ประเด็นทางกฎหมายจากการโจมตีโดยแรนซัมแวร์ในประเทศไทย[1]

Legal Issues in Thailand Raised by RANSOMWARE ATTACKS

Article contributed by HUNTON& WILLIAMS

ในช่วงหลายเดือนที่ผ่านมา ระบบคอมพิวเตอร์ในกว่า 150 ประเทศทั่วโลกได้รับผลกระทบจากการโจมตีทางไซเบอร์ขนานใหญ่โดยแรนซัมแวร์ (Ransomware) ที่รู้จักกันในชื่อ "WannaCry" และ "Petya" โดยส่งผลกระทบเป็นวงกว้างต่ออุตสาหกรรมต่าง ๆ รวมถึง กลุ่มธุรกิจโรงพยาบาล ระบบสาธารณูปโภค และหน่วยงานของรัฐทั่วโลก ซึ่งการทำงานของแรนซัมแวร์ดังกล่าวนี้จะเข้ายึดข้อมูลในระบบคอมพิวเตอร์ด้วยการเข้ารหัสไฟล์เป้าหมายผ่านช่องโหว่ของระบบปฏิบัติการวินโดวส์ (Windows) จากนั้นจึงเรียกค่าไถ่เพื่อแลกเปลี่ยนกับกุญแจที่ใช้สำหรับถอดรหัสไฟล์ที่ถูกเข้ารหัสไว้ ซึ่งหากผู้ใช้คอมพิวเตอร์ไม่ชำระค่าไถ่ภายในเวลาที่กำหนด แรนซัมแวร์ก็จะลบไฟล์ดังกล่าวทั้งหมด

การโจมตีโดยแรนซัมแวร์นั้น เป็นหนึ่งในการโจมตีทางไซเบอร์ที่เกิดขึ้นเมื่อไม่นานมานี้ และเป็นประเด็นทางกฎหมายต่อกิจการและอุตสาหกรรมต่าง ๆ ซึ่งต้องอาศัยการเข้าถึงข้อมูลในระบบคอมพิวเตอร์เป็นเครื่องมือหลักในการประกอบธุรกิจ โดยเฉพาะบริษัทที่ให้บริการทางด้านการเงินและสุขภาพ ซึ่งต้องการความสมบูรณ์และความน่าเชื่อถือของข้อมูลและความพร้อมในการใช้งานข้อมูลเป็นสำคัญในการประกอบธุรกิจ

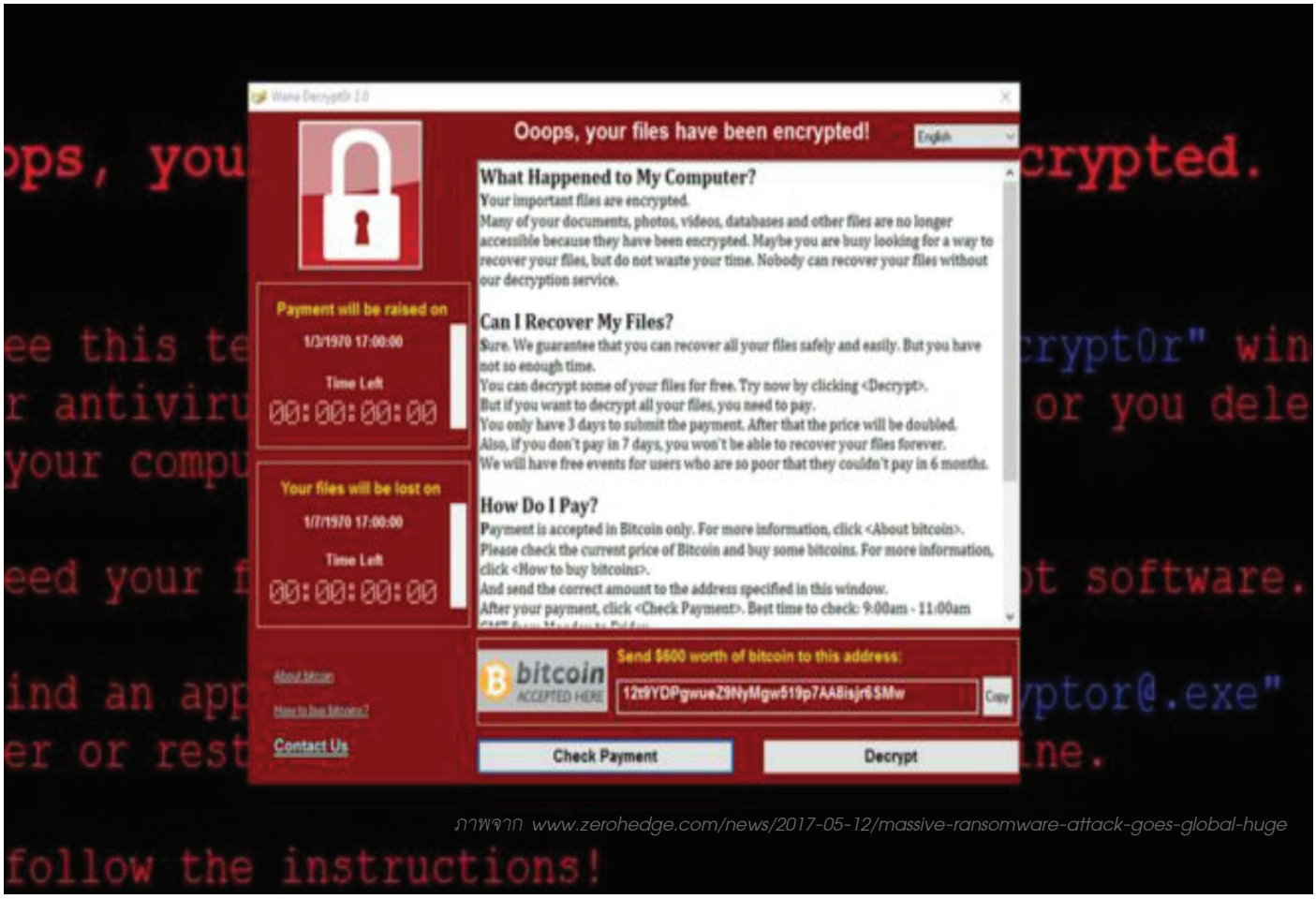
เพื่อทำความเข้าใจและเตรียมพร้อมในการรับมือกับความเสี่ยงที่อาจจะเกิดขึ้นจากการโจมตีของแรนซัมแวร์องค์กรต่าง ๆ ที่อาจได้รับผลกระทบจึงควรพิจารณาประเด็นสำคัญทางกฎหมายดังต่อไปนี้

ข้อพิจารณา

กฎหมายที่เกี่ยวข้อง

หน่วยงานกำกับดูแลด้านการแข่งขันทางการค้าในประเทศสหรัฐอเมริกา (Federal Trade Commission, FTC) ได้อาศัยอำนาจตามมาตรา 5 แห่งรัฐบัญญัติคณะกรรมการการแข่งขันทางการค้า (Federal Trade Commission Act) ในการดำเนินการเกี่ยวกับ "**การกระทำหรือการปฏิบัติการซึ่งไม่เป็นธรรมหรือเป็นการหลอกลวง**" เพื่อจัดการปัญหาที่เกี่ยวข้องกับความเป็นส่วนบุคคลและความปลอดภัยของข้อมูล กล่าวคือ หลักการเกี่ยวกับการหลอกลวง (Deceptive Doctrine) นั้นเป็นหลักที่ใช้ในการดำเนินการกับบริษัทที่ให้ข้อมูลเกี่ยวกับการนำข้อมูลส่วนบุคคลไปใช้อย่างไม่ถูกต้องหรือการใช้มาตรการเพื่อป้องกันข้อมูลส่วนบุคคลเหล่านั้น ส่วนหลักการความไม่เป็นธรรม (Unfairness Doctrine) นั้น เป็นหลักที่ใช้ในการดำเนินการกับบริษัทที่ไม่ได้ใช้มาตรการที่ดีเพียงพอในการป้องกันก่อนที่เหตุการณ์ที่กระทบต่อความปลอดภัยจะเกิดขึ้น (โดยไม่คำนึงถึงคำรับรองของบริษัท) จะเห็นได้ว่าสหรัฐอเมริกาให้ความสำคัญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างมาก อย่างไรก็ดี ประเทศไทยยังไม่มีกฎหมายในลักษณะข้างต้นดังนั้นผู้เสียหายที่ได้รับผลกระทบจากการที่บริษัทดังกล่าวไม่สามารถรักษาข้อมูลส่วน

[1] บทความนี้ได้รับการปรับปรุงจากต้นฉบับที่เผยแพร่ครั้งแรกใน Law360 โดยบทความต้นฉบับเขียนโดย ฮันตัน แอนด์ วิลเลี่ยมส์ โดย Lisa J. Sotto, Brittany M. Bacon, Jeffrey R. Dunifon และได้รับการแปลและปรับปรุงให้สอดคล้องกับกฎหมายไทย โดยคุณมานิดา ชินเมอร์แมน



ภาพจาก www.zerohedge.com/news/2017-05-12/massive-ransomware-attack-goes-global-huge

บุคคลที่ได้ให้ไว้กับบริษัทนั้น ผู้เสียหายอาจฟ้องเรียกร้องค่าเสียหายได้โดยอาศัยมูลละเมิด หรือมูลสัญญา หรือฟ้องคดีอาญาตามฐานความผิดที่มีกฎหมายกำหนด

สำหรับประเทศไทยมีแนวคิดที่จะกำหนดเรื่องการคุ้มครองข้อมูลส่วนบุคคลโดยการร่างพระราชบัญญัติข้อมูลข่าวสารส่วนบุคคล ซึ่งปัจจุบันยังอยู่ในขั้นตอนพิจารณาทบทวนร่างโดยคณะรัฐมนตรี[2] และได้มีการนำหลักการเกี่ยวกับการหลอกลวง (Deceptive Doctrine) และหลักการความไม่เป็นธรรม (Unfairness Doctrine) ในทำนองเดียวกันกับที่ระบุไว้ในรัฐบัญญัติคณะกรรมการการแข่งขันทางการค้าของประเทศสหรัฐอเมริกามาปรับใช้ เช่น มีการกำหนดห้ามไม่ให้ผู้ควบคุมข้อมูลส่วนบุคคล เก็บรวมรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่กฎหมายกำหนดข้อยกเว้นไว้ และยังต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวมข้อมูล และใช้ข้อมูลนั้นให้เป็นไปตามวัตถุประสงค์ที่แจ้งไว้แก่เจ้าของข้อมูลด้วย นอกจากนี้ ยังได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งหากไม่ปฏิบัติตามที่กฎหมายบัญญัติไว้ ร่างพระราชบัญญัติฉบับดังกล่าวยังได้กำหนดให้สิทธิผู้เสียหายในการเรียกร้องค่าสินไหมทดแทนทางแพ่ง และยังกำหนดโทษทางอาญา รวมทั้งกำหนดค่าปรับทางปกครองสำหรับการไม่ปฏิบัติตามกรณีดังกล่าวด้วย

การแจ้งเตือนเจ้าของข้อมูลในกรณีที่ข้อมูลรั่วไหล

ในประเทศสหรัฐอเมริกาและหลายประเทศทั่วโลกมีการออกกฎหมายกำหนดให้บริษัทหรือหน่วยงานที่เป็นผู้ดูแลข้อมูลส่วนบุคคลแจ้งให้เจ้าของข้อมูลทราบในกรณีที่มีการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลโดยไม่ได้รับอนุญาต สำหรับในประเทศไทยยังไม่มีกฎหมายในเรื่องการแจ้งเตือนดังกล่าวไว้เป็นการเฉพาะ

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ดังที่ได้เรียนมาในข้างต้นว่า ปัจจุบันประเทศไทยอยู่ในระหว่างการพิจารณาทบทวนร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งร่างพระราชบัญญัติดังกล่าว ได้ปรากฏหลักการในการกำหนดมาตรฐานในการจัดเก็บข้อมูลส่วนบุคคล และหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ความรับผิดทางแพ่ง และบทกำหนดโทษทางอาญาของผู้ควบคุมข้อมูลส่วนบุคคล

สำหรับการลงโทษผู้กระทำความผิดนั้นพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม มีบทบัญญัติซึ่งกำหนดโทษให้แก่ผู้เข้าถึงโดยมิชอบ ลวงรู้ ทำลาย ทำให้เสียหาย แก้ไขเปลี่ยนแปลงเพิ่มเติม ทำให้ชะลอ ถูกระงับ ขัดขวางการเข้าถึง รบกวน ซึ่งข้อมูลหรือระบบคอมพิวเตอร์ที่ถูกจัดเก็บโดยมีมาตรการป้องกันการเข้าถึงโดยเฉพาะ อย่างไรก็ดี ในทางปฏิบัติ หากผู้กระทำความผิดอาศัยอยู่ในต่างประเทศก็เป็นการยากที่

[2] ร่างพระราชบัญญัติข้อมูลข่าวสารส่วนบุคคล ได้รับการเสนอต่อสภานิติบัญญัติแห่งชาติเพื่อพิจารณาแล้ว ภายหลังคณะรัฐมนตรีได้มีมติขอถอนเรื่องดังกล่าวกลับมาพิจารณาทบทวนอีกครั้งหนึ่ง

จะนำตัวผู้กระทำความผิดมาลงโทษตามกฎหมายไทยได้

นอกจากนี้ ยังได้มีร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งขณะนี้กำลังอยู่ในระหว่างการพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา ที่กำหนดให้หน่วยงานของรัฐและเอกชนซึ่งเก็บรักษาฐานข้อมูลส่วนตัวของประชาชนจำเป็นจะต้องปฏิบัติตามกฎข้อบังคับที่เกี่ยวข้องซึ่งออกโดยคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หากหน่วยงานรัฐปฏิบัติขัดหรือแย้งต่อแนวทางมาตรการทางความปลอดภัยที่ถูกกำหนดไว้ในร่างพระราชบัญญัตินี้โดยไม่มีเหตุอันสมควร หน่วยงานราชการนั้นจะถูกลงโทษฐานกระทำผิดวินัย ส่วนในกรณีที่เอกชนไม่ปฏิบัติตามแนวทางหรือคำสั่งของพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ จะมีความรับผิดทางอาญา

การฟ้องร้องคดี

ในกรณีการโจมตีของแรนซัมแวร์นั้นอาจส่งผลให้ข้อมูลส่วนบุคคลที่องค์กรจัดเก็บไว้รั่วไหลออกสู่สาธารณะ องค์กรต่าง ๆ จึงไม่อาจหลีกเลี่ยงความเสี่ยงในการถูกฟ้องร้องได้ แม้ว่าการฟ้องร้องคดีต่อองค์กรที่ถูกโจมตีนั้นอาจจะมีขั้นตอนที่ซับซ้อนก็ตาม แต่ทนายความของฝ่ายผู้เสียหายก็มักจะดำเนินคดีในลักษณะที่กระทบต่อภาพลักษณ์ขององค์กร เพราะโดยทั่วไปแล้วองค์กรเหล่านั้นต้องชำระเงินจำนวนมากให้กับผู้เสียหายเพื่อที่จะระงับคดี นอกจากนี้ยังมีความเสี่ยงที่อาจจะโดนฟ้องร้องจากคู่ค้าซึ่งได้รับผลกระทบต่อข้อมูลส่วนบุคคลของตนจากการโจมตีด้วย รวมถึงการต่อสู้กับบริษัทประกันภัยเกี่ยวกับวงเงินความคุ้มครองภายใต้กรมธรรม์ประกันภัย นอกจากนี้องค์กรต่าง ๆ ควรคำนึงถึงกรณีที่ผู้ถือหุ้นฟ้องร้องคดีต่อคณะกรรมการแทนองค์กร หากพิสูจน์ได้ว่าจากความเสียหายจากการถูกโจมตีทางไซเบอร์เกิดจากการที่คณะกรรมการละเว้นการปฏิบัติหน้าที่

สำหรับกฎหมายไทยในปัจจุบัน เนื่องจากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ยังไม่ได้ประกาศใช้เป็นกฎหมายในกรณีที่มีการโจมตีของแรนซัมแวร์และทำให้เกิดการเปิดเผยข้อมูลส่วนบุคคลต่อแก่บุคคลภายนอกนั้น ผู้เสียหายอาจฟ้องร้องผู้เผยแพร่แรนซัมแวร์ได้โดยอาศัยพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้ผู้เผยแพร่แรนซัมแวร์ได้รับโทษทางอาญา รวมถึงอาจฟ้องร้องเป็นคดีแพ่งในมูลละเมิดหรือผิดสัญญาตามหลักทั่วไป ทั้งนี้ หากการเผยแพร่แรนซัมแวร์เกิดขึ้นจากภายนอกราชอาณาจักร ผู้กระทำผิดที่มีสัญชาติไทยและรัฐบาลแห่งประเทศที่มีความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษหรือผู้กระทำความผิดเป็นคนต่างด้าวและรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและได้ร้องขอให้ลงโทษ ผู้เผยแพร่แรนซัมแวร์จะต้องรับโทษในราชอาณาจักรไทย นอกจากนี้ ผู้เสียหายยังอาจฟ้องร้องต่อบริษัทผู้เก็บรักษาข้อมูลส่วนตัวในมูลละเมิด และความผิดตามกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายคุ้มครองข้อมูลส่วนบุคคล เมื่อร่างพระราชบัญญัติดังกล่าวประกาศใช้เป็นกฎหมาย

หลักการกำกับดูแลกิจการที่ดีสำหรับบริษัทจดทะเบียน

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ หรือ ก.ล.ต. ได้ออกหลักการกำกับดูแลกิจการที่ดี (Corporate Governance Code: CG Code) สำหรับบริษัทจดทะเบียนปี 2560 เพื่อเป็นแนวทางสำหรับคณะกรรมการบริษัทจดทะเบียนในการปฏิบัติหน้าที่ โดยในส่วนที่เกี่ยวกับความมั่นคงทางเทคโนโลยีสารสนเทศนั้นได้กำหนดให้ คณะกรรมการควรดูแลให้การบริหารความเสี่ยงขององค์กรครอบคลุมถึงการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และควรจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ตลอดจนกำกับดูแลให้มีระบบการรักษาความปลอดภัยของข้อมูล ซึ่งรวมถึงการกำหนดนโยบายและวิธีปฏิบัติในการรักษาความลับ (Confidentiality) การรักษาความน่าเชื่อถือ (Integrity) และความพร้อมใช้ของข้อมูล (Availability)

การปฏิบัติตามมาตรฐานและแนวทางปฏิบัติที่ดีทางธุรกิจและกลุ่มอุตสาหกรรม

นอกจากการปฏิบัติตามข้อกฎหมายที่กำหนดไว้อย่างชัดเจนแล้ว องค์กรต่าง ๆ ควรตรวจสอบเปรียบเทียบมาตรฐานทางธุรกิจกับการดำเนินงานของตนอย่างสม่ำเสมอ เนื่องจากมาตรฐานทางธุรกิจดังกล่าวจะได้รับการปรับปรุงแก้ไขเพิ่มเติมอย่างต่อเนื่อง เพื่อให้สะท้อนกับสภาวการณ์และข้อเท็จจริงที่เกิดขึ้น อันจะช่วยส่งเสริมให้องค์กรสามารถปรับเปลี่ยนแนวทางในการดำเนินการของตนให้สอดคล้องกับความคาดหวังของผู้บริโภค คู่ค้า และหน่วยงานที่กำกับดูแลได้

แนวทางปฏิบัติที่ดีอาจรวมถึง (1) การแบ่งปันข้อมูลที่เกี่ยวกับสถานการณ์การคุกคาม แนวทางการโจมตี และระบบต่าง ๆ ในขณะนั้นอย่างรอบด้าน (2) การนำการป้องกันพื้นฐานไปปฏิบัติ เช่น การแก้ไขช่องโหว่ที่ปรากฏให้เห็น (3) การออกแบบและการทดสอบวิธีการรับมือและการแก้ไขคืนสู่ภาวะปกติจากเหตุการณ์ละเมิดความปลอดภัย และ (4) การส่งเสริม ช่องทางและการร่วมมือภายในกลุ่มอุตสาหกรรมโดยให้ร่วมมืออย่างสม่ำเสมอและเป็นระเบียบแบบแผนมากขึ้น

ข้อสรุป

การโจมตีจากแรนซัมแวร์เป็นประเด็นที่ได้รับการกล่าวถึงมากขึ้นเรื่อยๆ โดยเฉพาะจากการโจมตีครั้งล่าสุด โดยการโจมตีดังกล่าวเป็นเพียงรูปแบบหนึ่งของการคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ ดังนี้ องค์กรและภาคธุรกิจต่าง ๆ จึงควรคำนึงถึงข้อคิดพิจารณาในเชิงกฎหมายตามที่กล่าวมาข้างต้นเพื่อประโยชน์ในการป้องกัน การตรวจสอบ และการแก้ไขคืนสู่ภาวะปกติจากการโจมตีเหล่านี้อย่างเหมาะสม

During the last few months, the attacks by ransomware named "WannaCry" and "Petya" have hit computers in tens of thousands of computer systems around the globe, including Thailand. A wide range of industries have been impacted by these attacks, including businesses, hospitals, utilities and government entities around the world. Ransomware leverages certain Windows vulnerabilities, encrypts files on infected systems and demands payment in exchange for the decryption key in order to gain access to those files again. If payment is not made within a specified timeframe, the files encrypted would never be recovered.

Ransomware is one of the many types of recent cyberattacks that can have legal implications for affected entities and industries for which data access, integrity and availability are critical; health care and financial companies are particularly vulnerable.

As affected entities work to understand and respond to the threat of ransomware, below is a summary of key legal issues.

Considerations

Legal Landscape

In the United States, the Federal Trade Commission has used its authority under Section 5 of the FTC Act to pursue "unfair or deceptive acts or practices" to address data privacy and security issues. The deception doctrine has been used to pursue companies that misrepresent their use of personal information or the security measures used to protect such data, while the unfairness doctrine has been used to bring actions against companies that fail to employ adequate safeguards prior to a security incident (regardless of the company's representations).

It can be seen that the United States places great importance on protection of personal data. Thailand does not have laws similar to the legislation described above. Nonetheless, where an injured party has been harmed by the release of personal information by a business or other organization, it can sue for damages on such legal grounds as wrongful acts or breach of contract or bring a criminal charge.

Thailand is pushing for laws to protect personal data as embodied by the draft Personal Data Protection Bill, which is under consideration by the Cabinet.[2] The aforementioned draft legislation incorporates the Deceptive Doctrine and the Unfairness Doctrine in the same manner as in the FTC Act, such as a prohibition against allowing data controllers to collect or use personal data without permission from the owner of the data or as permitted by law. There is also a requirement to inform the owner of the data as to the reasons for collecting the data and to use the data for those reasons as stated.

[1] This article has been derived from an article originally published in Law360 by Hunton & Williams lawyers Lisa J. Sotto, Brittany M. Bacon and Jeffrey R. Duniforn. It has been revised to be in conformity with Thai law by Manida Zinmerman.

[2] The draft Personal Data Protection Bill had been presented to the Thai National Legislative Assembly for consideration. Afterwards, the Cabinet rendered a resolution withdrawing the matter back for further consideration and review.

In addition, the draft law requires data controllers to have appropriate data security measures in place to guard against the unauthorized or unlawful loss, access, usage, modification or disclosure of personal data. In terms of penalty for violations, the draft law specifies civil damages for injured parties, criminal penalties and administrative fines.

Breach Notification Laws

In the United States and many countries around the world, there are laws that require data controllers to inform owners of personal data in the event of any breach of such data. As of now, Thailand does not specifically have any such laws in place.

Data Security Laws

As discussed, presently Thailand is considering a draft Data Protection Bill that addresses security measures and rules regarding the storage of personal data, as well as civil and criminal penalties applicable to data controllers.

As for criminals who unlawfully breach personal data, the Computer Crimes Act B.E. 2550 (2007), as amended, enforces penalties against those who unlawfully access personal data guarded by security measures, or who modify or affect its integrity in some manner. In practice, however, it is difficult to prosecute offenders outside of Thailand under the aforementioned law.

The draft Cyber Security and Safety Bill, which is currently being considered by the Council of State, requires government and private entities that store personal data belonging to the public to abide by the rules and regulations issued by the National Cyber Safety and Security Commission. If a government entity is in violation of any rules or regulations under the draft law, it will face punishment in the form of a disciplinary action. However, private entities would face criminal penalties.

Litigation

In the event that ransomware results in a compromise of covered information, litigation is another potential risk. Despite the difficulty of bringing successful lawsuits against affected entities, plaintiffs' lawyers continue to actively pursue newsworthy breaches, as businesses are paying significant amounts in settlements with affected individuals. Affected entities also may face lawsuits from their business partners whose data is involved in the attack, and often battle insurers over coverage of costs associated with the attack. Businesses must also be cognizant of cyber-related shareholder derivative lawsuits, which increasingly follow from catastrophic security breaches.

As for Thai law, since the draft Personal Data Protection Bill has still not been enacted, parties injured by a data breach have the right to file criminal proceedings against those responsible for ransomware attacks on the basis of the Computer Crimes Act. Furthermore, affected parties can file civil proceedings on the basis of wrongful acts or breach of contract. The draft law would also have extraterritorial effect in certain cases, such as where a Thai offender commits the act in a foreign country and the government of the foreign country or the victim files a complaint, or where the offender is not Thai, but the Thai government or a Thai victim files a complaint. In such cases, the offender faces punishment in the Kingdom of Thailand.

Good Corporate Governance

The Securities and Exchange Commission of Thailand, or SEC, has issued rules regarding good corporate governance, i.e., the Corporate Governance Code or CG Code for listed companies in 2017. The aforementioned code serves as a guideline for boards of directors of listed companies in performing their duties. Regarding information technology security, it requires boards of directors to oversee and manage IT-related risks. Furthermore, there is a requirement to put in place policies and security measures about the IT system and storage of data; the rules also incorporate policies and practices on confidentiality, integrity and availability of data.

Industry Standards and Best Practices

In addition to complying with explicit legal requirements, organizations should continually evaluate their practices against industry standards, which typically evolve and are updated more frequently than relevant legislation, and which help organizations better align their practices with the expectations of consumers, business partners and regulators.

Industry standards and best practices may include, among other things: (1) conducting comprehensive information sharing on current threats, attack vectors and the systems within the enterprise; (2) implementing baseline protections such as patching against known vulnerabilities; (3) designing and testing security incident response and recovery efforts; and (4) enhancing communications and collaboration by engaging in more regular and formalized collaboration within the sector.

Conclusion

Ransomware is a growing concern, and while the recent global attacks have been some of the most high profile to date, they are part of an overall trend in the evolving threat landscape. Businesses and other organizations should take into account the legal considerations discussed above in their efforts to prevent, investigate and recover from these disruptive attacks.
