การประชุมวิชาการระดับชาติ ม.อ.ตรัง วิจัย ประจำปี 2562 ครั้งที่ 8

โดย คณะพาณิชยศาสตร์และการบัญชี การวิจัยและนวัตกรรม

The 8th PSU Trang National Conference on Research across Disciplines 2019

สาขาวิชาบริหารธุรกิจ/การประกันภัย และการจัดการความเสี่ยง

PSUNC 2019 วิจัยล้ำสมัยเพื่อการพัฒนาที่ยั่งยืน

Research and Innovation for Sustainable Development

Faculty of Commerce and Management

รายนามกองบรรณาธิการและผู้ทรงคุณวุฒิ
พิจารณาผลงานวิจัย บทความวิชาการและผลงานสร้างสรรค์

1. กลุ่มสาขาวิชาบริหารธุรกิจ/การประกันภัยและการจัดการความเสี่ยง
   ผู้ช่วยศาสตราจารย์ ดร.ปรีชา วิจิตรธรรมรส
   คณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์
   ดร.อิสริยะ สัตกุลพิบูลย์
   คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย
   ดร.นุชษรา พึ่งวิริยะ
   คณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏสงขลา
   ดร.พงษ์พิช เพชรสกุลวงศ์
   คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง
   ดร.นฤบาล ยมะคุปต์
   คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

2. กลุ่มสาขาวิชาการตลาด
   รองศาสตราจารย์ ดร.ศิวฤทธิ์ พงศกรรังศิลป์
   สำนักวิชาการจัดการ มหาวิทยาลัยวลัยลักษณ์
   ผู้ช่วยศาสตราจารย์ ดร.ธีรศักดิ์ จินดาบถ
   คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่
   ดร.สิทธิชัย นวลเศรษฐ
   คณะเทคโนโลยีการจัดการ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย
   ดร.ปิยะนุช ปรีชานนท์
   คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง
   ดร.วรางคณา ตันฑสันติสกุล
   คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง
   ดร.พงศกร พิชยดนย์
   คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

3. กลุ่มสาขาวิชาการจัดการการท่องเที่ยว
   ผู้ช่วยศาสตราจารย์ ดร.วลัญชลี วัฒนาเจริญศิลป์
   วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล
   ผู้ช่วยศาสตราจารย์ ดร.สมพงษ์ อำนวยเงินตรา
   วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล
   ดร.เมธาวี ว่องกิจ
   คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

4. กลุ่มสาขาวิชาการจัดการเทคโนโลยีสารสนเทศ

ดร. สยาม แย้มแสงสังข์

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

อาจารย์รุชดี บิลหมัด

คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

ดร. สุพัฒธนา สุขรัตน์

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ดร. อัจฉรา หลีระพงศ์

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ดร. จุไรรัตน์ พุทธรักษ์

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

5. กลุ่มสาขาวิชาการบัญชี

ดร.ปัญญา สัมฤทธิ์ประดิษฐ์

บริษัท ปูนซิเมนต์ไทย จำกัด (มหาชน)

ผู้ช่วยศาสตราจารย์ ดร.ปาริชาติ มณีมัย

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ดร.มัทนชัย สุทธิพันธุ์

คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

ดร.สุรนัย ช่วยเรือง

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ดร.นิพัฒน์ โพธิ์วิจิตร

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ดร.ดลินา อมรเหมาบนท์

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

6. กลุ่มสาขาวิชารัฐประศาสนศาสตร์/การบริหารรัฐกิจ

ผู้ช่วยศาสตราจารย์ ดร.สุวิทย์ จันทร์เพ็ชร

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ดร.ทวนธง ครุฑจ้อน

คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยทักษิณ

ดร.กรวิทย์ เกาะกลาง

คณะศิลปศาสตร์และวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตสุราษฎร์ธานี

ดร.วิสุทธิณี ธานีรัตน์

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ดร.อรอุมา สุพัฒนกุล

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ดร.ณรงค์ฤทธิ์ ปริสุทธิ์กุล

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

7. กลุ่มสาขาวิชาภาษาอังกฤษธุรกิจ

ดร. ณัฐกฤตา โชติภัคธนสุข

คณะศิลปศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์

ผู้ช่วยศาสตราจารย์ ดร.จิราพร เยี่ยมคำนวณ

คณะพาณิชยศาสตร์และการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ผู้ช่วยศาสตราจารย์ ดร.รัชฎาภรณ์ จันทร์อุดม

คณะศิลปศาสตร์และวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตสุราษฎร์ธานี

8. กลุ่มสาขาวิชาศิลปะการแสดงและการจัดการ

ดร.สมโภชน์ เกตุแก้ว

สาขาวิชาศิลปะการแสดงและการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

รายนามผู้ทรงคุณวุฒิวิพากษ์
ผลงานวิจัยบทความวิชาการและผลงานสร้างสรรค์

1. กลุ่มสาขาวิชาบริหารธุรกิจ/การประกันภัยและการจัดการความเสี่ยง
   ดร.อิสริยะ สัตกุลพิบูลย์
   คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย

2. กลุ่มสาขาวิชาการตลาด
   รองศาสตราจารย์ ดร.ศศิวิมล สุขบท
   คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่
   ผู้ช่วยศาสตราจารย์ ดร.ธีรศักดิ์ จินดาบถ
   คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่
   ดร.นิจกานต์ หนูอุไร
   คณะเศรษฐศาสตร์และบริหารธุรกิจ มหาวิทยาลัยทักษิณ
   ดร.อรจันทร์ ศิริโชติ
   คณะเศรษฐศาสตร์และบริหารธุรกิจ มหาวิทยาลัยทักษิณ
   ดร.สิริภัทร์ โชติช่วง
   คณะศิลปศาสตร์และวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตสุราษฎร์ธานี

3. กลุ่มสาขาวิชาการจัดการการท่องเที่ยว
   ผู้ช่วยศาสตราจารย์ ดร.ชัยรัตน์ จุสปาโล
   คณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย
   ดร.ห้าวหาญ ทวีเส้ง
   คณะศิลปศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

4. กลุ่มสาขาวิชาการจัดการเทคโนโลยีสารสนเทศ
   ดร. สุณิสา สถาพรวจนา
   คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

5. กลุ่มสาขาวิชาการบัญชี
   รองศาสตราจารย์ ดร.พนารัตน์ ปานมณี
   คณะบัญชี มหาวิทยาลัยหอการค้าไทย

6. กลุ่มสาขาวิชารัฐประศาสนศาสตร์/การบริหารรัฐกิจ
   ดร.ดนุวัศ สุวรรณวงศ์
   วิทยาลัยนวัตกรรมและการจัดการ มหาวิทยาลัยราชภัฏสงขลา
   ดร.วิวัฒน์ ฤทธิมา
   วิทยาลัยการจัดการเพื่อการพัฒนา มหาวิทยาลัยทักษิณ

7. กลุ่มสาขาวิชาศิลปะการแสดงและการจัดการ

รองศาสตราจารย์ ดร.จินตนา สายทองคำ

คณะศิลปนาฏดุริยางค์ สถาบันบัณฑิตพัฒนศิลป์

ผู้ช่วยศาสตราจารย์ ดร.บุปผาชาติ อุปถัมภ์นรากร

คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏพระนคร

คุณกฤษฎิ์ ชัยศิลบุญ

ผู้จัดการบริษัทกฤษฎิ์ทีม ออร์แกไนเซอร์ แอนด์ เพอร์ฟอร์มแม้นส์

ผู้เชี่ยวชาญด้านศิลปะการแสดงและการจัดการธุรกิจการแสดง

นายยุทธนา อัมระรงค์

หัวหน้าคณะศิลปินคิดบวกสิปป์

ดร.สมโภชน์ เกตุแก้ว

สาขาวิชาศิลปะการแสดงและการจัดการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตตรัง

ปัจจัยกำหนดและการบริหารจัดการความเสี่ยงทางไซเบอร์ของธนาคารพาณิชย์
DETERMINE FACTORS AND MANAGEMENT CYBER RISK OF COMMERCIAL-BANK

นายเจตพล สุรธรรม[1] และ รศ.ดร.ธนินท์รัฐ รัตนพงศ์ภิญโญ[2]
Chettaphon suratham[1] and Assoc. Prof. Dr. Taninrat Rattanapongpinyo[2]

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยกำหนดที่ส่งผลต่อความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์และเพื่อศึกษาความเสี่ยงทางไซเบอร์มีความสัมพันธ์กับการจัดการความเสี่ยงในธุรกิจธนาคารพาณิชย์ ทำการศึกษากลุ่มตัวอย่างของประชากรพนักงานหรือผู้มีประสบการณ์ในการทำงานที่เกี่ยวกับธนาคารพาณิชย์ในเขตกรุงเทพมหานคร จำนวน 400 ตัวอย่างในปี พ.ศ. 2561 โดยใช้การเลือกกลุ่มตัวอย่างแบบตามสะดวก วิเคราะห์ข้อมูลด้วยค่าสถิติเชิงพรรณนา (Descriptive Statistics) ได้แก่ ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน และ ทดสอบสมมติฐานด้วยการวิเคราะห์ถดถอยเชิงพหูคูณ ณ ระดับนัยสำคัญทางสถิติ 0.05

ผลการวิจัยพบว่าปัจจัยภายนอกด้านเทคโนโลยีส่งผลต่อความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์มากที่สุด รองลงมาคือปัจจัยทางการจัดการด้านบุคลากรส่งผลมากที่สุด สำหรับปัจจัยทางการจัดการและปัจจัยภายนอกมีความสัมพันธ์เชิงบวกกับความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์ แสดงโดยสมการ $\hat{Y} = -1.068 + 0.726\hat{X}_1 + 0.582\hat{X}_2$ โดยมีค่า Adjusted R Square อยู่ที่ 0.738 ในส่วนของความสัมพันธ์ระหว่างความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์กับการจัดการความเสี่ยง พบว่า มีความสัมพันธ์เชิงบวกโดยมีค่าสัมประสิทธิ์สหสัมพันธ์ (r) เท่ากับ 0.862 ณ ระดับนัยสำคัญ 0.05

คำสำคัญ :ปัจจัยกำหนด, การบริหารจัดการ, ความเสี่ยงทางไซเบอร์, ธนาคารพาณิชย์

---

[1]นักศึกษาสาขาการจัดการธุรกิจทั่วไป คณะวิทยาการจัดการ มหาวิทยาลัยศิลปากร
Student, Faculty of Management Science, Silpakorn University, E-mail: jaetapol55@hotmail.com

[2]อาจารย์ประจำสาขาการจัดการธุรกิจทั่วไป คณะวิทยาการจัดการ มหาวิทยาลัยศิลปากร
Lecturer, Faculty of Management Science, Silpakorn University, E-mail: taninrata@gmail.com

ABSTRACT

The purpose of this research was to study about determine factors that effect to cyber risk of commercial banks. And was to study about cyber risk correlate with cyber risk management of commercial banks in bangkok.The samples used in this study were 400 people in 2018. Employees or who experienced in working with commercial banks . The tools used to collect data are questionnaire. Analyze data using descriptive statistics by Average and Standard Deviation, multiple regression for hypotheses testing

The research found that the External factors affected the cyber risk of commercial banks. By technology is the most effective. Management factors affected. By man is the most effective. Management factors and External factors are correlate with the cyber risk of commercial banks. Express by equation $\hat{Y} = -1.068 + 0.726\hat{X}_1 + 0.582\hat{X}_2$ with the adjusted r square value was 0.738. In terms of the cyber risk of commercial banks and cyber risk management, It was found that had a positive relationship, by the correlation coefficient (r) were 0.862 at 0.05 level of statistical significance.

Keywords : Determine factors, Management, Cyber Risk, Commercial Bank

บทนำ

ปัจจุบันพัฒนาการที่ก้าวหน้าเป็นอย่างมากของเทคโนโลยีด้านคอมพิวเตอร์และระบบเครือข่ายได้ก่อให้เกิดนวัตกรรมต่างๆ ขึ้น มากมาย แต่ในขณะเดียวกัน ก็ได้นำความเสี่ยงมาสู่ผู้ใช้อย่างไม่ทันรู้เนื้อรู้ตัว การใช้เทคโนโลยีนั้นมีความเสี่ยงจากภัยคุกคามด้านสารสนเทศและช่องโหว่ของระบบสารสนเทศที่เกี่ยวข้อง ซึ่งอาจถูกใช้เป็นช่องทางในการก่ออาชญากรรมในหลายรูปแบบทั้งที่อยู่ในลักษณะการใช้อินเทอร์เน็ตในการก่อความเสียหายโดยตรงซึ่งอาจเรียกว่า "อาชญากรรมทางไซเบอร์" หรือเป็นความเสี่ยงทางไซเบอร์ในลักษณะที่มีการใช้อินเทอร์เน็ตเป็นสื่อในการก่ออาชญากรรมต่าง ๆ ซึ่งความเสี่ยงทางไซเบอร์อาจหมายถึงโอกาสที่จะเกิดความเสียหายข้อมูลสารสนเทศขององค์กรหรือหน่วยงานที่ทำให้ธุรกิจหยุดชะงักหรือล่วงละเมิด การหลอกลวงทางออนไลน์ การลักขโมยและฉ้อฉลฉ้อโกงเพื่อผลประโยชน์ (Thai Reinsurance, 2015) ซึ่งความเสียหายหรือผลกระทบจากเหตุภัยคุกคามไซเบอร์ สามารถแบ่งได้ 8 ประเภทตามการจัดกลุ่มของ eCSIRT.net คือ Abusive Content, Malicious Code, Information Gathering, Information Security, Intrusion Attempts, Intrusions, Availability, Fraud (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2559)

ความเสียหายขององค์การอันเกิดจากอาชญากรรมด้านไซเบอร์ในประเทศไทยยังคงมีแนวโน้มเพิ่มมากขึ้นทุกปี และผลกระทบที่เกิดขึ้นกับองค์กรขนาดใหญ่ถึงแม้จะมีมูลค่าความเสียหายโดยรวมที่สูง แต่มูลค่าความเสียหายต่อพนักงานจะต่ำกว่าองค์กรที่มีขนาดเล็กหรือมีจำนวนพนักงานที่น้อยกว่า นอกจากนี้แล้ว ไม่ว่าจะเป็นธุรกิจหรืออุตสาหกรรมประเภทใด ก็ไม่สามารถที่จะรอดพ้นจากการคุกคามด้านไซเบอร์ได้ โดยธุรกิจที่เกี่ยวข้องกับพลังงานและสาธารณูปโภค ตลอดจนถึง ธุรกิจที่ให้บริการทางการเงิน เช่น ธนาคาร ก็มักจะเป็นเป้าหมายสำคัญของการโจมตีในแต่ละปี(Ponemon Institute, 2014) โดยผู้วิจัยได้จำแนกสาเหตุของความเสี่ยงทางไซเบอร์ออกเป็น ปัจจัยภายในองค์กร ได้แก่ บุคลากร(Man) เงิน (Money) ทรัพยากร(Material) เครื่องมือ(Machine)รวมถึงการจัดการ(Management) และ ปัจจัยภายนอกองค์กรได้แก่ สังคม(Social) เทคโนโลยี(Technology) เศรษฐกิจ(Economy) การเมืองการปกครอง (Politics) เพื่อให้สามารถนำไปใช้เป็นแนวทางในการวางแผนรักษาความปลอดภัยทางไซเบอร์ขององค์การให้มากขึ้นในอนาคต และส่งผลให้เทคโนโลยีสารสนเทศเกิดประสิทธิผล และมีความยั่งยืนต่อไป(เสกมนต์ สัมมาเพ็ชร์, 2559)

จึงกล่าวได้ว่าความมั่นคงปลอดภัยทางไซเบอร์ ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้นการที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการจัดการความเสี่ยงที่ดี ได้แก่ การระบุความเสี่ยง (Identifying Risk)การประเมินความเสี่ย(Risk Assessment) การวางแผนจัดการความเสี่ยง(Risk Management Planning)การติดตามและควบคุมความเสี่ยง (Monitoring and Controlling Risk) การสรุปและทบทวนความเสี่ยง (Conclusion and Reviewing Risk) เพื่อศึกษาทำความเข้าใจและใช้ประโยชน์จากการจัดการความเสี่ยงสำหรับผู้มีส่วนได้ส่วนเสียในการกำหนดกลยุทธ์ในการจัดการความเสี่ยงในอนาคต (ธนินท์รัฐ รัตนพงศ์ภิญโญ, 2650)

จากสถานการณ์ดังกล่าวจึงนำมาสู่การศึกษาเรื่อง "ปัจจัยกำหนดและการบริหารจัดการความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์"ในมุมมองของผู้ใช้เทคโนโลยีสารสนเทศ ในด้านปัจจัยทางการจัดการและปัจจัยภายนอกเพื่อให้ผู้มีส่วนเกี่ยวข้องกับธุรกิจธนาคารพาณิชย์ทราบถึงปัจจัยสำคัญที่มีผลให้เกิดความเสี่ยงทางไซเบอร์ และเพื่อให้หน่วยงานของรัฐ ภาคเอกชน และประชาชนตระหนักถึงความรุนแรงของผลกระทบ และความเสียหายที่อาจจะเกิดขึ้น และมีการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งจะทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยจากการถูกคุกคาม เพื่อเพิ่มประสิทธิภาพในภาพรวมต่อไป

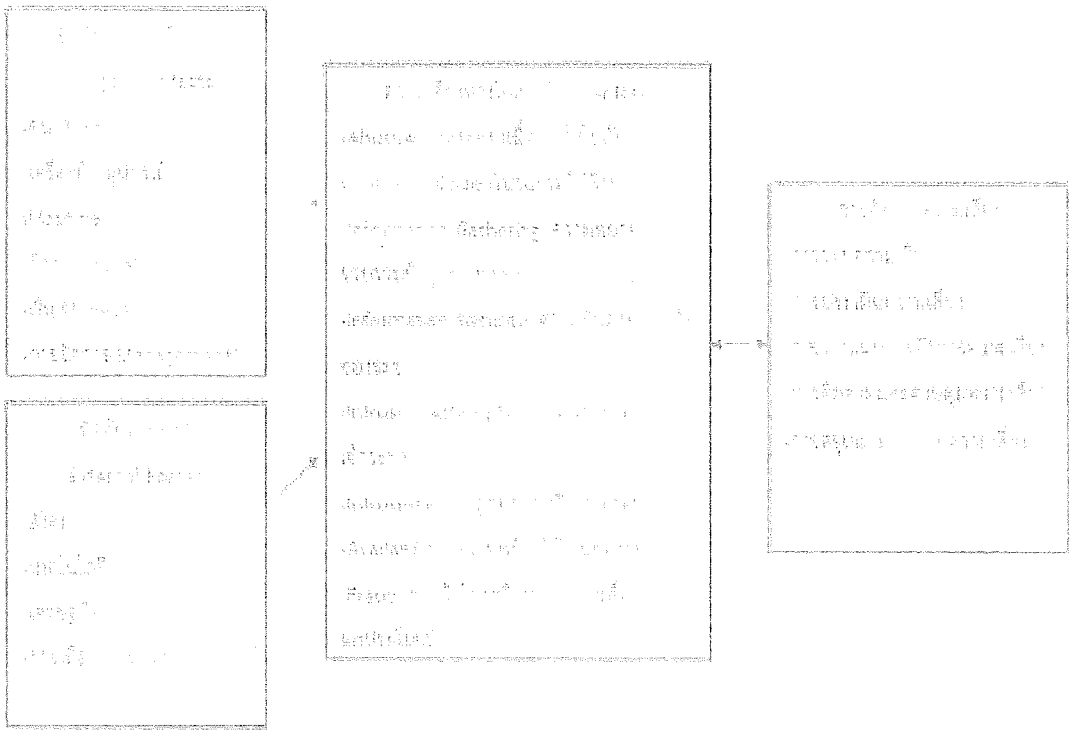
วัตถุประสงค์

1. เพื่อศึกษาปัจจัยกำหนดที่ส่งผลต่อความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์
2. .เพื่อศึกษาความเสี่ยงทางไซเบอร์มีความสัมพันธ์กับการจัดการความเสี่ยงในธุรกิจธนาคารพาณิชย์

ประโยชน์ที่ได้รับจากการวิจัย

1. ได้ทราบถึงปัจจัยกำหนดที่ส่งผลต่อความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์
2. ได้ทราบถึงความสัมพันธ์ของความเสี่ยงทางไซเบอร์ที่มีต่อการจัดการความเสี่ยงของธนาคารพาณิชย์

กรอบแนวคิด



การทบทวนวรรณกรรม

1. แนวคิดและทฤษฎีความเสี่ยง

ความหมายของความเสี่ยง

สำนักงานคณะกรรมการพัฒนาระบบราชการ (2552: 111) ได้ให้ความหมายของความเสี่ยง คือ เหตุการณ์/การกระทำใดๆ ที่อาจเกิดขึ้นในภายใต้สถานการณ์ที่ไม่แน่นอนและส่งผลกระทบ หรือ สร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่ จะบรรลุเป้าหมายของแผนงาน/โครงการที่สำคัญในแต่ละประเด็นยุทธศาสตร์ตามที่ระบุไว้ในแผน ปฏิบัติราชการประจาปีของส่วนราชการ

กิตติพันธ์ คงสวัสดิ์เกียรติ (2554: 63) ได้กล่าวว่า ความเสี่ยง คือ โอกาสที่ไม่แน่นอนของ เหตุการณ์ซึ่งไม่สามารถจะเดาได้ว่าจะเกดขึ้นเมื่อใด แต่ความเสี่ยงนั้นๆ จะมีแนวโน้มที่จะเกิดขึ้น ไม่มากก็น้อยในบริษัท

ปราชญา กล้าผจัญ (2551: 21) ให้ความหมายของความเสี่ยงไว้ดังนี้ หมายถึง โอกาสที่ บางสิ่งบางอย่างอาจจะเกิดขึ้น ซึ่งเป็นผลลัพธ์ของสิ่งที่เป็นอันตราย ความเสี่ยงนี้ เกิดจากความไม่แน่นอน (Uncertainty) ซึ่งสามารถวัดได้ความน่าจะเป็นของสิ่งที่เกิดขึ้น หรือผลลัพธ์ที่เกิดขึ้นแต่ละหน่วยงาน ต่างก็มีมุมมองเรื่องความเสี่ยงแตกต่างกันไป เช่น งานทรัพยากรมนุษย์ มองอย่างหนึ่ง งานผลิต มองอย่างหนึ่ง งานรักษาความปลอดภัย มองอย่างหนึ่งและงานวิศวกรรมความปลอดภัยขององค์กร ก็มองความเสี่ยงไปอีกอย่างหนึ่ง เป็นต้น

เจนเนตร มณีนาค (2548: 5) ได้กล่าวว่า ความเสี่ยง หมายถึง เหตุการณ์หรือ การกระทาใดๆ ที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสี่ยงหรือความ ล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมาย และวัตถุประสงค์ทั้งใน ระดับประเทศ ระดับองค์กร ระดับหน่วยงานและบุคลากรได

จากความหมายของความเสี่ยงที่บรรดานักวิชาการทั้งหลายได้กล่าวไว้ ผู้วิจัยสรุปได้ว่า ความเสี่ยง หมายถึง โอกาสที่บางสิ่งบางอย่าง การกระทำหรือหรือเหตุการณ์ที่อาจจะเกิดขึ้นภายใน สถานการณ์ที่ไม่แน่นอน และส่งผลกระทบ หรือสร้างความเสียหาย ความล้มเหลว หรือลดโอกาส ที่จะบรรลุเป้าหมายและวัตถุประสงค์ที่กำหนดไว้

2. แนวคิดและทฤษฎีการจัดการความเสี่ยง

ความหมายของการจัดการความเสี่ยง

ความสำเร็จหรือความล้มเหลวขององค์กรใดก็ตาม ขึ้นอยู่กับการบริหารงานของผู้บริหาร ได้มีผู้ให้ความหมายของการจัดการความเสี่ยงไว้หลายท่านดังนี้

สำนักงานคณะกรรมการพัฒนาระบบราชการ (2552: 111) ได้ให้ความหมายของการ บริหารความเสี่ยงคือ กระบวนการที่เป็นระบบในการบริหารปัจจัยและควบคุมกิจกรรมรวมทั้ง กระบวนการดาเนินการต่างๆ เพื่อลดมูลเหตุของโอกาสที่จะทาให้เกิดความเสียหายจากการดาเนินการ ที่ไม่เป็นไปตามแผน เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับ ที่สามารถยอมรับได้ ควบคุมได้ และตรวจสอบได้อย่างเป็นระบบ

ดวงใจ ช่วยตระกูล (2551: 25) ได้ให้ความหมายของการบริหารความเสี่ยงหมายถึงการ จัดกระบวนการดำเนินงานขององค์กรให้บรรลุเป้าหมายโดยมีการวางแผนวิเคราะห์ กากับ พัฒนา ทางเลือกในการบริหารความเสี่ยง ตรวจติดตามและควบคุมให้เป็นไปในแนวทางเดียวกันตาม วัตถุประสงค์ขององค์กร

ชัยเสฏฐ์ พรหมศรี (2550: 15) กล่าวว่าการบริหารความเสี่ยงหมายถึง กระบวนการ ในการป้องกันอำนาจและทรัพย์สินที่ได้มาของบริษัท โดยการลดโอกาสของการสูญเสียซึ่งมาจาก เหตุการณ์ที่ไม่สามารถควบคุมได้ นอกจากนี้การบริหารความเสี่ยงยังเป็นกระบวนการ ที่นำไปสู่การ ตัดสินใจ ที่ดี โดยการให้ความเข้าใจอย่างลึกซึ้งต่อความเสี่ยงและผลลัพธ์ที่จะเกิดขึ้น ซึ่งผู้บริหารใน บริษัททุกประเภทจะต้องตื่นตัวต่อความเสี่ยงที่มีต่อบริษัท และผลกระทบที่อาจส่งผลถึงกำไรของ บริษัทด้วย

จากความหมายของการจัดการความเสี่ยงที่มีนักวิชาการหลายท่านได้ให้ความหมายไว้ ผู้วิจัยสรุปได้ดังนี้ การจัดการความเสี่ยง หมายถึง วิธีการบริหารจัดการที่เป็นไปเพื่อการป้องกัน คาดการณ์ ลดโอกาสและลดมูลเหตุที่จะทำให้เกิดความเสียหายจากการดำเนินการขององค์กร ทั้งนี้ เพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์ได้โดยมีประสิทธิภาพและประสิทธิผลมากขึ้น

ประเภทของความเสี่ยงทางไซเบอร์

การแบ่งประเภทของความเสี่ยงจะทำให้เกิดความชัดเจนต่อการวิเคราะห์และประเมิน ความเสี่ยงเพื่อกำหนดแนวทางในการป้องกันและหลีกเลี่ยงความเสี่ยงได้อย่างเหมาะสม ทั้งนี้ขึ้นอยู่ กับบริบทขององค์กรต่างๆ เพื่อความชัดเจนและความเข้าใจประเภทของความเสี่ยง ผู้วิจัยได้ศึกษา การแบ่งประเภทของความเสี่ยงตามรายงานสำรวจสถานภาพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์(2559)ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งแบ่งได้ 8 ประเภท ดังนี้

1. Abusive Content (เนื้อหาที่เป็นภัย) ได้แก่ การถูกเผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือ ก่อให้เกิดความเข้าใจผิด เช่น ข้อความลามกอนาจาร, Harassment Child/Sexual Violence,หมิ่นประมาท, อีเมลสแปม (Spam)

2. Malicious Code (โปรแกรมไม่พึงประสงค์) ได้แก่ การถูกโปรแกรมประสงค์ร้าย เช่น มัลแวร์ (Malware), Virus, Worm, Trojan, Ransomware, APT (Advanced Persistent Threat) และ Spyware ต่าง ๆ เข้าควบคุมการทำงานของระบบ เช่น ขโมยข้อมูล โจมตีระบบอื่น ๆ ทำให้เกิดการความขัดข้องเสียหาย

3. Information Gathering (ความพยายามรวบรวมข้อมูลของระบบ) ได้แก่ การถูกรวบรวมข้อมูลจุดอ่อนของระบบ(Scanning) เช่น ข้อมูลปฏิบัติการ รวมถึงการดักรับข้อมูลเครือข่าย (Sniffing), Social Engineering

4. Information Security (ความมั่นคงปลอดภัยของระบบ) ได้แก่ การถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต(Unauthorized Access) หรือถูกเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized Modification) รวมไปถึงถูกเผยแพร่ข้อมูลที่รั่วไหล (Data Leakage)

5. Intrusion Attempts (ความพยายามบุกรุกเข้าระบบ) เพื่อจะควบคุมหรือทำให้เกิดความขัดข้องกับบริการของระบบเช่น การสุ่ม login เข้าระบบ (Login Attempt), Exploiting Known Vulnerabilities, New Attack Signature, BruteForce Attempts, Firewall Authentication Command & Control, SQL Injection.

6. Intrusions (การถูกบุกรุกหรือเจาะระบบ) ได้แก่ การถูกเข้าควบคุมและสั่งการระบบ จากการถูกเจาะระบบที่สำเร็จแล้ว เช่น การถูกปรับเปลี่ยนหน้าเว็บไซต์ (Web Defacement), Privilege Account Promise, UnprivilegedAccount Promise

7. Availability (ความพร้อมใช้งานของระบบ) ได้แก่ การถูกโจมตีความพร้อมใช้งานของระบบทำให้เกิดความล่าช้าในการบริการ จนถึงทำให้ระบบไม่สามารถทำงานได้ เช่น DDoS (Denial of Service), Open DNS Resolver, Flood, Sabotage

8. Fraud (การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์) ได้แก่ การถูกสร้างหน้าเว็บไซต์ปลอม (Web Phishing)เพื่อขโมยรหัสผ่านจากผู้ใช้, Unauthorized Use of Resources, Copyright, Masquerade

3. กระบวนการบริหารความเสี่ยง

กระบวนการจัดการความเสี่ยงเป็นองค์ประกอบที่สำคัญในการจัดการความเสี่ยงจะต้อง เป็นกระบวนการหรือขั้นตอนที่จะควบคุมกิจกรรมการดำเนินงานต่างๆ เพื่อลดมูลเหตุของโอกาส ที่จะเกิดความเสียหาย หรือการดำเนินการที่ไม่เป็นไปตามแผนงานหรือโครงการ ดังนั้นจึงได้มีการออกแบบกระบวนการจัดการความเสี่ยงไว้ ดังนี้

3.1 การระบุความเสี่ยง(Identifying Risk)เรียกชื่อได้หลายอย่างเช่นการจำหน่ายความเสี่ยง การเมืองที่ความเสี่ยงแต่โดยรวมแล้วหมายถึงขั้นตอนแรกในกระบวนการจัดการความเสี่ยงซึ่งมีวัตถุประสงค์ที่จะประเชิญความเสี่ยงและเรียนรู้ทำความรู้จักกับความเสี่ยงนั้นนั้นที่จะเกิดขึ้นโดยเร็วที่สุด เพื่อให้สามารถวัดระดับหรือขจัดความเสี่ยงดังกล่าวก่อนที่จะส่งผลรุนแรงต่อองค์กรทั้งนี้ด้วยการวิเคราะห์ความเสี่ยงจะทำให้ทราบสาเหตุของปัญหาหรือโอกาสการเกิดความเสี่ยงที่จะมากระทบโครงการและการดำเนินงานขององค์กรได้

3.2 การประเมินความเสี่ยง(Risk Assessment) มีผู้กล่าวไว้ว่า การประเมินความเสี่ยง เป็นการตัดสินใจบนทางเลือก(Trade off rule)ระหว่างการประเชิญหน้าความเสี่ยงความเสี่ยง(ความเสี่ยงประกอบด้วยLikelihood คือโอกาสการเกิดความเสี่ยงและ Consequence/ Impact คือผลกระทบของความเสี่ยงนั้นๆ) กับระดับการควบคุมภายในขององค์การ(Internal Control Level ประกอบด้วย Measures คือมาตรการจัดการความเสี่ยง และ Auditsคือการตรวจสอบการดำเนินงานตามมาตรการนั้นๆ) หากสิ่งหนึ่งสิ่งใดลงไปอีกสิ่งหนึ่งก็จะเกิดขึ้นมามากแทนที่เป็นต้นว่าหากระดับการฟังกุมภาในองค์การให้การดำเนินงานเป็นไปตามขั้นตอนปกติจนบรรลุวัตถุประสงค์ที่ตั้งไว้เกินรถลงไปเลยย่อหย่อนลงความเสี่ยงก็จะเกิดขึ้นมาแทนที่มากขึ้นและส่งผลกระทบต่อการดำเนินงานตามวัตถุประสงค์ขององค์กรอย่างหลีกเลี่ยงไม่ได้

3.3 การวางแผนจัดการความเสี่ยงแนวคิดเรื่องการจัดการความเสี่ยงสามารถแบ่งออกเป็น 2 ลักษณะใหญ่ๆ คือ

3.3.1 (Proactive Management : Protection or Pre-Event Control)แนวคิดนี้เป็นการจัดการความเสี่ยงสำหรับองค์การสมัยใหม่ที่กำหนดกลยุทธ์เชิงรุกสำหรับการป้องกันความเสี่ยงก่อนที่จะความเสี่ยงนั้นนั้นจะเกิดขึ้นโดยมีวัตถุประสงค์เพื่อลดโอกาสการเกิดความเสี่ยงอย่างหนึ่งที่มีความเป็นไปได้ที่จะเกิดขึ้นซึ่งจะก่อให้เกิดการพัฒนาประสิทธิภาพภายใน3ด้านด้วยกันคือการดำเนินงานภายในภาพรวมขั้นตอนของทุกกระบวนการและการกำหนดกลยุทธ์เพื่อการจัดการความเสี่ยง

3.3.2 (Reactive Management : Mitigation or Post-Event Control)แนวคิดนี้เป็นการจัดการความเสี่ยงสำหรับองค์การแบบดั้งเดิมที่กำหนดกลยุทธ์เชิงรับสำหรับการครอบคลุมระดับความรุนแรงจากผลของความเสี่ยงที่เกิดขึ้นแล้ว(After Risk Happening)โดยมีวัตถุประสงค์เพื่อลดผลกระทบอันเกิดจากความสิ่งหนึ่งหนึ่งที่เกิดขึ้น(Decreasing Risk Impacts/Results)ให้ลดลงอยู่ในระดับที่สามารถควบคุมได้แนวคิดนี้มันจะเกิดขึ้นกับการจัดการความเสี่ยงลักษณะที่ไม่มีประสบการณ์หรือในกรณีที่ผู้บริหารไม่ได้ให้ความสำคัญกับการป้องกันความเสี่ยงล่วงหน้าโดยคำนึงถึงเฉพาะภาระต้นทุนในการจัดการความเสี่ยงเป็นหลัก

3.4 การติดตามความเสี่ยง (Risk Monitoring)หมายถึงความพยายามในการรวบรวมข้อมูลสาระสนเทศที่จะกระทำในระหว่างการดำเนินการตามปกติทางธุรกิจโดยวัตถุประสงค์เพื่อทดสอบวิเคราะห์ว่าได้เกิดสถานการณ์ใดที่พึงระวังหรือให้ความสำคัญจึงมีเศษว่าอาจเกิดปัจจัยที่นำไปสู่ความเสี่ยงได้การติดตั้งความเสี่ยงเป็นหน้าที่ของผู้จัดการความเสี่ยงและทีมงานที่จะตรวจสอบสถานการณ์หรือหยุดการนั้นๆโดยในการติดตั้งความเสี่ยงมีแต่กรรมที่จะทำได้ 4 รูปแบบด้วยกันคือ 1.การจัดทำรายงานสถานการณ์เป็นประจำ 2.การระบุรายละเอียดของสิ่งที่เกิดขึ้นทันทีอย่างเป็นระบบ 3.การประเมินจากรายการความเสี่ยงที่อาจเกิดขึ้น 4.การตรวจสอบภายในเฉพาะธุรกิจ

3.5 การสรุปและทบทวนความเสี่ยง (Conclusion and Reviewing Risk) เพื่อศึกษาบทเรียนและใช้ประโยชน์จาการจัดการความเสี่ยงสำหรับผู้มีส่วนได้ส่วนเสีย ในการกำหนดกลยุทธ์เชิงรุกสำหรับการจัดการความเสี่ยงในอนาคต

จากความหมายของกระบวนการจัดการความเสี่ยง ผู้วิจัยสรุปได้ว่า กระบวนการจัดการความเสี่ยงหมายถึง วิธีการบริหารจัดการโดยมีวัตถุประสงค์เพื่อให้สิ่งที่ บุคคล องค์การ สังคมและชุมชน ดำเนินกิจกรรมไปสู่จุดหมายที่กำหนดไว้ โดยปราศจากปัญหา หรืออุปสรรคใดๆโดยมีประโยชน์เพื่อ การบรรลุกลยุทธ์การจัดการความเสี่ยงขององค์การ แผนและโครงการขององค์การประสบความสำเร็จ และ บุคคล สังคม ชุมชนที่เกี่ยวข้องกับองค์การมีคุณภาพชีวิตที่ดีขึ้น

4. การวิเคราะห์สภาพแวดล้อมภายนอก (STEP Analysis)

สภาพแวดล้อมทั่วไปประกอบ ด้วยปัจจัยซึ่งได้แก่ สังคม เทคโนโลยี เศรษฐกิจ และการเมือง

4.1 การเมือง (Political Component = P)

เป็นการวิเคราะห์นโยบายและกฎเกณฑ์ต่างๆ ของภาครัฐ ที่น่าจะมีผลทั้งในเชิงบวกและเชิงลบต่อการดำเนินงานขององค์กร เช่น นโยบายของรัฐบาล แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ กฎหมาย มติคณะรัฐมนตรี และกฎระเบียบต่างๆ ความมั่นคงของรัฐบาล ความขัดแย้งและความรุนแรงทางการเมือง พฤติกรรมทางการเมือง กลุ่มผู้มีอิทธิพล / เครือข่ายพันธมิตร ฯลฯ

4.2 เศรษฐกิจ (Economic Component = E)

เป็นการวิเคราะห์เศรษฐกิจระดับมหภาค / ระดับจุลภาค ซึ่งหมายถึงระบบเศรษฐกิจทั้งในและระหว่างประเทศที่เกี่ยวกับการดำเนินงานขององค์กร อาทิ อัตราการขยายตัวทางเศรษฐกิจ ผลผลิตมวลรวมในประเทศ การค้าระหว่างประเทศและดุลการชำระเงิน อัตราดอกเบี้ยและอัตราแลกเปลี่ยนเงินตราต่างประเทศภาวะการจ้างงานและค่าแรง การลงทุนภาคเอกชน ภาษีอากรและการใช้จ่ายของรัฐบาล การเงินการธนาคาร สภาพปัญหาของสาขาการพัฒนา / บริการ ฯลฯ

4.3 สังคมและวัฒนธรรม (Sociocultural Component = S)

เป็นการวิเคราะห์สภาวะทางสังคมและวัฒนธรรม ซึ่งหมายถึงโครงสร้างทางสังคมที่เกี่ยวข้องกับการดำเนินงานขององค์กร อาทิ ระดับการศึกษาและอัตราการรู้หนังสือของประชากร จำนวนประชากร โครงสร้างของประชากร ขนบธรรมเนียมประเพณี ความเชื่อ ค่านิยมและวัฒนธรรม แบบแผนการดำเนินชีวิตและพฤติกรรม การประกอบอาชีพ คุณภาพชีวิต ลักษณะของชุมชน และการตั้งถิ่นฐาน การกระจายรายได้และความเป็นธรรมในสังคม สภาพของบ้านเมืองและลักษณะทางภูมิศาสตร์ โครงสร้างพื้นฐาน ระบบสาธารณูปโภค สาธารณูปการ การคมนาคมและการติดต่อสื่อสาร ฯลฯ

4.4 เทคโนโลยี (Technological Component = T)

เป็นการวิเคราะห์สภาพการเปลี่ยนแปลงด้านเทคโนโลยีที่จะมีผลต่อการดำเนินงาน เช่น การผลิตคิดค้นเทคโนโลยีต่างๆ ความรู้และวิทยาการแขนงต่างๆ การใช้เทคโนโลยีเพื่อการสื่อสาร การแลกเปลี่ยนความรู้ระหว่างองค์กร ความก้าวหน้าในการวิจัยและพัฒนาในสาขาที่เกี่ยวข้อง รวมถึงการเสริมสร้างประสิทธิภาพการผลิตและการให้บริการโดยใช้อุปกรณ์อัตโนมัติต่าง ๆ

5. การวิเคราะห์สภาพแวดล้อมภายใน

ในการดำเนินธุรกิจใดๆก็ตาม ต้องอาศัยหลายๆปัจจัยประกอบกัน เพื่อก่อให้เกิด กิจกรรมในการประกอบธุรกิจ ซึ่งปัจจัยพื้นฐานในการดำเนินธุรกิจมี 5 ประเภท หรือที่เรียกว่า 5 *M* ได้แก่

1) คน (Man) ซึ่งถือว่าเป็นปัจจัยที่สำคัญที่สุด เพราะธุรกิจจะเกิดขึ้นได้ต้องอาศัยความคิด ของคน มีคนเป็นผู้ดำเนินการหรือจัดการทำให้เกิดกิจกรรมทางธุรกิจหลายรูปแบบ เพื่อให้ประสบ ความสำเร็จในการประกอบธุรกิจนั้น ๆ

2) เงิน (Money) เป็นปัจจัยในการดำเนินธุรกิจอีกชนิดหนึ่งที่ต้องนำมาประกอบ เพื่อให้เกิดธุรกิจ ซึ่งแต่ละธุรกิจจะใช้ปริมาณเงินที่แตกต่างกันไป ขึ้นอยู่ว่าธุรกิจนั้นมีขนาดเล็ก หรือ ใหญ่

3) วัสดุหรือวัตถุดิบ (Material) ซึ่งในการขายสินค้าหรือบริการ ต้องอาศัยวัตถุดิบในการผลิต ดังนั้น ผู้บริหารต้องรู้จักกับการบริหารวัตถุดิบให้มีประสิทธิภาพ เพื่อให้ได้ต้นทุนที่ต่ำ และทำให้ธุรกิจได้ผลกำไรสูงสุด

4) เครื่องจักรกล (Machine) เป็นอีกปัจจัยที่ใช้ในการดำเนินงานเพื่อให้ได้ผลผลิตและการบริการอย่างรวดเร็วและมีประสิทธิภาพ

5) วิธีการ/จัดการ (Method / Management) การปฏิบัติงานในแต่ละขั้นตอน ของการดำเนินธุรกิจควรมีการวางแผน และควบคุมให้การปฏิบัติงานนั้น มีประสิทธิภาพ ถูกนำเข้าในระบบเพื่อการประมวลผลหรือการบริการที่เติบโตและพัฒนาก้าวหน้าไปพร้อมกับ อุตสาหกรรมการผลิตและการบริการที่เติบโตและพัฒนาขึ้นไปอย่างรวดเร็ว

งานวิจัยที่เกี่ยวข้อง

S. Cheang ได้วิจัยเรื่อง กรอบแนวคิดสำหรับการประเมิน ความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับ สถาบันอุดมศึกษาในการพัฒนาประเทศ: กรณีศึกษาประเทศ กัมพูชาผลการวิจัยได้ค้นพบดัชนีความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานภาครัฐในประเทศกัมพูชาไว้ ประกอบด้วย 1) ด้านทรัพยากรมนุษย์ 2) ด้านโครงสร้างพื้นฐาน และ 3) ด้านสิ่งแวดล้อม

มหาวิทยาลัยวาซาดะ (Waseda University) ประเทศญี่ปุ่นซึ่งเป็นองค์กรทางการศึกษาที่มีชื่อเสียงในการจัดอันดับรัฐบาล อิเล็กทรอนิกส์และในปี 2556 ซึ่งได้กำหนดดัชนีความพร้อม ด้านความมั่นคงปลอดภัยไซเบอร์ไว้ประกอบด้วย 1) ด้านกฎหมายไซเบอร์ 2) ด้านองค์กรการการรักษาความมั่นคงปลอดภัยทางอินเทอร์เน็ต และ 3) ด้านอาชญากรรมไซเบอร์

อย่างไรก็ดีทาง ITU ยังได้ร่วมมือกับบริษัท ABI Research จัดทำดัชนีความมั่นคงปลอดภัยไซเบอร์ระดับโลก (Global Cybersecurity Index : GCI) ซึ่งได้กำหนดดัชนีความมั่นคงปลอดภัยไว้ดังต่อไปนี้ 1) มาตรการทางกฎหมาย 2) มาตรการทางด้านเทคนิค 3) มาตรการทางองค์กร 4) มาตรการพัฒนา บุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ และ 5) มาตรการความร่วมมือกับหน่วยงานอื่น ๆ

วิธีดำเนินการวิจัย

1. ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการศึกษาครั้งนี้ คือ พนักงานหรือผู้มีประสบการณ์ในการทำงานที่เกี่ยวกับธนาคารพาณิชย์

กลุ่มตัวอย่าง คือ พนักงานหรือผู้มีประสบการณ์ในการทำงานที่เกี่ยวกับธนาคารพาณิชย์ในเขตกรุงเทพมหานคร เนื่องจากเป็นพื้นที่ที่มีธนาคารจำนวนมาก ทำให้การวิจัยเป็นเรื่องที่น่าสนใจที่จะศึกษาความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์

เนื่องจากไม่ทราบจำนวนประชากรที่แน่นอนจึงได้ใช้สูตรการคำนวณกลุ่มตัวอย่างตามวิธี ของ Cochran (Cochran, 1977 อ้างในธีรวุฒิ เอกะกุล, 2543) ได้ขนาดกลุ่มตัวอย่างจำนวน 400 คน ผู้วิจัยเก็บข้อมูลโดยใช้วิธีสุ่มตัวอย่างแบบเจาะจง (Purposive sampling) ตามจำนวนดังกล่าว โดยการคำนวณจากในเขตพื้นที่กรุงเทพมหานคร

2. เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัยครั้งนี้เป็นแบบสอบถามปัจจัยกำหนดและการบริหารจัดการความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์

ส่วนที่ 1 แบบสอบถามข้อมูลที่เกี่ยวกับปัจจัยส่วนบุคคลของผู้ตอบแบบสอบถาม ได้แก่ เพศ อายุ ระดับการศึกษา รายได้ จำนวนทั้งหมด 4 ข้อ

ส่วนที่ 2 แบบสอบถามเกี่ยวกับปัจจัยทางการจัดการ ประกอบด้วย 5 ปัจจัยคือ บุคลากร(Man) เครื่องมือ อุปกรณ์ (Machine) วัสดุ(Material) เงิน(Money) การจัดการ(Management) จำนวนทั้งหมด 16 ข้อ

ส่วนที่ 3 แบบสอบถามเกี่ยวกับปัจจัยภายนอก ประกอบด้วย 4 ปัจจัย คือ สังคม เทคโนโลยี เศรษฐกิจ การเมืองการปกครอง จำนวนทั้งหมด 11 ข้อ

ส่วนที่ 4 แบบสอบถามเกี่ยวกับความเสี่ยงทางไซเบอร์ ประกอบด้วย 8 ปัจจัย คือ Abusive Content (เนื้อหาที่เป็นภัย) Malicious Code (โปรแกรมไม่พึงประสงค์) Information Gathering (ความพยายามรวบรวมข้อมูลของระบบ) Information Security (ความมั่นคงปลอดภัยของระบบ) Intrusion Attempts (ความพยายามบุกรุกเข้าระบบ) Intrusions (การถูกบุกรุกหรือเจาะระบบ) Availability (ความพร้อมใช้งานของระบบ) Fraud (การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์) จำนวนทั้งหมด 16 ข้อ

ส่วนที่ 5 แบบสอบถามเกี่ยวกับการจัดการความเสี่ยง ประกอบด้วย 5 ปัจจัย คือ การระบุความเสี่ยงการประเมินความเสี่ยง การวางแผนการจัดการความเสี่ยง การติดตามและควบคุมความเสี่ยง การสรุปและทบทวนความเสี่ยง จำนวนทั้งหมด 10 ข้อ

ในส่วนที่ 2-5 ลักษณะแบบสอบถามเป็นแบบมาตราส่วนประมาณค่า (Rating scale) โดยให้ เลือกตามลำดับความสำคัญ 5 ระดับได้แก่ 1 หมายถึง ไม่เห็นด้วยอย่างยิ่ง, 2 หมายถึง ไม่เห็นด้วย, 3 หมายถึง เฉยๆ, 4 หมายถึง เห็นด้วย และ 5 หมายถึง เห็นด้วยอย่างยิ่ง

นำแบบสอบถามไปทดสอบค่าความเชื่อมั่นในจังหวัดราชบุรี จำนวน 30 ชุดได้ค่าสัมประสิทธิ์ Cronbach's Alpha .965 แสดงว่าถือความเชื่อมั่นอยู่ในลำดับสูง

3. การเก็บรวบรวมข้อมูล

3.1 แหล่งข้อมูลปฐมภูมิ (Primary Data) คือ เป็นแหล่งข้อมูลจากการแจกแบบสอบถามให้แก่พนักงานหรือผู้มีประสบการณ์ในการทำงานที่เกี่ยวกับธนาคารพาณิชย์ในเขตกรุงเทพมหานครจำนวน 400 ชุด ผู้วิจัยได้ทำการเก็บรวบรวมแบบสอบถามในวันที่ 1 – 31 กันยายน 2561 เพื่อทำการวิเคราะห์ต่อไป

3.2 แหล่งข้อมูลทุติยภูมิ (Secondary Data) คือ เป็นแหล่งข้อมูลที่ผู้วิจัยได้จากการศึกษาหนังสือ ตำราเรียน ข้อมูลทางอินเตอร์เน็ต ผลงานวิจัยที่เกี่ยวข้องเพื่อเป็นข้อมูลพื้นฐานในการศึกษา

4. การวิเคราะห์ข้อมูล

ข้อมูลทั่วไปของแต่ละปัจจัย ใช้การวิเคราะห์ด้วยค่าสถิติเชิงพรรณนา (Descriptive Statistics) ได้แก่ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานและ ความเสี่ยงทางไซเบอร์ ใช้วิธีการวิเคราะห์ค่าด้วยค่าสถิติเชิงพรรณนา (Descriptive Statistics) ได้แก่ ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน

การวิเคราะห์ความสัมพันธ์ของปัจจัยทางการจัดการและปัจจัยภายนอก ส่งผลต่อความเสี่ยงทางไซเบอร์ ใช้วิธีการการวิเคราะห์ถดถอยตัวแปร(Multiple Regression)

สรุปผลการวิจัย

พบว่าปัจจัยภายนอกส่งผลต่อความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์ มากที่สุด โดยมีค่า Adjusted R Square อยู่ที่ 0.757 โดยมีด้านเทคโนโลยีส่งผลมากที่สุด ปัจจัยรองลงมาคือปัจจัยทางการจัดการโดยมีค่า Adjusted R Square อยู่ที่ 0.665 โดยมีด้านบุคลากร(Man)ส่งผลมากที่สุด โดยมี $\bar{X}$ เป็นระดับความคิดเห็นต่อปัจจัย และ S.D. เป็นค่าส่วนเบี่ยงเบนมาตรฐาน ดังแสดงโดยตาราง

ตารางที่ 1 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของปัจจัยทางการจัดการ

ปัจจัยทางการจัดการ (Management factors)	$\bar{X}$	S.D.
บุคลากร (Man)	3.6533	.46401
เงิน (Money)	3.3200	.42947
เครื่องมือ อุปกรณ์ (Machine)	3.4350	.36345
ทรัพยากร (Material)	3.4233	.35724
การจัดการ (Management)	3.4925	.46392

ตารางที่ 2 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของปัจจัยภายนอก

ปัจจัยภายนอก(External factors)	$\bar{X}$	S.D.
ปัจจัยด้านสังคม (Social)	3.3667	.34976
ปัจจัยด้านเทคโนโลยี (Technology)	3.8267	.47962
ปัจจัยด้านเศรษฐกิจ(Economy)	3.4500	.61340
ปัจจัยด้านการเมืองการปกครอง(Politics)	3.4167	.47467

จากด้านความเสี่ยงทางไซเบอร์และการจัดการความเสี่ยง พบว่า มีความสัมพันธ์กันโดยมีค่าสัมประสิทธ์สหสัมพันธ์ มีค่าเท่ากับ 0.862 ณ ระดับนัยสำคัญ 0.05

ตารางที่ 3 การวิเคราะห์การถดถอยเชิงพหุคูณ (Multiple Regression Analysis) ปัจจัยกำหนดและการบริหารจัดการความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	-1.068	.281		-3.798	.000
	ปัจจัยทางการจัดการ	.726	.103	.527	7.034	.000
	ปัจจัยภายนอก	.582	.109	.399	5.328	.000
Dependent Variable: ความเสี่ยงทางไซเบอร์ F = 140.676 , Adjusted R Square = 0.738 , P < 0.05 , Sig. = 0.10 *, 0.05 **, 0.01 ***						

จากตารางที่ 3 สามารถเขียนสมการพยากรณ์ได้ดังนี้ $\hat{Y}$= -1.068+ 0.726$\hat{X}_1$ + 0.582$\hat{X}_2$

จากตารางที่ 3 การวิเคราะห์การถดถอยเชิงพหุคูณ (Multiple Regression Analysis) เพื่อศึกษาความสัมพันธ์ระหว่างระดับปัจจัยทางการจัดการกับความเสี่ยงทางไซเบอร์ ผลการทดสอบสมมุติฐานการวิจัย พบว่า ปัจจัยทางการจัดการมีความสัมพันธ์ทางบวกกับความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์ มีค่าสัมประสิทธิ์ (B) = 0.726 หมายความว่าระดับปัจจัยทางการจัดการเพิ่มขึ้น 1 หน่วย ส่งผลให้ความเสี่ยงทางไซเบอร์ จะเพิ่มขึ้น 0.726 เมื่อทดสอบความมีนัยสำคัญ พบว่า (P < 0.05) ดังนั้น ปัจจัยทางการจัดการมีความสัมพันธ์ในทิศทางเดียวกันกับความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์ อย่างมีนัยสำคัญทางสถิติ 0.05

ปัจจัยภายนอกมีความสัมพันธ์ทางบวกกับความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์ มีค่าสัมประสิทธิ์ (B) = 0.582 หมายความว่าระดับปัจจัยภายนอกเพิ่มขึ้น 1 หน่วย ส่งผลให้ความเสี่ยงทางไซเบอร์ จะเพิ่มขึ้น 0.582 เมื่อทดสอบความมีนัยสำคัญ พบว่า (P < 0.05) ดังนั้น ปัจจัยภายนอกมีความสัมพันธ์ในทิศทางเดียวกันกับความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์ อย่างมีนัยสำคัญทางสถิติ 0.05 ทั้งนี้ สมการถดถอยดังกล่าว มีค่า Adjusted R Square = 0.738 หรือ 73.8%

อภิปรายผล

ปัจจัยภายนอกโดยมีด้านเทคโนโลยีส่งผลต่อความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์มากที่สุด โดยมีค่า Adjusted R Square อยู่ที่ 0.757 แสดงว่ามีความสัมพันธ์กันในเชิงบวก กล่าวคือ ความปลอดภัยในเทคโนโลยีในการใช้งานระบบสารสนเทศเป็นประจำอย่างไม่ระมัดระวังอาจก่อให้เกิดความเสี่ยงทางไซเบอร์จากการถูกฉ้อฉลหรือการขโมยข้อมูลหรือหลอกลวงเพื่อผลประโยชน์ได้ ซึ่งสอดคล้องกับงานวิจัยของ พงษ์ศักดิ์ ผกามาศ (2550) ได้ศึกษาเรื่องการพัฒนาระบบ เทคโนโลยีสารสนเทศและการสื่อสารสำหรับการบริหารจัดการมหาวิทยาลัยภาคตะวันออกเฉียงเหนือ : กรณีศึกษาคณะวิศวกรรมศาสตร์ พบว่า ในภาพรวมของการทดสอบ ประสิทธิภาพและความพึงพอใจในฐานะผู้ใช้งานระบบมีความคิดเห็นต่อระบบว่ามีความเหมาะสม อยู่ในระดับมากถึงระดับมากที่สุดและมีความสอดคล้องกับการบริหารจัดการภายในและใช้เป็นทรัพยากรด้านการจัดกิจกรรมการเรียน

ปัจจัยทางการจัดการด้านบุคลากร(Man) ส่งผลต่อความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์มากที่สุด โดยมีค่า Adjusted R Square อยู่ที่ 0.665 แสดงว่ามีความสัมพันธ์กันในเชิงบวก กล่าวคือ บุคลากรเป็นปัจจัยที่สำคัญที่ส่งผลต่อความเสี่ยงทางไซเบอร์และมีส่วนสำคัญในการกำหนดปัญหาและติดตามแก้ไขเพื่อการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัยเพื่อป้องกันความเสี่ยงทางไซเบอร์ที่อาจส่งผลกระทบต่อธุรกิจธนาคารพาณิชย์ได้ ซึ่งสอดคล้องกับงานวิจัยของ วิภารัตน์ ปหักขินัง(2557) ที่ศึกษางานวิจัยเรื่อง "การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อม ด้านความมั่นคงปลอดภัยทางไซเบอร์ ขององค์กร" พบว่า บุคลากรของสถาบัน การพลศึกษา เห็นว่าหน่วยงานควรมีการ คัดเลือกบุคลากร กำหนดเงื่อนไขการจ้างงาน การส่งมอบงานและตรวจสอบ ทรัพย์สิน ยกเลิกสิทธิ การจัดอบรมและสร้างความตระหนัก ให้กับบุคลากรเกี่ยวกับความมั่น คงปลอดภัยทางไซเบอร์

ด้านความเสี่ยงทางไซเบอร์มีความสัมพันธ์กับการจัดการความเสี่ยง โดยมีค่าสัมประสิทธิ์สหสัมพันธ์ เท่ากับ 0.862 ณ ระดับนัยสำคัญ 0.05 ซึ่งสอดคล้องกับงานวิจัยของ ณัชธิญา ปัทมทัตตานนท์ (2553)ที่ศึกษางานวิจัยเรื่อง การจัดการความเสี่ยงที่ส่งผลต่อประสิทธิผลของสถานศึกษา สังกัด สานักงานเขตพื้นที่การศึกษาในจังหวัดปทุมธานี พบว่า ความสัมพันธ์ระหว่างการจัดการความเสี่ยงกับประสิทธิผลของสถานศึกษา สังกัด สำนักงานเขตพื้นที่การศึกษาในจังหวัดปทุมธานี มีความสัมพันธ์กันเป็นเพราะ ในปัจจุบันสถานศึกษาได้นำแนวคิดและ หลักการจัดการความเสี่ยงมาใช้ในการบริหารสถานศึกษา ไม่ค่อยเด่นชัดนัก อาจเนื่องมาจากหลายสาเหตุดังนี้ คือ 1) ผู้บริหารไม่ให้การสนับสนุน 2) ขาดการสื่อสารที่ดีบุคลากรในองค์กร 3) ผู้มีหน้าที่ประเมินความเสี่ยง ไม่ได้วิเคราะห์ความเสี่ยงของหน่วยงานตามความเป็นจริง 4) การบริหารความเสี่ยงไม่สามารถดำเนินการได้ทั่วทั้งองค์กร ทำให้บุคลากรในองค์กรไม่เห็นถึงประสิทธิผลของการบริหารความเสี่ยงว่ามีส่วนให้องค์กรบรรลุผลสำเร็จได้

ข้อเสนอแนะจากผลการวิจัย

1. จากผลการวิจัยพบว่าปัจจัยด้านการจัดการในด้านบุคลากรมีผลกะทบต่อความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์มากที่สุด ดังนั้นองค์กรหรือธุรกิจธนาคารควรให้ความสำคัญกับโครงการฝึกอบรมบุคลากร โดยการจัดทำหลักสูตร Cyber Training การอบรมความรู้เกี่ยวกับการใช้ซอฟท์แวร์ (Software) และ ฮาร์ดแวร์ (Hardware) รวมทั้งการให้ทุนการศึกษาต่อใน ด้านการรักษาปลอดภัยไซเบอร์ที่ครอบคลุมถึงบุคลากรทุกระดับ

2. จากผลการวิจัยพบว่าปัจจัยภายนอกในด้านเทคโนโลยีมีผลต่อความเสี่ยงทางไซเบอร์มากที่สุด ดังนั้นองค์กรควรมีการจัดการองค์ความรู้ด้านไซเบอร์ (Cyber Knowledge Management: KM) ในหน่วยงาน เช่น สถานการณ์ด้านไซเบอร์ในปัจจุบัน วิธีการในการกำจัดไวรัสในตัวเครื่อง เป็นต้น เพื่อเป็นฐานข้อมูลให้ หน่วยชั้นตรงต่าง ๆ ได้ นำข้อมูลไปใช้ และควรพัฒนาระบบขององค์กรตลอดเวลาให้มีความปลอดภัย เหมาะสมและรวดเร็ว เพื่อพร้อมรับความเสี่ยงที่อาจเกิดขึ้นได้ทันท่วงที

ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

1. ควรมีการศึกษาความเสี่ยงทางไซเบอร์ในธุรกิจธนาคารพาณิชย์ในเชิงคุณภาพ โดยศึกษาจากพนักงานที่ทำงานเกี่ยวกับเทคโนโลยีสารสนเทศของธนาคารโดยตรง เพื่อให้ผู้ให้บริการเทคโนโลยีทางการเงินหรือผู้พัฒนาเทคโนโลยีสารสนเทศสามารถนำข้อมูลที่อธิบายเหตุและผลได้มากกว่าไปพัฒนาการบริการหรืองานระบบสารสนเทศที่มีความซับซ้อนให้มีความปลอดภัยและดียิ่งกว่าเดิม

2. ควรศึกษาความเสี่ยงของการใช้เทคโนโลยีสารสนเทศสำหรับการจัดการความเสี่ยงในองค์กรธุรกิจที่ตั้งอยู่ในภูมิภาคอื่นๆ หรือองค์กรธุรกิจในต่างประเทศ ทั้งในกลุ่มประเทศที่กำลังพัฒนา และกลุ่มประเทศที่พัฒนาแล้วเพื่อนำข้อมูลมาเปรียบเทียบกัน รวมทั้งอาจเพิ่มตัวแปรอิสระ เช่น การตระหนักรู้ การเตรียมพร้อม ความรู้ความเข้าใจของบุคลากรในพื้นที่นั้นๆ ในการศึกษาประเด็นนี้

เอกสารอ้างอิง

กัลยา วานิชย์บัญชา. (2545,2549,2550). การวิเคราะห์สถิติ.*สถิติสำหรับการบริหารและวิจัย.* (พิมพ์ ครั้งที่6) กรุงเทพมหานคร.โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2554). *กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสารระยะ พ.ศ. 2554- 2563 ของประเทศไทย.* (พิมพ์ครั้งที่1). กรุงเทพมหานคร : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ณัชธิญา ปัทมทัตตานนท์. (2553). *การจัดการความเสี่ยงที่ส่งผลต่อประสิทธิผลของสถานศึกษา สังกัดสำนักงานเขตพื้นที่การศึกษาในจังหวัดปทุมธานี.* สาขาวิชาเทคโนโลยีการบริหารการศึกษา คณะครุศาสตร์อุตสาหกรรม, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ธนาภา หิมารัตน์. (2559). *ปัจจัยที่ส่งผลต่อการยอมรับเทคโนโลยีทางการเงิน บริบท ธนาคารพาณิชย์* วิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเทคโนโลยี วิทยาลัยนวัตกรรม, มหาวิทยาลัยธรรมศาสตร์

ธนินท์รัฐ รัตพงศ์พิญโญ. (2560). *หลักพื้นฐานการจัดการความเสี่ยง (Fundamental of Risk Management).* (พิมพ์ครั้งที่2).กรุงเทพฯ : บริษัท พี.เอ.ลีฟวิ่ง จำกัด.

ธีระวัฒน์ จันทึก. (2561). *การวิจัยเชิงปริมาณ.* (พิมพ์ครั้งที่1). กรุงเทพฯ : โรงพิมพ์พิกกี้ มีเดีย.

ประวิทย์ ลี่สถาพรวงศา.(2560). Cybersecurity *ปัญหาความปลอดภัยบนโลกอินเทอร์เน็ต สังคมต้องช่วยกัน.* เข้าถึงเมื่อ (25 ตุลาคม พ.ศ.2561), สืบค้นจาก https://brandinside.asia/nbtc-cybersecurity//

ประชาภรณ์ ทัพโพธิ์. (2557). *ปัจจัยที่มีผลต่อการมีส่วนร่วมของบุคลากรในการพัฒนาคุณภาพโรงพยาบาลส่งเสริมสุขภาพตำบล จังหวัดนครปฐม.* สาขาการพัฒนาทรัพยากรมนุษย์และชุมชน คณะศึกษาศาสตร์และพัฒนศาสตร์, มหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตกำแพงแสน

วิภารัตน์ ปทักขินัง.(2557).*การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร.* บริหารธุรกิจบัณฑิต สาขาคอมพิวเตอร์ธุรกิจ วิทยาลัยเทคโนโลยีสยาม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์(องค์การมหาชน). (2559). *Cybersecurity Survey2016.* เข้าถึงเมื่อ (25 ตุลาคม 2561), สืบค้นจาก https://www.etda.or.th/publishingdetail/cybersecurity-survey-2016.html

เสกมนต์ ลัมมาเพ็ชร์.(2559).*ทรัพยากรการบริหารกับประสิทธิผลการปฏิบัติงาน ของเจ้าหน้าที่ทัณฑสถานบำบัดพิเศษกลาง กรุงเทพมหานคร.*รัฐประศาสนศาสตรมหาบัณฑิต คณะศิลปศาสตร์, มหาวิทยาลัยเกริก

Business Contituity Institute. (2557). *แนวโน้มภัยคุกคามด้านความมั่นคงปลอดภัยที่องค์กรทั่วโลกตระหนักปี ๒๐๑๔ (Threats and horizon scanning 2014).* เข้าถึงเมื่อ (25 ตุลาคม พ.ศ. 2561), สืบค้น จาก http://www.thebci.org.

CHEANG, S. (2009). *"Conceptual Model for Cybersecurity Readiness Assessement for Public Institutions In Developing Country: Cambodia"* IEEE Xplore Digital Library.

Dorfman, Mark S. (1997). *Introduction to Risk Management and Insurance.* (6 th ed), Prentice Hall.

ITU-T X.1200-X.1299,Series X (2014).*"Open System Communicotions and Security,"* Reach on 25 October 2018, Retrieved from:http://www.itu.int/ITU-D/cyb/cyber-security/docs/ITUNationalCybersecurityStrategyGuide.pdf.

Ponemon Institute. (2014). *Global Report on the Cost of Cyber Crime 2014*, Reach on 25 October 2018,Retrieved from https://www.octree.co.uk/Documents/2014-Global-Report-on-the-Costof-

Thai Reinsurance Public Co., Ltd. (2558).*Cyber Insurance Potential In Thailand.* เข้าถึงเมื่อ (25 ตุลาคม2561), สืบค้นจาก https://www.thaire.co.th/thaire_backend/upload/ourservices/publict_20151216111050.pdf