บทความซีรีย์ โควิด-19 กับความปลอดภัยทางข้อมูล
กรณีศึกษาประเทศจีน
ตอนที่ 1 Work From Home แล้วข้อมูลรั่วไหล ใครจะรับผิดชอบ?*

ในช่วงวิกฤตโรคระบาดโควิด-19 หลายเมืองในประเทศจีนได้ประกาศปิดเมือง เพื่อควบคุมการแพร่กระจายของโรคอย่างเข้มงวด โดยนอกจากจะจำกัดการเข้าออกเมืองแล้ว ยังมีการสั่งหยุดพักกิจการ ห้างสรรพสินค้า โรงเรียนทั้งหมด รวมถึงจำกัดการออกนอกที่พักอาศัยของประชาชน ซึ่งทำให้วิถีชีวิตของประชาชนเปลี่ยนแปลงไปอย่างมากโดยเฉพาะการทำงาน การทำงานที่บ้าน หรือ Work From Home จึงกลายเป็นหนทางใหม่ของผู้ประกอบการในการขับเคลื่อนธุรกิจให้เดินหน้าไปในวิกฤตการณ์เช่นนี้

ในบทความตอนนี้ผู้เขียนขอนำเสนอแง่มุมเกี่ยวกับปัญหาด้านความปลอดภัยทางข้อมูลที่ผู้ประกอบการเอกชนของประเทศจีนต้องประสบพบเจอในช่วงที่ต้องทำงานจากบ้าน พร้อมทั้งข้อแนะนำทางกฎหมาย

ใครเป็นผู้รับผิดชอบความปลอดภัย : ระบบที่ใช้ต่างกันผู้รับผิดชอบย่อมต่างออกไป

กฎหมายว่าด้วยความมั่นคงทางไซเบอร์ของประเทศจีน (Cybersecurity Law of the People's Republic of China)[1] กำหนดให้ **"ผู้ให้บริการเครือข่าย"** หรือ Network Operators เป็นผู้มีหน้าที่รับผิดชอบดูแลความปลอดภัยในการให้และใช้บริการผ่านระบบอินเทอร์เน็ต รวมถึงกำกับดูแลความปลอดภัยทางข้อมูลทางไซเบอร์ ซึ่งตามนิยามของกฎหมายนี้ผู้ให้บริการเครือข่ายหมายถึงบุคคลสามกลุ่ม ได้แก่ (1) **เจ้าของสัมปทานเครือข่ายอินเทอร์เน็ต** หรือที่เราเข้าใจกันในนามของ "เจ้าของเสา" ที่ชนะการประมูลสัญญาณ เช่น China Mobile และ China Unicom หรือยกตัวอย่างในประเทศไทย เช่น TOT 3BB True และ AIS (2) **ผู้กำกับดูแลระบบเครือข่ายอินเทอร์เน็ต** ซึ่งหมายถึง ผู้ดูแลระบบเครือข่ายของเจ้าของสัมปทาน สามารถเป็นได้ทั้งหน่วยงานของรัฐและผู้ประกอบการเอกชน เช่น สำนักงานพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารแห่งชาติ

---

*นางสาวพิชชานาถ คำยวง นักกฎหมายกฤษฎีกาปฏิบัติการ กองพัฒนากฎหมาย สำนักงานคณะกรรมการกฤษฎีกา Peking University (LL.B)

บทความนี้ดัดแปลงมาจากบทความ เรื่อง "ดินแดนลี้ลับในเมฆหมอก" ปัญหาความปลอดภัยทางข้อมูลที่ภาคธุรกิจพบบ่อยในช่วงทำงานที่บ้านและคำแนะนำ ("云深不知处"——企业远程办公的网络安全常见问题及建议)

[1]มาตรา 9 ผู้ให้บริการเครือข่ายที่ประกอบกิจการหรือให้บริการต้องปฏิบัติตามกฎหมายกฎระเบียบทางปกครอง เคารพศีลธรรมของสังคม ปฏิบัติตามจรรยาบรรณวิชาชีพ ซื่อสัตย์ สุจริต ปฏิบัติหน้าที่รักษาความมั่นคงทางไซเบอร์ ยอมรับการตรวจสอบจากรัฐและสาธารณะ และรับผิดชอบต่อสังคม

ซึ่งเป็นหน่วยงานของรัฐที่มีอำนาจหน้าที่คล้ายกับ สำนักงาน กสทช. ในประเทศไทย หรือผู้ดูแลระบบเครือข่ายของผู้ประกอบการเอง เช่น ฝ่ายเทคโนโลยีของ China-Unicom รวมถึงเจ้าของเสาเจ้าอื่นๆ และ (3) **ผู้ให้บริการผ่านเครือข่ายอินเทอร์เน็ต** ซึ่งมีความหมายค่อนข้างกว้าง โดยครอบคลุมตั้งแต่ผู้ประกอบการทั้งหมดที่ประกอบกิจการบนเครือข่ายอินเทอร์เน็ต ไม่ว่าจะเป็นเจ้าของเว็บไซต์ เจ้าของโปรแกรม หรือเจ้าของแอปพลิเคชัน รวมทั้งระดับบุคคล เช่น เจ้าของร้านค้าออนไลน์ เจ้าของบทความ เจ้าของความคิดเห็น เจ้าของรูปภาพและสื่ออื่น ๆ ที่นำข้อมูลเข้าสู่โลกออนไลน์ก็ล้วนแต่เป็นผู้ให้บริการผ่านเครือข่ายอินเทอร์เน็ตตามกฎหมายฉบับนี้ทั้งสิ้น

จากขอบเขตของนิยามคำว่า “ผู้ให้บริการเครือข่าย” ตามกฎหมายว่าด้วยความมั่นคงทางไซเบอร์ของประเทศจีนเห็นได้ชัดว่า ไม่ว่าจะเป็นหน่วยงานของรัฐ ผู้ประกอบการหรือประชาชนทั่วไปล้วนแต่มีหน้าที่และความรับผิดชอบต่อการกระทำของตนในโลกไซเบอร์

สำหรับปัญหาที่ว่าใครเป็นผู้มีหน้าที่รับผิดชอบดูแลความปลอดภัยในการให้บริการผ่านระบบอินเทอร์เน็ตรวมถึงกำกับดูแลความปลอดภัยทางข้อมูลในการทำงานที่บ้านนั้นขึ้นอยู่กับกรรมสิทธิ์ในระบบสำนักงานอัตโนมัติ (Office Automation System) ที่ผู้ประกอบการเลือกใช้ในการดำเนินกิจการของตน โดยทั่วไประบบสำนักงานอัตโนมัติสามารถแบ่งออกเป็น 3 ระบบ ได้แก่ (1) ระบบภายในองค์กร (2) ระบบคลาวน์ และ (3) ระบบผสม

(1) ระบบภายในองค์กร

ระบบภายในขององค์กรอาจสร้างขึ้นจากการวิจัยพัฒนาของผู้ประกอบการเองหรือการจ้างผู้ประกอบการอื่นพัฒนาระบบสำนักงานขึ้นมาเพื่อใช้เฉพาะภายในองค์กร รวมถึงการซื้อระบบสำนักงานสำเร็จรูปจากผู้ประกอบการอื่นมาใช้ เช่น บริษัท ก สร้างระบบสำนักงานขึ้นมาใช้เอง หรือบริษัท ก จ้างบริษัท ข ให้สร้างโปรแกรมสำนักงานขึ้นมาใช้สำหรับบริษัท ก โดยเฉพาะ หรือ บริษัท ก ซื้อระบบสำนักงานสำเร็จรูปจากบริษัท ค ซึ่งทำธุรกิจขายระบบสำนักงานสำเร็จรูป ไม่ว่าระบบสำนักงานนั้นจะได้มาโดยวิธีการใด ระบบที่บริษัท ก ใช้ ล้วนจัดว่าเป็นระบบภายในองค์กร นอกจากนี้ ระบบสำนักงานภายในองค์กรจะใช้งานได้ก็ต่อเมื่อผู้ใช้ต้องเชื่อมต่อเครือข่ายอินเทอร์เน็ตภายในขององค์กรเท่านั้น ตัวอย่างเช่น โปรแกรม KSDK Office ระบบสำนักงานอัตโนมัติของสำนักงานคณะกรรมการกฤษฎีกา ที่ต้องใช้งานจาก Wi-Fi ของสำนักงานฯ เท่านั้น แต่ถ้าหากต้องการใช้งานจากอินเทอร์เน็ตภายนอก ผู้ใช้จะต้องเชื่อมต่อ VPN[2] เพื่อเปลี่ยนที่อยู่ IP ให้เสมือนว่ากำลังใช้งานจากอินเทอร์เน็ตภายในองค์กรเสียก่อนจึงสามารถใช้งานระบบสำนักงานได้

---

[2]VPN ย่อมาจาก “Virtual Private Network” หรือที่เรียกว่า “เครือข่ายส่วนตัวเสมือน” เป็นซอฟแวร์ที่ใช้ปลี่ยนแปลงที่อยู่ IP ของผู้ใช้งานให้เสมือนว่ากำลังใช้งานจากสถานที่หนึ่งตามที่ต้องการ เช่น นาย ก อาศัยอยู่ในประเทศไทยต้องการรับชมวีดีโอหนึ่งบนเว็ปไซต์ www.youtube.com ที่จำกัดให้สามารถรับชมได้เฉพาะผู้ใช้งานที่อยู่ในประเทศสหรัฐอเมริกาเท่านั้น นาย ก จึงเชื่อมต่อ VPN ผ่านแอปพลิเคชันบนมือถือเพื่อย้ายที่อยู่ IP ไปยังประเทศอเมริกา เพียงเท่านี้นาย ก ก็สามารถรับชมวิดีโอได้แม้ตัวจะอยู่ในประเทศไทย

การเชื่อมต่อ VPN เพื่อใช้งานระบบสำนักงานภายในองค์กรก็ใช้หลักการเดียวกันคือการเปลี่ยนที่อยู่ IP จากบ้านหรือที่อื่น ๆ นอกองค์กรไปยังทีอยู่ IP ของอินเทอร์เน็ตภายในองค์กร จากนั้นจึงจะสามารถใช้งานระบบสำนักงานได้

ระบบสำนักงานประเภทนี้มีราคาค่อนข้างสูง แต่แลกมาด้วยความปลอดภัยทางข้อมูลที่สูงกว่าระบบสำนักงานประเภทอื่นมากเช่นกัน โดยส่วนใหญ่มักใช้ในหน่วยงานรัฐวิสาหกิจ สถาบันการเงิน และกิจการหรืออุตสหกรรมขนาดใหญ่ที่มีความพร้อมทางด้านทุนทรัพย์และให้ความสำคัญกับความปลอดภัยทางข้อมูล เช่น สำนักงานกฎหมาย บริษัทไอที

อย่างไรก็ดี ไม่ว่าระบบสำนักงานจะได้มาจากการพัฒนาขึ้นเองหรือการซื้อ หากผู้ถือกรรมสิทธิ์และมีอำนาจในการควบคุม แก้ไข และพัฒนาระบบเป็นของผู้ประกอบการ ในกรณีเช่นนี้ผู้ประกอบการคือผู้ให้บริการผ่านเครือข่ายอินเทอร์เน็ตตามกฎหมาย ซึ่งจะต้องเป็นผู้รับผิดชอบความปลอดภัยในการใช้งานระบบและความปลอดภัยทางข้อมูลเองทั้งหมด

(2) ระบบคลาวน์ (Cloud)

การทำงานผ่านระบบคลาวน์เป็นการทำงานผ่านสื่อกลาง หรือที่นิยมเรียกว่า Platform ที่ผู้ให้บริการพัฒนาขึ้นบนเครือข่ายอินเทอร์เน็ต โดยที่ผู้ใช้สามารถใช้งานได้โดยไม่จำเป็นต้องทำการติดตั้งซอฟต์แวร์ในอุปกรณ์คอมพิวเตอร์ของตนเอง Platform อาจอยู่ในรูปแบบของระบบ SaaS[3] บนเว็บไซต์ หรือแอปพลิเคชัน โดยส่วนใหญ่ภายใน Platform สำหรับการทำงานทางไกลหรือการทำงานที่บ้านมักประกอบด้วยระบบจัดเก็บฐานข้อมูล (Database) และระบบสำนักงานทั่วไป เช่น ระบบบันทึกเวลาเข้า-ออกงาน ระบบสร้างเอกสาร ระบบเสนองาน ระบบยื่นใบลาโดยผู้ให้บริการ Platform เป็นผู้มีกรรมสิทธิ์ในระบบที่ตนเองสร้างทั้งหมด ผู้ประกอบการที่ใช้ระบบสำนักงานบน Platform ถือว่าเป็นลูกค้าที่เข้าใช้บริการเท่านั้น ไม่มีสิทธิในการปรับปรุง แก้ไข หรือพัฒนาระบบแต่อย่างใด

เมื่อผู้ให้บริการเป็นผู้มีกรรมสิทธิ์ในการให้บริการ พัฒนา และควบคุมดูแล Platform ที่ตนเองสร้างขึ้นมาทั้งหมด ในกรณีเช่นนี้ผู้ให้บริการ Platform ถือว่าเป็นผู้ให้บริการผ่านเครือข่ายอินเทอร์เน็ตตามกฎหมาย ย่อมต้องเป็นผู้รับผิดชอบต่อความปลอดภัยของข้อมูลและการใช้งานที่เกิดขึ้นบน Platform ทั้งหมด

อย่างไรก็ดี ในทางปฏิบัติผู้ให้บริการ Platform มักทำข้อตกลงกับผู้ประกอบการเพื่อแบ่งหน้าที่และความผิดชอบก่อนให้บริการอยู่แล้ว เช่น กำหนดให้ผู้ประกอบการและผู้ใช้งาน ซึ่งหมายถึงพนักงานของผู้ประกอบการต้องปฏิบัติตามข้อบังคับการใช้ระบบ กำหนดให้ผู้ประกอบการเป็นผู้รับผิดชอบข้อมูลที่ตนและผู้ใช้เผยแพร่ในระบบ

---

[3]SaaS ย่อมาจาก “Software as a Service” หรือเรียกว่า “On Demand Software” คือ รูปแบบการให้บริการซอฟต์แวร์ผ่านทางอินเทอร์เน็ต คล้ายกับการเช่าใช้ เพียงแค่ผู้ซื้อจ่ายค่าซอฟต์แวร์ตามลักษณะการใช้งานที่ต้องการ (Pay-as-you-go) เช่น ตามจำนวนผู้ใช้และตามระยะเวลาที่ต้องการใช้ โดยผู้ซื้อสามารถเข้าใช้งานซอฟต์แวร์นั้น ๆ ได้ทันทีผ่านทางเว็บเบราเซอร์โดยที่ไม่ต้องติดตั้งโปรแกรมลงอุปกรณ์คอมพิวเตอร์ เหมือนการซื้อซอฟต์แวร์แบบดั้งเดิมที่เป็นลักษณะการซื้อแบบ License เช่น Microsoft Office 356 ผู้ซื้อบริการสามารถใช้สร้าง แก้ไข จัดการ หรือพิมพ์เอกสาร Word Powerpoint Excel และซอฟต์แวร์อื่นภายใต้ Microsoft Office ได้ เพียงแค่เข้าสู่ระบบ (Log in) ของเว็บไซต์ www.office.com โดยไม่ต้องติดตั้งซอฟต์แวร์ใด ๆ ในอุปกรณ์คอมพิวเตอร์

(3) ระบบผสม

ระบบผสม คือ ระบบสำนักงานที่ใช้ทั้งระบบภายในองค์กรและระบบคลาวน์ร่วมกัน ในกรณีนี้ผู้ที่มีหน้าที่รับผิดชอบต่อความปลอดภัยของข้อมูลและการใช้งานระบบอาจเป็นได้ทั้งผู้ประกอบการและผู้ให้บริการ Platform ขึ้นอยู่กับว่าระบบส่วนนั้นมีใครเป็นผู้ถือกรรมสิทธิ์ในการให้บริการและควบคุมดูแล การใช้ระบบผสมย่อมซับซ้อนกว่าการเลือกใช้ระบบใดระบบหนึ่งอย่างแน่นอน ปัญหาการควบคุมดูแลทับซ้อนจึงเกิดขึ้นอย่างหลีกเลี่ยงไม่ได้ ดังนั้น การทำข้อตกลงเพื่อแบ่งแยกกรรมสิทธิ์และหน้าที่ความรับผิดชอบจึงเป็นสิ่งสำคัญมากในการใช้ระบบสำนักงานแบบผสม และเพื่อให้การแบ่งหน้าที่และความผิดชอบเป็นไปอย่างชัดเจน ทั้งสองฝ่ายควรพิจารณาว่าใครเป็นผู้ถือกรรมสิทธิ์ใดในระบบ โดยมีประเด็นสำคัญที่ควรพิจารณา เช่น กรรมสิทธิ์และสิทธิในการเข้าถึงแม่ข่าย (Server) กรรมสิทธ์และสิทธิในการจัดการข้อมูลที่เกิดขึ้น กรรมสิทธิ์ในอุปกรณ์กระจายสัญญาณ กรรมสิทธิ์ในสิทธิประโยชน์ที่เกิดขึ้นจากข้อมูล

ปัญหาที่พบบ่อยเกี่ยวกับความปลอดภัยทางข้อมูลจากการ Work From Home

เมื่อได้ทราบหลักการการระบุผู้มีหน้าที่รับผิดชอบดูแลความปลอดภัยทางข้อมูลและความปลอดภัยในการใช้งานระบบสำนักงานแต่ละประเภทโดยสังเขปแล้ว ในส่วนนี้จะเล่าถึงสภาพปัญหาที่เกิดขึ้นจากการทำงานที่บ้านและบทวิเคราะห์เกี่ยวกับผู้มีหน้าที่รับผิดชอบและแก้ไขปัญหาเกี่ยวกับความปลอดภัยทางข้อมูลที่เกิดขึ้น

(1) ผู้ใช้มีจำนวนมากจนระบบค้าง ผู้ให้บริการต้องรับผิดชอบไหม

เมื่อวันที่ 3 กุมภาพันธ์ 2563 ซึ่งเป็นวันแรกของการทำงานหลังวันหยุดเทศกาลตรุษจีน ผู้ประกอบการส่วนใหญ่ได้ออกกฎให้พนักงานทำงานจากที่บ้าน แม้ว่าผู้ให้บริการ Platform ระบบสำนักงานออนไลน์จะเตรียมการเพื่อรองรับจำนวนผู้ใช้ที่มากขึ้นแต่ก็ยังคงเกิดข้อขัดข้องในการใช้งาน เช่น ส่งข้อมูลช้า วิดีโอกระตุก ระบบล่ม ท้ายที่สุดแม้ว่าผู้ให้บริการ Platform จะสามารถแก้ข้อขัดข้องจนทำให้ระบบกลับมาใช้งานได้ตามปกติภายในเวลาอันรวดเร็ว แต่ยังคงมีเสียงวิจารณ์ในเชิงลบจากผู้ใช้งานเป็นจำนวนมาก กรณีเช่นนี้ใครควรเป็นผู้รับผิดชอบดูแลความปลอดภัยทางข้อมูลในเหตุขัดข้องนี้

> มาตรา 22 วรรคหนึ่ง ผลิตภัณฑ์และบริการบนเครือข่ายต้องได้มาตรฐานตามที่ประเทศกำหนด ผู้ให้บริการและให้บริการผลิตภัณฑ์ต้องไม่ติดตั้งโปรแกรมที่เป็นอันตราย เมื่อผู้ให้บริการพบว่าผลิตภัณฑ์หรือบริการบนเครือข่ายมีความบกพร่องทางระบบรักษาความปลอดภัย มีช่องโหว่ หรือความเสี่ยงอื่น ๆ ที่ควรดำเนินการเยียวยา ให้ดำเนินการแจ้งผู้ใช้และหน่วยงานกำกับดูแลที่เกี่ยวข้องตามกฎระเบียบทันที

หากพิจารณาตามหลักการกำหนดผู้รับผิดชอบและหน้าที่ของผู้ให้บริการตามมาตรา 22 วรรคหนึ่ง ในข้างต้นแล้ว เห็นได้ชัดว่าผู้ให้บริการ Platform ย่อมต้องเป็นผู้รับผิดชอบความปลอดภัยในการใช้บริการและผลิตภัณฑ์ของตน รวมทั้งความปลอดภัยทางข้อมูล ในกรณีนี้ จากเหตุระบบขัดข้องที่เกิดขึ้น ผู้ให้บริการ Platform ต้องรับผิดทางละเมิดหรือรับผิดทางกฎหมายอื่น ๆ หรือไม่นั้นจำเป็นต้องพิจารณาปัจจัยอื่นร่วมด้วย เช่น สาเหตุของเหตุขัดข้อง ผลร้ายที่เกิดขึ้น ข้อตกลงร่วมกันระหว่างผู้ใช้และผู้ให้บริการ Platform

ในกรณีข้างต้นแม้ว่า Platform จะเกิดข้อขัดข้องขึ้นจนสร้างความไม่สะดวกให้แก่ผู้ใช้งาน แต่หากไม่มีความเสี่ยงว่าจะเกิดข้อบกพร่องทางระบบรักษาความปลอดภัย (security defect) หรือเกิดช่องโหว่ (vulnerability) ของตัว Platform หรือผลอันตรายอื่น ๆ เช่น ข้อมูลรั่วไหล ในกรณีเช่นนี้ผู้ให้บริการ Platform ไม่มีหน้าที่รับผิดชอบความปลอดภัยทางข้อมูลจากเหตุการณ์ที่เกิดขึ้น

(2) ระบบอินเทอร์เน็ตภายในหน่วยงานโดนแฮก ใครจะรับผิดชอบ

ในช่วงวิกฤตโรคระบาดนี้ หลายบริษัทถูกขบวนแฮกเกอร์ล้วงข้อมูลผ่านทางอีเมล์ที่อ้างตนว่าเป็นหน่วยงานควบคุมโรค เช่น กระทรวงสาธารณสุข โดยใช้ข่าวสารเกี่ยวกับสถานการณ์โรคระบาดล่อลวงให้ผู้ใช้งานกดเปิดอ่านอีเมล์ที่มีไวรัสอยู่ ซึ่งเพียงแค่กดลิงก์อาจจะทำให้คอมพิวเตอร์เครื่องนั้นถูกควบคุมจนข้อมูลสำคัญถูกขโมยและระบบภายในคอมพิวเตอร์ถูกทำลาย ในกรณีเช่นนี้ใครควรเป็นผู้รับผิดชอบความปลอดภัยทางข้อมูล

ในความเป็นจริงแล้วการทำงานที่บ้านทำให้ระบบอินเทอร์เน็ตภายในองค์กรเสี่ยงต่อการถูกบุกรุกมากขึ้น เพราะพนักงานต้องเชื่อมต่อเข้าสู่ระบบสำนักงานของบริษัทหรือเครือข่ายอินเทอร์เน็ตภายในผ่านอุปกรณ์คอมพิวเตอร์และสัญญาณอินเทอร์เน็ตส่วนตัว ซึ่งในบางกรณีพนักงานอาจใช้ Wi-Fi สาธารณะหรือเครือข่ายอินเทอร์เน็ตที่มีระบบรักษาความปลอดภัยไม่เพียงพอทำให้เกิดช่องโหว่ให้แฮกเกอร์สามารถลักลอบเชื่อมต่อเข้าสู่เครือข่ายอินเทอร์เน็ตภายในขององค์กรและเข้าไปล้วงข้อมูลทางธุรกิจของบริษัทได้ นอกจากนี้ อุปกรณ์คอมพิวเตอร์ส่วนตัวที่พนักงานใช้อาจถูกแฮกเกอร์ลักลอบติดตั้งแอปพลิเคชั่นหรือซอฟต์แวร์อื่นที่เป็นอันตรายต่อความปลอดภัยของทั้งตัวอุปกรณ์และเครือข่ายอินเทอร์เน็ตภายในขององค์กร โดยพบเห็นบ่อยในรูปแบบของลิ้งก์ข่าวสารสถานการณ์โรคระบาดจากอีเมล์ที่อ้างตนว่าเป็นหน่วยงานของรัฐ

มาตรา 21 ประเทศต้องมีมาตรการรักษาความมั่นคงทางไซเบอร์ ผู้ให้บริการเครือข่ายต้องปฏิบัติตามข้อกำหนดต่าง ๆ ว่าด้วยความมั่นคงทางไซเบอร์ และปฏิบัติหน้าที่รักษาความปลอดภัยดังต่อไปนี้ เพื่อให้เครือข่ายไม่ถูกรบกวน ทำลาย หรือเข้าถึงโดยไม่ได้รับความยินยอม และป้องกันไม่ให้ข้อมูลบนเครือข่ายรั่วไหล ถูกขโมยหรือปลอมแปลง

(1) สร้างกฎระเบียบและระบบดูแลความปลอดภัยภายใน ระบุผู้มีหน้าที่รักษาความมั่นคงทางไซเบอร์ และรับผิดชอบการรักษาความปลอดภัยทางไซเบอร์

(2) มีมาตรการทางเทคโนโลยีที่ใช้ป้องกันไวรัสคอมพิวเตอร์ การโจมตีเครือข่าย การบุกรุกเครือข่าย และการกระทำอื่นที่เป็นอันตรายต่อความมั่นคงทางไซเบอร์

(3) มีมาตรการทางเทคโนโลยีที่ใช้ติดตามและบันทึกสถานะการทำงานของเครือข่ายและเหตุการณ์ทางไซเบอร์ และต้องจัดเก็บบันทึกเหตุการณ์ทางไซเบอร์ประจำวันตามที่กฎหมายกำหนดเป็นเวลาไม่น้อยกว่าหกเดือน

(4) มีมาตรการ เช่น แยกประเภทข้อมูล สำรองข้อมูล หรือการเข้ารหัสข้อมูลสำหรับข้อมูลที่สำคัญ

(5) ปฏิบัติหน้าอื่นตามที่กฎหมายหรือกฎระเบียบทางปกครองกำหนด

มาตรา 25 ผู้ให้บริการเครือข่ายต้องมีแผนการสำหรับเหตุฉุกเฉินที่เกี่ยวกับความมั่นคงทางไซเบอร์ จัดการข้อบกพร่องของระบบ ไวรัสคอมพิวเตอร์ การโจมตีเครือข่าย การบุกรุกเครือข่าย และความเสี่ยงทางความมั่นคงทางไซเบอร์อื่น ๆ ได้ทันที เมื่อเกิดเหตุที่เป็นอันตรายต่อความมั่นคงทางไซเบอร์ ผู้ให้บริการที่เกี่ยวข้องต้องใช้แผนการสำหรับเหตุฉุกเฉินทันที มีมาตรการเยียวยาผลกระทบที่เกิดขึ้น และปฏิบัติตามข้อกำหนดของหน่วยงานผู้กำกับดูแลที่เกี่ยวข้อง

หากพิจารณาจากสภาพการณ์ข้างต้น บริษัทที่ถูกแฮกเกอร์โจมตีย่อมเป็นผู้เสียหายที่ต้องได้รับการดูแลความปลอดภัยทางข้อมูลจากทั้งผู้ให้บริการอินเทอร์เน็ต (ใช้อินเทอร์เน็ตเจ้าใด เจ้านั้นต้องรับผิดชอบ) และผู้ให้บริการ Platform ในกรณีที่ใช้ระบบสำนักงานแบบคลาวน์ แต่ถ้าหากพบว่าระบบเครือข่ายอินเทอร์เน็ตภายในของบริษัทไม่มีเทคโนโลยีรักษาความปลอดภัยหรือไม่ได้เตรียมมาตรการป้องกันตามที่มาตรา 21 และมาตรา 25 ของกฎหมายว่าด้วยความปลอดภัยทางไซเบอร์ฯ และกฎหมายอื่นกำหนดจนทำให้ข้อมูลภายในรั่วไหล ถูกขโมย ถูกปลอมแปลง หรือก่อให้เกิดความเสียหายแก่ลูกค้าของบริษัท ในกรณีเช่นนี้บริษัทผู้เสียหายอาจต้องรับผิดชอบผลร้ายที่เกิดขึ้นเองทั้งหมด

(3) พนักงานใช้ VPN เชื่อมต่อระบบภายในบริษัท จนทำให้ฐานข้อมูลเสียหาย บริษัทจะป้องกัน “เกลือเป็นหนอน” และรักษาความปลอดภัยของฐานข้อมูลไปพร้อม ๆ กันอย่างไร

ในคืนวันที่ 23 กุมภาพันธ์ 2563 ระบบ SaaS ที่ใช้จัดเก็บข้อมูลร้านค้าของบริษัท Weimob ผู้ให้บริการ Platform ร้านค้าแก่ธุรกิจออนไลน์จำนวนนับแสนรายเกิดเหตุขัดข้อง ทำให้ข้อมูลของร้านค้าสูญหาย สร้างความเสียหายให้แก่ร้านค้าผู้ใช้บริการ Platform เป็นจำนวนมาก โดยต่อมาในวันที่ 25 กุมภาพันธ์ บริษัท Weimob ได้ชี้แจงว่าต้นตอของเหตุการณ์ระบบขัดข้องเกิดขึ้นจากการกระทำของนายเจีย พนักงานแผนกวิจัยและพัฒนาซอฟต์แวร์ของบริษัท Weimob เนื่องด้วยสภาวะกดดันและอาการทางจิตทำให้นายเจียใช้ VPN เชื่อมต่อเข้ามาภายในระบบจัดเก็บข้อมูลร้านค้า และก่อเหตุทำลายระบบควบคุมและฐานข้อมูลบางส่วนจนทำให้ข้อมูลบน Platform ที่ร้านค้าบันทึกไว้หายไป ในกรณีเช่นนี้ผู้ให้บริการระบบ SaaS ที่บริษัท Weimob ใช้บริการหรือบริษัท Weimob ต้องเป็นผู้รับผิดชอบความเสียหายของข้อมูลของร้านค้า

ในกรณีนี้เหตุขัดข้องมีสาเหตุหลักมาจากระบบรักษาความปลอดภัยทางข้อมูลของบริษัท Weimob ที่ไม่รัดกุมเพียงพอ ซึ่งเปิดโอกาสให้พนักงานเข้าถึงฐานข้อมูลของบริษัทมากเกินจำเป็น แต่ไม่ได้เกิดจากข้อบกพร่องของผู้ให้บริการระบบ SaaS ที่บริษัท Weimob ใช้บริการ หากร้านค้าใดบน Platform ข้อมูลสูญหายและได้รับผลกระทบทางเศรษฐกิจจากเหตุขัดข้องที่เกิดขึ้น ในกรณีเช่นนี้บริษัท Weimob ผู้ให้บริการ Platform ต้องเป็นผู้รับผิดชอบทั้งหมด

การให้สิทธิพนักงานเข้าถึงข้อมูลเกินจำเป็นเป็นหนึ่งในสาเหตุหลักของปัญหาฐานข้อมูลเสียหายหรือข้อมูลรั่วไหล นอกจากนี้ การได้มาซึ่งข้อมูลส่วนบุคคลของผู้อื่นที่ไม่จำเป็นต่อการทำงานของตนนั้นยังเป็นหนึ่งในองค์ประกอบความผิดของการละเมิดสิทธิในข้อมูลส่วนบุคคลอีกด้วย ดังนั้น บริษัทจึงควรพิจารณาจำกัดสิทธิการเข้าถึงข้อมูลของพนักงานให้อยู่ในขอบเขตที่จำเป็นต่อการทำงาน ทั้งนี้ เพื่อรักษาสมดุลระหว่างประสิทธิภาพในการทำงานและความปลอดภัยทางข้อมูลของทั้งบริษัทและลูกค้าผู้ใช้บริการ

(4) ระหว่างทำงานที่บ้าน เจ้านายจะติดตามและตรวจสอบการทำงานของพนักงานอย่างไรจึงจะไม่เป็นการละเมิดสิทธิส่วนบุคคล

ในช่วงการทำงานที่บ้านนี้ บริษัทต่าง ๆ มีมาตรการหลากหลายในการติดตามและตรวจสอบการทำงานของพนักงาน เพื่อคงประสิทธิภาพและปริมาณงานให้เทียบเท่ากับการทำงานในสำนักงาน เช่น การส่งรายงานประจำวัน การลงชื่อเข้า-ออกงาน การให้พนักงานเปิดกล้องวิดีโอในเวลางานเพื่อเฝ้าดูการทำงาน โดยพนักงานต้องดำเนินการทั้งหมดผ่านระบบสำนักงานอัตโนมัติของบริษัท ซึ่งโดยทั่วไประบบสำนักงานอัตโนมัติมักจะบันทึกข้อมูลต่าง ๆ ที่จำเป็นต่อการติดตามการทำงานและยืนยันพิกัดของพนักงาน เช่น เวลาเข้างาน ที่อยู่ IP ของคอมพิวเตอร์ ตำแหน่งของคอมพิวเตอร์ที่ใช้เข้าสู่ระบบ และเอกสารที่ส่งในแต่วัน แต่ในขณะเดียวกันบางบริษัทได้ติดตั้งระบบติดตามการทำงานประเภทอื่นไว้ในระบบสำนักงานอัตโนมัติด้วย เช่น ระบบบันทึกวิดีโออัตโนมัติ ระบบบันทึกประวัติการใช้งานของเครื่องคอมพิวเตอร์ ระบบบันทึกประวัติการเข้าชมเว็บไซต์ ซึ่งเป็นที่ถกเถียงกันว่าการติดตั้งระบบเหล่านี้เป็นการละเมิดสิทธิส่วนบุคคลของพนักงานหรือไม่

หากพิจารณาจากมาตรการเก็บข้อมูลเพื่อติดตามและตรวจสอบการทำงานในข้างต้นจะสามารถแบ่งวิธีการได้มาซึ่งข้อมูลเป็น 2 กรณี คือ กรณีที่ 1 พนักงานเป็นผู้ให้ข้อมูลเอง และกรณีที่ 2 ระบบสำนักงานอัตโนมัติบันทึกข้อมูล ซึ่งทั้งสองกรณีถือว่าเป็นการเก็บข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยความมั่นคงทางไซเบอร์ฯ ดังนั้น บริษัทจำเป็นต้องปฏิบัติตามบทบัญญัติเกี่ยวกับหลักการการรวบรวมและใช้งานข้อมูลส่วนบุคคลตามมาตรา 41 วรรคหนึ่ง ของกฎหมายว่าด้วยความมั่นคงทางไซเบอร์ฯ ที่ว่า การรวบรวมและใช้งานข้อมูลส่วนบุคคลต้อง

(1) ถูกกฎหมาย เหมาะสม และเท่าที่จำเป็น

(2) เปิดเผยวิธีการรวบรวมและการนำไปใช้

(3) ชี้แจงเป้าหมาย วิธีการและขอบเขตการนำไปใช้

(4) ต้องได้รับความยินยอมจากผู้ให้ข้อมูล ซึ่งในที่นี้หมายถึงพนักงานของบริษัท

ดังนั้น ข้อถกเถียงที่ว่าการติดตั้งระบบติดตามงานบางประเภทไว้ในระบบสำนักงานอัตโนมัติเป็นการละเมิดสิทธิส่วนบุคคลของพนักงานหรือไม่นั้น จำเป็นต้องพิจารณาจากหลักการข้างต้น โดยเฉพาะข้อ (4) ที่กำหนดให้บริษัทต้องได้รับความยินยอมจากพนักงานเพราะแม้ว่าบริษัทจะชี้แจงถึงความจำเป็นในการเก็บข้อมูล หรือระบุเป้าหมายหรือขอบเขตการนำไปใช้อย่างชัดเจนเพียงใด หากไม่ได้รับความยินยอมจากพนักงานผู้ให้ข้อมูลก็ถือว่าไม่ครบองค์ประกอบของการเก็บข้อมูลที่ถูกต้องตามกฎหมาย ข้อมูลที่ได้มาจึงถือว่ามาจากการละเมิดสิทธิส่วนบุคคลของพนักงาน

บทส่งท้าย

ปรากฏการณ์ “โลกใหม่ใบเดิม” หรือ New Normal ในช่วงวิกฤตโรคระบาดครั้งนี้เป็นตัวช่วยผลักดันให้เทคโนโลยีการสื่อสารและด้านอื่น ๆ ในประเทศจีนพัฒนาไปอย่างรวดเร็วเพื่อรองรับวิถีชีวิต โดยเฉพาะวิธีการทำงานที่เปลี่ยนแปลงไปของผู้คน ในขณะเดียวกันรัฐบาลจีนก็สนับสนุนการพัฒนาเทคโนโลยีและนวัตกรรมที่ช่วยอำนวยความสะดวกในการทำงาน และการฟื้นฟูกิจการและการผลิต (Re-open) ในช่วงการควบคุมโรคอย่างเต็มที่ รวมทั้งให้ความสำคัญกับการกำกับดูแลความปลอดภัยทางไซเบอร์เพื่อตั้งรับปัญหาที่เกิดขึ้นจากเทคโนโลยีใหม่

บทความตอนนี้ได้เล่าถึงปัญหาความปลอดภัยทางข้อมูลในมุมมองของผู้ประกอบการไปแล้ว ในตอนต่อไปผู้เขียนจะขอเล่าถึงมุมมองของบุคคลทั่วไปกันบ้างว่าในช่วงวิกฤติโรคระบาดเช่นนี้ข้อมูลส่วนตัวรวมถึงสิทธิในการแสดงความคิดเห็นของประชาชนชาวจีนได้รับผลกระทบอย่างไรและเหตุใดจึงเกิดเหตุการณ์หมอถูกจับเพราะแจ้งข่าวโรคระบาดกับกลุ่มเพื่อนในแอปพลิเคชัน Chat ได้

<u>อ้างอิง</u>

1. Ning XuanFeng, Wu Han. (2563). *“ดินแดนลี้ลับในเมฆหมอก” ปัญหาความปลอดภัยทางข้อมูลที่ภาคธุรกิจพบบ่อยในช่วงทำงานที่บ้านและคำแนะนำ (“云深不知处”——企业远程办公的网络安全常见问题及建议).*
https://www.chinalawinsight.com/2020/03/articles/cybersecurity/%E4%BA%91%E6%B7%B1%E4%B8%8D%E7%9F%A5%E5%A4%84-%E4%BC%81%E4%B8%9A%E8%BF%9C%E7%A8%8B%E5%8A%9E%E5%85%AC%E7%9A%84%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E5%B8%B8%E8%A7%81/#_ftn1 (สืบค้นเมื่อวันที่ 15 เมษายน 2563)
2. Sohu. (2563). *ระบบในเครือบริษัท WeChat ล่ม ทำงานที่บ้านแบบนี้ใครจะ “รับผิดชอบ” (“‘企业微信钉钉崩溃，远程办公谁在‘江湖救急’？”).*
https://www.sohu.com/a/370534054_429401 (สืบค้นเมื่อวันที่ 15 เมษายน 2563)

3. Freebuf. (2563). *พวกฉวยโอกาส ระวังแฮกเกอร์อ้างตัวเป็นหน่วยงานควบคุมโรค ฉวยโอกาสวิกฤต 'โรคระบาด'ล้วงข้อมูล (趁火打劫，谨防黑客冒充权威疫情防控机构，利用'疫情'发起钓鱼攻击).*
https://www.freebuf.com/column/226800.html (สืบค้นเมื่อวันที่ 15 เมษายน 2563)
4.Tencent. (2563). ระบบบริษัท Weimob ล่มนานกว่า 24 ชั่วโมง น่าสงสัยว่าระบบความปลอดภัยของ SaaS รัดกุมแค่ไหน *(微盟系统故障超 24 小时 SaaS 行业客服安全受质疑).*
https://new.qq.com/omn/20200228/20200228A00AZQ00.html (สืบค้นเมื่อวันที่ 15 เมษายน 2563)