การสำรวจภัยคุกคามระบบสารสนเทศของบริษัทจดทะเบียน ในตลาดหลักทรัพย์แห่งประเทศไทย

วรัญญา สุมทุมทิพย์*
บริษัท โทเทิล แอ้คเซ็ส คอมมูนิเคชั่น จำกัด (มหาชน)
นิตยา วงศ์ภินันท์วัฒนา
ภาควิชาระบบสารสนเทศเพื่อการจัดการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

***Correspondence:** ws_nui@hotmail.com
doi: 10.14456/jisb.2017.16

บทคัดย่อ

วัตถุประสงค์ของงานวิจัยนี้คือ การสำรวจภัยคุกคามระบบสารสนเทศของบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย จำนวน 335 บริษัท ผลการสำรวจพบว่าลำดับภัยคุกคามที่เป็นภัยคุกคามจากมากไปน้อยมีดังนี้ (1) การแพร่กระจายไวรัส (2) การโจมตีด้วยมัลแวร์ (3) การเข้าถึงระบบโดยแฮกเกอร์ (4) การทำฟิชชิง (5) การแอบเข้าไปใช้ทรัพยากรทางคอมพิวเตอร์ที่เปิดให้มีการใช้งานร่วมกัน (6) การทำลายข้อมูลโดยเจ้าหน้าที่ (7) ข้อมูลที่ผิดพลาดจากการกระทำของเจ้าหน้าที่ (8) การใช้ซอฟต์แวร์เพื่อเข้าระบบโดยไม่ต้องผ่านการควบคุมในระบบ (9) การก่อวินาศกรรมหรือทำลาย (10) การเรียกค่าไถ่เพื่อแลกกับการไม่เปิดเผยข้อมูลที่ขโมยมา (11) ภัยธรรมชาติ (12) ข้อผิดพลาดจากการกระทำของมนุษย์ (13) การเข้าระบบโดยไม่ได้รับอนุญาต (14) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (15) การค้นหาข้อมูลที่สำคัญจากถังขยะ (16) ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ (17) การขโมยใช้งานบริการต่างๆ (18) การละเมิดทรัพย์สินทางปัญญา (19) ผู้ให้บริการระบบสารสนเทศไม่มีการควบคุมอย่างเหมาะสม (20) การใช้อินเทอร์เน็ตเพื่อกระจายข้อมูลที่ไม่เป็นจริงของบริษัท และ (21) เทคโนโลยีที่ล้าสมัยก่อให้เกิดความเสี่ยงที่ระบบสารสนเทศจะถูกโจมตีได้ โดยองค์กรสามารถนำผลการสำรวจไปดำเนินการป้องกันหรือรับมือกับภัยคุกคามที่อาจเกิดขึ้น รวมถึงนำไปเป็นแนวทางในการฝึกอบรมแก่พนักงานในองค์กร เพื่อให้เกิดประสิทธิภาพสูงสุด

คำสำคัญ: ภัยคุกคาม ความมั่นคงปลอดภัยของระบบสารสนเทศ ตลาดหลักทรัพย์แห่งประเทศไทย

Survey on the information system threats of listed companies in stock exchange of Thailand

Waranya Sumtumthip*

Total Access Communication Plc

Nitaya Wongpinunwatana

Department of Management Information Systems, Thammasat Business School, Thammasat University

***Correspondence:** ws_nui@hotmail.com

doi: 10.14456/jisb.2017.16

Abstract

The objective of this study is to survey on the information system threats of listed companies in stock exchange of Thailand (SET). This research collects information from 335 companies. From the survey, the rank of information system threat from high to low can be caused by (1) entry of computer viruses, (2) deliberate software attacks, (3) access to system by hackers, (4) phishing, (5) problems with the software, (6) accidental destruction data by employees, (7) accidental entry bad data by employees, (8) deliberate acts of trespass, (9) deliberate acts of sabotage or vandalism, (10) deliberate acts of information extortion, (11) force of nature, (12) human error/failures, (13) unauthorized access by employees, (14) technical hardware failures or errors, (15) dumpster diving, (16) technical software failures or error, (17) account or service hijacking, (18) compromises to intellectual property, (19) deviations in quality of service, (20) internet misinformation, and (21) technical obsolescence. The information system threats can cause problems in many ways. Knowing the threat that causes the problem, the responsible personal can find the way to handle the problems and help teaching the staffs within the company for the best benefits.

Keywords: Threat, Information security, Stock exchange of Thailand

1. บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศมีบทบาทสำคัญในการเพิ่มประสิทธิภาพการดำเนินงานและการจัดการ รวมทั้งการเสริมสร้างภาพลักษณ์ที่ดีขององค์กรทั้งภาครัฐและเอกชน ภัยคุกคามระบบสารสนเทศจึงอาจเกิดขึ้นได้ทั้งภายในองค์กรและภายนอกองค์กร ซึ่งหากผู้บริหารบางคนไม่ให้ความสำคัญต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่ใช้ภายในองค์กรแล้ว ก็จะทำให้มีความเสี่ยงที่จะเกิดภัยคุกคามแก่องค์กรเพิ่มขึ้นได้ เนื่องจากภัยคุกคามระบบสารสนเทศสามารถเกิดขึ้นได้กับทุกองค์กรไม่ว่าจะเป็นองค์กรขนาดใหญ่หรือเล็ก มีผลกำไรมากหรือน้อย ดังนั้น ภัยคุกคามระบบสารสนเทศจึงเป็นปัญหาที่มีความสำคัญซึ่งผู้บริหารควรตระหนักและหาแนวทางป้องกันไว้เพื่อมิให้กระทบต่อการดำเนินงานขององค์กร

ผู้วิจัยได้ศึกษางานวิจัยและผลสำรวจอัตราการเกิดภัยคุกคามระบบสารสนเทศในต่างประเทศ พบว่างานวิจัยต่างประเทศมีการศึกษาภัยคุกคามความมั่นคงปลอดภัยของระบบสารสนเทศเฉพาะภัยคุกคามที่เกี่ยวกับการขโมยข้อมูล (deliberate acts of theft) และจากการศึกษางานวิจัยของ Whitman (2004) พบว่า องค์กรมากกว่าร้อยละ 50 ประสบปัญหาภัยคุกคามระบบสารสนเทศในรูปแบบต่างๆ และจากผลการสำรวจของ CSI Computer Crime & Security Survey ซึ่งเป็นการศึกษาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ พบว่าองค์กรเกิดอาชญากรรมทางคอมพิวเตอร์มากที่สุดคือ องค์กรที่เกี่ยวข้องกับการเงิน

นอกจากนี้ข้อมูลจากอินเทอร์เน็ตและเว็บไซต์ที่เกี่ยวกับภัยคุกคามระบบสารสนเทศในประเทศไทยยังแสดงให้เห็นว่า ประเทศไทยยังไม่มีการสำรวจความเสี่ยงของภัยคุกคามในองค์กรมากนัก โดยผลที่ได้จากการสำรวจจะสามารถนำไปประยุกต์ใช้เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นกับองค์กรได้

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อสำรวจและจัดอันดับภัยคุกคามระบบสารสนเทศในองค์กร โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูลจากบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย (Security exchange of Thailand หรือ SET) เนื่องจากองค์กรขนาดเล็กมีแนวโน้มที่จะลงทุนในระบบสารสนเทศไม่มากเท่าองค์กรขนาดกลางและขนาดใหญ่

2. แนวคิดที่เกี่ยวข้อง

ภัยคุกคาม (Threat) หมายถึง ความเสียหายที่เกิดขึ้นกับ ฮาร์ดแวร์ (hardware) ซอฟต์แวร์ (software) และข้อมูล โดยแต่ละองค์กรอาจมีภัยคุกคามที่แตกต่างกันออกไป (Whitman and Mattord, 2002) ทั้งนี้ ภัยคุกคามอาจไม่เกิดขึ้นหากมีการเฝ้าระวังและมีการป้องกันที่ดี รวมทั้งมีเทคโนโลยีที่ใช้ในการป้องกันภัยคุกคามระบบสารสนเทศ (Colwill, 2010) และควบคุมการเข้าถึงข้อมูลของผู้ใช้ภายในองค์กร (Mcfadden, 1997)

จากการทบทวนเอกสารที่กล่าวถึงภัยคุกคามระบบสารสนเทศพบว่า Whitman (2004) และ Schuessler (2011) ได้จำแนกภัยคุกคามระบบสารสนเทศตามความสามารถในการจับต้องภัยคุกคามทางคอมพิวเตอร์ โดยแบ่งเป็นภัยคุกคามทางตรรกะ (logical) และภัยคุกคามทางด้านกายภาพ (physical) สำหรับ CSA (cloud security alliance) ได้จัดประเภทภัยคุกคามระบบสารสนเทศในลักษณะเดียวกับ Whitman (2004) แต่เน้นที่คอมพิวเตอร์กลุ่มเมฆ (cloud computing) เป็นหลักโดยมีรายละเอียดดังนี้

ภัยคุกคามทางตรรกะ คือ ภัยคุกคามที่มุ่งเน้นด้านข้อมูลหรือสารสนเทศ ไม่ว่าจะเป็นการเข้าถึงระบบสารสนเทศโดยได้รับอนุญาตหรือไม่ได้รับอนุญาตก็ตาม ซึ่งอาจขัดขวางไม่ให้ระบบสารสนเทศทำงานตามปกติ หรืออาจเข้าถึงข้อมูล ลบข้อมูล และแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ซึ่งการกระทำดังกล่าวนี้ ส่วนใหญ่เกิดจากการกระทำของผู้ใช้แทบทั้งสิ้น ภัยคุกคามทางตรรกะสามารถจัดประเภทได้ ดังนี้

(1) การกรรโชกข้อมูลสารสนเทศ (deliberate acts of information extortion) โดยเรียกร้องค่าตอบแทนหรือค่าไถ่แลกกับการไม่เปิดเผยข้อมูลลับที่ขโมยมา

(2) การโจมตีที่มาจากซอฟต์แวร์ (deliberate software attacks) เป็นการออกแบบซอฟต์แวร์อื่นให้เข้าไปโจมตีระบบสารสนเทศที่ใช้งานตามปกติให้เสียหาย ซอฟต์แวร์ที่ได้รับความนิยม เช่น มัลแวร์ (malware) โดยมัลแวร์มีมากมาย อาทิ ไวรัส (viruses) เวิร์ม (worms) โทรจันฮอร์ส (trojan horses) และ logic bombs เป็นต้น

(3) ข้อมูลที่ผิดพลาดจากการกระทำของพนักงาน (accidental entry bad data by employees)

(4) การทำลายข้อมูลจากการกระทำของพนักงาน (accidental destruction data by employees)

(5) การแพร่กระจายของไวรัสคอมพิวเตอร์ (entry of computer viruses)

(6) การเข้าถึงระบบโดยแฮกเกอร์ (access to system by hackers) หมายถึง การเข้าใช้งานระบบสารสนเทศของหน่วยงานหรือองค์กรอื่นโดยไม่ประสงค์ดี

(7) การเข้าระบบสารสนเทศโดยไม่ได้รับอนุญาต (unauthorized access by employees)

(8) Abuse and nefarious use of cloud computing หมายถึง การใช้คอมพิวเตอร์กลุ่มเมฆในทางที่ผิด

(9) Insecure interfaces and application programming interfaces (APIs) หมายถึง ความน่าเชื่อถือในด้านความมั่นคงปลอดภัยและสภาพที่ไม่พร้อมจะใช้งาน ทำให้ผู้ใช้บริการต้องอาศัย API ในการติดต่อซอฟต์แวร์หลังบ้านและบริการต่างๆที่อยู่ในคอมพิวเตอร์กลุ่มเมฆ

(10) Malicious insiders เป็นภัยคุกคามที่เกิดขึ้นจากบุคคลคนภายใน หรือจากผู้ให้บริการเอง เช่น การเข้าถึงข้อมูลได้เกินกว่าสิทธิของตนเอง เป็นต้น

(11) Shared technology risk เป็นความผิดพลาดของซอฟต์แวร์ที่ใช้ในการแบ่งปันการใช้ทรัพยากรต่างๆ ให้ผู้ใช้ซึ่งมีช่องโหว่ที่ทำให้แฮกเกอร์สามารถสวมรอยเป็นผู้ใช้บริการคอมพิวเตอร์กลุ่มเมฆได้

(12) Data loss or leakage หมายถึง การรั่วไหลของข้อมูล เนื่องจากอาจมีผู้อื่นมาใช้งานบนคอมพิวเตอร์กลุ่มเมฆโดยไม่ได้รับอนุญาต

(13) Account or service hijacking หมายถึง การถูกขโมยใช้งานบริการต่างๆ การหลอกลวงทางอินเทอร์เน็ต การถูกโจมตีตามช่องโหว่ของซอฟต์แวร์ที่ไม่ได้ติดตั้งการควบคุม ซึ่งสาเหตุส่วนหนึ่งมักจะมาจากการใช้รหัสผ่าน เป็นเวลานานหรือไม่มีการเปลี่ยนแปลงรหัสผ่านในเวลาที่เหมาะสม

(14) Unknown risk profile การที่ผู้ใช้บริการไม่รู้ว่าภัยคุกคามมีอะไรบ้าง จึงไม่ได้เตรียมการป้องกันเพื่อรองรับภัยคุกคามไว้

(15) การใช้อินเทอร์เน็ตเพื่อการกระจายข้อมูล (internet misinformation) เป็นการใช้อินเทอร์เน็ตเพื่อกระจายข้อมูลที่ไม่เป็นจริงเกี่ยวกับคนหรือบริษัท

(16) ความพยายามหลอกลวง (phishing) หมายถึง ความพยายามในการหลอกลวงเพื่อเรียกสิทธิ ความลับ หรือความสำคัญของผู้ใช้บริการ โดยการจำลองการสื่อสารทางอิเล็กทรอนิกส์จากองค์กรที่น่าเชื่อถือ

(17) การค้นหาข้อมูลที่สำคัญจากถังขยะ (dumpster diving) เป็นการค้นหาข้อมูลสำคัญ เช่น รหัสผ่าน ชื่อแฟ้มข้อมูล หรือสารสนเทศที่เป็นความลับของผู้ใช้บริการจากคู่มือ รายงานและเอกสารต่างๆ ที่นำไปทิ้งแล้ว เพื่อนำมาโจมตีหรือหลอกลวงต่อไป

(18) การโจมตีจากผู้ไม่หวังดี (reverse social engineering) เป็นการติดต่อเหยื่อเพื่อหลอกถามชื่อผู้ใช้งานและรหัสผ่านการใช้งานอินเทอร์เน็ตของเหยื่อ

ภัยคุกคามทางกายภาพ หมายถึง ภัยคุกคามที่ส่วนใหญ่มักจะเกิดจาก ภัยจากธรรมชาติ เช่น น้ำท่วม ไฟไหม้ ฟ้าฝ่า เป็นต้น ในบางครั้งอาจเกิดจากการกระทำของมนุษย์ที่ทำความเสียหายให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ ทั้งโดยเจตนาและไม่เจตนา ภัยคุกคามทางกายภาพสามารถแบ่งเป็นประเภทต่างๆ ดังนี้

(1) ข้อผิดพลาดจากการกระทำของมนุษย์ ทั้งโดยเจตนาและไม่เจตนาซึ่งอาจเกิดจากการขาดความรู้ความชำนาญ แต่สามารถสร้างความเสียหายให้กับระบบสารสนเทศได้
(2) การละเมิดทรัพย์สินทางปัญญา (compromises to intellectual property)
(3) การบุกรุก (deliberate acts of trespass) โดยผู้ที่ไม่ได้รับอนุญาต
(4) การก่อวินาศกรรมหรือการทำลาย (deliberate acts of sabotage or vandalism) เช่น การทำลายทรัพย์สินหรือภาพพจน์ที่ดี
(5) ภัยธรรมชาติ (forces of nature) เป็นภัยที่มีอันตรายมากเพราะมนุษย์ไม่สามารถควบคุมได้
(6) คุณภาพของผู้ให้บริการ (deviations in quality of service) เป็นการสนับสนุนจากภายนอกซึ่งจะมีผลต่อคุณภาพของระบบสารสนเทศได้
(7) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (technical hardware failures or errors) ทำให้การทำงานของอุปกรณ์ไม่เป็นไปตามความต้องการ
(8) ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ (technical software failures or errors) ทำให้ผู้ไม่มีสิทธิใช้งานเข้าสู่ระบบได้โดยปราศจากการตรวจเช็คความปลอดภัย
(9) เทคโนโลยีล้าสมัย (technical obsolescence) มีผลกระทบต่อการรักษาความปลอดภัยของระบบสารสนเทศได้

3. วิธีการวิจัย

งานวิจัยนี้จัดเก็บข้อมูลจากบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย จำนวน 335 บริษัท จากจำนวนบริษัททั้งสิ้น 497 บริษัท ด้วยการตอบแบบสอบถามจากผู้บริหารหรือพนักงานในฝ่ายเทคโนโลยีสารสนเทศของบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย และส่งกลับมายังผู้วิจัยผ่านทางไปรษณีย์ โทรสาร และจดหมายอิเล็กทรอนิกส์

ในการจัดอันดับภัยคุกคามระบบสารสนเทศนี้ ผู้วิจัยจัดอันดับภัยคุกคามด้วย DREAD ซึ่งเป็นการจัดอันดับภัยคุกคามสำหรับซอฟต์แวร์ที่จัดทำโดย Microsoft และนำมาปฏิบัติกันโดยทั่วไป (Sonia et al., 2011) โดย DREAD จัดอันดับภัยคุกคามเป็น 5 ประเภท ดังนี้

- ภัยคุกคามนั้นสร้างความเสียหายมากน้อยเพียงใด (Damage มาจาก D ใน DREAD)
- ภัยคุกคามนั้นสามารถทำซ้ำได้ง่ายเพียงใด (Reproducibility มาจาก R ใน DREAD)
- ภัยคุกคามนั้นต้องใช้ความพยายามมากน้อยเพียงใด (Exploitability มาจาก E ใน DREAD)
- ภัยคุกคามนั้นจะส่งผลกระทบต่อผู้ใช้จำนวนมากหรือน้อยเพียงใด (Affected users มาจาก A ใน DREAD)
- ภัยคุกคามนั้นจะถูกค้นพบได้ง่ายเพียงใด (Discoverability มาจาก D ใน DREAD)

รายละเอียดของแบบสอบถามที่ใช้ในการวิเคราะห์แบ่งออกเป็น 2 ส่วน โดยส่วนแรกเป็นข้อมูลเบื้องต้นของสถานประกอบการ และส่วนที่ 2 เป็นคำถามเกี่ยวกับภัยคุกคามความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กรโดยทำการวัดค่าตัวแปรด้วย interval scale ซึ่งกำหนดมาตรวัดแบบ scale (1-10) โดยแยกระดับความเสี่ยงเป็น 3 ระดับ คือ

ความเสี่ยงสูง (high risk), ความเสี่ยงปานกลาง (medium risk) และความเสี่ยงต่ำ (low risk) เพื่อให้สามารถวัดค่าความคิดเห็นของแต่ละปัจจัยได้ชัดเจนมากขึ้น

เมื่อได้รับแบบสอบถามกลับคืนมาแล้ว จะทำการตรวจสอบเพื่อคัดแยกข้อมูลที่ผู้ตอบกรอกข้อมูลไม่ครบตามที่ต้องการออกไป และนำข้อมูลมาวิเคราะห์โดยใช้เกณฑ์การจัดอันดับของ DREAD โดยการคำนวณแยกตามกลุ่มอุตสาหกรรมตามระดับความเสี่ยง ดังนี้

(1) นำคำตอบคะแนนความเสี่ยงภัยคุกคามตาม DREAD ที่แต่ละบริษัทตอบ (คะแนน 1-10) มาจัดเป็นรูปแบบ 3 สเกล คือ

1-3 คะแนน จะกำหนดค่าสเกลเท่ากับ 1

4-7 คะแนน จะกำหนดค่าสเกลเท่ากับ 2

8-10 คะแนน จะกำหนดค่าสเกลเท่ากับ 3

(2) นำค่าสเกลที่ได้ในข้อ 1 ของแต่ละบริษัทไปคำนวณคะแนนความเสี่ยงของภัยคุกคามตาม DREAD

(3) นำผลรวมคะแนนตามข้อ 2 ไปจัดอันดับความเสี่ยง โดยใช้หลักเกณฑ์ดังนี้

5-7 คะแนน มีอันดับความเสี่ยงต่ำ (low)

8-11 คะแนน มีอันดับความเสี่ยงปานกลาง (medium)

12-15 คะแนน มีอันดับความเสี่ยงสูง (high)

หลังจากนั้นนำผลการจัดอันดับความเสี่ยงของภัยคุกคามมาคำนวณเป็นค่าร้อยละในแต่ละระดับของกลุ่มประเภทอุตสาหกรรม

5. ผลการวิจัย

กลุ่มผู้ตอบแบบสอบถามเป็นบุคลากรระดับเจ้าหน้าที่และผู้จัดการของฝ่ายเทคโนโลยีสารสนเทศของแต่ละบริษัท อัตราการตอบกลับเท่ากับร้อยละ 60.40 ประเภทกลุ่มอุตสาหกรรมที่ตอบกลับมากที่สุด 3 อันดับแรก คือ กลุ่มอุตสาหกรรมบริการ กลุ่มอุตสาหกรรมสินค้าอุตสาหกรรม และกลุ่มอุตสาหกรรมอสังหาริมทรัพย์และก่อสร้าง

ผู้วิจัยได้จัดเก็บข้อมูลในลักษณะการจัดอันดับและนำข้อมูลที่ได้ไปถ่วงน้ำหนักความถี่ของคำตอบแต่ละอันดับจากกลุ่มอุตสาหกรรมแต่ละกลุ่มดังแสดงในตารางที่ 1

ตารางที่ 1 การเปรียบเทียบอันดับภัยคุกคามระบบสารสนเทศของแต่ละกลุ่มอุตสาหกรรม

ภัยคุกคาม	บริการ	สินค้าอุตสาหกรรม	อสังหาริมทรัพย์และก่อสร้าง	ธุรกิจการเงิน	เทคโนโลยี	เกษตรกรและอุตสาหกรรมอาหาร	สินค้าอุปโภคบริโภค	ทรัพยากร	รวมกลุ่มอุตสาหกรรม	
									รวม	อันดับ
การแพร่กระจายไวรัส	4	1	1	2	2	1	5	1	17	1
การโจมตีด้วยมัลแวร์	5	3	2	1	1	12	3	3	30	2
การเข้าถึงระบบโดยแฮกเกอร์	1	11	6	3	3	6	7	2	39	3
การทำฟิชชิง	15	2	12	4	7	3	2	3	48	4
การแอบเข้าไปใช้ทรัพยากรทางคอมพิวเตอร์ที่เปิดให้มีการใช้งานร่วมกัน	3	6	3	8	5	10	11	3	49	5
การทำลายข้อมูลโดยเจ้าหน้าที่	6	7	7	11	4	15	2	2	54	6
ข้อมูลที่ผิดพลาดจากการกระทำของเจ้าหน้าที่	9	15	4	6	10	9	1	2	56	7
การใช้ซอฟต์แวร์เพื่อเข้าระบบโดยไม่ต้องผ่านการควบคุมในระบบ	8	13	5	7	17	8	4	2	64	8
การก่อวินาศกรรมหรือทำลาย	10	5	9	20	12	4	2	3	65	9
การเรียกค่าไถ่เพื่อแลกกับการไม่เปิดเผยข้อมูลที่ขโมยมา	7	4	18	5	14	19	1	3	71	10
ภัยธรรมชาติ	11	17	8	14	13	5	4	3	75	11
ข้อผิดพลาดจากการกระทำของมนุษย์	13	8	14	9	11	13	6	3	77	12

ตารางที่ 1 การเปรียบเทียบอันดับภัยคุกคามระบบสารสนเทศของแต่ละกลุ่มอุตสาหกรรม (ต่อ)

ภัยคุกคาม	บริการ	สินค้าอุตสาหกรรม	อสังหาริมทรัพย์และก่อสร้าง	ธุรกิจการเงิน	เทคโนโลยี	เกษตรกรและอุตสาหกรรมอาหาร	สินค้าอุปโภคบริโภค	ทรัพยากร	รวมอุตสาหกรรม	
									รวม	อันดับ
การเข้าระบบโดยไม่ได้รับอนุญาต	2	14	16	10	8	17	9	3	79	13
ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์	18	9	10	16	19	2	5	4	83	14
การค้นหาข้อมูลที่สำคัญจากถังขยะ	16	20	13	17	9	7	8	3	93	15
ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์	17	10	11	19	20	14	4	3	98	16
การขโมยใช้งานบริการต่างๆ	12	12	19	13	15	21	10	4	106	17
การละเมิดทรัพย์สินทางปัญญา	14	16	17	18	16	18	8	2	109	18
ผู้ให้บริการระบบสารสนเทศไม่มีการควบคุมอย่างเหมาะสม	20	18	15	15	21	11	10	2	112	19
การใช้อินเทอร์เน็ตเพื่อกระจายข้อมูลที่ไม่เป็นจริงของบริษัท	19	19	20	21	6	20	8	3	116	20
เทคโนโลยีที่ล้าสมัยก่อให้เกิดความเสี่ยงที่ระบบสารสนเทศจะถูกโจมตีได้	21	21	21	12	18	16	10	3	122	21

จากตารางสรุปผลการจัดอันดับความเสี่ยงของภัยคุกคามความมั่นคงปลอดภัยของระบบสารสนเทศในกลุ่มอุตสาหกรรม โดยใช้สูตรการคำนวณดังนี้

อันดับของภัยคุกคาม = (ความถี่ของภัยคุกคาม x อันดับ 1) + (ความถี่ของภัยคุกคาม x อันดับ 2) + ... + (ความถี่ของภัยคุกคาม x อันดับ 21)

โดยคะแนนรวมของอันดับภัยคุกคามที่เกิดขึ้นที่มีค่าน้อยที่สุดแสดงว่าเป็นภัยคุกคามที่เกิดขึ้นมากที่สุดในองค์กร และอันดับภัยคุกคามที่เกิดขึ้นที่มีค่ามากที่สุดแสดงว่าเป็นภัยคุกคามที่เกิดขึ้นน้อยที่สุดในองค์กร จากภาพรวมสามารถแสดงให้เห็นถึงอันดับความเสี่ยงของภัยคุกคามความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร เพื่อให้องค์กรสามารถหาวิธีป้องกันหรือรับมือกับภัยคุกคามที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ หากสามารถทราบสาเหตุที่ทำให้เกิดภัยคุกคามความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร และสามารถรับมือกับภัยคุกคามที่เกิดขึ้นกับองค์กรได้อย่างเป็นระบบและต่อเนื่อง ทั้งนี้ความเสี่ยงของภัยคุกคามระบบสารสนเทศที่มีมาก 3 ลำดับแรก คือ

(1) การแพร่กระจายของไวรัสคอมพิวเตอร์ เป็นภัยคุกคามที่มีความเสี่ยงมากที่สุดอันดับแรก ซึ่งเกิดจากการแพร่กระจายของไวรัสคอมพิวเตอร์ไปในโปรแกรมประมวลผลหรือแฟ้มข้อมูลต่างๆ จึงก่อให้เกิดความเสียหายต่อระบบสารสนเทศภายในองค์กร เนื่องจากไวรัสส่วนใหญ่ถูกออกแบบมาให้มีการติดตั้งตัวเองและก่อให้เกิดการโจมตีต่อเครื่องคอมพิวเตอร์และระบบสารสนเทศ

(2) การโจมตีที่มาจากซอฟต์แวร์ เป็นภัยคุกคามที่มีความเสี่ยงเป็นอันดับ 2 ซึ่งเป็นการโจมตีระบบสารสนเทศโดยการนำซอฟต์แวร์เข้าไปในระบบสารสนเทศเพื่อทำให้เกิดความเสียหายทั้งข้อมูลและทรัพยากรอื่นๆ ในระบบสารสนเทศขององค์กร

(3) การเข้าถึงระบบโดยแฮกเกอร์ เป็นภัยคุกคามที่มีความเสี่ยงเป็นอันดับ 3 ซึ่งเป็นการเข้าถึงระบบสารสนเทศขององค์กรโดยแฮกเกอร์ เพื่อเข้าไปทำลายข้อมูล ปรับปรุง ลบโปรแกรมต่างๆ หรือรบกวนการให้บริการโดยไม่ได้รับอนุญาตซึ่งจะมีผลต่อความมั่นคงและปลอดภัยของระบบสารสนเทศ

6. สรุปผลการวิจัย

6.1 อภิปรายผลการวิจัย

ผลการสำรวจพบว่าภัยคุกคามระบบสารสนเทศที่องค์กรส่วนใหญ่ให้ความสำคัญสามลำดับแรก คือ การแพร่กระจายของไวรัสคอมพิวเตอร์ การโจมตีที่มาจากซอฟต์แวร์ และการเข้าถึงระบบโดยแฮกเกอร์ อย่างไรก็ตามการสำรวจนี้เป็นเพียงการสำรวจปัจจัยที่มีผลต่อการเกิดภัยคุกคามระบบสารสนเทศในบริษัทที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย (SET) จึงไม่ครอบคลุมในทุกองค์กรของประเทศไทย

6.2 ข้อเสนอแนะในเชิงปฏิบัติ

องค์กรที่ต้องการป้องกันภัยคุกคามระบบสารสนเทศสามารถนำผลการสำรวจมากำหนดวิธีการควบคุมเพื่อป้องกันภัยคุกคามในลำดับต้นๆ ก่อน ส่วนภัยคุกคามระบบสารสนเทศในลำดับหลังๆ อาจพิจารณาหาวิธีการควบคุมในภายหลังได้ เช่น มีงบประมาณเพียงพอ เป็นต้น

6.3 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง

เพื่อให้เกิดประโยชน์ในด้านการลำดับภัยคุกคามระบบสารสนเทศและการหาวิธีการควบคุมภัยคุกคามนั้น องค์กรควรสำรวจภัยคุกคามระบบสารสนเทศเป็นประจำทุกปี เนื่องจากความก้าวหน้าทางเทคโนโลยีทำให้มีภัยคุกคามระบบสารสนเทศใหม่ๆ เป็นประจำทุกปี เพื่อให้ทราบถึงภัยคุกคามระบบสารสนเทศที่เป็นปัจจุบันและติดตั้งวิธีควบคุมให้เหมาะสมและมีประสิทธิภาพต่อไป

บรรณานุกรม

Colwill, C. (2010). Human factors in information security: The insider threat - Who can you trust these days?. *Information security technical report*, I-II, 1-11.

Mcfadden, P. J. (1997). Guarding computer data. *Journal of Accountancy*, 2, 15-32.

Schuessler, J. H. (2011). Threats and countermeasures of the realm in 2011. Retrieved November 12, 2015, from http://researchgate.net/publication/308403873_Threats_and_Countermeasures_of_the_Realm_in_ 2011.

Sonia, Singhal, A., Banati, H. (2011). Fuzzy Logic Approach for Threat Prioritization in Agile Security Framework using DREAD Model. IJCSI International Journal of Computer Science Issues, 8(4), 182-190.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 24(1), 43-57.

Whitman, M. E. and Mattord, H. J. (2002). *Management of information Security*. Canada: Thomson Learning, Inc.