บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

อาจกล่าวได้ว่าในปัจจุบันนี้เป็นยุคแห่งเทคโนโลยีสารสนเทศ ที่ระบบคอมพิวเตอร์เข้ามามีบทบาทในเกือบทุกส่วนของการดำเนินชีวิตประจำวันของบุคคล การเชื่อมโยงเครือข่ายติดต่อสื่อสารกระทำได้อย่างเสรี โดยไร้ขีดจำกัดทางกายภาพ ผ่านทางระบบเชื่อมโยงต่างๆ อาทิ ระบบอินเตอร์เนต การเชื่อมโยงผ่านสายโทรศัพท์ เคเบิ้ลใยแก้วนำแสง หรือแม้แต่การส่งผ่านสัญญาณดาวเทียมก็ตาม การติดต่อสื่อสารดังกล่าวนี้ช่วยกระตุ้นให้เกิดการพัฒนาในด้านอื่นๆ ตามมาด้วย เป็นผลสืบเนื่องมาจากการกระจายความเจริญจากประเทศหนึ่งไปสู่อีกประเทศหนึ่งในต่างทวีป การเชื่อมโยงวัฒนธรรมและกระตุ้นให้เกิดการตื่นตัวในการพัฒนาความเจริญก้าวหน้าทางเทคโนโลยี เพื่อให้ได้ชื่อว่าเป็นผู้มีความเจริญก้าวหน้า ทันยุคสมัย มีความพยายามในการพัฒนาระบบคอมพิวเตอร์ขึ้นเพื่อใช้ในกิจการต่างๆ ทั้งในภาครัฐและเอกชน เนื่องจากความเชื่อถือในความถูกต้องของข้อมูลที่มีการจัดเก็บและประมวลผลโดยคอมพิวเตอร์ อีกทั้งยังแสดงถึงศักยภาพในการเป็นผู้นำด้านเทคโนโลยีของประเทศ รวมทั้งแสดงถึงความมั่นคงในแง่ขององค์กรธุรกิจอีกด้วย

จากการนำระบบคอมพิวเตอร์เข้ามาเป็นผู้จัดการกับข้อมูลที่อาจเรียกอีกอย่างหนึ่งว่าสินทรัพย์ที่มีมูลค่ามากที่สุดในทางธุรกิจ หรือแม้แต่ข้อมูลในภาครัฐเองก็ตาม ทำให้เกิดความพยายามในการแก้ไข ปรับเปลี่ยนข้อมูล หรือกระทำวิธีการใดๆ เพื่อให้ได้รับผลประโยชน์จากการควบคุมหรือนำระบบดังกล่าวเข้ามาใช้ จึงเกิดเป็นกระแสใหม่ของวิธีการประกอบอาชญากรรมที่ในปัจจุบันรู้จักกันทั่วไปในชื่อของ อาชญากรรมคอมพิวเตอร์ หรือ Computer Crime

ในอดีต ยังไม่มีการรวบรวมข้อมูลสถิติเกี่ยวกับการทุจริตทางคอมพิวเตอร์ที่แน่ชัดนัก แต่อย่างไรก็ตาม ระบบคอมพิวเตอร์ก็ยังคงเป็นส่วนสำคัญในการควบคุมสินทรัพย์ทางการเงินของกิจการ ดังนั้น ระบบคอมพิวเตอร์จึงยังคงเป็นเป้าหมายสำคัญของการกระทำ เพื่อให้ได้มาซึ่งผลประโยชน์ดังกล่าว หรือแม้แต่การกระทำใดๆ เพื่อเหตุผลส่วนตัวโดยไม่ได้หวังผลตอบแทนทางการเงินก็ตาม

การทุจริตทางคอมพิวเตอร์มีความสำคัญเนื่องจากมีกิจการหลายๆ แห่งที่ยอมรับว่ามีความสูญเสียเกิดขึ้นในส่วนที่เกี่ยวข้องกับระบบคอมพิวเตอร์ จากการศึกษาพบว่า ประมาณร้อยละ 25 - 50 ของหน่วยงานหลักในสหรัฐอเมริกาต้องประสบกับปัญหาการทุจริตทางคอมพิวเตอร์ในทุกๆ ปี และประมาณร้อยละ 90 ของกิจการเหล่านี้เคยประสบกับปัญหาอาชญากรรมคอมพิวเตอร์มาแล้วในอดีต

หน่วยงานสืบสวนสอบสวนกลางของสหรัฐอเมริกา (The Federal Bureau of Investigation : FBI) และหน่วยงานอื่นๆ ของสหรัฐได้ประมาณมูลค่าความเสียหายอันเกิดจากอาชญากรรมทางคอมพิวเตอร์ ว่ามีมูลค่าประมาณ 100 ล้านเหรียญ ถึง 5 พันล้านเหรียญสหรัฐต่อปี (Barthel Matt,1993 : 16 – 17)

ผลกระทบของความสูญเสีย เนื่องจากการประกอบอาชญากรรมทางคอมพิวเตอร์นั้น ส่งผลกระทบในวงกว้าง ความสูญเสียของการถูกโจมตีต่อหนึ่งครั้งอาจมีมูลค่าเพียงไม่กี่พันเหรียญ แต่การทุจริตทางคอมพิวเตอร์มักจะกระทำเป็นระบบและหลายๆ ครั้งในแต่ละปี ซึ่งผลก็คือมูลค่าความสูญเสียนับพันล้าน ผู้เชี่ยวชาญเชื่อว่า หากองค์กรไม่ได้กำหนดแนวทางการป้องกัน อาชญากรคอมพิวเตอร์ไว้ ก็จะต้องสิ้นเปลืองค่าใช้จ่ายในการตรวจสอบและการสืบเสาะเกี่ยวกับปัญหาดังกล่าวเกินกว่าวงเงินที่กำหนดไว้เสมอ ขึ้นอยู่กับขนาดของกิจการและผลกระทบทางการเงินต่อขอบเขตความเชื่อถือได้

เหตุผลที่สำคัญอีกประการหนึ่งของความเชื่อที่ว่า อาชญากรรมคอมพิวเตอร์เป็นเรื่องที่จะต้องให้ความสนใจก็คือ การให้ความสนใจเกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศ จากผู้จัดการและผู้บริหารระดับสูงของกิจการ ในการศึกษาพบว่า ผู้บริหารไม่ได้จัดลำดับความสำคัญของการรักษาความปลอดภัยเกี่ยวกับคอมพิวเตอร์ของกิจการไว้ และกว่าร้อยละ 41 ของกิจการ ที่ศึกษาไม่มีระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์

จากความตื่นตัวในการศึกษาเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ซึ่งกระทำผ่านทางระบบเทคโนโลยีสารสนเทศ ทำให้มีการศึกษาจากหน่วยงานต่างๆ จำนวน 158 หน่วยงาน ในประเทศออสเตรเลีย เกี่ยวกับแนวโน้มของการเกิดอาชญากรรมที่เกี่ยวข้องกับระบบคอมพิวเตอร์ในอนาคต ดังแสดงไว้ในตารางที่ 1.1

ตารางที่ 1.1 แสดงแนวโน้มของอาชญากรรมคอมพิวเตอร์ในอนาคต

ประเภทของอาชญากรรมคอมพิวเตอร์	จำนวนของผู้ที่ตอบรับ
การบุกรุกระบบหรือการลักลอบเข้าถึง (Hacking)	114
การลักลอบใช้ระบบสื่อสารข้อมูล	90
การใส่รหัสข้อมูล	76
การใช้รหัสโดยเจตนามุ่งร้าย	54
การลักขโมย	53
การกระทำโดยใช้ความเชี่ยวชาญเฉพาะด้าน	49
การฉ้อโกง	46
การเพิ่มขึ้นของศักยภาพในอาชญากรรมที่เสมือนจริง	30
การยกระดับจากอาชญากรรมธรรมดา	24
การใช้ข้อบ่งชี้ที่ผิด	23
สงครามสารสนเทศ	21
ภาวะอันตรายเกี่ยวกับตลาดมืดของสารสนเทศ	17
การใช้เงินสดอิเลคโทรนิคส์ และการปลอมแปลง	14
การปลอมลายมือ	12
อาชญากรรมขององค์กรเสมือนจริง	11
การข่มขู่ทางอิเลคโทรนิคส์	11
ภาวะอันตรายของกลุ่มองค์กรอาชญากรรม	9
การฟอกเงิน	6
อื่นๆ	2

ที่มา Office of Strategic Crime Assessment and Victoria Police, Australia 1997.

ในด้านเทคโนโลยีคอมพิวเตอร์แล้ว ข้อมูลในอดีต อาจไม่สามารถนำมาใช้พยากรณ์เหตุการณ์ในอนาคตได้ดีนัก แต่ถึงกระนั้น ผู้ที่เกี่ยวข้องก็ควรจะให้ความสำคัญกับการพัฒนาระบบสารสนเทศสำหรับการติดต่อสื่อสารขององค์กร การพยากรณ์ที่อ้างถึงการถูกโจมตีด้วยอาชญากรคอมพิวเตอร์ ผ่านทางระบบสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์, การลักลอบใช้บริการสื่อสาร และการใช้คอมพิวเตอร์ในการฉ้อโกงและเปลี่ยนแปลงข้อมูลในระบบ ซึ่งมีแนวโน้มที่จะทวีความรุนแรงมากขึ้นในอนาคตด้วย

จากการตรวจสอบของ FBI รายงานการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในปี ค.ศ.1994 และ ค.ศ.1998 ไว้ดังตารางที่ 1.2

ตารางที่ 1.2 การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในการตรวจสอบเปรียบเทียบระหว่างปี ค.ศ.1994 และ ค.ศ.1998

ประเภทของความผิด	จำนวน		ร้อยละ	
	1994	1998	1994	1998
การฉ้อโกง	108	-	20	13
การโจมตีโดยใช้ไวรัส	261	-	48	48
การขโมยข้อมูลหรือโปรแกรม	31	-	6	48
การลักลอบเข้าถึงข้อมูล (Hacking)	15	-	3	-
อื่นๆ	122	-	-	8
รวม	537	-	100	-

หมายเหตุ : อื่นๆ หมายรวมถึง การก่อวินาศกรรม, การบุกรุกสิทธิของผู้อื่น, การใช้ซอฟแวร์ผิดกฎหมายและการใช้งานส่วนตัว

ที่มา Andrzej Adamski, Crimes Related to the Computer Network..1999 p. 226

หอสมุดกลาง สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

อย่างไรก็ตามถึงแม้อาชญากรรมคอมพิวเตอร์จะเป็นเรื่องที่ทุกๆ ฝ่ายพยายามให้ความสนใจและหาวิธีป้องกัน แต่ก็ยังไม่มีกฎเกณฑ์ใดที่กำหนดได้อย่างแน่ชัดว่า อาชญากรรมคอมพิวเตอร์คืออะไร มีวิธีการกระทำอย่างไร ผลเสียหายที่เกิดขึ้นจากการกระทำ ดังกล่าว หรือบทบัญญัติของกฎหมายที่จะนำมาลงโทษผู้กระทำผิดดังกล่าว ผู้วิจัยจึงมีความสนใจศึกษาว่ามีปัจจัยใดบ้าง ที่มีผลต่อการลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์ในประเทศไทย

วัตถุประสงค์ของการวิจัย

งานวิจัยเรื่อง "การลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์" ในครั้งนี้ ผู้วิจัยกำหนดวัตถุประสงค์ในการวิจัยไว้ดังนี้คือ

1.เพื่อศึกษาถึงลักษณะพื้นฐานทางสังคมของผู้ที่ลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์

2.เพื่อให้ทราบถึงปัจจัยที่มีผลต่อการลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์

3. เพื่อศึกษาแนวทางป้องกันปัญหาการก่ออาชญากรรมคอมพิวเตอร์ในประเทศไทย

ขอบเขตของการวิจัย

งานวิจัยเรื่อง "การลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์" ในครั้งนี้ เนื่องด้วยงบประมาณและระยะเวลาที่จำกัด ผู้วิจัยจึงกำหนดขอบเขตในการวิจัยโดย เลือกศึกษาเฉพาะกรณีของผู้ใช้คอมพิวเตอร์และอินเตอร์เนตที่ลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์ในประเทศไทย โดยทำการเก็บข้อมูลจากผู้กระทำการลักลอบเข้าถึงข้อมูล ทั้งที่ผู้กระทำการโดยมีความผิดตามกฎหมาย หรือผู้ที่กระทำความผิดในรูปแบบอื่นๆ ที่ยังไม่มีกฎหมายในประเทศไทยรองรับว่าเป็นความผิด เพื่อให้ได้ข้อมูลเกี่ยวกับรูปแบบการก่ออาชญากรรมคอมพิวเตอร์และการลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์ในประเทศไทยที่ชัดเจนยิ่งขึ้น

ประโยชน์ที่คาดว่าจะได้รับ

งานวิจัยเรื่อง "การลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์" ในครั้งนี้ผู้วิจัยคาดหวังว่าจะเกิดประโยชน์ดังนี้

1.ทำให้ทราบถึงรูปแบบและพฤติกรรมการลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์และรูปแบบของอาชญากรรมคอมพิวเตอร์ในประเทศไทย

2.ทำให้สามารถการพยากรณ์เกี่ยวกับแนวโน้มการก่ออาชญากรรมทางคอมพิวเตอร์ในอนาคต ตลอดจนได้แนวทางในการป้องกันแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ที่เหมาะสมกับประเทศไทย