Cyber insurance potential in Thailand

พัฒนาการที่ก้าวหน้าเป็นอย่างมากของเทคโนโลยีด้านคอมพิวเตอร์และระบบเครือข่ายได้ก่อให้เกิดนวัตกรรมต่างๆ ขึ้นมากมาย แต่ในขณะเดียวกัน ก็ได้นำความเสี่ยงมาสู่ผู้ใช้อย่างไม่ทันรู้เนื้อรู้ตัว รายงานนี้จึงได้พยายามประเมินสถานการณ์และผลกระทบจากความเสี่ยงด้านไซเบอร์ (Cyber risks) ตลอดจนถึง รูปแบบวิธีการบริหารความเสี่ยงที่มีอยู่ในปัจจุบัน เพื่อเป็นข้อมูลสำหรับการพัฒนาแผนธุรกิจที่นับวันจะทวีความสำคัญมากยิ่งขึ้น

ความหมายของอาชญากรรมด้านไซเบอร์

Cyber crime หรือ อาชญากรรมด้านไซเบอร์มีความหมายที่หลากหลาย ขึ้นกับจุดมุ่งหมายและสถานการณ์ที่ใช้ แต่โดยทั่วไปแล้ว จะหมายถึง กิจกรรมที่ผิดกฎหมายใดๆ ที่ใช้หรือรุกรานระบบและเครือข่ายคอมพิวเตอร์ รวมไปถึงอินเตอร์เน็ต Capgemini [1] ได้จัดอาชญากรรมด้านไซเบอร์เป็น 3 รูปแบบด้วยกัน คือ 1. การทำให้ธุรกิจหยุดชะงักหรือล่วงละเมิด (Business disruption and misuse) เช่น การทำให้ระบบคอมพิวเตอร์หยุดการทำงานหรือทำงานได้ไม่เต็มประสิทธิภาพ เป็นต้น 2. การหลอกลวงทางออนไลน์ (Online scam) เช่น การทำให้ผู้ใช้หลงเชื่อเพื่อที่จะเข้าถึงข้อมูลส่วนตัวและข้อมูลสำคัญทางการเงิน และการหลอกขายสินค้าออนไลน์ เป็นต้น และ 3. การลักขโมยและฉ้อฉลฉ้อโกงเพื่อผลประโยชน์ (Theft and fraud) เช่น การขโมยอัตลักษณ์ของผู้ใช้เพื่อใช้ในการเปิดบัญชีกับธนาคาร การขโมยทรัพย์สินทางปัญญาหรือความลับทางธุรกิจ หรือ การทำให้เกิดความเสียหายกับหน่วยงานภาครัฐ เป็นต้น

ความเสียหายจากอาชญากรรมด้านไซเบอร์ในโลก

ความเสียหายเฉลี่ยทั่วโลกต่อปี

US$ 4 แสนล้าน

จากการประเมินของ MCAfee[2] ที่เผยแพร่ในปี 2557 พบว่า อาชญากรรมด้านไซเบอร์ก่อให้เกิดความเสียหายทั่วโลกคิดเป็นมูลค่าระหว่าง US$ 3.75 แสนล้าน จนถึง US$ 5.75 แสนล้านต่อปี โดยในปี 2557 คนอเมริกันราว 40 ล้านคนรายงานว่าข้อมูลสำคัญของตนได้ถูกขโมย และเกือบ 54 ล้านคนในประเทศตุรกีก็ต้องเผชิญกับชะตากรรมในลักษณะเดียวกัน ไม่เพียงเท่านั้น หลายประเทศในเอเชีย อย่างเช่น เกาหลีและจีน ที่พลเมืองของตนรวมกันราว 40 ล้านคนได้ประสบกับเหตุการณ์ข้อมูลส่วนบุคคลถูกขโมยจากช่องทางไซเบอร์ โดยในปีที่แล้วคาดว่าเหยื่อจากการโจรกรรมด้านไซเบอร์มีจำนวนสูงถึง 800 ล้านคน และมีมูลค่าความเสียหายสูงถึง US$ 1.6 แสนล้าน เพิ่มขึ้นจาก US$1.1 แสนล้านในปี 2556[3]

จำนวนผู้ที่ได้รับความเสียหายทั่วโลกต่อปี

800 ล้านคน

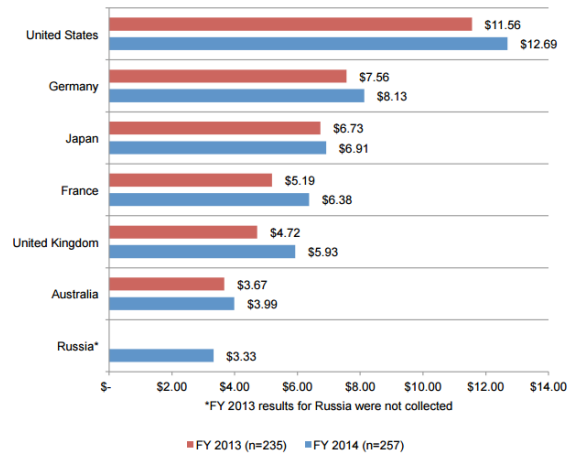
ผลกระทบที่เกิดขึ้นกับองค์กรมีความรุนแรงที่น่าเป็นห่วงเช่นกัน ผลจากการสัมภาษณ์ 257 บริษัทใน 7 ประเทศของ Ponemon Institute[4] ชี้ว่า ความเสียหายที่เกิดขึ้นใน ปี 2557 ของบริษัทที่ทำการสำรวจในประเทศสหรัฐอเมริกามีค่ารวมกันสูงถึง US$ 12.7 ล้าน อันดับที่สองคือบริษัทในประเทศเยอรมันนีที่ได้รับ

---

[1] Using Insurance to Mitigate Cybercrime Risk: Challenges and recommendations for insurers, 2012, Capgemini
[2] Net Losses: Estimating the Global Cost of Cybercrime, June 2014, McAfee
[3] 2013 Norton Report, Norton
[4] 2014 Global Report on the Cost of Cyber Crime, October 2014, Ponemon Institute

ความเสียหาย US$ 8.1 ล้าน สถาบันที่มีความเชี่ยวชาญด้านความปลอดภัยของข้อมูลแห่งนี้ ได้กล่าวสรุปไว้อย่างน่าสนใจว่า ความเสียหายขององค์กรอันเกิดจากอาชญากรรมด้านไซเบอร์ยังคงมีแนวโน้มเพิ่มมากขึ้นทุกปี และผลกระทบที่เกิดขึ้นกับ

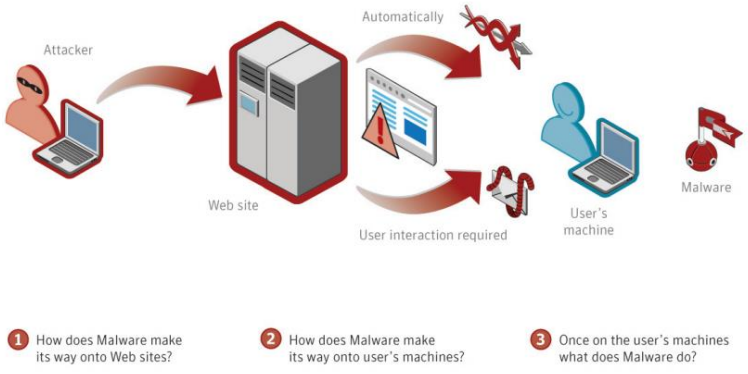
Figure 1. Total cost of cyber crime in seven countries
Cost expressed in US dollars (000,000), n = 257 separate companies



องค์กรขนาดใหญ่ถึงแม้จะมีมูลค่าความเสียหายโดยรวมที่สูง แต่มูลค่าความเสียหายต่อพนักงานจะต่ำกว่าองค์กรที่มีขนาดเล็กหรือมีจำนวนพนักงานที่น้อยกว่า นอกจากนี้แล้ว ไม่ว่าจะเป็นธุรกิจหรืออุตสาหกรรมประเภทใด ก็ไม่สามารถที่จะรอดพ้นจากการคุกคามด้านไซเบอร์ได้ โดยธุรกิจที่เกี่ยวข้องกับพลังงานและสาธารณูปโภค ตลอดจนถึง ธุรกิจที่ให้บริการทางการเงินมักจะเป็นเป้าหมายสำคัญของการโจมตีในแต่ละปี เป็นที่เชื่อว่าความที่เสียหายที่ประเมินเป็นตัวเลขได้นั้นน่าจะเป็นเพียงส่วนหนึ่งของความเสียหายทั้งหมดเท่านั้น เนื่องจากหลายองค์กรที่ประสบกับเหตุการณ์ไม่ต้องการที่จะเปิดเผยข้อมูล และอีกหลายกรณีที่องค์กรไม่รู้ตัวด้วยซ้ำไปว่าได้ถูกโจมตีแล้ว MCAfee ได้หยิบยกตัวอย่างของประเทศออสเตรเลียที่ว่า มีเพียง 4 จาก 10 บริษัทเท่านั้น ที่ยอมรับว่าระบบขององค์กรของตนได้รับการแทรกแซงจากผู้ไม่ประสงค์ดี เช่นเดียวกับ ประสบการณ์ของประเทศเนเธอร์แลนด์

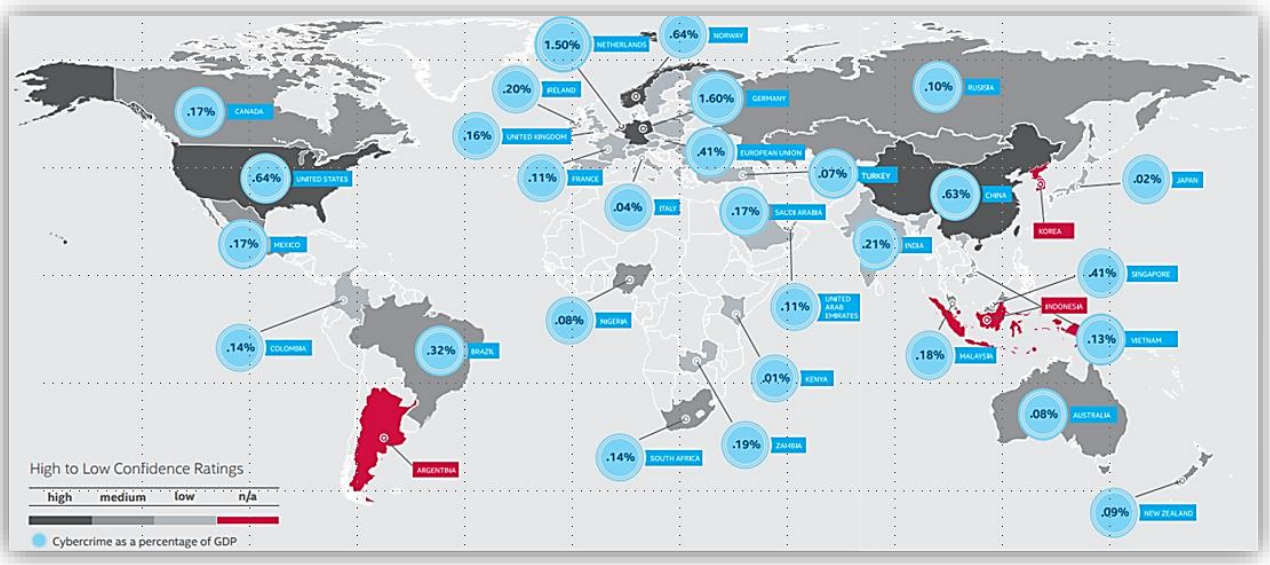
Ponemon Institute ได้ระบุเพิ่มเติมอีกด้วยว่า การโจมตีทางไซเบอร์มากกว่า 55% มีที่มาจาก 3 สาเหตุสำคัญคือ I. ภัยคุกคามที่เกิดขึ้นจากคนในหรือจากฝั่งผู้ให้บริการเอง (Malicious insiders) II. ภัยคุกคามบนระบบเครือข่าย อันเป็นผลมาจากการได้รับโปรแกรมที่มีจุดประสงค์ทำให้เครื่องคอมพิวเตอร์หรือระบบโครงข่ายหยุดการทำงาน (Denial of services) และ III. การโจมตีบนเว็บ (Web-based attacks) ซึ่งถือได้ว่าเป็นการโจมตีที่มีอัตราการเติบโตสูงมากในปัจจุบัน โดยใช้การฝังมัลแวร์ (Malware) หรือโปรแกรมที่ไม่พึงประสงค์ผ่านทางช่องโหว่ของ Internet browser โดยจะเข้าไปควบคุมการทำงานของโปรแกรม Internet browser ให้เป็นไปตามความต้องการของผู้ประสงค์ร้าย

Anatomy of a Web attack
We begin by looking at the overall anatomy of a typical Web based attack. The diagram illustrates the three distinct phases of activity which together make up a typical Web based attack.



ที่มา: White Paper: Web Based Attacks, February 2009, Symantec

เนื่องจากโลกปัจจุบันเสมือนดั่งเป็นหมู่บ้าน (Global village) ด้วยความเจริญก้าวหน้าทางเทคโนโลยีการสื่อสารและโทรคมนาคมจึงทำให้โลกเป็นสังคมที่ไร้พรมแดนและต้องเผชิญกับความเสี่ยงด้านไซเบอร์อย่างหลีกเลี่ยงไม่ได้ MCAfee กล่าวว่า ประเทศที่ร่ำรวยหรือองค์กรใหญ่มักจะตกเป็นเป้าของการคุกคามด้านไซเบอร์ เนื่องจากใช้ระดับความพยายามที่ไม่แตกต่างกัน แต่ได้รับผลตอบแทนที่สูงกว่า อย่างไรก็ตาม หากประเทศที่มีฐานะทางเศรษฐกิจไม่สู้จะดีนัก ได้หันมาใช้อินเตอร์เน็ตมากยิ่งขึ้นในการติดต่อค้าการขาย ภัยคุกคามด้านไซเบอร์และความเสียหายก็น่าจะเพิ่มมากยิ่งขึ้น ซึ่งในปัจจุบันอาชญากรได้มุ่งความสนใจกับอุปกรณ์สื่อสารมือถือที่เป็นที่นิยมอย่างสูงในประเทศเหล่านี้ MCAfee ระบุว่า 3 ทวีปที่ได้รับความเสียหายสูงที่สุดในโลก คือ ทวีปอเมริกาเหนือ ทวีปยุโรป และเอเชีย ในขณะที่ ทวีปแอฟริกาได้รับความเสียหายต่ำที่สุด โดยความเสียหายที่เกิดขึ้นนั้นคิดเป็นร้อยละของรายได้ หรือ GDP ของประเทศ ดังตัวเลขที่ได้แสดงในภาพข้างล่างนี้

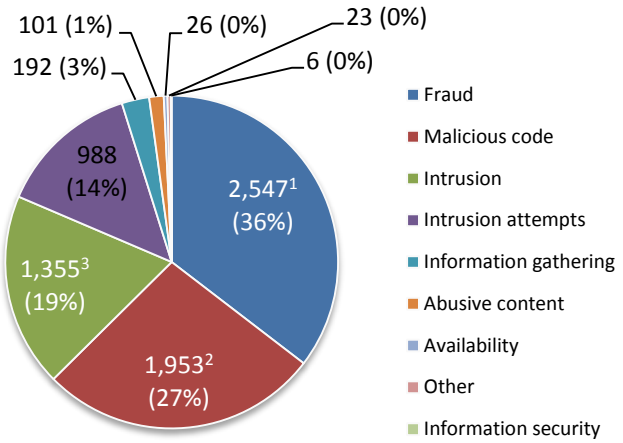


ที่มา: [2]

สถานการณ์ความเสี่ยงด้านไซเบอร์ในประเทศไทย

การติดตามถึงลักษณะของภัยคุมคามด้านไซเบอร์ ตลอดจนถึงมูลค่าความเสียหายที่เกิดขึ้นในประเทศไทย ถึงแม้ยังมิได้มีการรวบรวมและประเมินอย่างเป็นรูปธรรมเท่าใดนัก แต่จากสถิติที่ได้รับจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)[5] แสดงให้เห็นว่า รูปแบบของภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในประเทศไทยมีลักษณะที่คล้ายคลึงกับที่พบในประเทศอื่นๆ ทั่วโลก

[5] ไทยเซิร์ต จัดตั้งขึ้นในปี พ.ศ. 2543 เป็นศูนย์เทคโนโลยีอีเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สังกัดสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี อ่านรายละเอียดเพิ่มเติมได้ที่ www.thaicert.or.th



ที่มา: [5]

ไทยเซิร์ตได้จัดแยกประเภทของภัยคุกคามด้านไซเบอร์ออกเป็น 9 ประเภท คือ I. ภัยคุกคามจากการฉ้อฉลฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) II. ภัยคุกคามจากโปรแกรมที่ถูกพัฒนาขึ้นเพื่อให้เป็นอันตรายต่อระบบ (Malicious code) III. ภัยคุกคามจากการบุกรุก (Intrusion) IV. ภัยคุกคามจากความพยายามบุกรุก (Intrusion attempts) V. ภัยคุกคามจากการรวบรวมข้อมูล (Information gathering) VI. ภัยคุกคามที่เกิดจากการใช้หรือเผยแพร่ข้อมูลที่ไม่เหมาะสมหรือไม่เป็นจริง (Abusive content) VII. ภัยคุกคามต่อการพร้อมใช้ (Availability) VIII. ความมั่นคงปลอดภัยของข้อมูล (Information security) และ IX. ภัยคุกคามประเภทอื่นๆ (Other) โดยในระยะเวลา 4 ปีที่ผ่านมา (ตั้งแต่ ปี 2554 จนถึง 2557) ภัยสามอันดับแรกที่ได้กล่าวมาเบื้องต้น จัดว่าเป็นภัยคุกคามที่ได้รับการรายงานมากที่สุด คิดเป็นสัดส่วนรวมกันสูงถึง 81% ของภัยที่ได้รับการรายงานทั้งหมด และจากสถิติล่าสุดของปี 2558 (ตั้งแต่เดือน ม.ค. ถึง ก.พ.) ชี้ให้เห็นว่าความเสี่ยงจากการโจมตีด้วยโปรแกรมไม่พึงประสงค์ หรือ Malicious code ได้เพิ่มสูงขึ้นเป็นอย่างมาก ซึ่งภัยดังกล่าวได้รับการรายงานคิดเป็นสัดส่วนสูงถึง 28% ของรูปแบบการโจมตีทางไซเบอร์ทั้งหมดในไทยในช่วงระยะเวลา 2 เดือนแรกของปี ซึ่งก็เป็นแนวโน้มเดียวกันกับของโลก

Malicious code จัดว่าเป็นภัยคุกคามที่พบมากที่สุดในไทยในช่วง 2 เดือนแรกของปี 2558 คิดเป็นสัดส่วนมากถึง

28%

ข้อมูลสำคัญที่พอจะบ่งถึงสถานการณ์ความเสี่ยงด้านไซเบอร์ในไทยว่าเป็นอย่างไรนั้น พิจารณาได้จากอันดับของประเทศที่มีความเสี่ยงจากการโจมตีด้านไซเบอร์ที่จัดทำขึ้นโดย Sophos[6] ซึ่งเป็นบริษัทที่มีความเชี่ยวชาญด้านความปลอดภัยของระบบคอมพิวเตอร์สัญชาติสหราชอณาจักร จากการคำนวณอัตราของเครื่องคอมพิวเตอร์ที่ถูกโจมตีด้วยโปรแกรมที่ไม่พึงประสงค์ (Threat exposure rate, TER) ของ Sophos พบว่า ในปี 2555 ประมาณ 1 ใน 5 ของคอมพิวเตอร์ในประเทศไทยประสบกับการถูกโจมตีของโปรแกมที่ไม่พึงประสงค์ ซึ่งระดับดังกล่าวทำให้ประเทศไทยถูกจัดเป็นประเทศที่มีความเสี่ยงต่อภัยคุกคามด้านไซเบอร์สูงเป็นอันดับที่ 3 ของโลก โดยประเทศที่มีความเสี่ยงสูงที่สุดคือ ประเทศอินโดนิเซีย รองลงมาคือ ประเทศจีน

10 Riskiest Countries

	TER		TER
1. Indonesia	23.54%	6. India	15.88%
2. China	21.26%	7. Mexico	15.66%
3. Thailand	20.78%	8. UAE	13.67%
4. Philippines	19.81%	9. Taiwan	12.66%
5. Malaysia	17.44%	10. Hong Kong	11.47%

Threat exposure rate (TER): Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over a three month period.

ที่มา: [6]

[6] Security Threat Report 2013, Sophos

นอกจากจะเป็นเป้าจากการโจมตีแล้ว การให้ความสำคัญกับความปลอดภัยด้านไซเบอร์ขององค์กรในประเทศไทยเองก็ยังอยู่ในระดับที่น่าเป็นห่วงอีกด้วยเช่นกัน IMD[7] ซึ่งเป็นสถาบันการศึกษาชั้นนำของประเทศสวิตเซอร์แลนด์ ได้จัดอันดับการให้ความสำคัญกับความปลอดภัยด้านไซเบอร์ขององค์กรไทยอยู่ในอันดับที่ 48 จาก 60 ประเทศ ซึ่งเป็นอันดับที่ยังห่างชั้นกับประเทศชั้นนำอื่นๆ ในกลุ่ม AEC ด้วยกันอย่างมาก เช่น มาเลเซีย และ สิงคโปร์ ที่ได้รับการจัดอันดับที่ 9 และ 13 ตามลำดับ

พัฒนาการของ Cyber Insurance ในต่างประเทศ

แนวคิดเรื่องประกันภัยไซเบอร์ (Cyber insurance) มีต้นกำเนิดมาตั้งแต่ปี ค.ศ. 1980 ถึงแม้จะผ่านหลายเหตุการณ์สำคัญๆ เช่น Y2K และ 9/11 แต่ความสนใจก็ถูกจำกัดอยู่แต่ในวงของธุรกิจที่มีขนาดเล็กและกลาง รวมไปถึงธนาคารชุมชนขนาดย่อยเท่านั้น[8] แต่หลังจาก 1990 เป็นต้นมา แนวคิดเรื่องความปลอดภัยด้านข้อมูลเป็นที่ยอมรับและได้รับความสนใจมากขึ้น จึงทำให้เครื่องมือถ่ายโอนความเสี่ยงทางการเงินที่เกี่ยวข้องกับระบบเครือข่าย (Network) และคอมพิวเตอร์ไปยังบุคคลที่สามได้รับความนิยม และได้มีการศึกษาถึงวิธีที่การรับประกันภัยด้านไซเบอร์กันอย่างจริงจัง

ผลจากการสำรวจของ PartnerRe ร่วมกับ Advisen[9] ชี้ว่า ขนาดของการประกันภัยไซเบอร์ทั่วโลกในปี 2556 มีมูลค่ามากกว่า US$ 1.2 พันล้าน โดย 83% เป็นเบี้ยประกันภัยที่เกิดขึ้นในตลาดสหรัฐอเมริกาที่มีผู้รับประกันภัยประเภทนี้อยู่มากถึง 35 ราย โดยผลิตภัณฑ์ที่ได้รับความสนใจมีทั้งที่เป็นภัยหลัก (Stand-alone product) และที่เป็นภัยเพิ่ม (Endorsement) เป็นที่คาดว่าธุรกิจประกันภัยประเภทนี้จะโตถึง US$ 2 พันล้านในปี 2557

ตลาดยุโรปเป็นอีกแห่งที่ประกันภัยไซเบอร์ได้รับความนิยม สำนักข่าวรอยเตอร์ (Reuters)[10] ได้อ้างถึงการคาดการณ์ของ Marsh & McLennan ที่ว่า เบี้ยฯ ในภูมิภาคนี้มีมูลค่าไม่ต่ำกว่า US$ 150 ล้านในปี 2556 (โดยเบี้ยประกันภัยของธุรกิจการประกันภัยไซเบอร์ในสหราชอาณาจักรมีขนาด 0.01% ของเบี้ยประกันวินาศภัยทั้งหมดของประเทศ[11]) ถึงแม้ธุรกิจการประกันภัยไซเบอร์ในยุโรปยังมีขนาดที่ไม่ใหญ่โตนักเมื่อเทียบกับขนาดของธุรกิจในประเทศสหรัฐอเมริกา แต่ด้วยการตระหนักถึงภัยคุกคามด้านไซเบอร์ที่มากยิ่งขึ้นของหลายองค์กร พร้อมทั้งผู้เล่นรายใหญ่ (เช่น Zurich Insurance Group, Lloyd's of London, Hiscox, Allianz และ HDI-Gerling เป็นต้น) ก็พร้อมที่จะให้บริการ จึงเป็นที่คาดว่าตลาดประกันภัยไซเบอร์ในยุโรปมีแนวโน้มที่จะเติบโตขึ้นอย่างแน่นอน ดังจะเห็นได้จาก ในช่วงไม่กี่ปีที่ผ่านมา ธุรกิจประกันภัยไซเบอร์ในทวีปยุโรปมีอัตราการเติบโตที่สูงมากถึง 50%-100% ต่อปีเลยทีเดียว

สาเหตุที่ประกันภัยไซเบอร์ในประเทศสหรัฐอเมริกามีขนาดที่ใหญ่เช่นที่กล่าวมานั้น เนื่องมาจากคนอเมริกันนิยมใช้บัตรเครดิตในการจับจ่ายใช้สอย อาชญากรรมด้านไซเบอร์จึงก่อให้เกิดความสูญเสียที่มีมูลค่าสูง ดังเช่นที่เกิดขึ้นกับ Target (ในช่วงปลายปี 2556 ที่ข้อมูลสำคัญของบัตรเครดิตและบัตรเดบิตของลูกค้าเกือบ 40 ล้านใบได้ถูกขโมย) และ Home Depot Inc. (ข้อมูลบัตรเครดิตลูกค้า 56 ล้านคนได้ถูกโจรกรรม) เป็นต้น นอกจากนี้แล้ว ตัวบทกฎหมายในเรื่องของการ

---

[7] IMD World Competitiveness Ranking 2013, IMD, www.imd.org
[8] Bohme, R. and G. Schwartz, 2010, Modeling Cyber-Insurance: Towards A Unifying Framework, ICSI and UC Berkeley
[9] Cyber Liability Insurance Market Trends: Survey, October 2014, Advisen
[10] Insurers struggle to get grip on burgeoning cyber risk market, July 14, 2014, Reuters, http://www.reuters.com/article/2014/07/14/us-insurance-cybersecurity-idUSKBN0FJ0B820140714
[11] Cyber Insurance Demand Said Rising in Europe, Jan 28, 2015, WSJ, http://blogs.wsj.com/digits/2015/01/28/cyber-insurance-demand-said-rising-in-europe/

ปกป้องข้อมูล รวมไปถึงการบังคับใช้ที่เป็นไปอย่างเข้มงวด จึงทำให้ประเทศสหรัฐอเมริกาเป็นตลาดที่สำคัญของธุรกิจประกันภัยไซเบอร์

รูปแบบความคุ้มครองในปัจจุบันของกรมธรรม์ประกันภัยไซเบอร์ในตลาดต่างประเทศแบ่งออกได้เป็น 4 ลักษณะคือ

1. ความรับผิดจากการละเมิดข้อมูลสำคัญขององค์กร (Data breach and privacy management) เช่น ค่าใช้จ่ายที่เกิดขึ้นจากการกู้ข้อมูลที่ถูกลักขโมยไป รวมไปถึงค่าใช้จ่ายจากการสืบสวนสอบสวน และค่าใช้จ่ายทางกฎหมายที่จำเป็นอื่นๆ เป็นต้น
2. ความรับผิดจากการละเมิดระบบสื่อสารข้อมูลข่าวสารหลายชนิด โดยผ่านสื่อทางคอมพิวเตอร์ (Multimedia liability coverage) เช่น ความเสียหายอันเกิดจากการเปลี่ยนแปลงข้อมูลหรือตัวเลขบน Website หรือสื่อต่างๆ ตลอดไปจนถึง การละเมิดสิทธิทางปัญญา (Intellectual property rights) เป็นต้น
3. ความรับผิดจากการกรรโชกหรือขู่เข็ญ (Extortion liability coverage) เช่น การกระทำให้ระบบคอมพิวเตอร์หรือระบบโครงข่ายหยุดการให้บริการเพื่อเรียกร้องค่าไถ่ เป็นต้น
4. ความรับผิดจากการเจาะระบบโครงข่าย (Network security liability) เช่น ค่าเสียหายอันมีผลมาจากระบบโครงข่ายหยุดการทำงาน รวมไปถึง การโจรกรรมข้อมูลของผู้ไม่ประสงค์ดี เป็นต้น

หากพิจารณาในมุมของรูปแบบของกรมธรรม์แล้ว จะสามารถแบ่งออกได้เป็น 2 รูปแบบด้วยกันกล่าวคือ 1. การประกันภัยผู้เอาประกันภัย (First-party insurance) และ 2. การประกันภัยความรับผิดต่อบุคคลภายนอก (Third-party or liability insurance) ซึ่งรูปแบบความคุ้มครองสรุปได้ดังนี้[12]

First-Party Ins.	Third-Party/Liability Ins.
▪ คุ้มครองความเสียหายที่เกิดขึ้นกับข้อมูล รวมไปถึง software และ ระบบโครงข่ายขององค์กร ▪ คุ้มครองความเสียหายที่เกิดจากธุรกิจหยุดชะงัก อันมีสาเหตุมาจาก software หรือ ระบบโครงข่ายเกิดการขัดข้องจากการคุกคามด้านไซเบอร์ ▪ คุ้มครองความเสียหายจากการกระทำที่เป็นการรีดเอาทรัพย์หรือการกรรโชกจากอาชญากรรมไซเบอร์ (cyber-extortion protection) ได้แก่ ค่าไถ่ และ ค่าใช้จ่ายที่เกิดขึ้นจากการต่อรอง เป็นต้น	▪ คุ้มครองความเสียหายที่เกิดขึ้นกับลูกค้า เนื่องจากระบบความปลอดภัยขององค์กรถูกล่วงละเมิด (Security breach) ▪ คุ้มครองความเสียหายอันเกิดจากการจารกรรมข้อมูลของลูกค้า รวมไปถึงค่าชดใช้แก่ผู้ตกเป็นเหยื่อและค่าใช้จ่ายในการกู้คืนข้อมูล ▪ คุ้มครองความเสียหายอันเกิดจากระบบโครงข่ายหยุดให้บริการแก่ลูกค้า หรือความเสียหายอันมีผลมาจากการแพร่ระบาดของโปรแกรมที่ไม่พึงประสงค์ ▪ คุ้มครองความเสียหายจากการใช้สื่อออนไลน์ เช่น website, email, instant messaging, และ chat rooms ▪ คุ้มครองความเสียหายต่อบุคคลที่สามอันเกิดจากการละเลยหรือขาดความระมัดระวังขององค์กร

[12] Using Insurance to Mitigate Cybercrime Risk: Challenges and recommendations for insurers, 2012, Capgemini

การประกันภัยไซเบอร์ในประเทศไทยและความต้องการ

จากการสำรวจและสอบถามผู้เชี่ยวชาญในวงการประกันวินาศภัยไทยพบว่า บริษัทประกันภัยในประเทศไทยในปัจจุบันยังไม่ได้มีการนำเสนอกรมธรรม์ประกันภัยไซเบอร์แต่อย่างไร ซึ่งข้ออ้างนี้ได้รับจากการยืนยันจากสมาคมประกันภัยไทยด้วยเช่นกัน

สำหรับความต้องการกรมธรรม์ลักษณะเช่นนี้ในประเทศไทยนั้น เป็นที่คาดกันว่าจะมีอยู่ในระดับที่มากพอสมควรจากระดับความเสี่ยงที่เผชิญอยู่ในปัจจุบันและแนวโน้มที่ถูกมองว่ากำลังเพิ่มมากยิ่งขึ้นในอนาคตอันใกล้ ดังที่ได้แสดงในหัวข้อข้างต้น กอปรกับการที่หลายๆ ภาคส่วนได้ให้ความสำคัญกับเรื่องความปลอดภัยด้านไซเบอร์ในระดับต้นๆ

ในปัจจุบัน ภาครัฐได้ให้ความสำคัญกับความมั่นคงปลอดภัยด้านไซเบอร์เป็นอย่างมาก จึงได้มีแนวคิดในการกำหนดยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2556-2560) เพื่อเพิ่มขีดความสามารถของประเทศ ซึ่งยุทธศาสตร์ดังกล่าวได้ระบุกลุ่มหน่วยงานที่มีความสุ่มเสี่ยงต่อภัยคุกคามด้านไซเบอร์ไว้อย่างชัดเจน จึงเป็นที่คาดว่ากรมธรรม์ประกันภัยไซเบอร์น่าจะเป็นที่ต้องการของหน่วยงานต่างๆ เหล่านี้ ซึ่งประกอบด้วย

I. หน่วยงานด้านความมั่นคง และภาคบริการประชาชน เช่น กองทัพ สำนักงานตำรวจแห่งชาติ ศาล กรมสอบสวนคดีพิเศษ สำนักป้องกันและปราบปรามการฟอกเงิน (ปปง.) สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (ป.ป.ส.) เป็นต้น
II. หน่วยงานการให้บริการด้านสาธารณสุข
III. หน่วยงานด้านการเงิน การธนาคาร และพาณิชย์อิเล็กทรอนิกส์ เช่น ธนาคาร บริษัทหลักทรัพย์ ประกันภัย ตลาดหลักทรัพย์ ผู้ให้บริการด้านเครดิต เป็นต้น
IV. หน่วยงานด้านสาธารณูปโภคพื้นฐาน เช่น การไฟฟ้า การประปา เป็นต้น
V. หน่วยงานด้านพลังงาน
VI. หน่วยงานด้านการคมนาคม/ขนส่ง เช่น ธุรกิจด้านสายการบิน เป็นต้น
VII. หน่วยงานด้านสื่อสารและโทรคมนาคม เช่น บริษัทที่ให้บริการอินเตอร์เน็ต ผู้ให้บริการโทรศัพท์มือถือ ดาวเทียม สถานีโทรทัศน์ เป็นต้น

ศูนย์วิจัยเศรษฐกิจและธุรกิจ บมจ. ธนาคารไทยพาณิชย์ หรือ EIC ได้ประเมินไว้ในบทวิเคราะห์ Cyber insurance: โอกาสทางธุรกิจใหม่ของธุรกิจประกันภัย[13] ว่า ตลาดประกันภัยไซเบอร์ในไทยเป็นที่คาดว่าจะได้รับการตอบรับจากสถาบันการเงินและธุรกิจโทรคมนาคม เนื่องจากกลุ่มธุรกิจเหล่านี้มีจำนวนผู้ใช้บริการมากที่สุด และมีความเกี่ยวข้องกับข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลส่วนบุคคล เลขบัตรเครดิต เป็นต้น จึงมีความเสี่ยงหรือเป็นเป้าโจมตีของผู้ไม่ประสงค์ดี โดย EIC ได้กล่าวเพิ่มอีกว่า เนื่องจากกรมธรรม์ประกันภัยไซเบอร์ยังไม่มีบริษัทประกันภัยไทยรายใดเข้ามาทำตลาด จึงเป็นโอกาสของวงการประกันภัยไทยในอนาคตอันใกล้

[13] www.scbeic.com

บทสรุป

เป็นที่เชื่อมั่นว่าการประกันภัยไซเบอร์มีแนวโน้มที่จะได้รับความนิยมมากขึ้นเรื่อยๆ ในหลายๆ ประเทศทั่วโลก เนื่องจากภัยคุกคามด้านไซเบอร์ที่ได้ทวีความรุนแรงและมีความสลับซ้อนจนยากที่จะป้องกัน ดังนั้น เครื่องมือที่มีจะมีส่วนช่วยให้องค์กรบริหารจัดการความเสี่ยงเหล่านี้ได้อย่างมีประสิทธิผลจึงเป็นสิ่งจำเป็นและเป็นที่ต้องการ อย่างไรก็ตาม ธุรกิจประเภทนี้ก็เหมือนดังเช่นธุรกิจอื่นๆ ที่ต้องประสบกับข้อจำกัดหรือความท้าทายนานับประการ ไม่ว่าจะเป็นเรื่องความซับซ้อนในการประเมินผลกระทบทางธุรกิจที่จะเกิดขึ้นต่อองค์กรจากการโจมตีทางไซเบอร์ รวมไปถึง ข้อมูลที่อาจจะยังไม่มากเพียงพอในการที่จะนำมาใช้กำหนดอัตราเบี้ยประกันภัยได้อย่างเหมาะสม ความท้าทายที่สำคัญอีกประการคือ ความเสี่ยงด้านไซเบอร์เป็นความเสี่ยงที่มีผลกระทบในวงกว้าง และอาจนำมาซึ่งความเสียหายมูลค่ามหาศาล นอกจากนี้แล้ว ความเสี่ยงด้านไซเบอร์ยังมีลักษณะที่มีความเชื่อมโยงหรือสัมพันธ์กันค่อนข้างสูง ดังนั้น เมื่อระบบหนึ่งขององค์กรถูกโจมตี ก็จะเปิดโอกาสให้ระบบคอมพิวเตอร์อื่นๆ ขององค์กรเดียวกันได้รับผลกระทบด้วยเช่นกัน

ด้วยความเข้าใจในลักษณะความต้องการที่หลากหลาย และเข้าถึงประเด็นความท้าทายที่ได้กล่าวมานี้ จะทำให้การกำหนดผลิตภัณฑ์ประกันภัยไซเบอร์ได้อย่างเหมาะสม ซึ่งเป็นปัจจัยสำคัญของการดำเนินธุรกิจประกันภัย

ภาคผนวก

กรณีตัวอย่าง: ผลิตภัณฑ์ประกันภัยไซเบอร์ของ AIG[14]

กรมธรรม์ประกันภัยไซเบอร์ที่ AIG จำหน่ายอยู่ในปัจจุบันเรียกว่า CyberEdge เป็นผลิตภัณฑ์ที่มุ่งเน้นกลุ่มลูกค้าที่เป็นองค์กร โดยให้ความคุ้มครองในลักษณะผสมผสานกันระหว่างการประกันภัยผู้เอาประกันภัย (First-party insurance) และการประกันภัยความรับผิดต่อบุคคลภายนอก (Third-party liability insurance) ซึ่งความคุ้มครองประกอบด้วย

Third-Party Loss Resulting From a Security or Data Breach 	ความเสียหายต่อบุคคลที่สามอันเนื่องมาจากระบบความปลอดภัยของระบบโครงข่ายขององค์กรเกิดความผิดพลาด หรือความบกพร่องในการป้องกันข้อมูล นอกจากนี้แล้ว ความคุ้มครองยังรวมไปถึงค่าปรับจากการละเลยต่อการแจ้งเหตุการณ์จารกรรมข้อมูลขององค์กรต่อหน่วยงานกำกับ
Direct First-Party Costs of Responding to a Breach 	ค่าใช้จ่ายอันอาจจะเกิดขึ้นจากการประชาสัมพันธ์ หรือกิจกรรมจำเป็นใดๆ ที่เข้ามามีบทบาทในการบริหารจัดการสถานการณ์การบุกรุกทางไซเบอร์ขององค์กรไม่ให้ลุกลามและเกิดความเสียหายขึ้นในวงกว้าง หรือแม้กระทั่งค่าใช้จ่ายในเรื่องของการสืบสวนสอบสวน ค่าใช้จ่ายในเรื่องที่เกี่ยวข้องกับกฎหมายต่างๆ และการพิสูจน์หาผู้ที่ได้รับความเสียหาย
Lost Income and Operating Expense Resulting From a Security or Data Breach 	ค่าเสียหายอันเกิดจาก การสูญเสียรายได้และค่าใช้จ่ายในการดำเนินการจากการที่ธุรกิจต้องหยุดชะงัก อันมีเหตุมาจากความบกพร่องของระบบความปลอดภัยของระบบโครงข่ายที่ให้บริการแก่ลูกค้า
Threats to Disclose Data or Attack a System to Extort Money 	ค่าใช้จ่ายที่เกิดขึ้นเพื่อยุติการข่มขู่ทำร้ายระบบคอมพิวเตอร์ ระบบโครงข่าย ข้อมูลสำคัญ และความลับทางธุรกิจขององค์กร ตลอดจนถึง ค่าใช้จ่ายในการสืบสวนสอบสวนถึงสาเหตุของการข่มขู่อีกด้วย
Online Defamation and Copyright and Trademark Infringement 	ความเสียหายที่อาจจะเกิดขึ้นกับองค์กรจากเนื้อหาที่เผยแพร่บนเว็บไซต์ของบริษัท ซึ่งความคุ้มครองได้ครอบคลุมถึง การละเมิดลิขสิทธิ์ การละเมิดเครื่องหมายทางการค้า การทำให้เสียชื่อเสียง และการล่วงละเมิดความเป็นส่วนตัว เป็นต้น

[14] CyberEdge: End-to-End Cyber Risk Management Solutions, http://www.aig.com/chartisint/internet/US/en/files/AIG_CyberEdge0418finalsingle_tcm1247-575268.pdf

กรณีตัวอย่าง: ผลิตภัณฑ์ประกันภัยไซเบอร์ของ CNA

บริษัทประกันภัยใหญ่เป็นอันดับ 8 ของประเทศสหรัฐอเมริกาได้จำหน่ายกรมธรรม์ประกันภัยไซเบอร์ให้แก่องค์กรที่คำนึงถึงความปลอดภัยของข้อมูล โดยตั้งชื่อกรมธรรม์นี้ว่า CNA NetProtect[15] ซึ่งเป็นกรมธรรม์ที่ให้ความคุ้มครองแก่ทั้งผู้เอาประกันภัย (First-party insurance) และบุคคลภายนอก (Third-party liability insurance) โดยความคุ้มครองหลักๆ ครอบคลุมถึง การกรรโชกระบบโครงข่าย (Network extortion) ความเสียหายจากธุรกิจหยุดชะงัก ค่าเสียหายที่เกิดขึ้นกับระบบโครงข่าย ความเสียหายอันเกิดจากข้อมูลสารสนเทศที่เผยแพร่บนสื่อผ่านระบบคอมพิวเตอร์ (Media liability) ความเสียหายอันเกิดจากการละเมิดข้อมูลที่เป็นความลับหรือข้อมูลส่วนตัว (Privacy liability) ตลอดจนถึง ความเสียหายจากการเจาะระบบความปลอดภัยของระบบโครงข่าย

[15] www.cna.com