ประกันภัยไซเบอร์
ล็อกความเสี่ยงโจรกรรมข้อมูล

▶ ลดความสูญเสียจากภัยคุกคามของแฮ็กเกอร์จ้องโจรกรรมข้อมูล ด้วยประกันภัยไซเบอร์ ที่ให้ความคุ้มครองค่าใช้จ่ายจากการถูกโจรกรรมข้อมูล ครอบคลุมทั้งการจ้างผู้เชี่ยวชาญตรวจสอบ การกู้ข้อมูล การจ่ายค่าไถ่ การสูญเสียรายได้จากการหยุดชะงักของธุรกิจ และความรับผิดต่อบุคคลภายนอกจากการที่ข้อมูลของลูกค้าสูญหาย รวมทั้งค่าใช้จ่ายในการต่อสู้คดี

ท่ามกลางกระแสโลกที่เปลี่ยนแปลงเข้าสู่ยุคดิจิทัล ปัญหาที่สำคัญที่ผู้คนในทุกวงการเป็นกังวลคือเรื่องอาชญากรรมทางคอมพิวเตอร์ ซึ่งก็ได้มีการพัฒนาไปอย่างต่อเนื่อง และสามารถแพร่กระจายได้อย่างรวดเร็ว สร้างความเสียหายอย่างร้ายแรงได้อย่างคาดไม่ถึง ในระดับภาคธุรกิจและบุคคลทั่วไป

จากข้อมูลของ Hakmagaeddon ซึ่งทำการรวบรวมสถิติด้านอาชญากรรมทางคอมพิวเตอร์ พบว่าในเดือนมีนาคม 2560 เป้าหมายที่ถูกโจมตีเป็นอันดับ 1 คือ ภาคอุตสาหกรรม คิดเป็นสัดส่วน 21.5% ของการโจมตีทั้งหมด ตามด้วยภาครัฐบาลที่ 16.9% บุคคลธรรมดามีสัดส่วน 16.9% ภาคการศึกษามีสัดส่วน 12.3% และที่เหลือเป็นองค์กรต่างๆ กลุ่มที่เผยแพร่ข่าวสาร Healthcare และการเงินเป็นต้น

สำหรับภาคอุตสาหกรรมที่ถูกโจมตีมากที่สุดนำโดยกลุ่ม Software, การเงิน การธนาคาร, การขายตั๋วออนไลน์, การบริการทางธุรกิจ, ร้านอาหาร, ร้านค้าปลีก เป็นต้น

และล่าสุด จากสถานการณ์การระบาดของมัลแวร์สายพันธุ์ใหม่ ชื่อ PETYA หรือ Petrwrap ซึ่งเป็นไวรัสประเภทมัลแวร์ เรียกค่าไถ่ (RANSOMWARE) กำลังระบาดทั่วโลกไม่ว่าจะเป็นอเมริกาและยุโรป จนเป็นผลทำให้เครื่องคอมพิวเตอร์ขององค์กรที่ใช้ระบบปฏิบัติการ MS Windows ติดไวรัสดังกล่าวจนไม่สามารถใช้งานได้

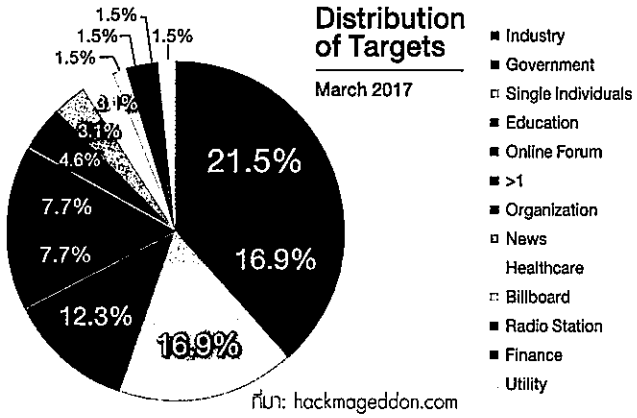
เนื่องจากถูกเข้ารหัสลับ Master File Table (MFT) ของพาร์ทิชัน ซึ่งเป็นตารางที่ใช้ระบุตำแหน่งชื่อไฟล์ และเนื้อหาของไฟล์ในฮาร์ดดิสก์ ทำให้ผู้ใช้ไม่สามารถเข้าถึงข้อมูลในฮาร์ดดิสก์ได้ หากต้องการถอดรหัสต้องจ่ายค่าไถ่เป็นเงิน 300 USD ผ่านอีเมล์ แต่เนื่องจากอีเมล์ดังกล่าวถูกผู้ให้บริการปิดแล้ว จึงทำให้ไม่สามารถจ่ายค่าไถ่ได้ จนส่งเกิดผลกระทบกับระบบของธุรกิจในประเทศต่างๆ ทั่วโลก

คปภ.กำหนดมาตรฐาน หนุนประกันภัยไซเบอร์

ดร.สุทธิพล ทวีชัยการ เลขาธิการคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) เปิดเผยว่า สำนักงาน คปภ. ได้ตระหนักถึงผลกระทบจากภัยคุกคามดังกล่าวต่อระบบประกันภัย จึงได้กำหนดมาตรการรับมือภัยคุกคามไว้ 2 มาตรการคือ ในส่วนขององค์กร ได้มีการจัดทำแนวทางปฏิบัติในการป้องกันไวรัสภายในองค์กร และสั่งการให้สำนักงาน คปภ. ทั่วประเทศ ดำเนินการตามแนวปฏิบัตินี้อย่างเคร่งครัด เพื่อเป็นการเฝ้าระวังและป้องกันภัยคุกคามที่อาจเจาะเข้ามาในระบบของสำนักงาน คปภ.

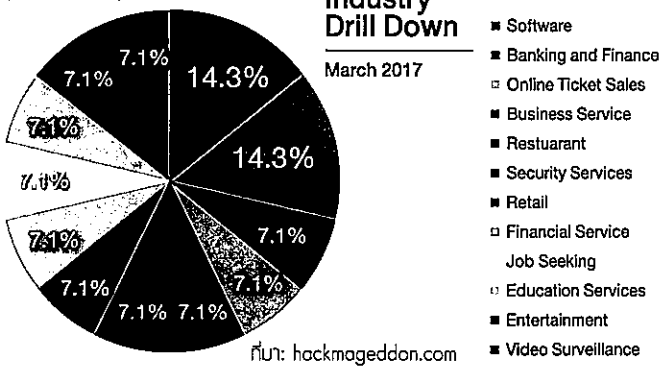
สำหรับในส่วนของภาคอุตสาหกรรมประกันภัย สำนักงาน คปภ. ในฐานะหน่วยงานกำกับ ได้เฝ้าติดตามสถานการณ์อย่างใกล้ชิด แม้ในขณะนี้ยังไม่ได้รับรายงานผลกระทบจากเหตุการณ์ดังกล่าวในธุรกิจประกันภัย แต่เพื่อเป็นการป้องกันภัยคุกคามทางคอมพิวเตอร์ของภาคธุรกิจประกันภัย จึงได้ประสานไปยังสมาคมประกันชีวิตไทย และสมาคมประกันวินาศภัยไทย เพื่อแจ้งให้บริษัทสมาชิกเฝ้าระวัง และเตรียมการอย่างเป็นระบบ ตั้งแต่การป้องกัน การรับมือกับภัยคุกคามทางคอมพิวเตอร์ รวมทั้งสื่อสารให้พนักงานและประชาชนรับทราบถึงแนวทางป้องกันการแพร่ระบาดอย่างเหมาะสม

สถิติเป้าหมายการโจมตีทางคอมพิวเตอร์ (มี.ค.2560)

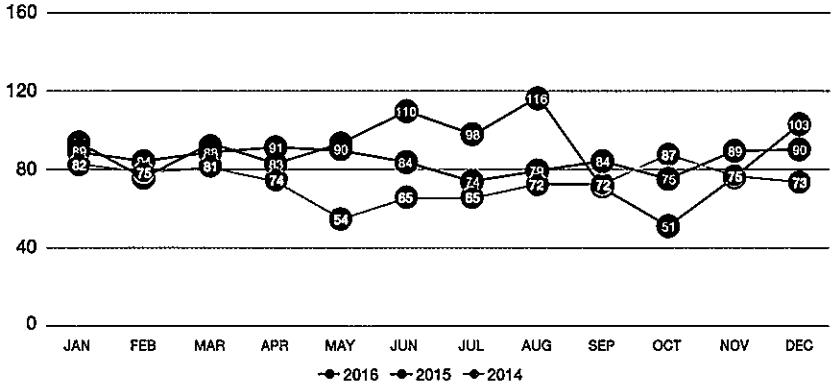


ที่มา: hackmageddon.com

สถิติเป้าหมายการโจมตีทางคอมพิวเตอร์ในภาคอุตสาหกรรมต่างๆ (มี.ค.2560)



ที่มา: hackmageddon.com



สถิติจำนวนครั้งการโจมตีทางคอมพิวเตอร์รายเดือน ช่วง 3 ปีที่ผ่านมา

Monthly Attacks
(2016vs2015vs2014)

ที่มา: hackmageddon.com

// เพื่อเป็นการเฝ้าระวังจากการถูกจู่โจมหรือคุกคามทางไซเบอร์ สำนักงาน คปภ. จึงได้ส่งเสริมและสนับสนุนให้บริษัทประกันภัยพัฒนากรมธรรม์ประกันภัยไซเบอร์ (Cyber Insurance) เพื่อตอบสนองความต้องการของผู้บริโภคที่ต้องการความคุ้มครองที่ครอบคลุมค่าเสียหายจากการโจรกรรมทางอิเล็กทรอนิกส์ //

โดยให้รายงานสถานการณ์เฝ้าระวังภัยคุกคามทางคอมพิวเตอร์ต่อ สำนักงาน คปภ. เป็นระยะๆ หากได้รับผลกระทบจากภัยดังกล่าว ขอให้แจ้งมายัง สำนักงาน คปภ. ทาง E-mail : it@oic.or.th หรือ สายด่วน คปภ. 1186 โดยเร็ว เพื่อประสานให้ความช่วยเหลือ และทำงานร่วมกันอย่างเป็นระบบเพื่อเตรียมการรับมือ

อย่างไรก็ตาม เพื่อเป็นการเฝ้าระวังจากการถูกจู่โจมหรือคุกคามทางไซเบอร์ สำนักงาน คปภ. จึงได้ส่งเสริมและสนับสนุนให้บริษัทประกันภัยพัฒนากรมธรรม์ประกันภัยไซเบอร์ (Cyber Insurance) เพื่อตอบสนองความต้องการของผู้บริโภคที่ต้องการความคุ้มครองที่ครอบคลุมค่าเสียหายจากการโจรกรรมทางอิเล็กทรอนิกส์

ซึ่งทางด้านของบริษัทประกันภัยเองก็ได้พัฒนาประกันภัยไซเบอร์เพื่อเข้ามารองรับความเสี่ยงจากการจู่โจมหรือคุกคามทางไซเบอร์ โดยประกันภัยไซเบอร์จะออกแบบมาเพื่อป้องกันความเสี่ยงต่อความเสียหายทางคอมพิวเตอร์ที่เกิดขึ้นกับธุรกิจในเชิงพาณิชย์ได้ทุกประเภท ไม่ว่าจะเป็น ผู้ผลิตสินค้า ผู้ให้บริการประเภทต่างๆ และโดยเฉพาะอย่างยิ่งสถาบันการเงินซึ่งมีความเสี่ยงภัยในระดับสูง โดยจะคุ้มครองทั้งในส่วนความรับผิดต่อผู้เอาประกันภัย (First Party) หรือความรับผิดต่อบุคคลภายนอก (Third Party) ซึ่งเกิดขึ้นกับข้อมูลของลูกค้าสูญหาย หรือถูกโจรกรรม

สำหรับความคุ้มครองหลักๆ ของประกันภัยไซเบอร์ที่สำนักงาน คปภ.กำหนดเป็นมาตรฐาน ประกอบด้วย 2 ส่วนคือ ส่วนแรก ความคุ้มครองต่อผู้เอาประกันภัย เช่น ความคุ้มครองจากการหยุดชะงักของธุรกิจ, ค่าเสียหายจากการถูกโจรกรรมทางอิเล็กทรอนิกส์ในการถ่ายโอนข้อมูลที่เป็นการกระทำฉ้อฉลในระบบคอมพิวเตอร์ หรือผ่านเครือข่ายในระบบคอมพิวเตอร์, ค่าเสียหายจากการสื่อสารทางอิเล็กทรอนิกส์ เนื่องจากการถ่ายโอนข้อมูลของลูกค้าที่เป็นการฉ้อฉลในระบบคอมพิวเตอร์ทำให้เกิดความเสียหายขึ้น และบริษัทของลูกค้า เป็นผู้รับผิดตามกฎหมาย

ค่าเสียหายจากการคุกคามทางอีเล็กทรอนิกส์ รวมถึงต้นทุนในการเจรจาต่อรองทางด้านการประกอบวิชาชีพ, ค่าใช้จ่ายในการแจ้งเกี่ยวกับข้อมูลความลับ รวมถึงต้นทุนการให้บริการตรวจสอบความน่าเชื่อถือสำหรับลูกค้าที่ได้รับผลกระทบ, ค่าเสียหายจากการทำลายทรัพย์สินทางอีเล็กทรอนิกส์ โดยมีสาเหตุจากพนักงาน, ค่าใช้จ่ายในภาวะวิกฤติ รวมถึงต้นทุนค่าที่ปรึกษาด้านประชาสัมพันธ์ และค่าเงินรางวัล รวมถึงต้นทุนการจ่ายผู้ให้ข้อมูล

ส่วนที่สอง ความคุ้มครองความรับผิดต่อบุคคลภายนอก เช่น ความรับผิดในการเปิดเผยข้อมูล รวมถึงคดีที่ลูกค้าเรียกร้องเนื่องมาจากความล้มเหลวของระบบความปลอดภัยจากการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต หรือการแพร่กระจายข้อมูลส่วนบุคคลบนอินเทอร์เน็ต, ความรับผิดต่อเนื้อหา รวมถึงคดีที่เกิดขึ้นจากการละเมิดทรัพย์สินทางปัญญา การละเมิดเครื่องหมายการค้าและลิขสิทธิ์, ความรับผิดต่อชื่อเสียง รวมถึงคดีที่ละเมิดทำให้เสื่อมเสียชื่อเสียงทางด้านสินค้าหรือการบริการการกล่าวร้ายการหมิ่นประมาท และบุกรุกความเป็นส่วนตัว

ความรับผิดในความเสียหายในระบบส่วนกลาง รวมถึงคดีเนื่องมาจากความล้มเหลวของระบบความปลอดภัยทำให้เกิดอันตรายกับระบบคอมพิวเตอร์ของบุคคลภายนอกและความรับผิดในความเสียหายจากการเข้าถึง รวมถึงคดีเนื่องมาจากความล้มเหลวของระบบความปลอดภัยทำให้ระบบของลูกค้าไม่สามารถติดต่อกับลูกค้ารายอื่นได้ และค่าใช้จ่ายในการต่อสู้คดีคุ้มครองถึงค่าใช้จ่ายที่เกิดขึ้น จากการต่อสู้คดีกับหน่วยงานของภาครัฐ หรือองค์กรที่ควบคุมกฎระเบียบหรือใบอนุญาต

โดยบริษัทประกันจะต้องดำเนินการจ่ายค่าใช้จ่ายในการต่อสู้คดีล่วงหน้าในการจัดการควบคุมสำหรับการเรียกร้องเนื่องจากความเสียหายทางคอมพิวเตอร์ภายใน 30 วันหลังจากวันที่ได้รับใบแจ้งหนี้ในส่วนค่าใช้จ่ายในการต่อสู้คดีนั้น

ทั้งนี้ สำนักงาน คปภ.ได้กำหนดอัตราเบี้ยประกันภัยรายปีไว้ที่ 0.1-5% ของจำนวนเงินจำกัดความรับผิด หรือรายได้ต่อปี หรือขนาดของสินทรัพย์ แล้วแต่กรณี โดยปัจจุบัน มีบริษัทประกันภัยที่ได้รับความเห็นชอบแบบกรมธรรม์ประกันภัยไซเบอร์แล้ว 7 บริษัท ประกอบด้วย บจ.เอฟพีจี ประกันภัย (ประเทศไทย) บมจ.ทิพยประกันภัย บมจ.ไทยประกันภัย บมจ.อลิอันซ์ ประกันภัย บจ.นิวแฮมพ์เชอร์ อินชัวรันส์ สาขาประเทศไทย บจ.เอไอจี ประกันภัย (ประเทศไทย) และ บมจ.โตเกียวมารีนประกันภัย (ประเทศไทย)

ตั้งทีมบุกขายประกันไซเบอร์ จัดแพ็กเกจคุ้มครองธุรกิจ

นายพุทธรัตน์ ศรีพร้อม ผู้อำนวยการฝ่ายประกันภัยไซเบอร์และโครงการพิเศษ บมจ.ทิพยประกันภัย เปิดเผยว่า บริษัทได้จัดตั้งฝ่าย Cyber เพื่อนำเสนอกรมธรรม์ไซเบอร์โดยเฉพาะ ซึ่งที่ผ่านมาบริษัทได้มีการนำร่องเสนอกรมธรรม์ไซเบอร์ผ่านฐานลูกค้าองค์กรเดิมของบริษัทแล้ว แต่เนื่องจากกรมธรรม์ไซเบอร์ยังใหม่สำหรับลูกค้าองค์กรในประเทศไทย จึงทำให้ที่ผ่านมาลูกค้าองค์กรยังไม่เห็นถึงความสำคัญและความเสี่ยงที่อาจจะเกิดขึ้นกับธุรกิจ จนกระทั่งเกิดเหตุภัยคุกคามไซเบอร์ จากวอนนาคราย และ PETYA ขึ้นทำให้ลูกค้าองค์กรเริ่มตระหนักถึงความเสี่ยงภัยจากการถูกคุกคามด้านไซเบอร์มากขึ้น

สำหรับ Cyber Insurance คือกรมธรรม์ที่ออกแบบมาเพื่อคุ้มครองความเสียหายทางการเงินที่เกิดจากภัยคุกคามทางไซเบอร์ เนื่องจากในปัจจุบันอยู่ในยุคของ Digital, Internet และ Online จึงทำให้ธุรกิจหันมาพึ่งพาระบบและ Internet ในกระบวนการทำงานมากขึ้น รวมไปถึงการทำธุรกรรม และค้าขายกันบนโลก Online ที่มากขึ้น จึงทำให้ธุรกิจมีความเสี่ยงภัยจากภัยทางไซเบอร์ ดังนั้น Cyber Insurance จึงเป็นเครื่องมือในการบริหารความเสี่ยงด้านไซเบอร์ ของภาคธุรกิจได้

โดย Cyber Insurance จะให้ความคุ้มครองความเสียหายทางการเงินของผู้เอาประกันภัยที่เกิดขึ้นจากการถูกโจมตีระบบ การถูกแอบเข้าระบบโดยไม่ได้รับอนุญาต และการที่ข้อมูลรั่วไหลออกไปสู่บุคคลภายนอก และยังคุ้มครองถึงความรับผิดต่อบุคคลภายนอกที่ได้รับผลกระทบจากการที่ข้อมูลรั่วไหลออกไป

นายพุทธรัตน์กล่าวว่า สำหรับขั้นตอนในการพิจารณารับประกันภัยนั้น บริษัทประกันภัยจะทำการประเมินความเสี่ยงเบื้องต้น โดยการนำเสนอใบคำขอที่มีแบบคำถามที่ลูกค้าต้องให้ข้อมูลอย่างละเอียด หลังจากนั้นบริษัทจะนำข้อมูลที่ได้จากลูกค้ามาเข้ากระบวนการพิจารณารับประกันภัย ก่อนที่จะนำเสนอความคุ้มครองและอัตราเบี้ยประกันภัย ซึ่งจะพิจารณาจากประเภทของธุรกิจ การดำเนินการ นโยบายด้านความปลอดภัยด้านไซเบอร์ การเก็บรักษาข้อมูล และระบบต่างๆ ที่ใช้ รวมถึงวงเงินเอาประกันภัยที่ผู้เอาประกันภัยต้องการที่เหมาะสมกับธุรกิจและความเสี่ยงของผู้เอาประกันภัยต่อไป

กรณีที่เกิดความเสียกับธุรกิจเนื่องจากภัยคุกคามทางไซเบอร์นั้น สิ่งที่ผู้ทำประกันต้องดำเนินการทันทีคือ เมื่อเกิดความเสียหายผู้เอาประกันภัยควรรีบแจ้งบริษัทประกันภัยโดยเร็วที่สุด จากนั้นบริษัทประกันภัยจะทำการส่งทีมผู้เชี่ยวชาญด้าน IT เข้าไปประเมินสถานการณ์ความเสียหายของธุรกิจ หากความเสียหายที่เกิดขึ้นอยู่ภายใต้ความคุ้มครองกรมธรรม์ ประกันภัยก็จะดำเนินเรื่องการชดใช้ค่าสินไหมทดแทนต่อไปตามขั้นตอนของการพิจารณาค่าสินไหมทดแทน

> ***Cyber Insurance จะให้ความคุ้มครองความเสียหายทางการเงิน ของผู้เอาประกันภัยที่เกิดขึ้นจากการถูกโจมตีระบบ การถูกแอบเข้าระบบโดยไม่ได้รับอนุญาต และการที่ข้อมูลรั่วไหลออกไปสู่บุคคลภายนอก และยังคุ้มครองถึงความรับผิดต่อบุคคลภายนอก ที่ได้รับผลกระทบจากการที่ข้อมูลรั่วไหลออกไป***

พุทธรัตน์ ศรีพร้อม

นายพุทธรัตน์กล่าวต่อว่า เนื่องจากโลกในยุคปัจจุบันที่ทุกภาคส่วนต่างพึ่งพาระบบคอมพิวเตอร์และ Internet ในการทำงานมากขึ้น ดังนั้น ประกันภัยชนิดนี้จึงเหมาะสมกับทุกองค์กร ไม่จำกัดเฉพาะแค่ธุรกิจสถาบันการเงิน หรือธุรกิจบริการเท่านั้น โดยแต่ละประเภทสามารถใช้กรมธรรม์ประกันภัย Cyber Insurance นี้ไปเป็นเครื่องมือบริหารความเสี่ยงด้าน Cyber Security ขององค์กรได้ โดยสามารถแบ่งกลุ่มลูกค้าออกเป็น 2 กลุ่มคือ กลุ่มลูกค้ารายบุคคลและกลุ่มลูกค้าองค์กร

สำหรับกลุ่มลูกค้าองค์กรนั้น บริษัทได้นำเสนอแพ็กเกจความคุ้มครองได้ไม่ต่ำกว่า 500 ล้าน 750 ล้านบาท และ 1,000 ล้านบาท ขึ้นอยู่กับความต้องการของลูกค้าเป็นหลักว่าต้องการความคุ้มครองในระดับใด อัตราเบี้ยประกันเท่าไหร่ ซึ่งขณะนี้มีลูกค้า 2 รายที่ตัดสินใจทำประกันไซเบอร์กับบริษัทแล้ว เพื่อลดความเสี่ยงจากการถูกแฮ็กข้อมูล และข้อมูลรั่วไหลออกไปยังบุคคลภายนอก

ในส่วนของกลุ่มลูกค้ารายบุคคล ขณะนี้ยังไม่มีความชัดเจนของรูปแบบกรมธรรม์และความคุ้มครองซึ่งอยู่ระหว่างการพัฒนาให้เหมาะสมกับความต้องการของลูกค้า ขณะที่ในต่างประเทศมีการนำเสนอกรมธรรม์ไซเบอร์มานานแล้ว ส่วนในแถบเอเชียมีเพียงสิงคโปร์และฮ่องกงเท่านั้นที่มีการนำเสนอกรมธรรม์ไซเบอร์ให้กับลูกค้ารายบุคคล เนื่องจากทั้งสองประเทศมีฐานลูกค้าที่สามารถเข้าถึงไอทีและการทำธุรกรรมออนไลน์อย่างกว้างขวาง จึงมองว่าการซื้อกรมธรรม์ไซเบอร์มีความจำเป็นและสามารถตอบสนองความต้องการของลูกค้าได้เป็นอย่างดี

สำหรับกรมธรรม์ไซเบอร์ที่ให้ความคุ้มครองลูกค้ารายบุคคลในต่างประเทศนั้น ส่วนใหญ่จะเป็นการให้ความคุ้มครองความสูญหายของข้อมูลบัตรเครดิต เช่น ลูกค้านำบัตรเครดิตไปรูดจ่ายค่าสินค้าในร้านค้าและถูกดูดข้อมูลของบัตรหรือบัตรถูกขโมยไป เป็นต้น โดยอัตราเบี้ยประกันของกรมธรรม์ไซเบอร์สำหรับรายย่อยในกรณีดังกล่าวจะมีอัตราเบี้ยประกันประมาณ 300-400 ดอลลาร์สหรัฐ โดยได้รับความคุ้มครองวงเงิน 50,000 ดอลลาร์สหรัฐ

ล่าสุดที่เกิดภัยคุกคามไซเบอร์จากวอนนาคราย นอกจากจะทำให้เกิดความเสียหายกับระบบคอมพิวเตอร์ของธุรกิจแล้ว ยังมีการโจมตีไปยังกลุ่มลูกค้ารายบุคคลจนได้รับความเสียหายด้วยโดยถูกแฮ็กเกอร์ส่งวอนนาคราย เข้าไปโจมตีระบบจนข้อมูลเกิดความเสียหาย พร้อมกับเรียกค่าไถ่ 300-2,000 ดอลลาร์สหรัฐ เพื่อรักษาฐานข้อมูล ซึ่งบางรายก็ยอมจ่ายค่าไถ่เพราะเป็นข้อมูลสำคัญ แต่บางรายก็ไม่ยอมจ่ายแต่ตัดสินใจทำระบบป้องกันใหม่เพื่อป้องกันไม่ให้ข้อมูลถูกคุกคามในอนาคต

"เหตุการณ์ที่เกิดขึ้น นอกจากจะทำให้ผู้ทำประกันเริ่มเห็นถึงความสำคัญของกรมธรรม์ไซเบอร์แล้ว บริษัทประกันภัยในต่างประเทศก็เริ่มมองหามาตรการที่จะเข้ามาช่วยดูแลเพื่อปรับปรุงเงื่อนไขความคุ้มครองให้เหมาะสมกับการจู่โจมทางไซเบอร์ที่อาจจะเกิดขึ้นอนาคตได้"

กระตุ้นธุรกิจทำประกันไซเบอร์ ชดเชยความเสียหายหลังถูกโจมตี

นายเสรี กวินรัชตโรจน์ รองกรรมการผู้จัดการ บมจ. โตเกียวมารีนประกันภัย เปิดเผยว่า จากกรณีภัยคุกคามไซเบอร์ที่เกิดขึ้นจากการโจมตีของวอนนาครายและเพทยาที่ทำให้ระบบคอมพิวเตอร์ของธุรกิจเกิดความสูญหายขึ้นนั้น แม้ว่าองค์กรธุรกิจจะมีความเข้าใจแล้วว่าปัจจุบันระบบคอมพิวเตอร์ขององค์กรมีความเสี่ยงที่อาจจะเกิดภัยคุกคามไซเบอร์ได้ และมีการสร้างกำแพงขึ้นมาป้องกันระบบแล้วก็ตาม แต่ก็ยังไม่สามารถที่จะป้องกันความสูญเสียที่เกิดจากภัยคุกคามไซเบอร์ได้

ทั้งนี้ แม้แต่ในต่างประเทศที่มีการป้องกันระบบขององค์กรแล้วเป็นอย่างดี แต่ก็ยังพบการคุมคามอยู่บ่อยครั้ง โดยเฉพาะการรั่วไหลของข้อมูลลูกค้า เช่น การรั่วไหลของข้อมูลบัตรเครดิตจากการคุกคามของเหล่าแฮ็กเกอร์ จนทำให้องค์กรธุรกิจเกิดความเสียหาย ลูกค้าฟ้องร้อง ซึ่งหากองค์กรธุรกิจนั้นไม่ได้มีการทำประกันไซเบอร์ความเสียหายที่เกิดขึ้น ธุรกิจนั้นก็ต้องเป็นผู้รับผิดชอบเองทั้งหมด

อย่างไรก็ตาม หากธุรกิจมีความทำประกันภัยไซเบอร์ไว้เพื่อป้องกันความเสี่ยง แม้จะเกิดความเสียหายจากการถูกคุกคามทางไซเบอร์ ความสูญเสียที่เกิดขึ้นกับบริษัทและบุคคลภายนอกก็จะได้รับความคุ้มครองดูแลจากบริษัทประกันภัย ทำให้ธุรกิจไม่ต้องกังวลเรื่องของค่าใช้จ่ายที่เกิดขึ้น เพราะบริษัทประกันภัยจะเป็นผู้ที่เข้ามาดูแลและรับความเสี่ยงภัยนั้นไว้เอง ดังนั้น ประกันภัยไซเบอร์ จึงเป็นอีกหนึ่งเครื่องมือที่จะเข้ามาช่วยลดภาระทางด้านการเงินของบริษัทได้

โดยบริษัทได้พัฒนากรมธรรม์ไซเบอร์ ซึ่งเป็นการนำกรมธรรม์ที่บริษัทแม่มีการนำเสนอขายอยู่แล้วในต่างประเทศมาปรับปรุงเงื่อนไขให้เหมาะสมกับความต้องการของกลุ่มลูกค้าองค์กรในประเทศไทย โดยกรมธรรม์ไซเบอร์ของบริษัทจะให้ความคุ้มครองใน 2 หมวดหลัก ประกอบด้วย

หมวดที่ 1 คุ้มครองความรับผิดต่อบุคคลภายนอก ซึ่งจะคุ้มครองสำหรับค่าใช้จ่ายที่เกิดขึ้นจากการที่บริษัทถูกผู้ทำประกันฟ้องร้องค่าเสียหายจากการที่ทำให้ข้อมูลส่วนตัวของลูกค้าสูญหายหรือถูกขโมยจากการคุกคามทางไซเบอร์ เช่น ค่าทนายความ ค่าปรับหลังจากที่ศาลตัดสินให้บริษัทต้องชดใช้ให้กับลูกค้าผู้เสียหาย จากการบริหารผิดพลาดของบริษัทจนทำให้ข้อมูลของลูกค้ารั่วไหลออกไปสู่บุคคลภายนอกได้ เป็นต้น

หมวดที่ 2 คุ้มครองผู้รับประกันภัย คุ้มครองค่าใช้จ่ายที่เกิดขึ้นในกรณีที่ข้อมูลมีการรั่วไหลออกไปจากระบบของธุรกิจ แต่เป็นข้อมูลสำคัญที่ธุรกิจต้องนำกลับเข้าสู่ระบบเหมือนเดิม จนทำให้เกิดมีค่าใช้จ่ายในการนำข้อมูลกลับเข้าสู่ระบบ เช่น ระบบของบริษัทถูกแฮ็กเกอร์เข้าโจมตี และลบข้อมูลสำคัญนั้นออกจากระบบทั้งหมด ธุรกิจจำเป็นที่ต้องนำข้อมูลนั้นเข้าไปไว้ในระบบให้เหมือนเดิมโดยการสร้างฐานข้อมูลใหม่กลับเข้าสู่ระบบโดยการจ้างผู้เชี่ยวชาญเข้ามาดำเนินการกู้ข้อมูล การจ้างคนมาคีย์ข้อมูลเพื่อจัดเก็บเข้าสู่ระบบ เป็นต้น ค่าใช้จ่ายเหล่า

นี้ที่เกิดขึ้น ก็จะได้รับความคุ้มครองตามเงื่อนไขของกรมธรรม์ไซเบอร์ด้วย

ขณะเดียวกัน การถูกจู่โจมจากมวอนนาคราย ที่อาศัยช่องโหว่ของวินโดว์ส เข้าไป Encript File (EFS) หรือการเข้ารหัสในระบบขององค์กรธุรกิจจนไม่สามารถเปิดใช้งานระบบได้จนกว่ายอมจ่ายค่าไถ่นั้น หากองค์กรตัดสินใจที่จะจ่ายค่าไถ่เพื่อรักษาข้อมูลเอาไว้ ค่าไถ่ที่จ่ายไปนั้น กรมธรรม์ไซเบอร์ของบริษัทก็จะให้ความคุ้มครองค่าใช้จ่ายที่นำไปจ่ายเป็นค่าไถ่ด้วย

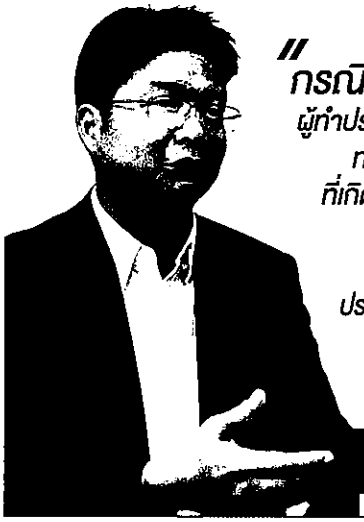
แต่ทั้งนี้ ต้องขึ้นอยู่ความเห็นชอบของผู้เชี่ยวชาญด้านไอทีของบริษัทประกันภัยที่ถูกส่งเข้าไปประเมินความเสียหายจากการถูกโจมตีระบบของบริษัทก่อนว่าองค์กรควรจะต้องจ่ายค่าไถ่ให้กับแฮกเกอร์หรือไม่ หากองค์กรตัดสินใจจ่ายค่าไถ่ให้กับแฮ็กเกอร์ก่อนที่จะได้รับความเห็นชอบจากผู้เชี่ยวชาญด้านไอทีของบริษัทประกันภัย ในส่วนนี้จะไม่ได้รับความคุ้มครองตามเงื่อนไขของกรมธรรม์

นอกจากนี้ กรมธรรม์ไซเบอร์ ยังให้ความคุ้มครองในกรณีที่ซอฟต์แวร์ของระบบถูกรุกล้ำเพื่อนำข้อมูลไปใช้ในทางที่ผิด จนก่อนให้เกิดความเสียหายกับองค์กร เช่น มีการส่งไวรัสเข้าสู่ระบบ เพื่อนำข้อมูลเข้ามาทำอันตรายกับระบบและทำให้ข้อมูลสูญหาย จนทำให้องค์กรต้องจ้างผู้เชี่ยวชาญเข้ามากอบกู้ระบบกลับคืนสู่สภาพเดิม ซึ่งค่าใช้จ่ายในส่วนนี้กรมธรรม์ไซเบอร์ก็ให้ความคุ้มครองด้วย

นายเสรีกล่าวว่า สำหรับองค์กรธุรกิจที่ควรจะต้องทำประกันภัยไซเบอร์นั้น ส่วนใหญ่จะเป็นกลุ่มองค์กรธุรกิจที่มีการเก็บข้อมูลลูกค้า หรือข้อมูลสำคัญ ซึ่งหากข้อมูลรั่วไหลออกไปก็จะทำให้เกิดความเสียหายต่อธุรกิจและฐานลูกค้าได้ รวมถึงธุรกิจอีคอมเมิร์ซ ที่มีการสร้างเซิร์ฟเวอร์เพื่อเก็บข้อมูลในการซื้อขาย หากถูก Ddos Attact ซึ่งเป็นการสร้างทราฟฟิกเข้าไปในเซิร์ฟเวอร์ จนระบบรองรับไม่ไหวจนทำให้ผู้ประกอบการไม่สามารถที่จะขายสินค้าได้ อีกทั้งองค์กรธุรกิจทั่วไปที่มีการนำเทคโนโลยีเข้ามาใช้ในการบริหารจัดการระบบการทำงาน เป็นต้น

โดยในการทำประกันภัยไซเบอร์นั้น สิ่งแรกที่ผู้ประกอบการต้องทำคือ การประเมินความเสี่ยงของธุรกิจตนเองก่อนว่ามีความเสี่ยงภัยด้านไซเบอร์ในเรื่องใดบ้าง ระบบมีการป้องกันเพียงพอหรือไม่ หากเกิดความเสียหายที่ไม่อาจป้องกันได้เกิดขึ้นจะทำให้ธุรกิจเสียหายเท่าไหร่ จากนั้นค้นหาข้อมูลของบริษัทที่ให้บริการประกันภัยไซเบอร์เพื่อศึกษารายละเอียดความคุ้มครองของกรมธรรม์ให้ละเอียด รวมถึงบริการหลังการขายที่สะดวกรวดเร็ว จากนั้นติดต่อไปยังบริษัทประกันภัยที่ผู้ประกอบการให้ความสนใจ

ด้านบริษัทประกันภัย เมื่อได้รับการติดต่อจากผู้ประกอบการที่สนใจทำประกันภัยไซเบอร์แล้ว บริษัทประกันภัยจะส่งทีมพิจารณารับประกันภัยที่บริษัทจัดตั้งขึ้น เพื่อเข้าไปทำการประเมินความเสี่ยงของบริษัท เช่น พิจารณาลักษณะการทำธุรกิจในปัจจุบัน รวมทั้งระบบไอที ว่ามีขั้นตอนการทำงานอย่างไร มีระบบป้องกันข้อมูลที่เพียงพอหรือไม่ เป็นต้น โดยบริษัทประกันภัยจะมีการนำเสนอใบคำขอรับประกันภัยเพื่อให้ผู้ประกอบการทำการกรอกรายละเอียดต่างๆ ของบริษัทอย่างละเอียด เพื่อนำมาใช้ในการพิจารณากำหนดอัตราเบี้ยประกันและความคุ้มครองที่เหมาะสมต่อไป



> "กรณีที่เกิดความเสียหายขึ้น ผู้ทำประกันสามารถเรียกร้องค่าสินไหมทดแทนจากบริษัทประกันภัย ทันทีที่เกิดเหตุขึ้น จากนั้นบริษัทประกันภัยจะส่งทีมสินไหมซึ่งประกอบด้วยผู้เชี่ยวชาญด้านไอทีเพื่อเข้าไปประเมินความเสียหายของระบบพร้อมให้คำแนะนำและจัดการให้ระบบกลับคืนสู่ภาวะปกติให้เร็วที่สุด"
>
> นายเสรี กวินรัชตโรจน์

กรณีที่ผู้ทำประกันเลือกความคุ้มครองที่ไม่สูงมากนัก บริษัทประกันภัยสามารถใช้เพียงข้อมูลที่ผู้ประกอบการกรอกไว้ในใบคำขอเพื่อนำมาใช้ในการพิจารณารับประกันภัย หากผู้ทำประกันมีการดูแลเรื่องของระบบคอมพิวเตอร์ให้มีความปลอดภัยเพียงพอกับความเสี่ยงที่อาจจะเกิดภัยขึ้นกับธุรกิจของตนเองอย่างเพียงพอ ก็จะมีผลต่ออัตราเบี้ยประกัน และความคุ้มครองที่เหมาะสม เช่น ในต่างประเทศนั้นลูกค้ารายย่อยสามารถกรอกข้อมูลประเมินความเสี่ยงของตนเองได้เพื่อทำประกันภัยได้ โดยซื้อความคุ้มครองเริ่มต้นที่ประมาณ 10,000 ดอลลาร์สหรัฐ

แต่ถ้าผู้ทำประกันต้องการความคุ้มครองที่สูงเกินกว่ามาตรฐานที่บริษัทกำหนดไว้ นอกจากข้อมูลในใบคำขอทำประกันภัยแล้ว ทีมพิจารณารับประกันภัยพร้อมผู้เชี่ยวชาญด้านไอทีของบริษัทประกันภัยต้องมีการเข้าไปตรวจสอบระบบภายในของบริษัทเพิ่มเติมด้วย เพื่อนำมาใช้ในการพิจารณารับประกันภัย ซึ่งในการเข้าตรวจสอบระบบนี้จะต้องได้รับความยินยอมจากองค์กรธุรกิจก่อนจึงจะสามารถดำเนินการ

ในกรณีที่เกิดความเสียหายขึ้น ผู้ทำประกันสามารถเรียกร้องค่าสินไหมทดแทนจากบริษัทประกันภัย โดยการแจ้งไปยังบริษัทประกันภัยทันทีที่เกิดเหตุขึ้น ซึ่งประกอบด้วยผู้เชี่ยวชาญด้านไอที เพื่อเข้าไปประเมินความเสียหายของระบบพร้อมให้คำแนะนำและจัดการให้ระบบกลับคืนสู่ภาวะปกติให้เร็วที่สุด

และหากมีค่าใช้จ่ายที่เกิดขึ้นจากการคุกคามทางไซเบอร์ กรมธรรม์ก็จะให้ความคุ้มครองโดยเป็นไปตามเงื่อนไขของกรมธรรม์เป็นหลัก โดยบริษัทจะนำเสนอกรมธรรม์ไซเบอร์ในเดือนสิงหาคม 2560 เป็นต้นไป โดยนำร่องที่ฐานลูกค้าองค์กรของบริษัทก่อนจากนั้นจึงจะขยายตลาดออกไปยังกลุ่มลูกค้าทั่วไป

> *เพื่อเป็นการป้องกันความเสี่ยงที่อาจจะทำให้เกิดความสูญเสียทางธุรกิจอย่างมหาศาล บริษัทจึงเตรียมออกกรมธรรม์ไซเบอร์ (Cyber Insurance) เพื่อเป็นเครื่องมือในการป้องกันความเสี่ยงภัยให้กับองค์กรธุรกิจ*

ดร.อภิสิทธิ์ อนันตนาถรัตน

วางระบบรับประกันไซเบอร์ พร้อมยื่นขออนุมัติ คปภ.

ดร.อภิสิทธิ์ อนันตนาถรัตน กรรมการผู้อำนวยการใหญ่ บมจ.กรุงเทพประกันภัย เปิดเผยว่า ปัจจุบันประชาชนเริ่มตระหนักถึงความเสี่ยงจากการถูกคุกคามทางไซเบอร์มากขึ้น ดังนั้น เพื่อเป็นการป้องกันความเสี่ยงที่อาจจะทำให้เกิดความสูญเสียทางธุรกิจอย่างมหาศาล บริษัทจึงเตรียมออกกรมธรรม์ไซเบอร์ (Cyber Insurance) เพื่อเป็นเครื่องมือในการป้องกันความเสี่ยงภัยให้กับองค์กรธุรกิจ

สำหรับ Cyber Insurance เป็นกรมธรรม์ที่ถูกออกแบบมาเพื่อให้คุ้มครองความรับผิดของผู้ประกอบการ (Business Liability) ในกรณีที่เกิดความเสียหายจากการรั่วไหลของข้อมูลข่าวสาร (Information) ที่ผู้เอาประกันภัยเป็นผู้เก็บรักษาและใช้งานโดยชอบด้วยกฎหมาย ข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคล (Personal Data) ที่เกี่ยวข้องเฉพาะตัวบุคคลหรือที่สามารถบ่งชี้ลักษณะเฉพาะที่เกี่ยวข้องกับตัวบุคคลซึ่งเจ้าของข้อมูล (Data Subject) เป็นบุคคลธรรมดา (Natural Person) โดยความคุ้มครองอาจจะครอบคลุมตั้งแต่ค่าเสียหาย (Damages) ค่าใช้จ่ายในการต่อสู้คดี (Defence Costs) ไปจนถึงค่าใช้จ่ายในการกู้วิกฤติหรือกอบกู้ชื่อเสียงที่เสียไปคืนมา

นอกจากนี้ อาจจะมีการขยายความคุ้มครองไปถึงการสูญเสียรายได้ของผู้ประกอบการจากเหตุการณ์การรั่วไหลของข้อมูลดังกล่าว และอาจจะรวมถึงความรับผิดอื่นๆ ที่เกิดจากการใช้สื่อออนไลน์ การที่ข้อมูลถูกทำลาย อาชญากรรมทางคอมพิวเตอร์ (Computer Fraud) การถูกหลอกให้โอนเงินทางอิเล็กทรอนิกส์ (Fund Transfer Loss) หรือ การถูกคุกคามหรือถูกโจมตีทางไซเบอร์ (Cyber Extortion) โดย บริษัทอยู่ระหว่างการขออนุมัติกรมธรรม์จากสำนักงาน คปภ.

ประชาชนตระหนักภัยไซเบอร์ คาดอัตราเบี้ยประกันลดลง

ดร.จุฑาทอง จารุมิลินท เลขาธิการสำนักงานอัตราเบี้ยประกันวินาศภัย เปิดเผยว่า ปัจจุบันประเทศไทยได้มีการนำเอาเทคโนโลยีเข้ามาช่วยในการบริหารจัดการระบบการทำงานขององค์กรมากขึ้น จนบางครั้งอาจจะไม่ได้ระวังว่าบนความก้าวหน้าของเทคโนโลยียังมีภัยคุกคามที่เรียกว่า ภัยจากไซเบอร์ ซ้อนเร้นอยู่ ซึ่งที่ผ่านมาภัยคุกคามดังกล่าวได้สร้างความเสียหายทางเศรษฐกิจอย่างต่อเนื่องไปทั่วโลก

ทั้งนี้ จากการศึกษาของ Lloyd ในตลาดของเอเชียตะวันออกเฉียงใต้ พบว่า มูลค่าความเสียหายที่เกิดขึ้นจากภัยจากไซเบอร์นั้น มีมูลค่าเกือบเทียบเท่าความเสียหายจากภัยแล้งเลยทีเดียวและความเสียหายอาจจะเริ่มทวีความรุนแรงมากขึ้นและกระจายเป็นวงกว้างในอนาคต เนื่องจากปัจจุบันมีการเชื่อมต่อผ่านช่องทางดิจิทัลต่างๆ แพร่กระจายไปทั่วโลกโดยไม่จำกัดอยู่เพียงประเทศใดประเทศหนึ่ง หรือภูมิภาคใดภูมิภาคหนึ่ง

ดังนั้น บริษัทประกันภัยในฐานะที่เป็นผู้บริหารจัดการความเสี่ยง จึงได้เริ่มมีการศึกษาประเมินความเสี่ยงและผลกระทบที่เกิดขึ้นและมีการพัฒนาผลิตภัณฑ์ประกันภัยที่เรียกว่า กรมธรรม์ประกันภัยไซเบอร์ขึ้น เพื่อให้ความคุ้มครองแก่ผู้ที่จะได้รับความเสี่ยงดังกล่าว โดยจะให้ความคุ้มครองเกี่ยวกับ การสูญเสียทางการเงิน การต่อสู้คดี การกู้คืนข้อมูล และความรับผิดต่อบุคคลภายนอก

ซึ่งในปัจจุบันได้มีบริษัทประกันภัยยื่นขอรับความเห็นชอบแบบและข้อความของกรมธรรม์ประกันภัยไซเบอร์กับสำนักงาน คปภ. เพื่อออกขายผลิตภัณฑ์ดังกล่าวแล้ว และคาดว่าในอนาคตจะมีจำนวนบริษัทที่ยื่นขอรับความเห็นชอบกรมธรรม์ประกันภัยดังกล่าวเพิ่มมากขึ้น ซึ่งถือเป็นแนวโน้มที่ดีขึ้นอีก

ทั้งนี้ จากการติดตามความเสียหายที่เกิดขึ้นจากภัยคุกคามไซเบอร์ในปี 2559 จากตลาดประกันภัยทั่วโลก มีมูลค่าความเสียหายประมาณ 3,500 ล้านดอลลาร์สหรัฐ ซึ่งจากรายงานความเสียหายจากภัยคุกคามไซเบอร์ เมื่อเดือนมิถุนายน 2560 คาดว่าความเสียหายน่าจะอยู่ที่ประมาณ 4,000 ล้านดอลลาร์สหรัฐ อย่างไรก็ตาม การที่ประชาชนและผู้ประกอบการเริ่มตระหนักถึงความเสี่ยงภัยมากขึ้น อีกทั้งองค์กรธุรกิจมีการลงทุนสร้างระบบรักษาความปลอดภัยที่ดีขึ้น จึงทำให้ในอนาคตแนวโน้มอัตราเบี้ยประกันภัยจะมีการปรับลดลงกว่าในปัจจุบัน

ดร.จุฑาทองแนะนำว่า สำหรับผู้ที่ต้องการจะทำประกันภัยไซเบอร์นั้น สิ่งแรกคือต้องทำการประเมินระบบการบริหารจัดการภายในองค์กรของตนเองก่อน ว่ามีการป้องกันระบบคอมพิวเตอร์ที่ปลอดภัยเพียงพอหรือไม่ เนื่องจากจะมีผลต่อการคำนวณอัตราเบี้ยประกันภัย และความคุ้มครองจากบริษัทประกันภัย หากมีการป้องกันที่เพียงพอก็จะทำให้จ่ายเบี้ยถูก

ดร.จุฑาทอง จารุมิลินท

> **"จากการติดตามความเสียหายที่เกิดขึ้นจากภัยคุกคามไซเบอร์**
> *ในปี 2559 จากตลาดประกันภัยทั่วโลก มีมูลค่าความเสียหายประมาณ 3,500 ล้านดอลลาร์สหรัฐ ซึ่งจากรายงานความเสียหายจากภัยคุกคามไซเบอร์เมื่อเดือนมิถุนายน 2560 คาดว่าความเสียหายน่าจะอยู่ที่ประมาณ 4,000 ล้านดอลลาร์สหรัฐ"*

กว่าระบบที่ไม่มีการป้องกันที่เพียงพอซึ่งที่ผ่านมาการประกันความเสี่ยงด้านอิเล็กทรอนิกส์ อัตราเบี้ยประกันอยู่ที่ประมาณ 0.1-10% ของวงเงินความคุ้มครอง

กรณีที่ผู้ทำประกันต้องการให้กรมธรรม์คุ้มครองกรณีธุรกิจหยุดชะงักด้วยนั้น ผู้ทำประกันต้องให้ข้อมูลแก่บริษัทประกันภัยด้วยว่าหากเกิดความเสียหายขึ้นจะสามารถฟื้นฟูธุรกิจให้กลับสู่สภาวะปกติได้ภายในระยะเวลาเท่าไหร่ เช่น ภายใน 3 เดือน 6 เดือน หรือ 12 เดือน เป็นต้น ซึ่งระยะเวลาที่ผู้ทำประกันกำหนดบริษัทประกันภัยจะนำมาใช้ในการคำนวณอัตราเบี้ยประกันภัยด้วย หากธุรกิจใช้ระยะเวลาในการฟื้นฟูกิจการนาน อัตราเบี้ยประกันภัยก็จะสูงขึ้นกว่าการฟื้นฟูธุรกิจได้ในระยะเวลาที่น้อยกว่า อย่างไรก็ตาม บริษัทประกันภัยจะจำกัดความคุ้มครองสำหรับธุรกิจหยุดชะงักไว้ไม่เกิน 2 ปีเท่านั้น

จากนั้นจึงดำเนินการเลือกบริษัทประกันภัย ศึกษารายละเอียดความคุ้มครอง บริการที่จะได้รับหลังการขายจากบริษัทประกัน ขั้นตอนการรับประกันภัย การเรียกร้องค่าสินไหมทดแทนที่สะดวกรวดเร็ว ทีมงานผู้เชี่ยวชาญที่มีประสบการณ์ เป็นต้น

ปัจจุบัน กลุ่มลูกค้าประกันภัยไซเบอร์ แบ่งเป็น 2 กลุ่มคือ กลุ่มลูกค้าองค์กร และกลุ่มลูกค้ารายบุคคล โดยในประเทศไทยนั้น กลุ่มลูกค้าหลักคือ กลุ่มลูกค้าองค์กรธุรกิจ เนื่องจากเป็นกลุ่มที่มีความเข้าใจถึงความเสี่ยงในการถูกคุกคามจากภัยไซเบอร์ โดยมองว่าการทำประกันภัยไซเบอร์คุ้มค่ากับการลงทุนเพื่อนำมาใช้ในการบริหารความเสี่ยงทางธุรกิจหากเกิดความเสียหายจากการภัยไซเบอร์ในอนาคต

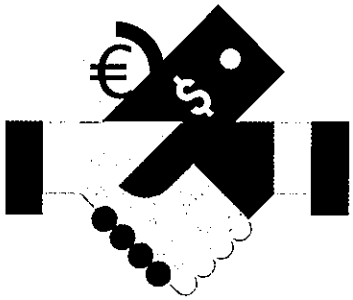
ส่วนกลุ่มรายย่อยนั้น ได้มีการนำเสนอกรมธรรม์ไซเบอร์สำหรับรายบุคคลแล้วในประเทศสิงคโปร์ โดยเป็นการประกันความเสี่ยงด้านการสื่อสาร (Cyber Protector) ของ แอ็กซ่า ประกันภัย สิงคโปร์ ซึ่งเป็นการประกันความเสี่ยงแบบออนไลน์ครั้งแรกในสิงคโปร์ เพื่อคุ้มครองบุคคลและครอบครัวในกรณีที่มีการละเมิดทางออนไลน์โดยบุคคลที่สาม

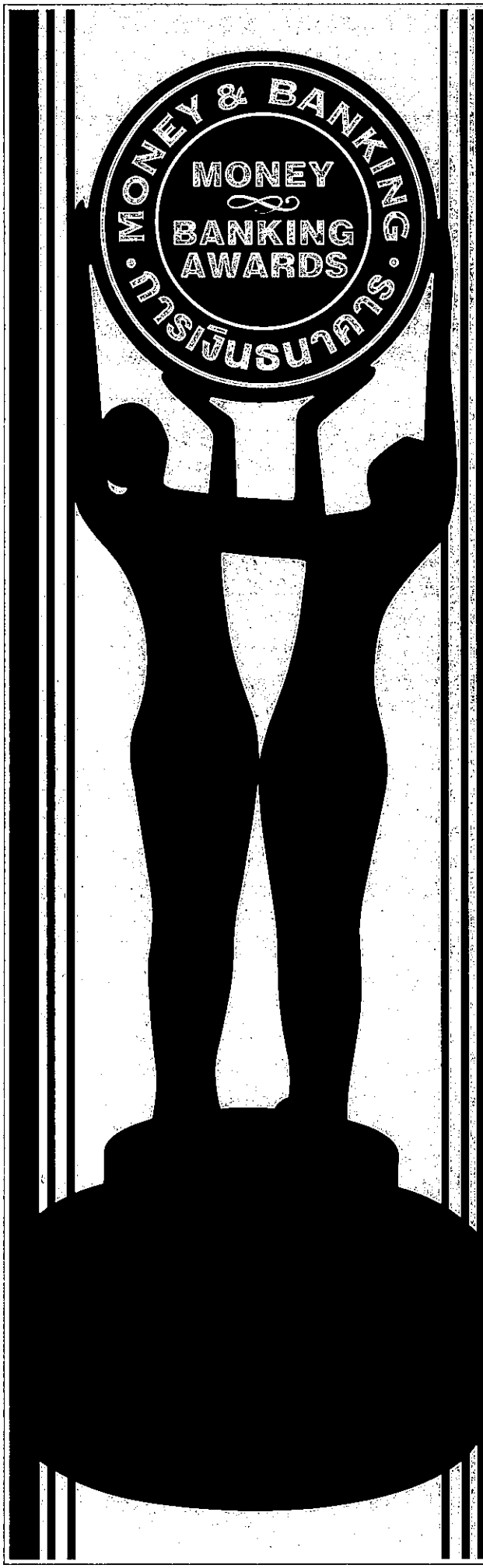
โดยให้ความคุ้มครองทางกฎหมาย ที่ให้ผู้ทำประกันสามารถปรึกษาด้านกฎหมายผ่านทางโทรศัพท์ได้ และหากจำเป็นต้องฟ้องร้องก็จะจัดหาตัวแทนทางกฎหมายเพื่อดำเนินคดีกับบุคคลที่สาม, คุ้มครองความเสียหายต่อ E-Reputation โดยให้ผู้เชี่ยวชาญด้าน IT ลบหรือระงับเนื้อหาและจัดให้ผู้ทำประกันปรึกษานักจิตวิทยาหากเกิดความเครียด

ส่วนกรณีเกิดการโจรกรรมข้อมูลและเกิดค่าใช้จ่ายที่ไม่ได้มาจากการใช้จ่ายของผู้ทำประกัน บริษัทประกันภัยจะชำระคืนค่าใช้จ่ายนั้นให้กับผู้ทำประกัน รวมทั้งจ่ายคืนค่าซื้อสินค้าโดยไม่ได้รับอนุญาตและคืนค่าใช้จ่ายของผู้ทำประกันในการแก้ไขปัญหาที่เกิดขึ้นกับธนาคาร และหากเกิดข้อพิพาทกับร้านค้าออนไลน์ บริษัทประกันภัยจะคืนค่าใช้จ่ายสำหรับการซื้อสินค้าออนไลน์ของผู้ทำประกันที่ไม่ได้จัดส่ง หรือส่งมอบชำรุด หรือส่งมอบอย่างไม่ถูกต้องให้กับผู้ทำประกัน

โดยผู้ที่มีสิทธิ์ในการสมัคร Cyber Protector นั้น ต้องมีเอกสารประจำตัวของสิงคโปร์ที่ถูกต้อง เช่น Singapore NRIC, วีซ่าการพำนัก, ใบอนุญาตทำงาน, บัตรเข้าชมงานระยะยาว หรือบัตรนักเรียนที่พำนักในสิงคโปร์ ซึ่งในการเรียกร้องค่าสินไหมทดแทน ต้องดำเนินการภายใน 6 เดือน หลังจากถูกคุกคามทางไซเบอร์

ขณะที่กลุ่มลูกค้ารายบุคคลในประเทศไทยนั้น มองว่ายังไม่ได้รับความสนใจมากนัก เนื่องจากอัตราเบี้ยประกันภัยที่สูง อีกทั้งระบบป้องกันภัยของคอมพิวเตอร์ส่วนบุคคลยังไม่เพียงพอที่จะได้รับความคุ้มครองจากประกันภัย Ⓜ





MONEY & BANKING AWARDS 2017