนโลยีในนัยทางธุรกิจ
- กับทาง CEO, ผู้นำทางธุรกิจของบริษัท, และผู้นำหน่วยธุรกิจแล้ว CIO จะเป็นผู้ให้เสนอเลือกของเทคโนโลยีที่จะจับคู่เข้ากับวิสัยทัศน์ของธุรกิจ และการลงทุนทางธุรกิจที่ดี แต่ในท้ายที่สุดแล้วก็จะเป็นหน้าที่ของผู้นำหน่วยธุรกิจจะตัดสินใจเลือก
- การเข้ามาเกี่ยวข้องของผู้บริหารทางธุรกิจระดับสูงเป็นความจำเป็นอย่างยิ่งยวดต่อการพัฒนาโครงสร้างพื้นฐานทางเทคโนโลยีที่ทีประสิทธิภาพ เพื่อให้บรรลุผลประโยชน์ทางธุรกิจจากการใช้เทคโนโลยีนี้ ทาง CIO และผู้นำทางธุรกิจจะต้องได้รับการสนับสนุน, อย่างเปิดเผย, พูดจากันแบบตรงไปตรงมา โดยปราศจากการแบบแผน

อะไรคือบทบาทของ CIO สมัยใหม่?

ในปี 1999, องค์กรค้นคว้าทางด้านการบริหารที่ชื่อ Korn/Ferry International ได้ทำการสำรวจ CIO จำนวน 340 ท่าน ในอเมริกา, อังกฤษ, เยอรมัน และฝรั่งเศส ก็พบเรื่องที่มีการพูดถึงกันมากคือ CIO รู้สึกว่าพวกเขาอยู่ หรือควรจะอยู่ ตรงขอบของการเปลี่ยนผ่านจากบทบาทผู้กำหนดยุทธวิธี (tactical role) ที่พวกเขาเกี่ยวข้องกับการแผนทางเทคนิคระยะสั้น และการติดตั้ง hardware หรือ software ไปเป็นผู้กำหนดยุทธศาสตร์ (strategic role) ที่พวกเขาเข้าไปเกี่ยวข้องกับการวางแผนขององค์กร

ในช่วงหลังปี 1990 ก็ได้มีเทคโนโลยีใหม่ๆ เข้าสู่ตลาดมากมาย, วิธีที่ได้เรียนรู้มาจาก “ร้านขายของชำ (Grocery shopping)” -คือการเดินไปตามช่องทางเดิน แล้วซื้อสินค้าชิ้นหนึ่งจากหลายๆชิ้น จนกระทั้งบัดนี้ก็เกินกว่า CIO จะอ้าแขนรับรับไว้ได้ เห็นได้ชัดว่า CIO เริ่มที่จะต้องเข้าไปจับคู่โอกาสทางเทคโนโลยีเข้ากับตัวขับเคลื่อนธุรกิจและเป้าหมายของบริษัทอย่างเข้มงวด และเพียงแค่หนึ่งแนวทาง (solution) ของเทคโนโลยี ก็จะไม่อาจนำไปใช้กับทุกๆหน่วยธุรกิจได้

บทบาทใหม่ของ CIO จะปรากฏให้เห็นอย่างรวดเร็ว บทบาทนั้นต้องการให้ CIO

- สร้าง (Establish) , ทำให้เป็นจริง (Implement), และสื่อสารวิสัยทัศน์ทางยุทธศาสตร์ IT, และการวางแผน, ให้มีการประสานกันในทุกๆยุทธศาสตร์ธุรกิจ

- ให้แน่ใจว่า IT จะถูกนำไปใช้อย่างมีประสิทธิภาพเพื่อให้บรรลุเป้าในภาพรวมของธุรกิจ ที่เกี่ยวกับเรื่องของการเติบโตของรายได้, ผลกำไร, และความมีประสิทธิภาพในการลงทุน
- สร้าง และพัฒนาทักษะทางด้าน IT, ความสามารถ, และการทำงานเป็นทีมให้เกิดขึ้นทั่วทั้งองค์กรอย่างต่อเนื่อง
- เพิ่มประสิทธิภาพให้ผู้ชำนาญการทางเทคนิค และลดความซ้ำซ้อนของการทำงานในองค์กร
- ประสานและผลักดันในเรื่องของเหมาะสม, นโยบายทาง IT, ยุทธศาสตร์, มาตรฐาน, ข้อเสนอที่เหมือนๆกัน, การแบ่งปันการให้บริการ, และการจัดสรรทรัพยากรตลอดทั่วทั้งองค์กร
- บริการในแบบตัวต่อตัว (point person) (ภายใน และภายนอก) ก็คือการเป็นกระบอกเสียงทางเทคโนโลยีขององค์กร (Single voice for technology)

การพัฒนาและสื่อสารเกี่ยวกับวิสัยทัศน์และแผนของยุทธศาสตร์ IT

วิสัยทัศน์ของยุทธศาสตร์ทาง IT ต้องสดใหม่, ชัดเจน, และง่ายพอที่สมาชิกทุกๆท่านสามารถเข้าใจได้โดยไม่ต้องอธิบายเพิ่มเติม มันต้องเป็นเรื่องที่ง่ายต่อผู้บริการ, ผู้จัดการ, บุคลากรทาง IT, และผู้ใช้งานทั่วๆไปในบริษัท ที่จะจดจำและทบทวนได้ อย่างไรก็ตาม ถ้ามันเกี่ยวข้องกับการบริหารจัดการ วิสัยทัศน์นั้นจะต้องมั่นคงแน่วแน่อยู่บนพื้นฐานความเข้าใจในยุทธศาสตร์ของธุรกิจเป็นอย่างดี

ให้แน่ใจว่า IT ได้ถูกใช้ อย่างมีประสิทธิภาพ

หนึ่งในความรับผิดชอบอันยิ่งใหญ่ของ CIO ที่จะช่วยให้ CEO ไม่ทำในสิ่งที่ไม่เหมาะสมและการตัดสินใจผิดพลาดในบางครั้งที่เกี่ยวข้องการลงทุนทาง IT

บ่อยครั้งที่การใช้จ่ายในเรื่องนี้จะเกิดจากความต้องการของ operation function หรือผู้นำหน่วยธุรกิจ และเจ้าหน้าที่ทางการตลาดหรือผลิตภัณฑ์ของพวกเขา หรือจากพวกที่รู้เกี่ยวกับ IT แบบครึ่งๆกลางๆ CIO ต้องสามารถที่จะยืนขึ้นและบอกแก่คนเหล่านั้นได้ว่า “ผมมีอำนาจภายในบริษัทแห่งนี้ที่จะบอกคุณว่านี่ไม่ได้เป็นการใช้ทรัพยากรทาง IT อย่างมีประสิทธิภาพ ถ้าคุณรู้สึกจริงจังมากเกี่ยวกับเรื่องนี้ คุณต้องใช้งบประมาณของคุณเอง แล้วผมจะให้การสนับสนุนช่วยเหลือเท่าที่จำเป็น”

IT จะต้องมีความเหมาะสมและดีพอสำหรับงานในมือ เครื่องมือที่เหมาะสมต่องานอาจจะไม่ได้เป็นอะไรที่ทุกคน หรือบางคนต้องการในวันนี้

เพราะฉะนั้น IT ต้องเป็นเรื่องที่ชัดเจนมากๆ และได้การกำหนดอย่างระมัดระวัง ผู้ใช้งานต่างๆ ไม่ได้รู้เสมอไปหรอกว่าจริงๆแล้วพวกเขาต้องการอะไรกันแน่

สร้างทักษะและความสามารถทาง IT

วันนี้ ทักษะเป็นสิ่งจำเป็นสำหรับองค์กร IT และมีความหลากหลายแตกต่างกันไปในหน่วยธุรกิจต่างๆในบริษัท ทักษะทุกๆรูปแบบจะเป็นที่ต้องการ ไม่ใช่แต่ทักษะทางเทคนิค สำหรับบุคคลกรทาง IT ที่มีหัวก้าวหน้า พวกเขาต้องการพัฒนาความสามารถที่สัมพันธ์สอดคล้องกับการบริหารโครงการ, การบริหารการเงิน, การวัดประสิทธิภาพ, การสื่อสารระหว่างบุคคลหรือเป็นกลุ่ม รวมทั้งการสื่อสารแบบด้วยการเขียน, การพัฒนาองค์กรและบุคคล, และการบริหารความสัมพันธ์

บุคคลและทักษะที่เขาใช้จะเป็นทรัพย์สินที่สำคัญมากขององค์กรทางด้าน IT เพราะว่ามีการเปลี่ยนแปลงที่เร็วมากในทางเทคโนโลยี, ทางเทคนิค และทักษะการให้การวิเคราะห์ทางธุรกิจของแต่ละบุคคลที่ทำงานในองค์กร IT ต้องได้รับปรับใหม่อย่างต่อเนื่อง

ผู้นำที่มีความรู้ความสามารถทางเทคนิค ที่ไม่มีความรู้ในทางการบริหารจักการในธุรกิจจะไม่สามรถช่วยให้องค์กร IT มีการพัฒนาทักษะที่สำคัญนี้ได้

ประสานงานทางนโยบาย, ยุทธศาสตร์, มาตรฐาน และรูปแบบการดำเนินการ

CIO จะอยู่ ณ. ที่จุดศูนย์กลาง (hub) ของนโยบาย, ยุทธศาสตร์, มาตรฐาน, และรูปแบบการดำเนินการทาง IT แทนที่จะไปอยู่บนยอกหอคอย (pinnacle) เขาจะต้องเล่นบทบาทของผู้นำกองเชียร์และผู้มีอิทธิพลที่จะโน้มน้าวได้, ทำงานร่วมกับหน่วยธุรกิจ, จัดการโครงสร้างองค์กร IT, มีความเป็นผู้นำทางการบริหาร, และบทบาทของผู้ใช้ในแบบทั่วๆไป

ทักษะอะไรที่ CIO สมัยใหม่ต้องการ?

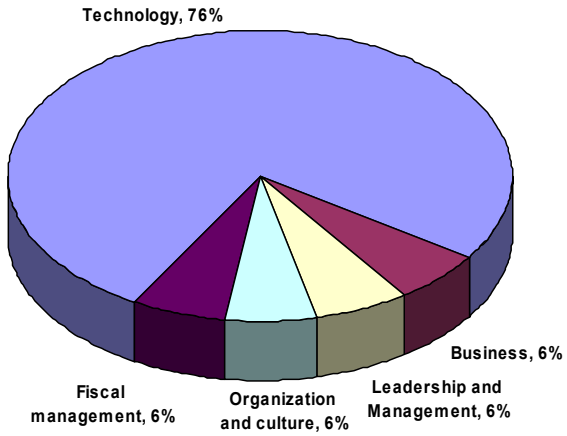
ทักษะที่จำเป็นของความเป็นผู้นำในองค์กรสมัยใหม่ สามารถแบ่งออกได้เป็น 5 แบบ

1. ทักษะทางธุรกิจ
2. ทักษะทางเทคโนโลยี
3. ทักษะของการเป็นผู้นำและการบริหารจัดการ
4. ทักษะการจัดการองค์กรและวัฒนธรรม (Organization and Culture skills)

5. ทักษะทางการบริการจัดการทางการเงิน (fiscal management)

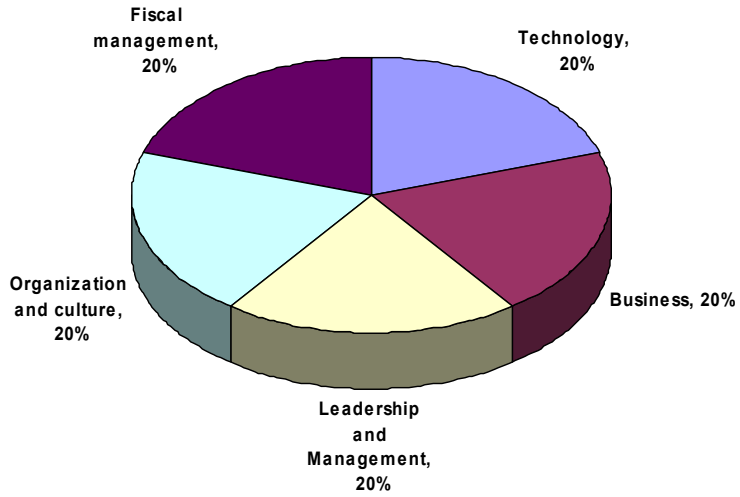
ผู้นำ (leaders) แลผู้จัดการ (managers) ที่อยู่ใน function area ของธุรกิจที่ต่างกัน ก็จะต้องการทักษะมากน้อยแตกต่างกันไปใน 5 area เหล่านั้น แต่จะไม่มีผู้นำเก่งๆใดเลยจะขาดเรื่องใดเรื่องหนึ่งอย่างสมบูรณ์ คือต้องรู้หรือมีทักษะในทุกๆเรื่อง

ส่วน CIO ในทศวรรษที่ 21 นั้นต้องการทักษะที่แตกต่างไปจาก CIO รุ่นเก่าอย่างมาก CIO และผู้จัดการ IT ในช่วง 1970 ถึง 1990 จะหนักไปทางด้านเรื่องของการศึกษา (education) และการฝึกอบรมในทางเทคโนโลยีและทางวิศวกรรมดังรูป



แสดงขนาดของทักษะของ CIO และ ผู้จัดการ IT

ด้วยการเปรียบเทียบ CIO แห่งทศวรรษที่ 21 จะต้องการให้มีความสมดุลของกลุ่มทักษะมากกว่า



แสดงความต้องการของทักษะที่มีความสมดุลสำหรับ CIO วันนี้

ทักษะทางธุรกิจ (Business skills)

CIO ต้องรู้เรื่องธุรกิจของบริษัทดีพอที่จะสามารถให้คำแนะนำที่ถูกต้อง ในเรื่องของการวางยุทศาสตร์ทางธุรกิจ และเพื่อระบุประเด็นหลักของโอกาสทางเทคโนโลยีที่จะทำให้ยุทธศาสตร์ของบริษัทเคลื่อนไปข้างหน้าได้ CIO ต้องมีความสามารถที่จะรวมยุทธศาสตร์ของบริษัทกับวิสัยทัศน์ทาง IT และยุทธศาสตร์ที่เขาพัฒนาขึ้นเข้าด้วยกันได้

ทักษะที่เฉพาะในงานทางธุรกิจจะรวมถึงความเข้าใจใน:

- ยุทธศาสตร์ทางธุรกิจของบริษัทในแนวกว้าง
- หน่วยธุรกิจทั้งหมดและการเชื่อมโยงหลักระหว่างกัน
- ประเด็นหลักใหญ่ๆของบริษัท

ทักษะทางเทคโนโลยี

CIO กับทีมผู้นำทาง IT ของเขาต้องสามารถที่จะสามารถกำหนดมาตรฐานในเรื่องของการเลือก (selection), บูรณการ (integration), และการปฏิบัติงานในแนวทางที่มีความสลับซับซ้อนได้ ในการให้คำปรึกษาแก่บริษัทและหัวหน้าหน่วยธุรกิจนั้น พวกเขาต้องสร้างระบบการวัด และระบบบริหารจัดการความมีประสิทธิภาพที่เหมาะสม เพื่อให้มั่นใจได้ว่าได้มีการยึดถือข้อกำหนดมาตรฐานตามที่ได้ตกลงกันไว้แล้ว

CIO ต้องมีทักษะที่จำเป็นต่อการวางแผนและประสานงานการพัฒนาโครงสร้างพื้นฐานของโครงข่ายสื่อสารที่เอาจริงเอาจัง, ยืดหยุ่น, และมีต้นทุนที่ต่ำ

สุดท้าย เป้าหมายของ CIO ควรจะต้องมีการทำการค้นคว้าโดยตรง และการประเมินเทคโนโลยีที่น่าสนใจได้อย่างเท่าทันและล้ำหน้า (advanced)

ทักษะเฉพาะในกลุ่มเทคโนโลยีได้แก่

- ความรู้ในระดับของเชิงยุทธศาสตร์ (Strategic-level) ของความสามารถและตามทันเทคโนโลยี
- มีความรู้ในทางปฏิบัติในเรื่องของการติดตั้ง (Implementation) และทำให้เรื่องต่างๆเป็นไปตามแผน

ทักษะความเป็นผู้นำและการบริหารจัดการ

การได้ที่นั่นในระดับผู้นำในองค์กร ไม่ใช่เพียงแค่การได้รับเชิญให้นั่ง เพื่อเป็นการรักษาที่นั่งนั้น CIO ต้องผู้นำทางธุรกิจที่แท้จริง ประเด็นใหญ่ของการเป็นผู้นำทางธุรกิจคือ ต้องสามารถที่จะอำนวยความสะดวกทางด้านการสื่อสารเกี่ยวกับ IT ในกลุ่มธุรกิจที่กระจายอยู่ทั่วโลกกับผู้นำ IT ผ่านช่องทางติดต่อตามปกติ ทั้งแต่บุคคลถึงบุคคล หรือการประชุมเป็นกลุ่มได้ หรือแม้กระทั้งการสื่อสารกันด้วยวิธีการเขียน ทั้งแบบทางการและไม่เป็นทางการ

CIO ต้องสามารถนำ (lead) การพัฒนาแผนการทางเทคโนโลยีในสายงานธุรกิจในองค์รวมได้ สุดท้ายการบริหารความสัมพันธ์และการจัดการ vendors ทั้งที่เป็นผู้ผลิตหรือ outsource จะเป็นงานที่ใหญ่ขึ้นในงานบริหารจักการของ CIO

ทักษะเฉพาะในกลุ่มของความเป็นผู้นำหรือการจัดการคือ

- การแสดงออกถึงการเป็นนักบริหาร
- ความสามารถในการทำงาอย่างมีประสิทธิภาพในระดับ board
- ความสามารถในการส่งผ่าน (transfer) ทักษะ, ความรู้, และวิธีปฏิบัติที่ดีที่สุด
- มีความยากที่จะแสดงออกต่อสาธารณะ, ครบค้าสมาคม (collegial), เป็นคนเน้นที่ผลลัพธ์

ทักษะการจัดการองค์กรและวัฒนธรรม

CIO ต้องมีการบริหารจัดการในเรื่องของการดูแลเอาใจใส่กลุ่มเจ้าหน้าที่ IT ขนาดใหญ่ บ่อยครั้งก็อาจขยายวงออกไปถึงนอกบริษัท CIO ต้องสามารถที่อดทนต่อสิ่งเร้าใจที่จะก่อให้เกิดการมีองค์กรแบบทหารได้ โดยการไปเน้นที่การสร้างทีม, พัฒนาทักษะ และวัฒนธรรมแห่งความน่าเชื่อถือให้เกิดขึ้นแทน

ทักษะเฉพาะในการจัดการภายในองค์กรและวัฒนธรรมคือ

- มีความสามารถที่จะเข้าใจในเรื่องงานบริหารทรัพยากรบุคคล, การจัดการองค์กร, เรื่องของพฤติกรรม, และเทคนิคการบริหารการเปลี่ยนแปลงได้
- มีความสามารถที่จะทำงานภายใต้ความหลากหลายทางวัฒนธรรมได้
- มีความสามารถที่จะก่อให้เกิดการเปลี่ยนแปลงองค์กรครั้งใหญ่ได้

ทักษะทางการบริการจัดการทางการเงิน

CIO ต้องสามารถที่จะดำเนินการบริหารจัดการทางด้านการเงินที่เหมาะสม และควบคุมการใช้ IT ทั้งองค์กรได้ ต้องได้รับความไว้วางใจให้รับผิดชอบทางทางด้านการเงินสำหรับ IT รวมทั้งพัฒนาและคอยตรวจสอบงบประมาณของ IT, ตรวจดูและอนุมัติการใช้จ่ายทางด้าน IT และพัฒนาระบบการวัดการใช้จ่ายและประสิทธิภาพของการปฏิบัติงานภายในองค์การ IT ได้

ทักษะเฉพาะที่จะต้องมีในเรื่องนี้คือ

- สามารถที่จะทำงานร่วมกันกับหน่วยธุรกิจ, จัดสรรงบประมาณทางด้าน IT เพื่อใช้ดำเนินธุรกิจ ด้วยความโปร่งใส่ได้
- สามารถที่จะดำเนินการจัดสรรงบประมาณที่ซับซ้อนได้, บริหารการลงทุนได้, บริการการเงินได้, และควบคุมแนวความคิดของสภาพแวดล้อมของ IT ได้
- มีความเข้าใจในการใช้ IT ขับเคลื่อนธุรกิจ และการวัดประสิทธิภาพทางการเงิน, เข้าใจในผลกระทบที่อาจเกิดขึ้น, และเข้าใจถึงการใช้ IT อย่างมีประสิทธิภาพเพื่อให้บรรลุการเปลี่ยนแปลงพฤติกรรมตามที่ต้องการ

อะไรที่ CIO สมัยใหม่ต้องรับผิดชอบเป็นเบื้องต้น?

CIO สมัยใหม่จะมีความรับผิดชอบในเบื้องต้นใน 3 เรื่องคือ

1. คน (People)
2. การจัดลำดับความสำคัญ (Priorities)
3. ประสิทธิภาพ (Performance)

คน (People)

ก็เหมือนกันกับ CIO วันนี้ ที่สมาชิกขององค์กรทางด้าน IT ในทุกๆระดับชั้นก็ต้องการการพัฒนาทักษะใหม่ๆ CIO ก็ต้องเข้าไปรับผิดชอบในเรื่องงานบริหารทัพยากรบุคคล, การรับสมัครคนระดับหัวกะทิเข้ามาสู่องค์กร IT อย่างใกล้ชิด, และสร้างเส้นทางความก้าวหน้าในอาชีพให้แก่สมาชิก, สร้างระบบการวัดประสิทธิภาพและการประเมินผลที่สมบูรณ์, วางแผนเส้นทางความก้าวหน้าในอาชีพ และก็คอยตรวจสอบ (monitor)

CIO ยังต้องวิธีการที่จะให้เกิดการเรียนรู้แบบคร่อมสายงาน, ให้มีการแลกเปลี่ยนทักษะและความสามารถกันในระดับองค์รวมขององค์กร และสับเปลี่ยนหมุนเวียนเจ้าหน้าที่ทาง IT ไปในสายงานธุรกิจหรืองานการปฏิบัติการต่างๆ

การจัดลำดับความสำคัญ (Priorities)

วันนี้ CIO ต้องเริ่มที่จะกำหนดลำดับความสำคัญ โดยเริ่มจากด้วยการสร้าง (establishing), จากนั้นก็ใช้ชีวิตอยู่กับมัน กลุ่มของกฎหลักๆทางด้าน IT และสำนึกไว้ว่าการเปลี่ยนแปลงเป็นสิ่งที่แน่นอนอย่างที่พวกเขาหรือลูกทีมของเขารู้ๆกันอยู่ พวกเขาต้องเป็นที่เก่งที่สุดทางด้าน IT, มีความต้องการที่จะได้เป็นเจ้าของธุรกิจและสามารถอธิบายชี้แจงเกี่ยวกับความแน่นอนของการเปลี่ยนแปลงลำดับความสำคัญของ IT ในแบบ zero-sum game ของค่าใช้จ่ายทาง IT ที่ทั้งแบบ fixed หรือลดน้อยถอยลง

CIO จะต้องขับเขี่ยวต่อสู้กับความมุ่งมั่นที่จะวางนโยบาย 2-3 อย่างที่เกี่ยวข้องกับการพัฒนาลำดับความสำคัญของธุรกิจให้สัมพันธ์กัน, มีการลงทุนทาง IT ที่มีประสิทธิภาพ CIO ต้องเข้าใจอีกว่าลำดับความสำคัญที่มีประสิทธิภาพไม่สามารถกำหนดได้ในสุญญากาศ IT ได้ และนั่นสัมพันธ์โดยตรงกับการบริหารงานในหน่วยธุรกิจและด้านผู้ใช้เองก็ต้องเห็นเป็นภาวะปกติด้วย

ประสิทธิภาพ (Performance)

CIO ในฐานบุคลากรทางธุรกิจ ควรจะดูแลปกป้องการวัดขอบเขตมูลค่าของธุรกิจ IT การวัดเหล่านี้จะต้องมีความยืดหยุ่น (Dynamic) ไปตามสถานการณ์ปัจจุบัน และสนับสนุนผลลัพธ์และการปรับปรุงที่จะเกิดขึ้นตามมา ความรับผิดชอบของ CIO ก็คือทำให้แน่ใจว่าค่าผลการวัดของธุรกิจ IT ที่เกี่ยวข้องจะถูกนำไปใช้ ให้องค์กรได้ใช้เป็นแนวทางที่จะไปมุ่งเน้น (focus) เพียง 2-3 อย่าง แทนที่จะไปมุ่งเน้นในหลากหลายเรื่อง

อีกอย่าง CIO จะต้องมั่นใจว่าทุกๆคนในองค์กร IT จะต้องมุ่งเน้นที่การระบุต้นเหตุของปัญหาในระดับรากหญ้าที่พวกเขาได้พบ แล้วดำเนินการที่จำเป็นเพื่อแก้ปัญหาและปรับปรุงกระบวนการด้วย

สุดท้าย, CIO วันนี้ยังรับผิดชอบต่อการบูรนาการทุกๆชิ้นส่วนของ IT เข้าด้วยกัน พวกเขาต้องเข้าใจในผลกระทบของการลงทุนโดยรวมที่เกิดขึ้นในทางลบ และไม่เพียงแค่กระทำเฉพาะชิ้นส่วน IT ที่มีการเคลื่อนไหวในเวลานั้น

ถ้ามีการใช้อย่างมีประสิทธิภาพ ค่าจากการวัดธุรกิจ IT จะกลายเป็นหนึ่งในเครื่องมือที่สำคัญที่สุดในการบริหารจัดการทางธุรกิจของ CIO

3. IT Software Development

นักพัฒนาด้านไอที มีบทบาทหลายด้าน

- พัฒนาซอฟท์แวร์
- จัดการฐานข้อมูล
- ติดต่อ ประสานงาน และให้ความช่วยเหลือแก่ user
- จัดการแก้ไขปัญหาด้าน Hardware / Software ประเภท troubleshooter

คุณสมบัติ

- ต้องมีความรู้ในหลายๆด้าน ทั้ง Hardware / Software database
- ต้องมีมนุษยสัมพันธ์อันดี กับ user และเพื่อนร่วมงาน สามารถเข้ากับคนอื่นได้ง่าย

ทักษะและความสามารถทั่วไป

- Software architecture, design, and development
- Software project management
- Test strategy design and test plan development
- Test case design and execution
- Automated test suite development

ความสามารถด้าน Web Technology:

- Java, JSP, EJB, Servelet, Applets, HTML, XML, WML, Apache, Tomcat, JRun, WebLogic, RMI, ASP

ความสามารถด้าน Scripting Language:

- Java Script, CGI/Perl, VB script, TCL/tk, Unix Shell Scripts

ความสามารถด้าน Development Tools:

- Developer Studio (VB, VC++), Crystal Report, D2K, Symantec Cafe, JDK, Java Developer, Power Builder, Rational Rose

ความสามารถด้าน Database:

- Oracle 8i, Sybase, MS SQL Server 7.0/2000, Access, DB2

ความสามารถด้าน Programming Language:

- C, C++, Java, C# Platforms: NT, Win 95, Win 98, Linux, Unix

ความสามารถด้าน Technology:

- COM/DCOM, ActiveX, UML, .Net, J2EE, UML

4. IT Security

เมื่อกล่าวถึงการบริหารจัดการระบบความปลอดภัยข้อมูลคอมพิวเตอร์ในทุกวันนี้ถือเป็นเรื่องสำคัญขององค์กรทุกองค์กรที่นำคอมพิวเตอร์และเทคโนโลยี IT เข้ามาใช้งาน เพราะปัญหาต่าง ๆ ที่เกิดขึ้นกับระบบคอมพิวเตอร์ขององค์กรไม่ว่าจะเป็นปัญหาไวรัสคอมพิวเตอร์, ปัญหา SPAM Mail, ปัญหาการถูก Hacker เข้าโจมตีโดยการเปลี่ยนหน้า Web Page (Web Defacement) ตลอดจนปัญหาระบบช้า หรือ ระบบล่ม ไม่สามารถให้บริการผู้ใช้ หรือ ลูกค้าได้ ซึ่งอาจเกิดจากการโจมตีแบบ DoS or DDoS Attack ก็เป็นสิ่งที่ CIO (Chief Information Officer) , CSO (Chief Security Officer) หรือ IT Manager ต้องรับผิดชอบ และ คอยเฝ้าระวังในลักษณะ "Proactive Management" คือ ไม่ใช่รอให้เกิดปัญหาก่อนแล้วค่อยแก้ไข แต่ ใช้หลักการตรวจสอบระบบอยู่เสมอ (Continuous Auditing) มีการติดตั้งระบบ IDS (Intrusion Detection System) เพื่อใช้ในการตรวจจับ Traffic ในระบบเครือข่ายว่ามีสัญญาณของการโจมตีของ ไวรัส หรือ Hacker หรือไม่เพื่อที่จะได้เตือนให้ทันท่วงที เพราะปัญหาเหล่านี้จะเกิดขึ้นเร็วมาก อาจส่งผลกระทบกับองค์กรในเวลาเพียงไม่กี่นาทีเท่านั้น

จากปัญหาดังกล่าว มีการสำรวจและวิจัยแล้วพบว่า องค์กรที่ใช้ IT โดยทั่วไป ต้องการบุคลากรที่จะมาดูแลจัดการเรื่อง "Information Security" โดยเฉพาะ ตั้งแต่มีการพูดถึงตำแหน่ง CSO (Chief Security Officer) หรือ CISO (Chief Information Security Officer), พูดถึงการจัดตั้งหน่วยงานดูแลด้าน Information Security โดยตรงซึ่งแยกออกมาจากฝ่าย IT เดิม (Infosec Department), มีการตั้งหน่วยงาน IT Internal Audit เพื่อตรวจสอบระบบอยู่เป็นระยะ ๆ

แต่ถึงองค์กรสมัยใหม่จะมีการเปลี่ยนแปลงด้าน IT ไปหลายๆ อย่างแล้วก็อาจยังไม่เพียงพอ เพราะบุคลากรขององค์กรจำเป็นต้องมี "ความรู้เชิงลึก" (In-depth Knowledge) ในด้านของ Information Security หรือ Infosec และ ต้องเข้าใจกลไกการจู่โจมของ Hacker และ ไวรัส เสียก่อน ถึงจะสามารถป้องกันระบบอย่างได้ผล ตลอดจนต้องคอยหมั่นเฝ้าระวังอยู่ตลอดเวลา (Real-Time Intrusion Detection) ซึ่งต้องเสียกำลังคน และทรัพยากรไปไม่ใช่น้อย บางองค์กรก็ได้ผลลัพธ์ออกมาไม่คุ้มกับที่ลงทุนไปในเรื่องนี้

ทางออกของการแก้ปัญหาในระยะยาวก็คือ การทำ "IT Outsourcing" ซึ่งเป็นแนวทางที่กำลังได้รับความนิยมอย่างสูงในเวลานี้ เนื่องจากองค์กรไม่ต้องดูแลรับผิดชอบทุกสิ่งทุกอย่างเอง แต่ได้ "Outsource" งานต่าง ๆ ออกไปเพื่อที่จะให้มีผู้ร่วมรับผิดชอบมากขึ้น และประหยัดค่าใช้จ่ายโดยรวมขององค์กร

การทำ "IT Outsourcing" กับ "Information Security Outsourcing" นั้น มีความแตกต่างกันพอสมควร จากการที่องค์กร Outsource งาน IT ทั่วๆไป เช่น งานดูแลเครือข่าย หรือ งาน Help Desk นั้น องค์กรสามารถ Outsource ได้โดยง่าย เพราะงานไม่ค่อยมีความซับซ้อนเท่าไร แต่พอพูดถึง "Information Security Outsourcing" หลายคนอาจจะปฏิเสธเรื่องนี้ไปเลย เพราะปัญหาเรื่องของ "Trust" หรือความไว้วางใจ ในบริษัทที่จะเข้ามาเป็นผู้ดูแลระบบความปลอดภัยให้กับเราที่เรียกว่า MSSP (Managed Security Services Provider) เพราะ เราไม่อยากให้ MSSP ต้องเข้ามารู้ข้อมูลภายในองค์กรของเรา และ เราจะไว้ใจ MSSP ได้แค่ไหน ระบบความปลอดภัยนั้นถือเป็นหัวใจสำคัญขององค์กรทำไมเราไม่ดูแลเอง แต่กลับไปให้ MSSP มาดูแทน จะเห็นว่าเกิดคำถามขึ้นมามากมาย

แต่ข้อมูลจากการวิจัยพบว่า การจัดจ้าง MSSP ในสหรัฐอเมริกา, ยุโรป และทั่วโลกกำลังได้รับความนิยมสูงขึ้นเรื่อย ๆ และ จากการสำรวจของบริษัทวิจัยต่าง ๆ ไม่ว่าจะเป็น Gartner Group หรือ IDC ล้วนกล่าวเป็นเสียงเดียวกันว่าในอีกปีสองปีข้างหน้านี้ ธุรกิจ MSSP จะเติบโตแบบก้าวกระโดด และ องค์กรต่าง ๆ จะนิยมทำ "Information Security Outsourcing" กันมากขึ้นเรื่อย ๆ

หน้าที่ความรับผิดชอบหลักๆของ "MSSP"

บริการแจ้งข่าวสารความเคลื่อนไหวด้าน Information Security โดยเฉพาะเรื่อง New Vulnerability/Exploit และ New Virus ให้ทราบในลักษณะวันต่อวัน (Day by Day Report)

1. บริหารจัดการ และ เฝ้าระวัง (Managing and Monitoring) Network Perimeter Security ที่ External Firewall, Border Router, IDS/IPS, VPN ตลอดจน Server ในบริเวณ DMZ
2. บริหารจัดการ Vulnerability ให้กับระบบขององค์กรอย่างต่อเนื่อง เช่น การทำ Vulnerability Assessment และ Penetration Testing รายเดือน เป็นต้น
3. เฝ้าระวัง Internal Network จาก Virus และ Hacker ตลอดจน Internal Firewall and Server Farm ภายในระบบ LAN ขององค์กร
4. รับปรึกษาปัญหาเวลาเกิด Security Breach Incident, รับแก้ปัญหาในลักษณะ Incident Response และ Digital Forensic
5. บริหารจัดการ Centralized Log Management และ Centralized Patch Management อย่างเป็นระบบ

เราจะเห็นแล้วว่า "Outsourcing Information Security" นั้นเป็นเรื่องที่น่าสนใจและมีประโยชน์กับองค์กร แต่ต้องทำด้วยความระมัดระวัง โดยที่ CIO/CSO หรือ ผู้บริหาร IT ต้องมีสิ่งสำคัญ ที่เรียกว่า "Due Care" และ "Due Diligence" คือ มีความละเอียดรอบคอบเข้าใจปัญหาด้านความปลอดภัยข้อมูลคอมพิวเตอร์เป็นอย่างดี และ มีการทำสัญญากับ MSSP อย่างรัดกุมโดยกำหนด SLA (Service Level Agreement) อย่างชัดเจน จะทำให้ ไม่เกิดปัญหาทั้งสองฝ่ายเมื่อได้เข้ามาร่วมงานกัน เพราะ องค์กร (ผู้ว่าจ้าง) กับ MSSP (ผู้รับจ้าง) จะต้องทำงานร่วมกันอยู่ตลอดเวลา แต่ทำงานคนละบทบาท และ มีการแบ่งแยกขอบเขตของความรับผิดชอบ โดยระบุรายละเอียดใน SLA ไว้ให้ชัดเจน

ข้อดีหรือประโยชน์จากการใช้บริการ "MSSP" ได้แก่

1. ลดต้นทุน การจ้าง "MSSP" นั้น ควรช่วยองค์กรประหยัดค่าใช้จ่ายในการจ้างพนักงานประจำ (Full Time Employee) หรือ พนักงาน In-House Security Engineer ระดับ Expert ที่จะมาดูแลระบบให้องค์กรโดยตรง ซึ่งมีค่าตัวค่อนข้างสูงถึงสูงมาก อาจไม่เหมาะกับการจ้างในรูปแบบเงินเดือน ถ้าเป็นองค์กรใหญ่ๆ อาจจะไม่มีปัญหาเรื่องนี้ แต่สำหรับองค์กรขนาดกลางหรือ SME นั้นการจัดตั้งแผนก "INFOSEC" ถือเป็นการเพิ่มค่าใช้จ่ายให้องค์กร ซึ่งผู้บริหารต้องทบทวนเรื่องนี้พอสมควร
2. แก้ปัญหาเรื่องขาดบุคลากรเชี่ยวชาญเฉพาะด้าน INFOSEC ปัญหาใหญ่ของหน่วยงานและองค์กรโดยทั่วไปก็คือการขาดคนที่มีความรู้ ทักษะและความสามารถเฉพาะทางด้านระบบความปลอดภัยข้อมูลโดยตรง ทำให้ต้องมีการรับสมัครงาน การฝึกอบรมพนักงาน การจูงใจต่างๆ ให้พนักงานที่มีความเชี่ยวชาญและความชำนาญแล้วยังคงทำงานกับองค์กรต่อไป โดยไม่ลาออกไปทำงานที่อื่นซึ่งเสนออัตราเงินเดือนสูงที่กว่าเป็นต้น แต่เมื่อองค์กรจัดจัดจ้าง "MSSP" แล้วหน้าที่ต่างๆ เหล่านี้จะ

เป็นของ "MSSP" ไม่ใช่ขององค์กร โดยผู้บริหารไม่ต้องมากังวลเรื่องปัญหาบุคลากรอีกต่อไป เนื่องจาก "MSSP" จะเป็นผู้คัดสรรและจัดเตรียมคนที่จะทำงานร่วมกันตามสัญญาที่ระบุไว้ใน SLA เป็นหน้าที่ของ "MSSP" ที่ต้องดูแล Security Expert ของตนเพื่อให้บริการกับลูกค้าอยู่แล้ว บุคลากรที่เป็น Security Expert นั้นถือเป็นหัวใจสำคัญที่ "MSSP" ทุกที่ต้องม

3. มีความเชี่ยวชาญมากกว่า เราต้องยอมรับว่าบุคลากรไอทีภายในองค์กรของเรา มีโอกาสพบกับการแก้ปัญหาเรื่อง INFOSEC น้อยมาก อาจพบเฉพาะปัญหาที่เกิดขึ้นกับองค์กรเสียเป็นส่วนใหญ่ ขณะที่บุคลากรของ "MSSP" นั้น มีโอกาสได้รับข้อมูลเรื่องนี้อยู่เวลา และ มีประสบการณ์การแก้ปัญหาเรื่อง INFOSEC กับลูกค้าหลายราย บุคลากรของ "MSSP" มีการศึกษาวิจัย Focus เฉพาะเรื่อง "INFOSEC" อย่างเดียว ตลอดจนได้เข้ารับการฝึกอบรมอย่างสม่ำเสมอต่อเนื่อง จึงมีความเชี่ยวชาญและความชำนาญมากกว่า เราจึงได้ประโยชน์จากการจ้าง "MSSP" ในข้อนี้อย่างเห็นได้ชัด

4. สถานที่และอุปกรณ์ที่พร้อมกว่า "MSSP" ต้องมีการลงทุนกับศูนย์ปฏิบัติการด้านการเฝ้าระวังเครือข่ายหรือที่เรียกว่า Security Operation Center (SOC) ซึ่งต้องมีเครื่องไม้เครื่องมือทั้ง Hardware และ Software ที่เกี่ยวข้องกับระบบรักษาความปลอดภัย อาทิ Firewall, IDS, Centralized Log System และ Correlation Log Analysis System ตลอดจนบุคลากรคุณภาพต่างๆ ที่ต้องจัดจ้างไว้ตลอด 24 ชั่วโมงเพื่อเฝ้าระวังข้อมูลให้ลูกค้าของตน ซึ่งการลงทุนเหล่านี้ ถือเป็นประโยชน์ขององค์กร ที่จ้าง "MSSP" เพราะเราไม่ต้องลงทุนเองแต่ใช้ Facilities ที่มีความพร้อมของ "MSSP" แทน

5. ความเป็นอิสระในการให้ความเห็นอย่างมืออาชีพจาก "MSSP" "MSSP" เป็นองค์กรที่มีลักษณะของมืออาชีพที่ต้องให้ความเห็นอย่างตรงไปตรงมาและเข้าประเด็นเพื่อแก้ปัญหาเรื่องความปลอดภัยข้อมูลของผู้ว่าจ้างได้อย่างมีประสิทธิภาพ จึงเป็นการตรวจสอบการทำงานภายในของหน่วยงานผู้ว่าจ้างไปในตัวด้วยว่า ได้มีการจัดการด้านการรักษาความปลอดภัยอย่างเพียงพอและเป็นไปตามนโยบายความปลอดภัยขององค์กร (Corporate Security Policy) หรือไม่

6. ข้อมูลที่ลึกและรู้ก่อนจาก "MSSP" โดยปกติแล้ว "MSSP" จะมี "Security Awareness" ในระดับที่สูงกว่าองค์กรทั่วๆ ไป เพราะว่าได้ทำงานด้านนี้โดยตรง ข่าวสารการค้นพบช่องโหว่ของระบบหรือ Vulnerability ใหม่ๆ และ Exploit ใหม่ๆ ที่ยังเป็น Zero-Day อยู่ ซึ่งยังไม่ประกาศเตือนโดย "CERT" (www.cert.org) อย่างเป็นทางการนั้น "MSSP" จะรู้ข้อมูลก่อนจากเครือข่ายใต้ดินของกลุ่มแฮกเกอร์ที่ "MSSP" ต้องส่งบุคลากรไปศึกษาและล้วงข้อมูลจากบรรดา "BlackHat Hacker" เข้าทำนองสายตำรวจหรือสายลับ เพื่อที่จะได้รู้ข้อมูลล่วงหน้าก่อนที่จะได้เตือนลูกค้าให้เฝ้าระวังและเตรียมป้องกันได้อย่างทันท่วงที

7. ติดตั้งประสานงานกับตำรวจ หรือ DSI (Department of Special Investigation) เพื่อนำ Hacker มาลงโทษ "MSSP" ที่ดีควรมีหน้าที่ในการประสานงานกับสำนักงานตำรวจแห่งชาติ หรือ กรม

สอบสวนคดีพิเศษ (DSI) ในการตามจับตัวแฮกเกอร์ และ หาที่มาของการจู่โจมซึ่ง "MSSP" ใช้วิธีที่เรียกว่า "นิติคอมพิวเตอร์" หรือ "Computer Forensic" ในการแกะรอยแฮกเกอร์หรือผู้ต้องสงสัย เพื่อหาหลักฐาน (Evidence) มาประกอบในชั้นศาล เมื่อกฎหมายอาชญากรรมคอมพิวเตอร์ประกาศใช้ก็สามารถนำผู้กระทำผิดมาลงโทษได้จากข้อมูลดังกล่าว

8. การบริการที่พร้อมอยู่เสมอ "MSSP" ส่วนใหญ่จะปฏิบัติงานดูแลลูกค้าแบบ 24 ชั่วโมง x 7 วัน อยู่แล้ว ลูกค้าสามารถเรียกใช้บริการได้ตาม SLA ที่ตกลงกันในการจัดจ้าง และ "MSSP" ต้องเตรียมความพร้อมอยู่ตลอดเวลาในกรณีที่ลูกค้าต้องการความช่วยเหลืออย่างเร่งด่วน

9. "MSSP" มีเทคโนโลยีที่ทันสมัยกว่าและหน่วยงานผู้ว่าจ้างไม่ต้องคอยดูแลตามเทคโนโลยีใหม่ ๆ อยู่ตลอดเวลา อุปกรณ์เครื่องมือทั้งหลายที่ "MSSP" ทำมาใช้นั้น "MSSP" ต้องเป็นผู้ลงทุนเองเช่น Vulnerability Scanner รวมถึงการทำ Maintenance เพื่อ Update Signature ซึ่ง "MSSP" เป็นผู้รับผิดชอบทั้งหมด การใช้โปรแกรมใหม่ๆ หรือเทคโนโลยีใหม่ๆ ก็เป็นหน้าที่ที่ "MSSP" จะต้องรับไป เพราะถือว่า "MSSP" เป็นมืออาชีพที่ต้องทำหน้าที่เป็น ที่ปรึกษาด้านความมั่นคงปลอดภัย (INFOSEC Consultant) ไปในตัว

อย่างไรก็ตามการใช้บริการ "MSSP" เองก็มีจุดอ่อนหรือข้อเสียอยู่บ้างที่ต้องระมัดระวังได้แก่

ข้อเสียที่ควรระวังในการจัดจ้าง "MSSP"

1. ความไว้วางใจใน "MSSP" ถามว่าเราจะไว้ใจ "MSSP" ได้แคไหนในการที่จะให้มารับผิดชอบดูแลระบบรักษาความปลอดภัยของเรา เราควรมีการตรวจสอบประวัติการทำงาน และ Customer Site References ของ "MSSP" ก่อนที่เราจะจัดจ้าง "MSSP" ว่ามีความเชื่อถือได้มากน้อยเพียงใด ข้อมูลที่มีความละเอียดอ่อนหรือ Sensitive มากๆนั้น หน่วยงานผู้ว่าจ้างอาจต้องดูแลด้วยตัวเอง คือไม่ "Outsource" ไปเสียทั้งหมด เราควร "Outsource" เฉพาะในส่วนของการเฝ้าระวังด้วยระบบป้องกันการบุกรุก (IDS) การวิเคราะห์ Log ที่เกิดขึ้นจากอุปกรณ์ต่างๆ ในลักษณะวันต่อวัน การให้ปรึกษาและ แนะนำในเรื่องใหม่ ๆ เกี่ยวกับ INFOSEC และการเตือนภัยล่วงหน้าจาก "MSSP"

2. การยึดกับ "MSSP" มากเกินไป ความคิดที่ว่าหากองค์กรจ้าง "MSSP" ในการดูแลระบบความปลอดภัยแล้วเราไม่ต้องสนใจความปลอดภัยระบบของเราอีกเลย เพราะมี "MSSP" ดูให้ เป็นความคิดที่ผิดพลาด เพราะอย่างไรเราก็ต้องดูแลด้วยบุคลากรภายในองค์กรเองอยู่ในระดับหนึ่ง เรียกว่าเป็นการควบคุมการทำงานของ "MSSP" การลดภาระงานหรือ Work Load ต่างๆ ที่ต้องเกิดกับองค์กรของเราโดยให้เป็นหน้าที่ของ "MSSP" เพราะเราจ้าง "MSSP" แล้วก็ต้องให้เขารับผิดชอบให้มากที่สุดเท่าที่จะทำได้แต่ไม่ใช่ทั้งหมด

3. ความรู้สึกเป็นเจ้าของระบบที่แตกต่างกัน ถ้าเป็นระบบขององค์กรเราเอง เราย่อมต้องดูแลเป็นอย่างดี แต่ถ้าเราจ้าง "MSSP" มาดูแลระบบเรานั้นความรู้สึกในความเป็นเจ้าของระบบย่อมแตกต่าง

กัน เพราะ "MSSP" เป็นเพียงผู้รับจ้างดูแลระบบแต่ไม่ใช่เจ้าของระบบเอง ดังนั้นความมีการกำหนดข้อตกลงรายละเอียดต่างๆ ให้ชัดเจนใน SLA ว่าใครต้องรับผิดชอบอะไร และมีการตรวจสอบการทำงานของ "MSSP" ทุกเดือน ว่าเป็นไปตาม SLA หรือไม่

4. ปัญหาการใช้ทรัพยากรร่วมกัน ทรัพยากรของ MSSP ส่วนใหญ่ จะมีการแบ่งใช้ในการบริการลูกค้าหลายๆ ราย ซึ่งต้องมีการจัดการอย่างดี ไม่ให้มีการเชื่อมโยงถึงกัน ข้อมูลของลูกค้าแต่ละรายต้องแยกออกจากกันอย่างสิ้นเชิง ไม่ให้มีการรั่วไหลที่ "MSSP" เสียเอง และ "MSSP" จะต้องเขียน NDA (Non-Discloser Agreement) เพื่อรับรองว่าจะไม่นำความลับหรือข้อมูลที่สำคัญของลูกค้าไปเปิดเผย

5. ปัญหาเรื่องการติดตั้งระบบเฝ้าระวังและตรวจจับผู้บุกรุก (Intrusion Detection System) การติดตั้งระบบเฝ้าระวังและตรวจจับผู้บุกรุก (Intrusion Detection Systems) และ Centralized Log System ต้องติดตั้งโดย "MSSP" ที่มีความชำนาญงานโดยเฉพาะซึ่งต้องมีการวางแผนเป็นอย่างดีไม่ให้กระทบหรือเกิดช่องโหว่ขึ้นในระบบ

6. ปัญหาการทำงานร่วมกัน บางครั้งทีมงานของ "MSSP" ไม่สามารถทำงานร่วมกับทีมงานของผู้ว่าจ้างได้ เพราะไม่ค่อยได้พูดจากัน หรือ อาจเกิดข้อพิพาทระหว่างกัน ทำให้มีทัศนคติในเชิงลบต่อกัน เกิดช่องว่าง หรือ "GAP" ในการประสานงาน เพราะฉะนั้น "MSSP" และ ผู้ว่าจ้างควรมีการจัดการประชุมในทางสร้างสรรค์เพื่อพบปะกันเป็นระยะๆ มีการโต้ตอบ อีเมล์และมีการพูดคุยกันทางโทรศัพท์อยู่เสมอ เพื่อที่จะได้ประสานงานร่วมกันได้อย่างมีประสิทธิภาพ

7. ต้นทุนแฝงที่อาจเกิดขึ้น หากมีการทำงานที่เกิดขึ้นนอกข้อกำหนดใน SLA ซึ่งต้องมีค่าใช้จ่ายที่เพิ่มขึ้นแล้วใครจะเป็นผู้รับผิดชอบระหว่าง "MSSP" กับผู้ว่าจ้าง ดังนั้นควรมีการกำหนดใน SLA ให้ละเอียดว่าจะมี Additional Expenses หรือ ค่าใช้จ่ายเพิ่มเติมอะไรบ้างที่นอกเหนือจากข้อตกลงปกติ

8. ความเข้าใจที่ไม่ลงตัวระหว่าง "MSSP" กับ ผู้ว่าจ้าง ปัญหาข้อนี้ จะคล้ายๆ กับข้อ 7 ก็คือขณะที่ร่างสัญญา SLA นั้นไม่มีความรัดกุมเพียงพอ ดังนั้นควรจะใช้เวลาส่วนใหญ่กับการร่างสัญญา SLA ให้มีความรัดกุม เพื่อไม่เกิดปัญหาระหว่างทั้งสองฝ่ายในภายหลังและควรทำความเข้าใจในเรื่องต่างๆ กันเสียก่อนที่จะร่วมมือกัน จะป้องกันปัญหาที่อาจเกิดขึ้นในอนาคต

กล่าวโดยสรุป การทำสัญญาใช้บริการจาก MSSP (Managed Security Service Provider) มาดูแลระบบความมั่นคงปลอดภัยในองค์กรเรานั้น ถือเป็นสิ่งสำคัญและจำเป็นสำหรับองค์กรในอนาคตอันใกล้นี้ ทว่าควรมีการจัดจ้างที่ระมัดระวังและรัดกุมโดยกำหนดใน SLA (Service Level Agreement) ให้ชัดเจน แล้วประโยชน์โดยรวมก็จะอยู่ที่องค์กรในที่สุด

ตำแหน่งผู้บริหารใหม่ในองค์กรยุคไฮเทค CSO (Chief Security Officer) /CISO (Chief Information Security Officer) ทำไมต้องมี CSO/ CISO

ในยุคที่โลกกลายเป็นเครือข่ายที่ไร้พรมแดน เราสามารถเข้าถึงข้อมูลข่าวสารซึ่งอยู่ในรูปแบบดิจิตอลได้อย่างรวดเร็ว Broadband Internet กำลังได้รับความนิยมเพิ่มขึ้น ขณะที่ไวรัสคอมพิวเตอร์ก็เริ่มทวีความรุนแรงเพิ่มเป็นเงาตามตัวเช่นกัน "Information Security" หรือ "InfoSec" กลายเป็นศาสตร์ที่เราต้องศึกษาเรียนรู้เพื่อป้องกันความปลอดภัยข้อมูลสารสนเทศที่อยู่ในระบบเครือข่ายซึ่งมีการต่อเชื่อมกับระบบอินเทอร์เน็ตโดยใช้โปรโตคอล TCP/IP การจู่โจมของแฮกเกอร์และไวรัสมีอัตราเพิ่มสูงขึ้นตามอัตราการเพิ่มขึ้นของช่องโหว่ (Vulnerability) ในตัวโปรโตคอล TCP/IP เองและในระบบปฏิบัติการที่เราใช้อยู่เป็นประจำไม่ว่าจะเป็น Windows, UNIX หรือ Linux แต่เดิมเราเน้นเรื่องการป้องกันระบบความปลอดภัยข้อมูลสารสนเทศในมุมมองทางด้านเทคนิคเพียงอย่างเดียว โดยที่เราไม่ค่อยได้ให้ความสำคัญกับมุมมองในด้านการจัดการบริหารให้มีประสิทธิภาพ และประสิทธิผล ปัญหาเรื่องความปลอดภัยข้อมูลสารสนเทศ ไม่ใช่แค่ซื้อ Firewall และ Anti-Virus Program แล้วจะจบ แต่กลายเป็นปัญหาด้านอื่นที่ต้องพิจารณาเช่นการทำ Patch Management, Users & Executives Information Security Awareness Training ตลอดจนปัญหาด้าน Physical Security ก็เป็นเรื่องที่มองข้ามไม่ได้เช่นกัน

CSO หรือ CISO เป็นตำแหน่งผู้บริหารระดับสูงทางด้านการรักษาความปลอดภัยให้กับโครงสร้างเครือข่ายและความปลอดภัยข้อมูลสารสนเทศ CSO มีหน้าที่ในการจัดการกับปัญหาความปลอดภัยดังกล่าว โดย CSO ต้องมีความเข้าใจในระบบธุรกิจเป็นอย่างดี (Business Process) และต้องเข้าใจเรื่องของการจัดการกับความเสี่ยง (Risk Management) ที่มีโอกาสเกิดขึ้นแล้วมีผลกระทบกับธุรกิจขององค์กรทั้งทางตรงและทางอ้อม ในมุมมองทั้งด้านเทคนิค การจัดการตลอดจนกำหนดนโยบายการรักษาความปลอดภัยระบบเครือข่ายและข้อมูลสารสนเทศให้ได้ตามมาตรฐานสากล โดยนำนโยบายมาตรฐานเช่น ISO/IEC17799 หรือ ISACA CobiT Framework มาจัดการกับระบบในองค์กรให้มีความปลอดภัยในลักษณะบรรษัทภิบาลหรือที่เราเรียกว่า "Corporate Governance"

ความรับผิดชอบของ CSO/ CISO 10 ข้อ

1. กำหนดเป้าหมาย นโยบายด้านการรักษาความปลอดภัยข้อมูล โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ขององค์กร (Corporate Strategic Plan)
2. จัดการพัฒนานโยบายด้านการรักษาความปลอดภัยข้อมูล Policy, Standard, Procedure and Guideline เพื่อให้องค์กรได้มาซึ่ง การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)

ยกตัวอย่าง การรับผิดชอบจัดทำแผน Information Security Awareness Training ให้กับบุคลากรขององค์กรที่ต้องใช้คอมพิวเตอร์ในการทำงานให้มีความรู้ความเข้าใจกับภัยอินเทอร์เน็ต

3. จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่างๆ ที่อาจเกิดขึ้นกับระบบ โดยใช้ระบบเตือนผู้บุกรุก Intrusion Detection System (IDS), ระบบป้องกันผู้บุกรุก Intrusion Prevention System (IPS) หรือระบบจัดการกำจัดไวรัส (Anti-Virus Systems) ตลอดจนวางแผน Business Continuity และ Disaster Recovery (BCP and DRP) เพื่อกู้ระบบยามฉุกเฉิน
4. มีการบริหารความเสี่ยง (Risk Management) และการวิเคราะห์ความเสี่ยง (Risk Analysis) ที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจขององค์กร
5. นำเสนอผู้บริหารระดับสูงเช่น CIO หรือ CEO ในเรื่องของแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง ตลอดจนแผนการ Outsource ด้านความปลอดภัยข้อมูลเพื่อขอดำเนินการอนุมัติ และเพื่อให้ผู้บริหารระดับสูงมีความตระหนัก (Awareness) ในความสำคัญเรื่อง Information Security
6. เป็นที่ปรึกษาด้านระบบความปลอดภัยข้อมูลให้กับแผนกอื่นๆ ที่ต้องใช้ IT ในการปฏิบัติงาน
7. ติดต่อและรักษาความสัมพันธ์กับคู่ค้า, องค์กร หรือบุคคลภายนอกที่มีความเกี่ยวข้องกับเรื่องความปลอดภัยข้อมูลทั้งภาครัฐและเอกชนเช่น ตำรวจ, นักข่าว, Systems Integrator (SI), Outsourcer, Managed Security Services Provider (MSSP) และผู้ตรวจสอบ (Auditor)
8. ออกข้อกำหนดในการจัดซื้อจัดจ้างระบบรักษาความปลอดภัยข้อมูลสารสนเทศ Requests for Proposal (RPF)
9. จัดตั้งและควบคุมบริหารทีม Incident Response เพื่อให้สามารถปฏิบัติงานในยามที่เกิดภาวะฉุกเฉินขึ้นในองค์กร เช่น การระบาดของไวรัสคอมพิวเตอร์
10. เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ๆ ทางด้าน Information Security อย่างสม่ำเสมอ

คุณสมบัติของ CSO/ CISO

1. มีความรู้ความสามารถด้าน Information Technology และ Information Security ในระดับบริหารจัดการ และ ควรสอบผ่านประกาศนียบัตร CISSP (Certified Information Systems Security Professional) (see http://www.isc2.org)

2. มีคุณสมบัติความเป็นผู้นำและมีประสบการณ์การทำงานในระดับผู้จัดการระบบสารสนเทศมาไม่ต่ำกว่า 5 ปี และ มีอายุระหว่าง 30-45 ปี
3. ควรมีประสบการณ์เฉพาะด้าน Risk Management, BCP, DRP, IT Audit, SLA Contract and Vendor Negotiation
4. ควรมีประสบการณ์เกี่ยวกันการแก้ปัญหาที่เกี่ยวกับไวรัสคอมพิวเตอร์หรือแฮกเกอร์ตลอดจนพื้นฐานความเข้าใจเรื่องกฎหมายอาชญากรรมคอมพิวเตอร์ (Computer Crime Laws)
5. มีความรู้เรื่องพื้นฐานด้านระบบความปลอดภัยเช่น Firewall, IDS, Anti-Virus, VPN, PKI, Vulnerability Assessment และ Penetration Testing
6. มีความสามารถและทักษะในการติดต่อสื่อสารกับผู้บังคับบัญชาและผู้ใต้บังคับบัญชาเป็นอย่างดี ทั้ง Technical Staff และ Non-Technical Staff

สรุปบทบาท CSO/CISO

กล่าวโดยสรุปตำแหน่ง CSO/ CISO เป็นตำแหน่งที่มีความสำคัญอย่างยิ่งในการบริหารงานความปลอดภัยระบบสารสนเทศขององค์กรในทุกวันนี้ และ ควรมีการกำหนดบทบาทหน้าที่ตลอดจนโครงสร้างขององค์กร (Organization Chart) ให้รองรับกับตำแหน่ง CSO/CISO ซึ่งอาจจะขึ้นกับ CIO หรือ ขึ้นกับ CEO โดยตรง เราควรพิจารณาตามลักษณะการดำเนินธุรกิจและยุทธศาสตร์ขององค์กร โดยมีจุดประสงค์หลัก คือลดผลกระทบจากความเสี่ยงที่อาจจะเกิดขึ้นกับองค์กรให้น้อยที่สุดเท่าที่จะทำได้ (Risk Management and IT governance)

5. IT Support

หน้าที่ของ IT Support สามารถแยกตามระดับ ได้ดังนี้

<u>Level one</u>

งานที่เกี่ยวข้องการกราประยุกต์ใช้ความรู้ที่เรียนมา ในความหลายหลายของสายงาน อาจเป็นงานประจำทุกวัน และสามารถคาดการณ์เหตุการณ์ได้

- บุคลากร/ประชาชน
- ด้านเทคนิค/การจัดการ
- ด้านข้อมูล/การบริหาร

Level Two

งานที่เกี่ยวข้องการกราประยุกต์ใช้ความรู้ที่เรียนมา ในความหลายหลายของสายงาน อาจเกี่ยวข้องกับกิจกรรมที่ไม่ได้ทำเป็นประจำ หรือต้องการความรับผิดชอบที่แยกออกมา การประสานงานระหว่างผู้ร่วมงานจึงมีความจำเป็นอย่างมาก

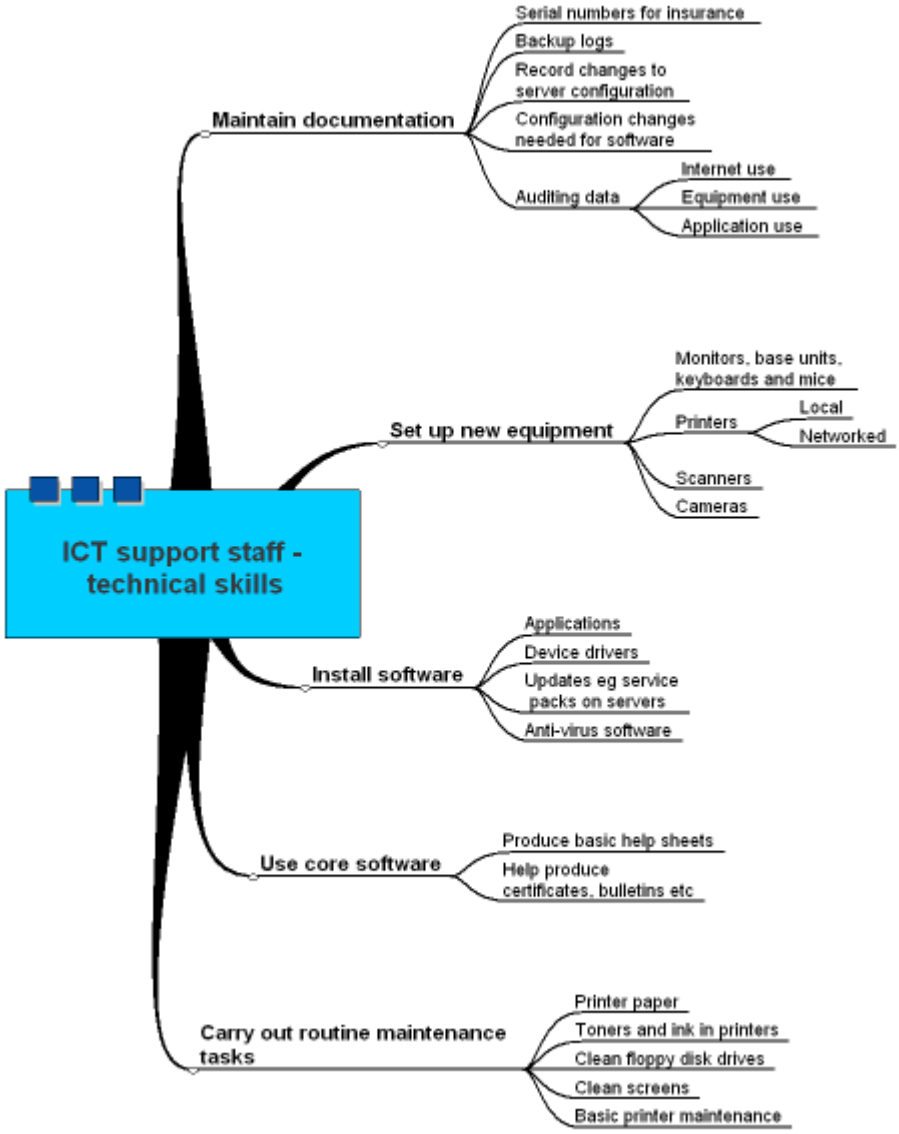
- บุคลากร/ประชาชน
- ด้านเทคนิค/การจัดการ
- ด้านข้อมูล/การบริหาร
- การให้ความช่วยเหลือด้านเทคนิค

Level Three

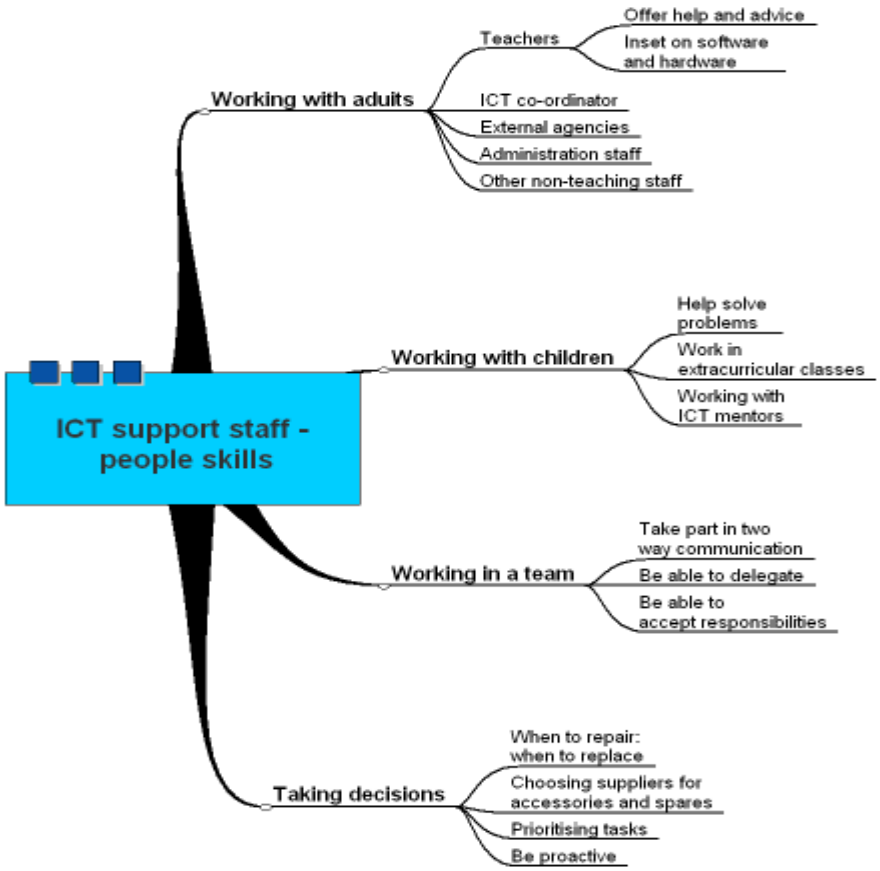
งานที่เกี่ยวข้องการกราประยุกต์ใช้ความรู้ที่เรียนมา รวมถึงความรู้อันหลายหลาย ใช้ในเนื้องานที่มีความแตกต่างกันออกไป ส่วนใหญ่เป็นงานที่ซับซ้อน ซึ่งไม่ได้เกิดขึ้นทุกวัน จำเป็นต้องมีความผิดชอบเฉพาะด้านเพื่อแก้ปัญหานั้นๆ การ ควบคุมและการดูแลเอาใจใส่จึงมีความจำเป็นอย่างยิ่ง

- บุคลากร/ประชาชน
- ด้านเทคนิค/การจัดการ
- ด้านข้อมูล/การบริหาร
- การให้ความช่วยเหลือด้านเทคนิค
- การจัดการด้านเวลา
- การจัดการทีมของช่างเทคนิค รวมถึงพนักงานช่วยเหลือ

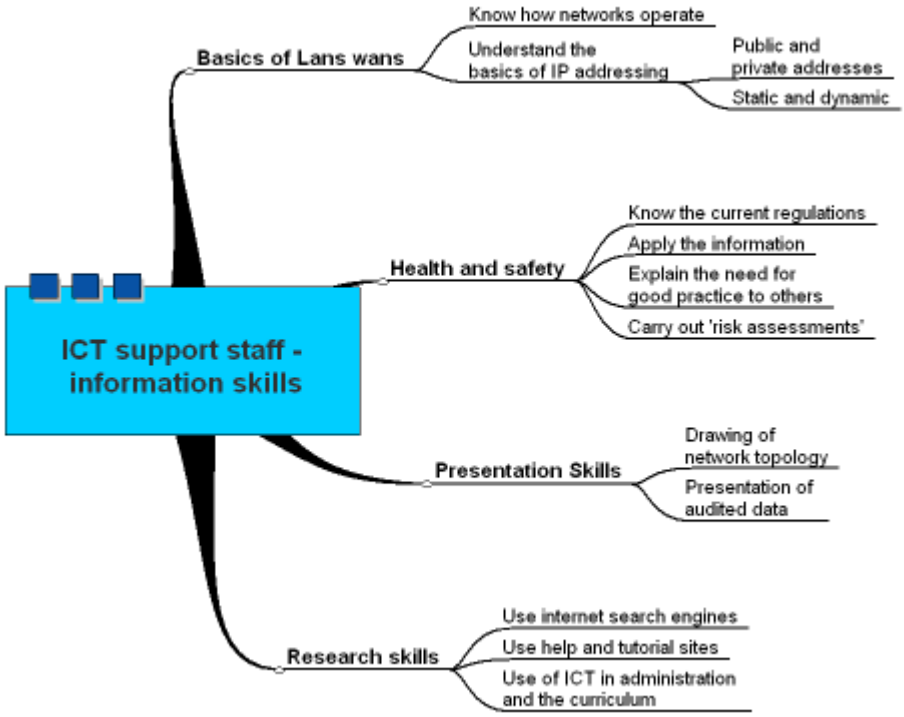
ICT support staff - technical skills



ICT support staff - people skills



ICT support staff - information skills



6. IT Trianer

เจ้าหน้าที่ฝึกอบรมหรือวิทยากรด้านไอทีเป็นผู้รับผิดชอบในการฝึกอบรม มีบทบาทเป็นทั้งผู้ประสานและให้บริการในการ จัดการฝึกอบรม เป็นผู้ให้คำแนะนำและเป็นที่ปรึกษาของผู้บริหารในองค์การ และเป็นผู้สร้างเสริมทัศนคติเชิงบวกที่ก่อให้เกิดการ ปรับเปลี่ยนพฤติกรรมของบุคลากรในองค์การ ดังนั้น เจ้าหน้าที่ฝึกอบรมต้องมีความพร้อมในตนเองไม่ว่าจะเป็นด้านความรู้และ ทักษะในงานฝึกอบรมโดยตรง ความรู้ในการดำเนินธุรกิจขององค์การ ความเข้าใจในวัฒนธรรมองค์การ ความเข้าใจในปัญหาและ พฤติกรรมของบุคลากรในองค์การโดยภาพรวม และที่สำคัญที่สุด เจ้าหน้าที่ฝึกอบรมองต้องมีทัศนคติที่ดีต่องานฝึกอบรม ทุ่มเท เสียสละ และมีจิตสำนึกที่ดีงามต่องาน ต่อผู้บริหาร และต่อองค์การของตนเอง ยิ่งไปกว่านั้นเจ้าหน้าที่ฝึกอบรมควรเป็นผู้มีมนุษยสัมพันธ์ที่ดีจึงจะได้รับความร่วมมือจากทุกฝ่ายที่เกี่ยวข้อง ทั้งฝ่ายจัดการและผู้บริหารขององค์การ ผู้บริหารงานฝึกอบรม ผู้บังคับ บัญชาต้นสังกัดของผู้เข้ารับการฝึกอบรม ผู้เข้ารับการฝึกอบรม วิทยากร และผู้เกี่ยวข้องทุกฝ่าย

การพัฒนาบุคลากรด้านไอทีในองค์การต่างๆ เริ่มมองหาผู้เชี่ยวชาญจากภายนอกเข้ามาให้ความรู้แก่คนในองค์การมากยิ่งขึ้น เพราะถ้ามัวแต่สอนกันเอง เรียนกันเอง อาจจะพลาดโอกาสทางการแข่งขันที่ดีๆไปได้ เพราะมุมมอง ความน่าเชื่อถือและการยอมรับของวิทยากรภายในนั้นมีน้อยกว่าการเชิญวิทยากรจากภายนอกเข้ามา หลายองค์การเริ่มเปลี่ยนแปลงการคัดเลือกวิทยากรแบบมีคนแนะนำ ไปสู่การสรรหาและคัดเลือกอย่างเป็นระบบมากยิ่งขึ้น ทำให้การบริการทางวิชาการของวิทยากรเป็นลักษณะของ Out-source มากขึ้น

เมื่อบทบาทของวิทยากรไอทีถูกจัดให้เป็นผู้ขาย(Supplier)ที่ผู้สนับสนุนวัตถุดิบทางความรู้ให้กับองค์การแล้ว วิทยากรควรจะต้องปรับเปลี่ยนบทบาทให้ก้าวทันกับความต้องการของลูกค้า (Customers Needs) ให้ได้ การแข่งขันในตลาดวิทยากรก็ย่อมมีมากขึ้น ซึ่งน่าจะเป็นสัญญาณที่ดีและเป็นโอกาสที่ดีสำหรับวิทยากรที่มีคุณภาพ ในขณะเดียวกันก็เป็นโอกาสที่ดีของผู้ใช้บริการที่จะสามารถมีตัวเลือกได้มากขึ้น ซึ่งวิทยากรด้านไอทีที่มีคุณภาพและเป็นที่ต้องการของลูกค้าควรจะมีคุณสมบัติดังนี้

- **วิทยากรต้องมีแนวคิดแบบ Supplier**
  การเป็น Supplier จะต้องทำหน้าที่หนักกว่าวิทยากรที่เคยมีมาในอดีต คือ ต้องเข้าไปศึกษาความต้องการของลูกค้าก่อนที่จะขายสินค้า ไม่ใช่มีความรู้สำเร็จรูปแล้วนำออกไปขาย แต่ต้องทำในลักษณะทำตามคำสั่งซื้อมากขึ้น นอกจากนี้การเป็นผู้ขายนั้นจะถูกกำหนดสเปก

สินค้าและบริการอย่างเข้มงวดมากขึ้น มีการตรวจสอบทุกขั้นตอนมากขึ้น โอกาสที่จะถูกปฏิเสธ(reject) การสั่งซื้อในครั้งต่อไปก็มีมากขึ้นเช่นกัน ดังนั้นวิทยากรจะมัวแต่คิดว่าตัวเองเป็นผู้มีเกียรติ เล่นตัว หรือผู้เรียนจะแตะต้องไม่ได้ คงจะไม่มีอีกต่อไป

- **วิทยากรต้องเป็นผู้เชี่ยวชาญเฉพาะด้านมากขึ้น**
  วิทยากรบางท่านสามารถบรรยายได้ตั้งแต่หลักสูตรเด็กอนุบาล(basic) จนถึงหลักสูตรผู้บริหารระดับสูง (advance) ขอให้บอกมาเถอะจะบรรยายได้หมด แต่บรรยายแล้วรู้เรื่องหรือไม่นั้นเป็นเรื่องของผู้ฟังไม่ใช่เรื่องของวิทยากร วิทยากรแบบนี้มีแนวโน้มลดลงและจางหายไปในที่สุด คงเหลือเฉพาะวิทยากรที่ชำนาญเฉพาะด้านมีความรู้จริงและรู้ลึกมากขึ้น
- **วิทยากรต้องสามารถเชื่อมโยงความเชี่ยวชาญเฉพาะด้านสู่ภาพรวมขององค์การได้**
  วิทยากรแบบตาบอดคลำช้างจะจางหายไป เหลือแต่วิทยากรที่เข้าใจว่าช้างทั้งตัวเป็นอย่างไร และส่วนที่ตัวเองคลำอยู่นั้นอยู่ตรงส่วนไหนของช้าง และส่วนนั้นๆมีความสำคัญต่อการดำรงชีวิตของช้างอย่างไร ดังนั้น วิทยากรจะต้องพัฒนาความรู้ทั้งที่เป็นความรู้เฉพาะที่ตัวเองถนัดควบคู่ไปกับความรู้ระบบใหญ่ขององค์การด้วย
- **วิทยากรต้องมีส่วนร่วมรับผิดชอบต่อผลการพัฒนาฝึกอบรมของลูกค้า**
  วิทยากรจะต้องเข้าไปมีส่วนร่วมกับลูกค้าตั้งแต่การกำหนดความจำเป็นในการฝึกอบรม การจัดฝึกอบรม การวัดผลและติดตามผลการฝึกอบรมมากยิ่งขึ้น เพราะถ้าผู้จัดฝึกอบรมไม่ประสบความสำเร็จในการพัฒนาคนในสายตาของผู้บริหาร ย่อมเป็นที่แน่นอนว่างบประมาณการจัดฝึกอบรมจะน้อยลง รายได้ของวิทยากรก็จะน้อยลงตามไปด้วย ดังนั้นวิทยากรจะต้องดูแลและช่วยเหลือให้แหล่งรายได้ของวิทยากรยังคงอยู่และเติบโตต่อไป
- **ต้องเป็นวิทยากรออนไลน์**
  วิทยากรยุคนี้และยุคหน้าจะต้องติดตามข้อมูลข่าวสาร วิชาการและองค์ความรู้อยู่ตลอดเวลา และถ้ามัวแต่อ่านหนังสือเพียงอย่างเดียวอาจจะไม่ทันกิน วิทยากรต้องทันสมัยก้าวทันเทคโนโลยี เพราะทุกอนูของเทคโนโลยีย่อมซ่อนเร้นไปด้วยองค์ความรู้หรือจะนำเราไปสู่แหล่งความรู้เสมอ วิทยากรต้องใช้อินเตอร์เน็ตให้เป็นประโยชน์ทั้งในแง่การค้นคว้าหาข้อมูล การนำเสนอ การบริการวิชาการต่อลูกค้า การติดต่อสื่อสารกับลูกค้า วิทยากรจะต้องสามารถบริการลูกค้าได้โดยไม่ติดขัดเรื่องข้อจำกัดของระยะทาง
- **เปลี่ยนจากวิทยากร Hard Copy เป็นวิทยากรแบบ Soft Copy**
  พื้นฐานการทำงานของผู้เรียนเปลี่ยนไปสู่การทำงานแบบออนไลน์แล้ว สำนักงานเป็นแบบไร้กระดาษไปแล้ว ไม่มีใครอยากเก็บองค์ความรู้อยู่ในรูปของกระดาษหรือเอกสารอีกต่อไปแล้ว ดังนั้น วิทยากรจึงต้องเปลี่ยนแปลงตามให้ทันด้วย อนาคตแผ่นใสจะกลายเป็น

การนำเสนอด้วยคอมพิวเตอร์ เอกสารประกอบการสัมมนาจะกลายเป็นแผ่นดิสเก็ตหรือไฟล์ข้อมูลที่ส่งไปให้ผู้เรียนทางอีเมล

- **วิทยากรต้องมีบริการหลังการขาย**
  การแข่งขันในตลาดของวิทยากรจะทวีความรุนแรงมากขึ้น วิทยากรจึงต้องมีการเพิ่มเติมบริการให้กับลูกค้าให้มากขึ้น และที่สำคัญคือวิทยากรจะต้องมีทางเลือกให้กับลูกค้าในเรื่องของการให้บริการหลังการบรรยายหรือฝึกอบรม เพื่อสนับสนุนข้อมูลหรือความรู้เพิ่มเติม รวมถึงการเข้าไปร่วมแก้ไขปัญหาอันสืบเนื่องมาจากการนำเอาความรู้ไปใช้งานจริง เมื่อเป็นเช่นนี้วิทยากรจะต้องรู้ลึกรู้จริงไม่เพียงแต่ทฤษฎีแต่จะต้องสามารถให้คำปรึกษาแก่ผู้เรียนในเชิงปฏิบัติได้ด้วย
- **วิทยากรต้องกำหนด Positioning ของตัวเอง**
  วิทยากรต้องกำหนดกลยุทธ์ในการให้บริการให้ชัดเจนว่าเรื่องใดคือหลักสูตรหลัก (Core Curriculum) หลักสูตรใดเป็นหลักสูตรรอง (Non-core curriculum) และหลักสูตรแบบใดที่เราจะไม่ทำ จะเข้าสู่ตลาดกลุ่มใด ลูกค้าระดับใด ต้องสร้าง Brand Loyalty ให้ลูกค้าจงรักภักดีให้ได้ ถ้าพูดถึงหลักสูตรนี้จะต้องพูดถึงเราหรืออย่างน้อยชื่อเราจะต้องอยู่ในอันดับท๊อปไฟว์ของวิทยากรชั้นนำในเรื่องนั้นๆ
- **วิทยากรแบบ Me Too จะลดลงโดยปริยาย**
  การกำหนด Positioning ของวิทยากรแต่ละคน แต่ละกลุ่มจะทำให้วิทยากรที่ไม่ค่อยคิดอะไรใหม่ๆ ชอบลอกของคนอื่น ใครทำอะไรได้ดีก็ขอทำตามด้วยคนจะมีแนวโน้มลดลงและหมดไป เพราะอะไรก็ตามที่ทำตามคนอื่นที่เขาประสบความสำเร็จไปแล้ว ย่อมต้องออกแรงมากกว่าคนอื่นเสมอ เพื่อฝ่าด่านการยอมรับของลูกค้าและเอาชนะความรู้ต้นแบบซึ่งไม่ใช่เรื่องง่ายๆอีกต่อไป นอกจากนี้การควบคุมเรื่องสินทรัพย์ทางปัญญาจะมีความเข้มงวดมากขึ้น

จากคุณสมบัติของวิทยากรด้านไอทีที่ควรจะเป็นจะเห็นว่าแนวโน้มคนที่จะเข้ามาสู่วิชาชีพนี้มีเสรีมากขึ้น คงไม่จำกัดเพียงคนที่มีชื่อเสียง คนที่เคยประสบความสำเร็จในอาชีพมาแล้ว หรือคนที่จบการศึกษาระดับสูงมาเท่านั้น แต่จะเปิดโอกาสให้กับคนทุกคนที่มีความรู้ความสามารถและมีใจรักในอาชีพนี้ และวิทยากรไอทียุคใหม่ต้องปรับตัวปรับใจให้เป็นหุ้นส่วนความสำเร็จทางธุรกิจให้กับลูกค้า (Business Partner) ให้ได้จึงจะอยู่สบายและอยู่ได้นาน

7. IT Certificate

ประกาศนียบัตรในผลิตภัณฑ์ต่างๆ นั้น เป็นเสมือนสิ่งที่รับรองบุคคลว่า บุคคลที่ได้รับประกาศนียบัตรนั้นมีความรู้ความชำนาญในเรื่องของผลิตภัณฑ์นั้น สามารถที่จะทำงานที่เกี่ยวข้องกับผลิตภัณฑ์นั้นได้อย่างมีประสิทธิภาพ หลายบริษัทและองค์กรต่างมีการออกประกาศนียบัตรเพื่อรับรองถึงคุณภาพของบุคลากรที่ได้รับประกาศนียบัตรของตน ซึ่งต้องมีการทดสอบในเรื่องความรู้และความชำนาญในผลิตภัณฑ์ของตน บทความนี้เป็นการบอกเล่าถึงประกาศนียบัตรประเภทต่างๆ ของแต่ละบริษัท เช่น ไมโครซอฟท์ ซิสโก้ ซัน และโนเวล นอกจากนี้ในตอนท้ายมีขั้นตอนในการเตรียมพร้อมเพื่อให้สามารถประสบความสำเร็จในการสอบใบประกาศนียบัตร

หากกล่าวถึงเรื่องของประกาศนียบัตร (Certificate) หรือใบรับรองความสามารถนั้น นับได้ว่าเป็นสิ่งที่รับรองถึงความรู้ความสามารถของบุคลากรด้านเทคโนโลยีสารสนเทศหรือไอทีจนถึงขั้นที่ว่าเป็นมาตรฐานเลยทีเดียว ในปัจจุบันผลิตภัณฑ์ด้านคอมพิวเตอร์ของบริษัทผู้ผลิต และองค์กรบางองค์กรได้ออกประกาศนียบัตรเพื่อรับรองถึงคุณภาพของบุคลากรที่ได้รับประกาศนียบัตรของตน

เทคโนโลยีในด้านต่างๆ มีการเคลื่อนไหวเปลี่ยนแปลงอย่างต่อเนื่องและรวดเร็ว โดยเฉพาะในส่วนของเทคโนโลยีด้านเทคโนโลยีสารสนเทศและคอมพิวเตอร์นั้นมีการพัฒนาปรับปรุงอยู่ตลอดเวลา บริษัทและองค์กรต่างๆ ที่มีการนำเทคโนโลยีเหล่านี้มาใช้ภายในองค์กรนั้น ย่อมต้องมีบุคลากรที่มีความรู้ในด้านของเทคโนโลยีดังกล่าว เมื่อความรู้และเทคโนโลยีมีการเปลี่ยนแปลง บุคลากรเหล่านั้ย่อมหลีกเลี่ยงไม่ได้ที่จะต้องเผชิญกับความเปลี่ยนแปลงเหล่านี้ จึงเป็นธรรมดาที่ต้องพัฒนายกระดับความรู้ความสามารถของตนเองให้สามารถทำงานกับเทคโนโลยีที่เปลี่ยนแปลงให้ได้ การพัฒนาความรู้ความสามารถของบุคลากรทำได้หลายทาง ยกตัวอย่าง เช่น การศึกษาหาความรู้ด้วยตนเอง การสอบถามจากบุคคลอื่นที่มีความรู้และความชำนาญมากกว่า และการเข้ารับการอบรม เป็นต้น การสอบเพื่อให้ได้ใบประกาศนียบัตรเป็นหนึ่งในแนวทางการยกระดับความรู้ความสามารถทางด้านเทคโนโลยีสารสนเทศของบุคลากร รวมถึงองค์กรตลอดจนถึงระดับประเทศด้วย

ปัจจุบัน เจ้าของผลิตภัณฑ์ต่างๆ นั้นมีการจัดสอบเพื่อวัดระดับความรู้ของบุคคลมีต่อผลิตภัณฑ์ของตนเพื่อที่จะสามารถประเมินได้อย่างคร่าวๆ ว่าบุคคลนั้นมีความรู้ความชำนาญในเรื่องของผลิตภัณฑ์มากน้อยเพียงไร บริษัทผู้เป็นเจ้าของผลิตภัณฑ์อันเป็นที่นิยมอาทิเช่น ไมโครซอฟท์ ซัน ไมโครซิสเต็ม ซิสโก้ซิสเต็ม ออราเคิล และโนเวล ซึ่งประกาศนียบัตรของแต่ละผลิตภัณฑ์มีรายละเอียดที่แตกต่างกันไป ซึ่งประกาศนียบัตรต่างๆของผู้ผลิตซึ่งเป็นเจ้าของผลิตภัณฑ์นั้นๆที่สำคัญ ได้แก่

1. ประกาศนียบัตรของไมโครซอฟต์

ผลิตภัณฑ์ของบริษัทไมโครซอฟท์จัดได้ว่าเป็นที่นิยมอย่างแพร่หลาย ประกาศนียบัตรต่างๆ ของไมโครซอฟท์จึงเน้นในส่วนของระบบปฏิบัติการไมโครซอฟท์ วินโดวส์ 2000 มีดังต่อไปนี้

1. Microsoft Certified Professional (MCP)

เป็นประกาศนียบัตรที่ง่ายสุด เพียงสอบผ่านวิชาใดวิชาหนึ่งเพียง 1 วิชา ก็ได้รับ MCP แล้ว แต่มียกเว้นอยู่ 2 วิชาคือ Networking Essentials และ Microsoft Windows 2000 Accelerated Exam for MCPs Certified on Microsoft Windows NT 4.0 เท่านั้น

2. Microsoft Certified Systems Administrator (MCSA)

มีข้อกำหนดว่าผู้ที่ได้รับประกาศนียบัตร MCSA ต้องสอบผ่าน 3 วิชาหลัก (Core Exam) และ 1 วิชาเลือก (Elective Exam) ผู้ที่เป็น MCSA เป็นผู้ที่มีความรู้ในการจัดการระบบ และสามารถแก้ปัญหาที่เกี่ยวข้องกับระบบปฏิบัติการได้ ประกาศนียบัตร MCSA นี้เหมาะกับบุคลากรที่มีอาชีพดังนี้ system administrator, information system administrator, network administrator, network technician, network operation analyst และ technical support specialist เป็นต้น

3. Microsoft Certified Systems Engineer (MCSE)

นับได้ว่าประกาศนียบัตรนี้เป็นประกาศนียบัตรหลัก มีความสำคัญ และเป็นที่ยอมรับมากที่สุด ผู้ที่ได้รับประกาศนียบัตร MCSE ต้องสอบผ่าน 5 วิชาหลัก และ 2 วิชาเลือก ผู้ที่เป็น MCSE เป็นผู้ที่มีความรู้ในการวางแผนและจัดการระบบ สามารถติดตั้งและดูแลบริหารงานระบบ รวมถึงสามารถใช้งานในส่วนของเซิร์ฟเวอร์แบบต่างๆ และแก้ปัญหาที่เกิดขึ้นแก่ระบบปฏิบัติการได้ ประกาศนียบัตร MCSE นี้เหมาะกับบุคลากรที่มีอาชีพดังนี้ system engineer, system analyst, network engineer, network analyst และ consultant ต่างๆ เป็นต้น

4. Microsoft Certified Database Administrator (MCDBA)

ผู้ที่ได้รับประกาศนียบัตร MCDBA ต้องสอบผ่าน 3 วิชาหลัก และ 1 วิชาเลือก ผู้ที่เป็น MCDBA มีความสามารถในการติดตั้งและดูแลจัดการในเรื่องของระบบฐานข้อมูลที่เป็น Microsoft SQL ได้เป็นอย่างดี ประกาศนียบัตร MCDBA นี้เหมาะกับบุคลากรที่มีอาชีพดังนี้ database administrator และ database operator เป็นต้น

5. Microsoft Certified Solution Developer (MCSD)

ผู้ที่ได้รับประกาศนียบัตร MCSD ต้องสอบผ่าน 3 วิชาหลัก และ 1 วิชาเลือก ผู้ที่เป็น MCSD เป็นผู้ที่สามารถออกแบบและพัฒนาระบบตามความต้องการทางด้านธุรกิจได้ ประกาศนียบัตร MCSD นี้เหมาะกับบุคลากรที่มีอาชีพดังนี้ software engineer, software developer, software application developer และ application analyst เป็นต้น

6. Microsoft Certified Application Developer (MCAD)

ผู้ที่ได้รับประกาศนียบัตร MCAD ต้องสอบผ่าน 2 วิชาหลัก และ 1 วิชาเลือก ผู้ที่เป็น MCAD เป็นผู้มีความรู้ในการดูแลและพัฒนาระบบงาน ประกาศนียบัตร MCAD นี้เหมาะกับบุคลากรที่มีอาชีพดังนี้ programmer, software engineer, software developer และ software application specialist เป็นต้น

7. Microsoft Certified Trainer (MCT)

ผู้ที่ได้รับประกาศนียบัตร MCT เป็นผู้ที่มีความรู้และความสามารถในการถ่ายทอดเทคโนโลยีของทางไมโครซอฟท์ โดยใช้เอกสารประกอบการอบรมของ Microsoft Official Curriculum (MOC) การที่จะได้รับประกาศนียบัตร MCT ต้องมีการสอบ MCT ซึ่งมีขั้นตอนดังนี้ คือ ต้องสอบได้ประกาศนียบัตร MCP และเข้ารับการอบรมในสถาบันที่ไมโครซอฟท์ยอมรับเป็น Microsoft CTEC และเรียนรู้ทักษะในการเป็นผู้สอน สุดท้ายสมัครและจัดส่งเอกสารให้แก่ทางไมโครซอฟท์ โดยอาจกระทำผ่านทางเว็บไซต์ของไมโครซอฟท์ก็ได้

8. Microsoft Office User Specialist (MOUS)

ผู้ที่ได้รับประกาศนียบัตร MOUS เป็นผู้ที่สามารถใช้งานแอพพลิเคชันต่างๆ ของไมโครซอฟท์ ออฟฟิศ ได้อย่างมีประสิทธิภาพ ชุดของผลิตภัณฑ์ไมโครซอฟท์ ออฟฟิศ ที่สามารถใช้ในการสอบประกาศนียบัตร MOUS นี้ได้แก่ Microsoft Office 97, Microsoft Office 2000 และ Microsoft Office XP รวมถึง Microsoft Project 2000 ด้วย

9. Microsoft Office User Specialist (MOUS) Master Instructor

ผู้ที่ได้รับประกาศนียบัตร MOUS Master Instructor เป็นผู้มีความรู้และความสามารถในการถ่ายทอดความรู้ในส่วนของแอพพลิเคชันต่างๆ ของไมโครซอฟท์ ออฟฟิศโดยใช้ MOC ได้อย่างมีประสิทธิภาพ การที่จะได้รับประกาศนียบัตร MOUS Master Instructor มีขั้นตอนคล้ายกับประกาศนียบัตร MCT

2. ประกาศนียบัตรของซิสโก้ ซิสเต็ม

ซิสโก้เป็นบริษัทชั้นนำและมีชื่อเสียงเป็นอย่างมากในเรื่องของเทคโนโลยีในส่วนของระบบเครือข่ายและผลิตภัณฑ์อุปกรณ์เครือข่าย โดยเฉพาะอย่างยิ่งอุปกรณ์เราเตอร์ โดยทั่วไปประกาศนียบัตรของซิสโก้จะแบ่งออกเป็น 3 ประเภท ได้แก่

1. Network Installation and Support Certification
2. Network Engineering and Design Certification
3. Communication and Services Certification

นอกจากนั้นแล้วประกาศนียบัตรเหล่านี้ยังมีการแบ่งออกเป็นระดับอีก 3 ระดับ คือ ระดับ associate ระดับ professional และระดับ expert ประกาศนียบัตรต่างๆ ของซิสโก้ ได้แก่

1. Cisco Certified Network Associate (CCNA)

เป็นประกาศนียบัตรที่ผู้ที่ได้รับต้องมีความรู้ในเรื่องของระบบเครือข่าย สามารถติดตั้งและดูแลจัดการระบบเครือข่ายขนาดเล็กได้ CCNA นี้ไม่มีวิชาบังคับที่ต้องได้รับมาก่อน (Exam Prerequisite) เมื่อสอบผ่านวิชาใดวิชาหนึ่ง ก็สามารถได้รับประกาศนียบัตรนี้

2. Cisco Certified Network Professional (CCNP)

เป็นประกาศนียบัตรที่ผู้ที่ได้รับต้องมีความรู้เป็นอย่างดีในเรื่องของระบบเครือข่าย สามารถติดตั้งและดูแลจัดการระบบเครือข่ายขนาดใหญ่ได้ การที่จะสามารถสอบ CCNP ได้ต้องสอบผ่าน CCNA มาก่อน

3. Cisco Certified Design Associate (CCDA)

เป็นประกาศนียบัตรที่ผู้ที่ได้รับต้องมีความรู้ในเรื่องการออกแบบระบบเครือข่ายขนาดเล็กได้

4. Cisco Certified Design Professional (CCDP)

เป็นประกาศนียบัตรที่ผู้ที่ได้รับต้องมีความรู้ในเรื่องการออกแบบระบบเครือข่ายขนาดใหญ่ได้ การที่จะสามารถสอบ CCDP ได้ต้องสอบผ่าน CCNA และ CCDA มาก่อน

5. Cisco Certified Internetwork Professional (CCIP)

เป็นประกาศนียบัตรที่ผู้ที่ได้รับต้องมีความรู้ในเรื่องการออกแบบ วางแผนในการจัดการระบบเครือข่าย สามารถติดตั้งและดูแลบริการระบบเครือข่ายได้

6. Cisco Certified Internetwork Expert (CCIE)

เป็นประกาศนียบัตรขั้นสูงสุดในส่วนของ Network Installation and Support Certification และ Communication and Services Certification

3. ประกาศนียบัตรของซัน

ประกาศนียบัตรของซัน เป็นเครื่องบ่งบอกถึงความสามารถของผู้ได้รับประกาศนียบัตรนี้ ในเรื่องของเทคโนโลยีในส่วนของจาวา และระบบปฏิบัติการโซลาริส มีประกาศนียบัตรในส่วนต่างๆ ได้แก่

1. Java Technology

ในส่วนของเทคโนโลยีจาวามีประกาศนียบัตรต่างๆ คือ Sun Certified Programmer for the JavaTM 2 Platform เป็นประกาศนียบัตรในเรื่องของการใช้งานเทคโนโลยีจาวาแพลตฟอร์มของซัน Sun Certified Developer for the JavaTM 2 Platform เป็นประกาศนียบัตรที่ผู้ได้รับต้องมีพื้นฐานในเรื่องของโครงสร้างและซินแท็กของภาษาจาวาสำหรับการพัฒนาแอพพลิเคชันได้เป็นอย่างดี Sun Certified Web Component Developer for J2EETM 2 Platform เป็นประกาศนียบัตรสำหรับผู้พัฒนา

เว็บแอพพลิเคชันด้วย J2EE และสุดท้าย Sun Certified Enterprise Architect for JavaTM 2 Platform, EnterpriseTM Edition เป็นประกาศนียบัตรที่เหมะสำหรับผู้ออกแบบโครงสร้างระบบด้วยภาษาจาวาในมาตรฐาน J2EE

2. iPlanet

มีประกาศนียบัตร คือ iPlanetTM Application Server 6.0 Certification เป็นประกาศนียบัตรการใช้งานแพลตฟอร์ม iPlanetTM Application Server 6.0 ของซัน

3. Solaris Operating Environment

ในส่วนของ Solaris Operating Environment นี้มีประกาศนียบัตรต่างๆ คือ Sun Certified System Administrator for the SolarisTM Operating Environment เป็นประกาศนียบัตรที่ผู้ที่ได้รับต้องมีความสามารถในการใช้งานระบบปฏิบัติการโซลาริสได้เป็นอย่างดี Sun Certified Network Administrator for the SolarisTM Operating Environment เป็นประกาศนียบัตรที่ผู้ที่ได้รับต้องมีความรู้ในเรื่องของระบบเครือข่ายบนระบบปฏิบัติการโซลาริส

4. NetSun Certification Track

ในส่วนนี้มีประกาศนียบัตรต่างๆ คือ Sun Certified Data Management Engineer เป็นประกาศนียบัตรที่ผู้ที่ได้รับต้องมีความรู้และความสามารถในเรื่องของการจัดการส่วนของระบบฐานข้อมูล Sun Certified Backup and Recovery Engineer เป็นประกาศนียบัตรที่ผู้ที่ได้รับต้องมีความสามารถในเรื่องของการสำรองและกู้คืนในส่วนของข้อมูลต่างๆ Sun Certified Storage Architect เป็นประกาศนียบัตรที่รับรองผู้ที่มีความสามารถในการออกแบบและดูแลระบบการจัดเก็บข้อมูลบนฐานข้อมูลได้อย่างมีประสิทธิภาพ

4. ประกาศนียบัตรของโอราเคิล

ประกาศนียบัตรของซัน เป็นเครื่องบ่งบอกถึงความสามารถของผู้ได้รับประกาศนียบัตรนี้ในเรื่องของเทคโนโลยีในส่วนของฐานข้อมูลและ Database มีประกาศนียบัตรในส่วนต่างๆ ได้แก่

1) Database Administrator
   - Oracle 10g Certified Associate, Professional and Master
   - Oracle9i Certified Associate, Professional and Master
   - OCP DBA Upgrade Paths
   - Oracle8i Certified Professional
2) Application Developer
   - Oracle9i PL/SQL Developer Certified Associate
   - Oracle9i Forms Developer Certified Professional

- Oracle9i Forms Developer OCP Upgrade Path
- Oracle Forms Developer Certified Professional, Release 6/6i

3) Web Application Server Administrator

- Oracle9i Application Server Certified Associate

เอกสารอ้างอิง

1. Managing IT as a business

   By: Mark D. Lutchen PriceWaterHouseCoopers Wiley

2. สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (http://www.nitc.go.th/document/attached_document.html)

3. กรมปศุสัตว์ (http://www.dld.go.th/ict/article/general/gen10.html)

4. HR Center (http://www.hrcenter.co.th/)

5. Oracle Corporation (Thailand) Co., Ltd.(http://www.oracle.com)

6. Microsoft Corporation (http://www.microsoft.com)

7. Cisco Systems, Inc. (http://www.cisco.com)

8. Sun Microsystems , Inc. (http://www.sun.com)

9. สถาบันพัฒนาผู้เชี่ยวชาญระบบเครือข่าย (http://www.asicisonline.net/acis.html)