การศึกษาแนวโน้มของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ โดยใช้เทคนิคเดลฟาย

พีรพันธ์ รุจิพงษ์กุล[1*] และ เกียรติศักดิ์ โยชะนัง[2]

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาแนวโน้มของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ 2) วิเคราะห์หาแนวทางของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายใน มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ โดยแบ่งออกเป็น 5 ด้าน คือ ด้านนโยบาย ด้านฮาร์ดแวร์ ด้านซอฟต์แวร์ ด้านบุคลากร และด้านกระบวนการ กลุ่มตัวอย่างที่ใช้ในการวิจัยประกอบด้วยผู้บริหาร จำนวน 10 คน ผู้เชี่ยวชาญและผู้ปฏิบัติงานด้านการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ จำนวน 30 คน รวม 40 คน เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล เป็นแบบสอบถาม จำนวน 3 รอบ สถิติที่ใช้ ได้แก่ ค่ามัธยฐาน ค่าฐานนิยม และค่าพิสัยระหว่างควอไทล์ ผลการวิจัยพบว่าระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ฮาร์ดแวร์และซอฟแวร์ต้องมีประสิทธิภาพสูง มีมาตรฐาน ราคาต้องคุ้มค่า มีการกำหนดนโยบายที่ชัดเจนเป็นลายลักษณ์อักษรพร้อมบทลงโทษ บุคลากรต้องมีความรู้ความสามารถมีการฝึกอบรมอยู่เสมอ มีกระบวนการทำงานที่เป็นขั้นตอน ชัดเจน พร้อมจัดทำคู่มือและขั้นตอนการปฏิบัติงานให้ทันสมัยอยู่เสมอ

คำสำคัญ: ระบบรักษาความปลอดภัย แนวโน้มในอนาคต เทคนิคเดลฟาย

---

[1] นักศึกษาระดับปริญญาโท สาขาวิชาเทคโนโลยีสารสนเทศ ภาควิชาการสื่อสารข้อมูลและเครือข่าย คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

[2] อาจารย์ ภาควิชาการสื่อสารข้อมูลและเครือข่าย คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

[*] ผู้นิพนธ์ประสานงาน โทร. 08-9118-8225 อีเมล: peerapunr@kmutnb.ac.th

Study of Trend Study of Computer Network Security in King Mongkut's University of Technology North Bangkok for the Planning Using Delphi Technique

Peerapun Rujipongkul[1*] and Kiattisak Yochanang[2]

Abstract

The purpose of this study is 1) to analyze the current status and the requirement of computer network security in King Mongkut's University of Technology North Bangkok for the planning by using the Delphi Technique. 2) This study investigates the trend of the needs in five categories, those are policy, hardware, software, personnel, and procedure. The population of the study includes 10 executives and 30 experts in computer network system of in King Mongkut's University of Technology North Bangkok. The questionnaires are distributed to collect data in three rounds. Median, mode, and interquartile range are employed to evaluate the results. The experimental results illustrate that high efficiency, standard compilation, and cost effectiveness of hardware and software are highly needed. The policy is necessarily defined and enforced with punishment. The competent personnel are required, and regularly trained to update the skill. Lastly, the procedure is also necessarily prepared in an accessible form of handbook.

Keywords: The Security System, Future Trends, Delphi Technique

[1] Master Program Student, Department Of Data Communication And Networking, King Mongkut's University Of Technology North Bangkok

[2] Teacher, Department Of Data Communication And Networking, King Mongkut's University Of Technology North Bangkok

[*] Corresponding Tel. 08-9118-8225 E-Mail: peerapunr@kmutnb.ac.th

1. บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศได้เจริญก้าวหน้าอย่างรวดเร็ว โดยเฉพาะระบบอินเทอร์เน็ตได้เข้ามามีส่วนในชีวิตประจำวันมากยิ่งขึ้น ทำให้องค์กรต่าง ๆ ทั้งภาครัฐและเอกชน ได้นำระบบเครือข่ายคอมพิวเตอร์เข้ามามีส่วนช่วยในการพัฒนาการทำงานให้เกิดความคล่องตัว สะดวกและรวดเร็วยิ่งขึ้น สำหรับมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ได้นำระบบระบบเครือข่ายคอมพิวเตอร์มาใช้ในการอำนวยความสะดวกให้แก่อาจารย์ เจ้าหน้าที่ และนักศึกษา เพื่อการสืบค้นข้อมูลผ่านระบบอินเทอร์เน็ต ซึ่งเป็นแหล่งข้อมูลที่ใหญ่ที่สุด อีกทั้งเพื่อรองรับต่อระบบสารสนเทศด้านต่าง ๆ ที่สำคัญของมหาวิทยาลัย เช่น ระบบการลงทะเบียนนักศึกษา ระบบสารสนเทศบุคลากร ระบบสำนักงานอัตโนมัติ ซึ่งนับว่าเป็นจุดแข็งในการบริหารจัดการข้อมูลที่สำคัญเพื่อรองรับการพัฒนาระบบงานให้เกิดประสิทธิภาพ แต่ในปัจจุบันศักยภาพในการใช้งานระบบเครือข่ายคอมพิวเตอร์ยังไม่สามารถทำงานได้อย่างเต็มที่ อีกทั้งยังไม่มีแนวทางหรือมาตราการในการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ที่ชัดเจน ซึ่งถือเป็นความเสี่ยงต่อการถูกโจมตีข้อมูลและระบบต่าง ๆ อันเป็นจุดอ่อนที่สำคัญก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเป็นอย่างมาก

ปัญหาภัยคุกคาม ตลอดจนการละเมิดความปลอดภัยของระบบคอมพิวเตอร์ซึ่งเป็นจุดอ่อนนั้น มีแนวโน้มเพิ่มขึ้นอย่างรวดเร็ว โดยเฉพาะสถาบัน การศึกษาซึ่งถือเป็นเป้าหมายหลักของการถูกโจมตี [1] เนื่องจากมีลักษณะที่น่าดึงดูด คือมีข้อมูลที่เป็นความลับ อีกทั้งมีผู้ใช้และวิธีการเข้าถึงที่หลากหลาย และมีกิจกรรมที่เสี่ยงสูงบนเครือข่าย จากระบบที่อนุญาตให้ผู้ใช้สามารถแลก เปลี่ยนไฟล์ระหว่างกันผ่านโปรแกรมที่ใช้ในการสื่อสารบน Social Media อันเป็นที่นิยมในปัจจุบันเช่น Line, Facebook เป็นต้น ตลอดจนการเรียน การสอนผ่านสื่ออิเล็กทรอนิกส์ (E-Learning) ถึงแม้ว่าในปัจจุบันมหาวิทยาลัยจะมีการป้องกันบนเครือข่าย แต่ก็ยังเกิดช่องโหว่ที่ทำให้เกิดจากการโจมตีจากผู้โจมตี (Attacker) ภายนอกได้ ซึ่งปัญหาที่เกิดขึ้นส่งผลกระทบต่อความปลอดภัยข้อมูลข่าวสาร ทั้งต่อข้อมูล ส่วนบุคคล ทรัพย์สินทางปัญญา ความเสียหายทางการเงิน และการคุกคามโครงสร้างพื้นฐานที่มีความเกี่ยวข้องกับเครือข่ายมหาวิทยาลัย ซึ่งนับวันอาชญากรรมทางคอมพิวเตอร์ยิ่งทวีความรุนแรงมากขึ้น “ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ จึงไม่ใช่แค่เพียงอาศัยขีดความสามารถของระบบปฏิบัติการเท่านั้น แต่ยังต้องการนโยบายความมั่นคงปลอดภัยโดยรวมทั้งระบบ” [2] เพื่อป้องกันความเสียหายที่จะเกิดขึ้น

จากปัญหาที่เกิดขึ้นดังกล่าว ผู้วิจัยจึงได้นำเทคนิคเดลฟาย (Delphi Technique) [3] ซึ่งเป็นวิธีการวินิจฉัยหรือตัดสินใจปัญหาต่าง ๆ อย่างเป็นระบบ โดยไม่มีการเผชิญหน้ากันโดยตรงของกลุ่มผู้เชี่ยวชาญ ทำให้ผู้เชี่ยวชาญแต่ละคนสามารถแสดงความคิดเห็นของตนเองอย่างเต็มที่และอิสระ นอกจากนี้ผู้เชี่ยวชาญยังมีโอกาสกลั่นกรองความคิดเห็นของตนอย่างรอบคอบทำให้ได้ข้อมูลที่น่าเชื่อถือและนำไปใช้ประกอบการตัดสินใจในด้านต่าง ๆ ได้ โดยมุ่งเน้นการศึกษาวิจัยเชิงลึกเพื่อให้มีความรู้และความเข้าใจเกี่ยวกับอนาคตที่คาดว่าจะเป็นการแสวงหาทางเลือกที่จะดำเนินการในอนาคตอันจะนำไปสู่การเตรียมการควบคุม การแก้ไข และการบริหารจัดการในอนาคตให้เป็นไปตามความต้องการ มาใช้ในการวิจัยเพื่อคาดการณ์แนวโน้มในอนาคตของระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ เพื่อศึกษาการพัฒนาและแนวโน้มการพัฒนาของระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือต่อไป

2. วัตถุประสงค์ของการวิจัย

2.1 เพื่อศึกษาแนวโน้มของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

2.2 เพื่อวิเคราะห์หาแนวทางของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

3. เอกสารและงานวิจัยที่เกี่ยวข้อง

3.1 ทฤษฎีเกี่ยวข้องกับระบบรักษาความปลอดภัยเครือข่าย (Network Security)

การรักษาความปลอดภัยของระบบคอมพิวเตอร์สามารถแบ่งออกเป็นหมวดหมู่ใหญ่ ๆ ได้ 3 หมวดหมู่ ได้แก่ 1) การรักษาความปลอดภัยด้านกายภาพ 2) การรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่ายและลูกข่าย และ 3) การรักษาความปลอดภัยของอุปกรณ์เครือข่ายและระบบเครือข่าย [4]

3.2 ทฤษฎีเกี่ยวข้องกับภัยคุกคามระบบเครือข่าย

ภัยคุกคาม (Threat) หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ภัยคุกคามนั้นอาจจะไม่เกิดขึ้นหากมีการป้องกันที่ดี หรือถ้ามีการเตรียมการที่ดี เมื่อมีเหตุการณ์เกิดขึ้นก็จะช่วยลดความเสียหายได้ การกระทำที่อาจก่อให้เกิดความเสียหายความเสียหายเรียกว่าการโจมตี (Attack) ส่วนผู้ที่ทำเช่นนั้น หรือผู้ที่เป็นเหตุการณ์ดังกล่าวเกิดขึ้น เรียกว่าผู้โจมตี (Attacker) หรือแฮคเกอร์ (Hacker) หรือแคร็คเกอร์ (Cracker) [5]

3.3 เทคนิคเดลฟาย

เป็นเทคนิคการวิจัยที่ได้รับการยอมรับและเป็นที่นิยมแพร่หลาย ไม่ว่าจะเป็นด้านธุรกิจ การเมือง เศรษฐกิจ และการศึกษา สำหรับทางเทคโนโลยีการศึกษาได้มีการนำมาใช้อย่างกว้างขวาง เช่น การวิจัยเกี่ยวกับแนวโน้มของเทคโนโลยีการศึกษา อีก 5 ปี ทิศทางการวิจัยเทคโนโลยีการศึกษาในอนาคต เป็นต้น ซึ่งเทคนิคเดลฟายเป็นวิธีการวินิจฉัยหรือตัดสินใจปัญหาต่าง ๆ อย่างเป็นระบบโดยไม่มีการเผชิญหน้าโดยตรงของกลุ่มผู้เชี่ยวชาญ ทำให้ผู้เชี่ยวชาญแต่ละคนสามารถแสดงความคิดเห็นของตนเองอย่างเต็มที่และอิสระ โดยไม่ต้องคำนึงถึงความคิดเห็นของผู้อื่น

Johnson [6] ได้ให้ความหมายของเทคนิคเดลฟายว่าเป็นกระบวนการหรือเครื่องมือที่ใช้ในการตัดสินใจหรือลงข้อสรุปในเรื่องใดเรื่องหนึ่งอย่างเป็นระบบที่ปราศจากการเผชิญหน้าโดยตรงของกลุ่มผู้เชี่ยวชาญโดยรวบรวมและสอบถามความคิดเห็นของผู้เชี่ยวชาญ

4. วิธีการดำเนินการวิจัย

4.1 ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัย คือ ผู้เชี่ยวชาญและผู้ปฏิบัติงานด้านระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

กลุ่มตัวอย่างที่ใช้ในการวิจัย ได้มาโดยการสุ่มตัวอย่างแบบเจาะจง ประกอบด้วย 1) ผู้บริหาร จำนวน 10 คน 2) ผู้เชี่ยวชาญและผู้ปฏิบัติงานด้านการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ จำนวน 30 คน รวม 40 คน

4.2 กรอบแนวคิดที่ใช้ในการวิจัย

การศึกษาแนวโน้มของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ โดยใช้เทคนิคเดลฟาย ผู้วิจัยได้กำหนดขอบเขตในการวิจัยให้เหมาะสมกับมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ โดยแบ่งออกเป็น 5 ด้าน ตามองค์ประกอบของระบบเครือข่ายคอมพิวเตอร์ความมั่นคงปลอดภัย คือ 1) ด้านนโยบาย (Policy) 2) ด้านฮาร์ดแวร์ (Hardware) 3) ด้านซอฟต์แวร์ (Software) 4) ด้านบุคลากร (Personnel) และ 5) ด้านกระบวนการ (Procedure)

4.3 เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัยครั้งนี้ ได้แก่ แบบสอบถามชนิดปลายเปิด และแบบสอบถามชนิดปลายปิด โดยแบบสอบถามดังกล่าว ได้แบ่งออกเป็น 3 รอบ ดังนี้

รอบที่ 1 แบบสอบถามปลายเปิดเพื่อให้กลุ่มผู้เชี่ยวชาญบรรยายและนำประเด็นไปสร้างแบบสอบถามรอบที่ 2

รอบที่ 2 แบบสอบถามปลายปิด แบบให้น้ำหนัก (Rating Scale) ให้กลุ่มผู้เชี่ยวชาญเลือกแสดงความคิดเห็น 5 ระดับ คือ เห็นด้วยอย่างยิ่ง เห็นด้วย ไม่แน่ใจ ไม่เห็นด้วย และไม่เห็นด้วยอย่างยิ่ง

รอบที่ 3 แบบสอบถามปลายปิด ให้กลุ่มผู้เชี่ยวชาญแสดงความคิดเห็น 5 ระดับ คือ เห็นด้วยอย่างยิ่ง เห็นด้วย ไม่แน่ใจ ไม่เห็นด้วย และไม่เห็นด้วยอย่างยิ่ง โดยเพิ่มตำแหน่งของค่ามัธยฐาน ค่าฐานนิยมและค่าพิสัยระหว่างควอไทล์

นำแบบสอบถามไปทดลองใช้ (Try Out) กับกลุ่มทดลองที่ไม่ใช่กลุ่มตัวอย่าง ได้แก่ อาจารย์ที่สอนทางด้านระบบเครือข่าย จำนวน 15 คน ทำการหาค่าความเชื่อมั่น (Reliability) ของแบบสอบถาม โดยใช้สูตรสัมประสิทธิ์

แอลฟา (Alpha Coefficient) ด้วยวิธีการของครอนบาค (Cronbach's Alpha) ได้ค่าความเชื่อมั่น (Reliability) เท่ากับ 0.93 แล้วจึงนำไปเก็บรวบรวมข้อมูลจริงจากกลุ่มตัวอย่าง จำนวน 40 คน

4.4 การเก็บรวบรวมข้อมูล

ผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลตามขั้นตอนดังนี้

4.4.1 ขอความร่วมมือให้ผู้บริหารและผู้เชี่ยวชาญตอบแบบสอบถามและเก็บรวบรวมข้อมูล

4.4.2 ผู้วิจัยดำเนินการส่งแบบสอบถามไปยังผู้เชี่ยวชาญและดำเนินการเก็บแบบสอบถามด้วยตนเอง จำนวน 3 รอบ

4.5 การวิเคราะห์ข้อมูลและสถิติที่ใช้ในการวิเคราะห์ข้อมูล

สถิติที่ใช้ในการวิเคราะห์จะเป็นสถิติเบื้องต้น คือ การวัดแนวโน้มเข้าสู่ส่วนกลาง ได้แก่ 1) ฐานนิยม (Mode) 2) ค่ามัธยฐาน (Median) และวัดการกระจายของข้อมูล 3) ค่าพิสัยระหว่างควอไทล์ (Interquartile Rang)

5. ผลการวิจัย

5.1 การวิเคราะห์ระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ในมหาวิทยาลัยในปัจจุบัน

ตารางที่ 1 แสดงค่ามัธยฐาน ค่าฐานนิยม และค่าพิสัยระหว่างควอไทล์ ของระดับคะแนนความคิดเห็นเกี่ยวกับภาพรวมของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยในปัจจุบัน รอบที่ 3

ภาพรวมของระบบรักษาความปลอดภัยในปัจจุบัน	รอบที่ 3			ความสอดคล้องของความคิดเห็น
	Md	Mo	Ir	
1. ผู้บริหารให้ความสำคัญด้านเทคโนโลยีมากกว่ากระบวนการและนโยบาย	4	4	2	ไม่สอดคล้อง
2. ผู้บริหารไม่ให้ความสำคัญและเห็นถึงความจำเป็นทางด้านบุคลากร	4	4	1	สอดคล้อง

ตารางที่ 1 แสดงค่ามัธยฐาน ค่าฐานนิยม และค่าพิสัยระหว่างควอไทล์ ของระดับคะแนนความคิดเห็นเกี่ยวกับภาพรวมของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยในปัจจุบัน รอบที่ 3 (ต่อ)

ภาพรวมของระบบรักษาความปลอดภัยในปัจจุบัน	รอบที่ 3			ความสอดคล้องของความคิดเห็น
	Md	Mo	Ir	
3. ขาดความร่วมมือจากบุคลากรต่อการให้ความ สำคัญและร่วม กันป้องกัน	4	4	1	สอดคล้อง
4. ระบบสามารถป้องกันได้ในระดับหนึ่ง แต่ยังไม่เพียงและยังคงต้องมีการพัฒนาในส่วนต่างๆ เพิ่มขึ้นในอนาคต	5	5	1	สอดคล้อง
5. อุปกรณ์มีราคาที่สูงทำให้การจัดหาทรัพยากรเป็นไปได้ค่อนข้างยาก	4	5	1	สอดคล้อง
6. ผู้บริหารไม่ให้ความสำคัญกับระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์	4	3	2	ไม่สอดคล้อง
7. ระบบรักษาความปลอดภัยยังมีความหละหลวม ส่วนงานให้ความสำคัญในด้าน การใช้งานอินเทอร์เน็ตมากกว่า	4	4	2	ไม่สอดคล้อง
8. ขาดบุคลากรที่ทำหน้าที่รักษาความปลอดภัยโดยตรง	4	4	2	ไม่สอดคล้อง

จากตารางที่ 1 พบว่า กลุ่มผู้เชี่ยวชาญมีความเห็นสอดคล้องกันในภาพรวมของระบบรักษาความปลอดภัยทั้งหมด 4 ข้อ ข้อคำถามมีความจำเป็นในระดับมากที่สุด 1 ข้อ ได้แก่ ระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยในปัจจุบันนั้นสามารถป้องกันได้ในระดับหนึ่ง แต่ยังไม่เพียงพอและยังคงต้องมีการพัฒนาในส่วนต่างๆ เพิ่มขึ้นในอนาคต

5.2 ความคิดเห็นเกี่ยวกับระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัย

ตารางที่ 2 แสดงค่ามัธยฐาน ค่าฐานนิยม และค่าพิสัยระหว่างควอไทล์ ของระดับคะแนนความคิดเห็นเกี่ยวกับภาพรวมของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยรอบที่ 3

ภาพรวมของระบบรักษาความปลอดภัย	รอบที่ 3			ความสอดคล้องของความคิดเห็น
	Md	Mo	Ir	
1. ควรจัดทำนโยบายที่เป็นลายลักษณ์อักษรร่วมกันระหว่างผู้บริหาร เจ้าหน้าที่และผู้ใช้งาน	5	5	1	สอดคล้อง
2. ควรมีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ	5	5	1	สอดคล้อง
3.ควรจัดหาฮาร์ดแวร์และอุปกรณ์ที่มีรองรับการใช้งานอย่างมีประสิทธิภาพในราคาที่เหมาะสม	4	4	1	สอดคล้อง
4. ควรมีการปรับปรุงระบบปฏิบัติการของฮาร์แวร์และอุปกรณ์อย่างสม่ำเสมอ	5	5	1	สอดคล้อง
5.ระบบซอฟต์แวร์ที่ใช้ต้องมีเสถียรภาพสูง	5	5	1	สอดคล้อง
6. ซอฟต์แวร์ควรมีประสิทธิภาพสูง มีการประมวลผลอัตราการส่งข้อมูลที่รวดเร็ว	4.5	5	1	สอดคล้อง
7. ควรมีบุคลากรที่ทำหน้าที่ดูแลรักษาความปลอดภัยโดยตรง	4.5	5	1	สอดคล้อง
8. ควรมีการจัดทำขั้นตอนการทำงานเป็นเอกสารและมีการพัฒนาแก้ไขให้เป็นปัจจุบันอยู่เสมอ	4	5	1	สอดคล้อง

จากตารางที่ 2 พบว่า กลุ่มผู้เชี่ยวชาญมีความเห็นสอดคล้องกันทุกข้อ ในภาพรวมของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัย โดยมีความจำเป็นอยู่ในระดับมากที่สุด 6 ข้อ ได้แก่

1) ควรจัดทำนโยบายที่เป็นลายลักษณ์อักษรทั้งผู้บริหาร และเจ้าหน้าที่และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบายร่วมกัน

2) ควรมีการทบทวนและปรับปรุงนโยบายด้านการรักษาความปลอดภัยให้เป็นปัจจุบันอยู่เสมอ

3) ควรมีการปรับปรุงระบบปฏิบัติการของฮาร์ดแวร์และอุปกรณ์อย่างสม่ำเสมอ

4) ระบบซอฟต์แวร์ที่ใช้ต้องมีเสถียรภาพสูง

5) ซอฟต์แวร์ที่ทำหน้าที่ในการรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยนั้นควรมีประสิทธิภาพสูง มีการประมวลผลอัตราการส่งข้อมูลที่รวดเร็ว

6) มหาวิทยาลัยควรมีบุคลากรที่ทำหน้าที่ดูแลและรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในโดยตรง

6. สรุปผลการวิจัยและข้อเสนอแนะ

จากการศึกษา เรื่อง แนวโน้มของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ โดยใช้เทคนิคเดลฟาย สรุปผลการวิจัย ได้ดังนี้

6.1 ความคิดเห็นเกี่ยวกับแนวทางการรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาพรวมของแนวทางการรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ จะต้องมีการกำหนดนโยบายที่ชัดเจนและมีบทลงโทษ การปฏิบัติอย่างเคร่งครัดจากบุคลากรทุกคนภายในมหาวิทยาลัย โดยที่มีมาตรฐานที่ยอมรับกันอย่างแพร่หลาย ดังงานวิจัยของเดชาวัต [7] ผลการวิจัยพบว่า เทคโนโลยีมีการพัฒนาอย่างรวดเร็ว ดังนั้นนโยบายรักษาความมั่นคงปลอดภัยของสารสนเทศจำเป็นที่จะต้องพัฒนา และปรับให้เหมาะสมตลอดเวลา และไม่เกิดช่องโหว่ของนโยบายเพื่อให้เหมาะสมต่อสภาวะปัจจุบันและรองรับการเจริญเติบโตขององค์กร

นโยบายด้านการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ต้องมีเป็นลายลักษณ์อักษร โดยมีการจัดทำนโยบายร่วมกันระหว่างผู้บริหาร เจ้าหน้าที่ฝ่ายคอมพิวเตอร์ และบุคลากรผู้ใช้งาน อีกทั้งมีการประกาศนโยบายอย่างแพร่หลาย มีการทบทวนนโยบายและปรับปรุงให้มีความทันสมัยอยู่เสมอ สอดคล้องกับงานวิจัย

ของจิตติมาและกว้าน [8] ได้ทำการวิจัย เรื่อง การพัฒนาระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ สำหรับมหาวิทยาลัยราชภัฏสวนดุสิตผลการวิจัยพบว่า นโยบายมีความจำเป็นอย่างยิ่งในการใช้งานระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย เพราะมีผู้ใช้งานมากขึ้นตามความต้องการ การใช้งานก็มีหลากหลายและมีพฤติกรรมแตกต่างกัน จึงควรมีการกำหนดนโยบายให้ชัดเจน เพื่อจะได้เป็นแนวปฏิบัติเดียวกันและต้องทำอย่างจริงจัง ควรมีการเผยแพร่นโยบายและสร้างความตระหนักให้เกิดกับบุคลากรของมหาวิทยาลัย

ฮาร์ดแวร์ หรือ อุปกรณ์ที่ทำหน้าที่เกี่ยวกับระบบเครือข่าย และระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยนั้นจะต้องมีประสิทธิภาพที่สูงและเหมาะสมกับราคา สามารถรองรับระบบจัดการกลาง (Centralization Management) และสามารถใช้งานร่วมกับอุปกรณ์อื่น ๆ ได้อย่างประสิทธิภาพ สามารถตรวจสอบล็อกกิ้ง (Logging) ได้ตลอดเวลา รองรับโปรโตคอลเกี่ยวกับระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยที่ทันสมัยอยู่เสมอ

ซอฟต์แวร์ที่ทำหน้าที่เกี่ยวกับระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยและซอฟต์แวร์ที่ทำงานอยู่ในระบบเครือข่ายนั้นต้องสามารถตรวจสอบการทำงานได้และรองรับระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในองค์กร สามารถทำงานร่วมกับซอฟต์แวร์ หรืออุปกรณ์ที่ทำหน้าที่รักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัย โดยรองรับระบบการจัดการกลาง และมีการปรับปรุงให้มีประสิทธิภาพสูงอย่างเสมอ โดยที่ความต้องการทางด้านฮาร์ดแวร์นั้นจะต้องไม่สูงมากจนเกินไป

บุคลากรที่ทำหน้าที่เกี่ยวกับรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยนั้นจะต้องมีความรู้ความสามารถเพียงพอที่ปฏิบัติหน้าที่ และมีใบรับรองผ่านการสอบวัดความรู้ความสามารถเกี่ยวกับระบบความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์จากหน่วยงานภายนอก หรือสถาบันรับรองคุณวุฒิมาตราฐาน ทั้งนี้ อาจเนื่องจากว่าผู้ดูแลที่ขาดประสบการณ์ หรือความรู้ความสามารถไม่เพียงพออาจทำให้ข้อมูลเสียหายได้โดยไม่ตั้งใจ

กระบวนการทำงาน ต้องมีขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลงได้ในกรณีฉุกเฉิน ควรมีการจัดเก็บบันทึกเหตุการณ์ที่เกิดขึ้นรายงานต่อผู้บริหารเพื่อพร้อมรับและหาแนวทางในการแก้ไขปัญหาได้อย่างทันท่วงที ควรมีการจัดทำคู่มือการปฏิบัติงาน ขั้นตอนการทำงานที่เป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ และมีการเผยแพร่ให้ผู้ปฏิบัติงานได้ทราบเพื่อพร้อมต่อการปฏิบัติงานต่อไป

6.2 การวิเคราะห์ระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ในมหาวิทยาลัยในปัจจุบัน

ในภาพรวมปัจจุบันมหาวิทยาลัยให้ความสำคัญกับเทคโนโลยีมากกว่ากระบวนการหรือนโยบายในการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยทำให้ไม่มีประสิทธิภาพ อีกทั้งไม่ได้ให้ความสนใจด้านการจัดการบุคลากรที่เกี่ยวข้องของระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัย บุคลากรในแต่ละหน่วยงานนั้นยังไม่ได้ให้ความร่วมมือกันอย่างเต็มที่ทำให้ระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยนั้นไม่มีประสิทธิภาพและไม่เกิดประสิทธิผล

ระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยนั้นสามารถป้องกันอันตรายได้ในระดับหนึ่งแต่ยังไม่เพียงพอ และต้องมีการ พัฒนาในส่วนต่าง ๆ เพิ่มขึ้นในอนาคต อุปกรณ์ที่ใช้ในระบบเครือข่ายและระบบรักษาความปลอดภัยที่รองรับเกี่ยวกับระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัย นั้นยังมีราคาที่สูงทำให้การจัดการในเรื่องของงบประมาณและทรัพยากรนั้นเป็น ไปได้ค่อนข้างยาก ซึ่งสอดคล้องกับงานวิจัยของสุนทรีย์ [9] ที่พบว่างบประมาณ ด้านระบบคอมพิวเตอร์เครือข่ายไร้สายในองค์กรอุตสาหกรรมในปัจจุบันมีอย่างจำกัด ซึ่งไม่เพียงพอต่อราคาของอุปกรณ์ ค่าบำรุงรักษา และการอบรมต่าง ๆ ที่สูงขึ้นซึ่งไม่เพียงพอต่อการพัฒนาเทคโนโลยีการรักษาความปลอดภัยระบบคอมพิวเตอร์เครือข่ายไร้สายให้ทันสมัยอยู่เสมอ เนื่องจากการรักษาความปลอดภัยระบบคอมพิวเตอร์เครือข่ายไร้สายไม่ใช่ผลิตภัณฑ์ที่ก่อให้เกิดรายได้ให้แก่องค์กรอุตสาหกรรม

นโยบายของแต่ละส่วนงานภายในมหาวิทยาลัยได้ให้ความสำคัญเกี่ยวกับประสิทธิภาพมากกว่าความปลอดภัย ซึ่งประสิทธิภาพของระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยจะขึ้นอยู่กับความสามารถบุคลากรที่ทำหน้าที่ดูแลระบบเครือข่ายคอมพิวเตอร์ ไม่ได้มีผู้ที่ทำหน้าที่เกี่ยวกับระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์โดยตรง ทำให้การแบ่งแยกทำหน้าที่ การทำความเข้าใจ และอำนาจตัดสินใจของบุคลากรที่ทำหน้าที่รับผิดชอบไม่ได้มีขอบเขตอย่างชัดเจน ทำให้ระบบรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยในปัจจุบันนั้นไม่มีประสิทธิภาพ

จากผลการวิจัยดังกล่าว ผู้วิจัยสามารถสรุปผลการวิเคราะห์จุดอ่อน จุดแข็ง อุปสรรค โอกาสด้วยรูปแบบ SWOT Analysis ของระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ในมหาวิทยาลัยในปัจจุบัน ได้ดังตารางที่ 3 การวิเคราะห์จุดอ่อน จุดแข็ง อุปสรรค โอกาส (SWOT Analysis) ระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ในมหาวิทยาลัยในปัจจุบัน ดังนี้

ตารางที่ 3 การวิเคราะห์จุดอ่อน จุดแข็ง อุปสรรค โอกาส (SWOT Analysis) ระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ในมหาวิทยาลัยในปัจจุบัน

S : Strengths จุดแข็ง	**W: Weaknesses จุดอ่อน**
1. มีเทคโนโลยีและอุปกรณ์ที่ทันสมัย 2. มีระบบป้องกันไวรัสที่ทันสมัยและถูกลิขสิทธิ์	1. ผู้บริหารให้ความสำคัญด้านนโยบายมากกว่าเทคโนโลยี 2. ขาดบุคลากรที่ดูแลด้านการรักษาความปลอดภัยโดยตรง 3. มีภัยคุกคามจากภายนอกเข้ามาโจมตีระบบอยู่เสมอ 4. ผู้ดูแลระบบขาดการฝึกอบรมเฉพาะด้าน 5. บุคลากรผู้ใช้งานขาดความรู้ด้านการใช้งานอย่างถูกวิธี
O : Opportunities โอกาส	**T : Threats อุปสรรค**
1. มีนโยบายติดตั้งอุปกรณ์และซอฟแวร์สำหรับการรักษาความปลอดภัยเพิ่มในอนาคต 2. บุคลากรมีโอกาสได้รับการถ่ายทอดความรู้ด้านเทคโนโลยีใหม่ๆ เสมอ	1. อุปกรณ์ด้านการรักษาความปลอดภัยมีราคาสูง 2. ความก้าวหน้าทางเทคโนโลยีทำให้เกิดความเสี่ยงในการโจมตีระบบรักษาความปลอดภัยเพิ่มขึ้น 3. การพัฒนาบุคลากรด้านการรักษาความปลอดภัยใช้งบประมาณในการอบรมสูง

7. ปัญหาและข้อจำกัดของงานวิจัย

จากการดำเนินการวิจัยทำให้พบปัญหาและข้อจำกัดดังนี้

7.1 เนื่องจากผู้วิจัยเลือกใช้เทคนิคเดลฟายทำให้ต้องใช้เวลาในการติดต่อประสานงาน การตรวจสอบแบบสอบถาม และรอผลไปได้ช้าเนื่องจากผู้เชี่ยวชาญแต่ละท่านนั้นติดภารกิจ

7.2 การกำหนดขอบเขตของวิจัยนั้นกว้างทำให้หาผู้เชี่ยวชาญที่ชำนาญในด้านระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัยโดยตรงนั้นยาก โดยไม่ได้ระบุให้แคบกว่านี้ว่าต้องเป็นมหาวิทยาลัยประเภทใด

7.3 ระยะเวลาในการดำเนินการนั้นไม่เพียงพอกับการดำเนินการวิจัยเพราะการวิจัยหาแนวโน้มในอนาคตโดยใช้เทคนิคเดลฟายนั้นจำเป็นต้องใช้เวลาในการดำเนินงานวิจัยอย่างมาก

8. ข้อเสนอแนะในการดำเนินงานวิจัยครั้งต่อไป

8.1 ควรกำหนดขอบเขตของงานวิจัยให้ชัดเจน ไม่ต้องกว้างมากเกินไป ควรศึกษาในเรื่องที่ต้องการรู้เฉพาะด้านจะทำให้การดำเนินงานวิจัยได้รวดเร็วขึ้น

8.2 ควรทำการตกลงกับผู้เชี่ยวชาญให้ชัดเจนเกี่ยวกับการตอบแบบสอบถามหรือการสัมภาษณ์เพราะถ้าผู้เชี่ยวชาญไม่สามารถตอบแบบสอบถามได้ตามระยะเวลาที่กำหนด จะทำให้งานวิจัยล่าช้า

8.3 หัวข้อที่จะทำงานศึกษานั้นต้องเป็นหัวข้อที่เป็นที่แพร่หลาย และมีงานวิจัยอื่นๆ ที่เคยได้ศึกษาเกี่ยวกับหัวข้อนี้มาแล้ว เพื่อง่ายต่อการหาผู้เชี่ยวชาญ

9. เอกสารอ้างอิง

[1] Burd And Steffani A. (2006).**Impact Of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy and Practice**. Washing, DC : US. Department of Justice.

[2] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. (2550). **มาตราฐานการรักษาความปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั้น 2.5) ประจำปี 2550**. กรุงเทพฯ : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี.

[3] Jensen, C. (1996). **Delphi in Depth: Power Techniques from the Experts**. Singapore: Osborne McGraw-Hill.

[4] จตุชัย แพงจันทร์. (2550). **Master in Security.** กรุงเทพฯ : อินโฟรเพรส.

[5] ธวัชชัย ชมศิริ. (2553). **ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์**. กรุงเทพฯ : โปรวิชั่น.

[6] Johnson, P.L. (1993). **ISO 900 Meeting the New International Standard**. Singapore: McGraw-Hill.

[7] เดชาวัต นิชาญานันท์. (2555). **การจัดทำนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรกรณีศึกษาสำหรับบริษัทสินแพทย์ จำกัด (โรงพยาบาลสินแพทย์)**. วิทยาศาสตรมหาบัณฑิต สาขาวิชาความมั่นคงทางระบบสารสนเทศ คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

[8] จิตติมา เทียมบุญประเสริฐ และกว้าน สีตะธนี. (2550). **การพัฒนาระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต**. วารสารวิจัย มสด สาขาสังคมศาสตร์และมนุษยศาสตร์. ปีที่ 3 ฉบับที่ 3 กันยายน–ธันวาคม : 110-123.

[9] สุนทรีย์ พัวพรพงษ์. (2556). **แนวโน้มนโยบายการรักษาความปลอดภัยของระบบคอมพิวเตอร์เครือข่ายไร้สายในองค์กรอุตสาหกรรม อีก 5 ปีข้างหน้า (2556-2560) โดยใช้เทคนิคเดลฟาย**. วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.