คปภ. มุ่งพัฒนาความมั่นคงด้าน IT! เตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์

• เลขาธิการนำทีมผู้บริหารระดับสูงเข้ารับการอบรมหลักสูตร Information Security Awareness Training for Management

ดร.สุทธิพล ทวีชัยการ เลขาธิการคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) เปิดเผยว่า ปัจจุบันสภาพแวดล้อมของธุรกิจการเงินมีความละเอียดซับซ้อน และมีแนวโน้มถูกขับเคลื่อนโดยเทคโนโลยีมากยิ่งขึ้น ซึ่งสำหรับธุรกิจประกันภัยนั้น ยุคดิจิทัลนำมาซึ่งโอกาสและความท้าทาย อุตสาหกรรมประกันภัยต้องเร่งปรับตัวเพื่อให้สามารถก้าวทันนวัตกรรม ความเสี่ยง และภัยคุกคามใหม่ๆ ที่เกิดขึ้น อีกทั้งยังต้องมีการเฝ้าระวัง และวางมาตรการรับมือกับการเปลี่ยนแปลงของเทคโนโลยีอย่างรัดกุม โดยเฉพาะอย่างยิ่งการกำกับดูแลเรื่องการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management) เพราะในอนาคตอันใกล้ปริมาณข้อมูลด้านการประกันภัยจะเพิ่มขึ้นอย่างรวดเร็ว จึงจำเป็นต้องมีการบริหารจัดการด้านความปลอดภัยของข้อมูลที่ดีและเป็นระบบเพื่อให้ประชาชนเกิดความเชื่อมั่นต่อระบบประกันภัย

ทั้งนี้ สำนักงาน คปภ. ให้ความสำคัญและดำเนินมาตรการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งพัฒนาระบบการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างต่อเนื่อง โดยล่าสุดเมื่อวันที่ 1 สิงหาคม 2561 สำนักงาน คปภ. ได้จัดอบรมหลักสูตร “Information Security Awareness Training for Management” โดยเลขาธิการ คปภ. ได้เป็นประธานเปิดการอบรม พร้อมเข้ารับการอบรมร่วมกับผู้บริหารของสำนักงาน คปภ. ซึ่งการอบรมในครั้งนี้มีวัตถุประสงค์เพื่อพัฒนาองค์ความรู้ด้านการพัฒนาระบบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่สมัย มีแนวทางที่ชัดเจนสามารถปฏิบัติได้อย่างเป็นระบบ เป็นไปตามมาตรฐานสากล และง่ายต่อการตรวจสอบ รวมถึงสร้างความตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของระบบสารสนเทศ และข้อมูลสารสนเทศ โดยได้รับเกียรติจาก อาจารย์ปริญญา หอมเอนก ประธาน และผู้ก่อตั้ง ACIS Professional Center Co., Ltd. เป็นวิทยากร

เลขาธิการ คปภ. กล่าวต่อว่า ภัยคุกคามทางไซเบอร์เป็นสิ่งที่ สำนักงาน คปภ. ไม่สามารถมองข้ามได้เนื่องจากถือเป็นภัยที่พัฒนารูปแบบขึ้นตามยุคสมัยส่งผลกระทบรุนแรงในวงกว้าง ดังจะเห็นตัวอย่างได้จากกรณีข้อมูลรั่วไหล (Data breach) ที่เพิ่งเกิดขึ้นของทางธนาคารขนาดใหญ่ 2 ธนาคาร โดยธนาคารแห่งประเทศไทยได้ออกมาแถลงข่าวในเวลาที่เหมาะสม และมีมาตรการรับมือที่ชัดเจนรวดเร็วทันต่อเหตุการณ์ ในส่วนของสำนักงาน คปภ. เองได้ตระหนักถึงภัยคุกคามทางไซเบอร์ และจัดเตรียมแผนรับมือภัยคุกคามไซเบอร์ (Incident response plan) จึงได้มีหนังสือถึงสมาคมประกันชีวิตไทยและสมาคมประกันวินาศภัยไทยให้ติดตามเฝ้าระวังและเตรียมพร้อมรับมือกับภัยไซเบอร์ รวมถึงรายงานผลกระทบต่อสำนักงาน คปภ. อย่างใกล้ชิดทั้งนี้เพื่อสร้างความเชื่อมั่น ลดผลกระทบต่อภาคอุตสาหกรรมประกันภัย

“การสร้างความตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของระบบสารสนเทศ และข้อมูลสารสนเทศ์ ครั้งนี้มุ่งเน้นการพัฒนาความรู้ในเรื่องภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น 3 ระดับ ระดับแรกคือ Information Security ซึ่งหากหน่วยงานได้รับการรับรองตามมาตรฐานสากล ISO27001 แล้วก็จะถือว่าเป็นหน่วยงานที่มีความปลอดภัยของข้อมูล โดยสำนักงาน คปภ. ได้รับการรับรองตามมาตรฐานสากลดังกล่าวแล้วตั้งแต่ปี 2557 และได้มีการตรวจติดตามเพื่อรับรองตามมาตรฐานเป็นประจำทุกปี รวมทั้งออกประกาศเรื่องหลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัย และการชดใช้เงินตามสัญญาประกันภัย โดยใช้วิธีการทางอิเล็กทรอนิกส์ ตั้งแต่ปี พ.ศ. 2560 ซึ่งสำนักงาน คปภ. ได้กำหนดหลักเกณฑ์และวิธีการให้บริษัทหรือตัวแทน หรือนายหน้าประกันภัย หรือธนาคาร ที่ใช้วิธีการเสนอขายผ่านช่องทางดังกล่าวต้องปฏิบัติ ซึ่งนอกจากผู้ขายจะต้องมีนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเป็นส่วนตัวและข้อมูลส่วนบุคคลแล้ว ยังต้องจัดให้มีการตรวจรับรองระบบสารสนเทศจากผู้ตรวจสอบอิสระที่ได้รับใบอนุญาต หรือโดยหน่วยงานรับรองระบบสารสนเทศ (Certified Body) รวมถึงต้องขึ้นทะเบียนกับ สำนักงาน คปภ. ก่อนดำเนินธุรกรรมด้วย เพื่อให้มั่นใจว่าวิธีการเสนอขายผ่านช่องทางอิเล็กทรอนิกส์จะมีมาตรฐานการรักษาความมั่นคงปลอดภัย ระดับสองคือ Cybersecurity เป็นการดำเนินการที่เข้มข้นด้านการป้องกันภัยคุกคามทางไซเบอร์โดยอ้างอิงมาตรฐานสากล “NIST Cybersecurity Framework” ประกอบด้วย Identify Protect Detect Response และ Recover ต้องมีการทำ Penetration Testing และ Source Code Review โดยแนวปฏิบัติดังกล่าวตนได้ให้ความเห็นชอบแนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity) ให้บริษัทประกันภัยนำไปใช้ปฏิบัติแล้วตั้งแต่วันที่ 28 ธันวาคม 2560 และระดับสามคือ Cyber Resilience กล่าวคือเมื่อโดนโจรกรรมข้อมูลแล้วองค์กรยังสามารถดำเนินกิจการได้อย่างต่อเนื่อง ดังนั้น กรมธรรม์คุ้มครองไซเบอร์อาจเรียกได้ว่าเป็นโอกาสของภาคอุตสาหกรรมประกันภัย หากได้มีการ Paradigm Shift ที่เปลี่ยนจาก Preventive เป็น Responsive ได้อย่างรวดเร็ว และเหมาะสม” เลขาธิการ คปภ. กล่าวในตอนท้าย