องค์กรเทคโนโลยียักษ์ใหญ่กับวิกฤตการละเมิดข้อมูลส่วนบุคคล: การจัดการวิกฤตยุคดิจิทัล

Tech Giants and Crisis in Data Breaches: Crisis Management in Digital Era

อภิภู กิติกำธร[1] **Abhibhu Kitikamdhorn**

Received: 9 August 2019, Revised: 18 November 2019, Accepted: 13 December 2019

บทคัดย่อ

บทความนี้ใช้วิธีการวิจัยเอกสาร (documentary research method) ศึกษาและถอดบทเรียนการจัดการวิกฤตการละเมิดข้อมูลส่วนบุคคลของผู้ใช้ของ Facebook ที่ตกเป็นข่าวดังในช่วงปี ค.ศ. 2018, Yahoo ที่ตกเป็นข่าวในช่วงปี ค.ศ. 2016, และ Google+ ที่ตกเป็นข่าวช่วงปลายปี ค.ศ. 2018 โดยใช้แนวคิดการจัดการวิกฤตเป็นกรอบแนวคิดในการวิเคราะห์ข้อมูล ผลการศึกษาแสดงให้เห็นรูปแบบการจัดการวิกฤตของทั้ง 3 องค์กร คือ พบการมองข้ามความสำคัญและการละเลยที่จะแก้ไขข้อบกพร่องของระบบรักษาความปลอดภัยข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยทั้ง 3 องค์กรขาดการจัดการวิกฤต กล่าวคือ ไม่มีการดำเนินการเพื่อเตรียมรับมือและป้องกันวิกฤตในขั้นก่อนวิกฤต ขาดการจัดการในขั้นวิกฤตที่รัดกุม และไม่มี

---

[1] อภิภู กิติกำธร (นิสิตหลักสูตรนิเทศศาสตรดุษฎีบัณฑิต คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย)
Abhibhu Kitikamdhorn (PhD Student in Communication Arts, Faculty of Communication Arts, Chulalongkorn University)
คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย 254 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพมหานคร 10330
Faculty of Communication Arts, Chulalongkorn University, 254 Phayathai Road, Pathumwan, Bangkok Thailand 10330
Corresponding Author E-mail: abhibhu@hotmail.com

การจัดการในขั้นหลังวิกฤต หากพิจารณาในภาพรวมแล้ว สามารถสรุปได้ว่า ปัจจัยทั้งภายในที่หมายถึงการให้ความสำคัญต่อการปกป้องข้อมูลส่วนบุคคลของผู้ใช้ และภายนอกองค์กรที่หมายถึงกลุ่ม/องค์กรที่สร้างความเสียหายต่อองค์กรทั้ง 3 โดยปัจจัยทั้ง 2 รูปแบบนี้ ส่งผลต่อระดับความรุนแรงของวิกฤต รวมถึงประสิทธิภาพการจัดการวิกฤตขององค์กรในภาพรวม

คำสำคัญ วิกฤต, การจัดการวิกฤต, การละเมิดข้อมูล, ข้อมูลส่วนบุคคล, Facebook, Yahoo, Google+

Abstract

This paper employs documentary research method to study and learn a lesson on tech giants' crisis management. In other words, crisis management is used as a theoretical framework for examines tech giants' crisis management and learns their lessons at time of crisis in data breaches involving the news about Facebook's data breaches which were reported in 2018, Yahoo data breaches which were reported in 2016, and Google+ data breach which was reported in late 2018. The analysis showed that these companies took protection of data privacy for granted and were not incorporating crisis management into their system since the beginning, therefore that crisis situation arose, defused and worsen due to their apparent lack of proper precrisis management system. All in all, there are both internal and external factors affecting the organizations' degree of success or failure in crisis management, together with their overall capability to deal with the crisis.

Keywords crisis, crisis management, data breach, data privacy, Facebook, Yahoo, Google+

บทนำ

การมองข้ามความสำคัญ และการจัดการระบบความรักษาปลอดภัยที่ไม่รัดกุมในการปกป้องข้อมูลส่วนบุคคลของผู้ใช้ที่ต้องระบุข้อมูลส่วนบุคคลเพื่อเข้าใช้บริการพื้นที่การสื่อสารอาจนำไปสู่วิกฤตที่ใหญ่หลวงได้ ดังเห็นได้จากกรณีศึกษาของสื่อสังคมออนไลน์ยักษ์ใหญ่ คือ Facebook, Google+, และ Yahoo ที่เป็นผู้ให้บริการพื้นที่การสื่อสารและเป็นเหมือนคลังข้อมูลที่จัดเก็บฐานข้อมูลส่วนบุคคลขนาดใหญ่เอาไว้[2] หลากหลายภาคส่วนในระดับปัจเจก องค์กร หน่วยงานทั้งภาครัฐและเอกชนต่างใช้บริการพื้นที่การสื่อสารเหล่านี้ โดยเฉพาะ Facebook กันมากขึ้น (Bhimani, Mention & Barlatier, 2018) พื้นที่นี้ถูกมองเป็นทั้งช่องทางการสื่อสาร ช่องทางธุรกิจ และเป็นภาพแทนตัวตนที่ผู้ใช้สมัครใจระบุข้อมูลส่วนบุคคลด้วยตนเอง ซึ่งบางครั้งผู้ใช้ก็ไม่ตระหนักถึงความสำคัญของการปกป้องข้อมูลส่วนบุคคล ละเลยการอ่านข้อกำหนดและนโยบายการใช้ต่างๆ (terms and policies) ข้ามไปตอบ *“ตกลง”* รับรู้ความเสี่ยงจากการใช้บริการ และแสดงความยินยอมให้มีการเข้าถึงข้อมูลส่วนตัวได้จากการตอบตกลงเพื่อเล่นเกมหรือใช้แอปพลิเคชัน (application) ต่างๆ ซึ่งการมองข้ามความสำคัญของการป้องกันสิทธิเหนือข้อมูลส่วนบุคคลของตน เป็นช่องว่างทำให้เกิดการละเมิดข้อมูลได้ (Winston, 2018)

ในอีกมุม Facebook ในฐานะองค์กรให้บริการแพลตฟอร์มที่เป็นพื้นที่การสื่อสารก็ไม่ตระหนักถึงความสำคัญของการปกป้องข้อมูลส่วนตัวของผู้ใช้เท่าที่ควร ทั้งที่ข้อมูลส่วนบุคคลเหล่านี้ถือเป็นหัวใจของ Facebook[3] จึงนำไปสู่วิกฤตข้อมูลรั่วครั้งใหญ่ถึง 2 ครั้งในรอบปี ที่นอกจากจะกระทบต่อภาพลักษณ์และความน่าเชื่อถือขององค์กร

---

[2] อิงจากสถิติการใช้สื่อสังคมออนไลน์ในปี ค.ศ. 2018 ที่พบว่า ประชากรเกือบครึ่งโลก (44%) ใช้สื่อสังคมออนไลน์เป็นช่องทางการรับข้อมูลและสื่อสาร และจากจำนวนผู้ใช้สื่อสังคมออนไลน์ทั่วโลก 3.397 พันล้านคน Facebook ถือเป็นอันดับหนึ่ง (Kemp, 2018 ที่ถือส่วนแบ่งการตลาดของสื่อสังคมออนไลน์ถึง 80% ในปี ค.ศ. 2018 (Houser & Voss, 2018, p. 5) นอกจากนี้หากอิงสถิติเรื่องการจัดอันดับเว็บไซต์ที่ได้รับความนิยมแล้ว ยังมี Google และ Yahoo ที่ติด 10 อันดับสูงสุดอีกด้วย (Kemp, 2018) ทั้งนี้ Google+ เป็นบริการในรูปแบบสื่อสังคมออนไลน์ภายใต้ Google ที่ถูกพัฒนาขึ้นมาตั้งแต่ปี 2011 เพื่อหวังให้เป็นคู่แข่งของ Facebook (D’Onfro, 2018a)

[3] แม้ว่า Facebook จะไม่เก็บค่าใช้บริการ แต่รายได้หลักขององค์กรมาจากการอนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้ (Houser & Voss, 2018, p. 3)

ในฐานะผู้เก็บข้อมูลของผู้ใช้ เหตุการณ์นี้ นอกจากจะลุกลามไปถึงขั้นเกิดกระแสเรียกร้องที่แพร่ไปทั่วโลกให้มีการลบ Facebook—*"#deletefacebook"* แล้ว ยังเป็นการกระตุ้นให้โลกหันกลับมาตระหนักถึงความสำคัญของการป้องกันข้อมูลและสิทธิส่วนบุคคลอีกด้วย (Bennett, 2018, p. 239) ในทำนองเดียวกัน Google+ ที่เป็นบริการในรูปแบบสื่อสังคมออนไลน์คล้ายกับ Facebook เผชิญกับวิกฤตที่กระทบข้อมูลส่วนบุคคลของผู้ใช้ จนต้องประกาศว่าจะปิดตัวลงในปี ค.ศ. 2019 (Lee, 2018; Newman, 2018; Wong & Solon, 2018) Yahoo ที่แม้ไม่ได้เป็นสื่อสังคมออนไลน์แต่ก็เป็นอีกหนึ่งองค์กรที่รับผิดชอบข้อมูลส่วนบุคคลของผู้ใช้จำนวนมากเช่นเดียวกัน และได้เผชิญกับวิกฤตการละเมิดข้อมูลส่วนบุคคลของผู้ใช้ครั้งใหญ่ที่สุดในประวัติศาสตร์ เพราะกระทบผู้ใช้กว่า 3 พันล้านราย จากเหตุการละเมิดข้อมูลถึง 2 ครั้งซ้อน ข่าวประเด็นนี้กระทบความน่าเชื่อถือและภาพลักษณ์ขององค์กรอย่างรุนแรงและทำให้องค์กรสูญเสียรายได้มหาศาล (News BTC, 2018; Armerding, 2018; Clement, 2019; Techworld," 2018)

หากมองเรื่องนี้ในมุมขององค์กร โดยใช้กรอบคิดเรื่องการจัดการวิกฤต สามารถกล่าวได้ว่า *"ไม่มีองค์กรไหน หลีกหนีวิกฤตได้...ฉะนั้น สิ่งที่ควรทำก็คือเตรียมรับมือ"* (Coombs, 2012, p. 1) อย่างไรก็ตาม ด้วยความตระหนักรู้ถึงความสำคัญของสิทธิข้อมูลส่วนบุคคลในโลกออนไลน์ในระดับปัจเจกบุคคลยังมีไม่มากเท่าที่ควร[4] และหากเทียบกับต่างประเทศโดยเฉพาะฝั่งตะวันตกที่มีการกำหนดกฎ นโยบาย หรือการกำกับดูแลที่เกี่ยวข้องแล้ว (Bennett, 2018; Isaak & Hanna, 2018; Tuttle, 2018) ประเทศไทยยังไม่ให้ความสนใจและตื่นตัวกับเรื่องนี้เท่าที่ควร (นิธิมา คณานิธินันท์, 2544; เอกพันธ์ พัฒนาวิจิตร, 2559) การศึกษาการจัดการวิกฤตขององค์กรที่ดูแลข้อมูลส่วนบุคคลเหล่านี้ จะเป็นการถอดบทเรียนของกรณีศึกษาที่จะเป็นประโยชน์ต่อการพัฒนาความรู้ของแนวคิดเรื่องการจัดการวิกฤต และสร้างความตระหนักรู้ถึงความสำคัญของข้อมูลส่วนบุคคลออนไลน์ในบริบทประเทศไทยได้ บทความนี้มีวัตถุประสงค์เพื่อศึกษากรณีตัวอย่างเกี่ยวกับภาวะวิกฤตเรื่องข้อมูลส่วนบุคคลของผู้ใช้ที่ถูกละเมิดที่ Facebook เผชิญในช่วงเดือนมีนาคมและกันยายน ค.ศ. 2018 รวมถึงวิกฤตเรื่องข้อมูลส่วนบุคคลหลุดที่ Yahoo และ Google+ ประสบในปี ค.ศ. 2016

[4] อิงจากสถิติที่แสดงระดับความสนใจและความกังวลเรื่องความเป็นส่วนตัวของข้อมูลในระดับประเทศและโลกในปี ค.ศ. 2018 ความสนใจและความกังวลดังกล่าวอยู่ในระดับ 42% (Kemp, 2018)

และ 2018 ตามลำดับ ด้วยวิธีการวิจัยเอกสาร (documentary research) โดยการนำเสนอเนื้อหาของบทความแบ่งออกเป็น 4 ส่วน ได้แก่ บทนำ การทบทวนวรรณกรรม การวิเคราะห์ข้อมูล และสรุปผล

การทบทวนวรรณกรรม

ดังที่ได้กล่าวไปข้างต้นว่า ทุกองค์กรมีโอกาสเผชิญกับภาวะวิกฤต คำจำกัดความของคำว่า *"วิกฤต"* (crisis) จึงสะท้อนความเกี่ยวข้องกับองค์กร ซึ่งหมายถึง *"ความตระหนักรู้ของผู้มีส่วนได้ส่วนเสียถึงภัยคุกคามจากเหตุการณ์เหนือความคาดหมายที่สามารถสร้างผลกระทบร้ายแรงต่อองค์กร หรืออาจจะส่งผลเสียที่เกี่ยวข้องได้"* (Coombs, 2012, p. 2) กล่าวคือ ภาวะวิกฤตจะเกิดขึ้น เมื่อใดก็ตามที่ผู้มีส่วนได้ส่วนเสียเชื่อว่าองค์กรตกอยู่ในภาวะวิกฤต จากนิยามนี้จึงนำไปสู่คำถามว่า เหตุการณ์แบบไหนถึงจะเข้าข่ายภาวะที่เรียกว่าวิกฤต โดยทั่วไปวิกฤตที่องค์กรเผชิญมีองค์ประกอบสำคัญ 4 ประการ คือ คาดเดาไม่ได้ (unexpected/surprise) ไม่ปกติ (nonroutine) ทำให้เกิดความไม่มั่นคง (produces uncertainty) และกระทบกับเป้าหมายสำคัญขององค์กร (threatens high-priority goals) ในภาพกว้าง มีการจำแนกวิกฤตออกเป็น 2 กลุ่มใหญ่ ได้แก่ วิกฤตที่เกิดขึ้นโดยเจตนา/จากความตั้งใจ (intentional crises) เช่น การตั้งใจปองร้าย และวิกฤตที่เกิดขึ้นโดยไม่เจตนา/ไม่ตั้งใจ (unintentional crises) เช่น ภัยธรรมชาติ (Ulmer, Sellnow, & Seeger, 2007, pp. 7-13) ทางออกที่ดีที่สุดสำหรับองค์กร คือ การเตรียมตัวให้พร้อมเมื่อเกิดวิกฤตและควรเรียนรู้การจัดการวิกฤต (crisis management) (Coombs, 2012, pp. 1-2; Frandsen & Johansen, 2017, p. 52) หรือควรมีกระบวนการรับมือ/เครื่องมือที่ใช้ต่อกรกับวิกฤตเพื่อป้องกันหรือลดความเสียหายลง (Coombs, 2012, p. 5)

โดยพื้นฐานแนวคิดการจัดการวิกฤตเชื่อว่า ภาวะวิกฤตมีวงจรชีวิต (life cycle) ที่สามารถสังเกตได้ และจำเป็นต้องใช้แนวทางการรับมือกับวิกฤตในแต่ละช่วงของวงจรต่างกัน (Gonzalez-Herrero & Pratt, 1995; Struges, 1994 as cited in Coombs, 2012, p. 6) ทั้งนี้ งานศึกษาที่ผ่านมา ได้มีการสร้างแบบจำลองเพื่อนำเสนอแนวทางการจัดการวิกฤตที่ถูกพัฒนาให้สอดรับกับบริบทการสื่อสารที่เปลี่ยนแปลงไปตามความก้าวหน้าของเทคโนโลยี ซึ่งมีแบบจำลองหลักอยู่ 3 แบบ ได้แก่ แบบจำลองของ Fink (1986) ที่แบ่งขั้นตอนการจัดการวิกฤตเป็น 3 ขั้นตอน แบบจำลองของ

Mitroff (1994) ที่เป็นการนำแบบจำลองแรกมาพัฒนาต่อยอด แบ่งออกเป็น 5 ขั้นตอนย่อย และแบบจำลอง 3 ขั้นตอน ที่นิยมใช้กันอย่างแพร่หลายมาจนถึงปัจจุบัน แนะนำโดยนักคิดและนักวิชาการที่เกี่ยวข้องจำนวนหนึ่ง (Coombs, 2012, pp. 10-13; Frandsen & Johansen, 2017, pp. 69-87) รายละเอียดตาม**ตารางที่ 1**

นอกจากแบบจำลองการจัดการวิกฤต 3 ขั้นตอน ยังมีองค์ประกอบและมิติอื่นที่เกี่ยวข้องกับกระบวนการจัดการวิกฤตดังนี้ ในขั้นก่อนวิกฤตครอบคลุมถึงปัจจัยอื่นที่เกี่ยวข้อง ได้แก่ การจัดตั้งหน่วยจัดการวิกฤต (crisis management team) การพัฒนาแผนการจัดการวิกฤต (crisis management plan) การจัดการผู้มีส่วนได้ส่วนเสีย (stakeholders management) การวิเคราะห์สภาพแวดล้อม (environmental scanning) การประเมินและจัดการความเสี่ยง (risk assessment and management) การจัดการประเด็น (issue management) ในขั้นวิกฤตเกี่ยวโยงกับการตัดสินใจแบบกลุ่มย่อย (small-group decision making) การตัดสินใจในภาวะวิกฤต และการสื่อสารในภาวะวิกฤต (crisis communication) ส่วนขั้นหลังวิกฤต ได้แก่ วิธีการประเมินการดำเนินงานต่างๆ (evaluation methods) การจัดการชื่อเสียงและภาพลักษณ์ (reputation management) และในภาพรวมมีกระบวนการเกี่ยวข้อง คือ การจำลองวิกฤตเพื่อหาจุดอ่อนของการจัดการวิกฤต (crisis simulation) ทั้งนี้ กระบวนการจัดการวิกฤตทั้งกระบวนการ เปรียบเสมือนการวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรคขององค์กร (SWOT analysis) ในมุมที่เกี่ยวข้องกับความเสี่ยงและวิกฤต โดยองค์ประกอบเหล่านี้ และการดำเนินการตามแบบจำลอง จะเป็นตัวชี้วัดประสิทธิภาพการจัดการวิกฤตขององค์กร (Coombs, 2012, pp. xi-18; Frandsen & Johansen, 2017, pp. 69-87)

ตารางที่ 1 แสดงรายละเอียดแบบจำลองสำหรับการจัดการวิกฤตทั้ง 3 แบบ

Fink (1986)	Mitroff (1994)	Three-stage
สัญญาณเตือน (prodromal): จุดสังเกตที่เตือนถึงการเกิดวิกฤต	**ตรวจจับสัญญาณ (signal detection):** พบสัญญาณเตือนการเกิดวิกฤต และควรมีการดำเนินการในส่วนที่เกี่ยวข้องเพื่อรับมือ	**ก่อนวิกฤต (precrisis):** การเตรียมการก่อนวิกฤต แบ่งเป็น 3 ข้อย่อย ได้แก่ 1) ตรวจจับสัญญาณ (signal detection) 2) ป้องกัน (prevention) 3) เตรียมรับวิกฤต (crisis preparation)
	ตรวจสอบและป้องกัน (probing and prevention): สมาชิกองค์กรหาตัวแปรความเสี่ยงที่อาจนำไปสู่ภาวะวิกฤต และดำเนินการพยายามลดความเสียหายที่อาจเกิด หากเกิดวิกฤต	
ภาวะวิกฤต (crisis breakout): วิกฤตการณ์และความเสียหายที่เกิดขึ้น	**การจำกัดความเสียหาย (damage containment):** เกิดวิกฤตขึ้น โดยสมาชิกองค์กรพยายามจำกัดความเสียหายไม่ให้ลุกลามไปยังส่วนอื่นๆ ที่ยังไม่ได้รับผลกระทบ	**ภาวะวิกฤต (crisis):** เกิดภาวะวิกฤต โดยผู้เกี่ยวข้องดำเนินการเพื่อรับมือ แบ่งเป็น 2 ข้อย่อย ได้แก่ 1) ยอมรับวิกฤต (crisis recognition): เข้าใจและยอมรับว่าเกิดภาวะวิกฤตแล้ว 2) จำกัดวิกฤต (crisis containment) การตอบสนองต่อวิกฤต (crisis response): กลยุทธ์การตอบสนองวิกฤต (crisis response strategies)
ภาวะเรื้อรัง (chronic): ผลจากวิกฤตที่ยังคงอยู่	**ฟื้นตัว (recovery):** สมาชิกองค์กรกลับสู่การทำงานตามปกติให้เร็วที่สุด	
คลี่คลาย (resolution): ภาวะวิกฤตจบลง	**การเรียนรู้ (learning):** องค์กรทบทวน วิจารณ์ และบันทึกความพยายามในการจัดการวิกฤตของตน	**หลังวิกฤต (postcrisis):** ช่วงหลังจากแก้วิกฤตได้แล้ว แบ่งเป็น 3 ข้อย่อย ได้แก่ 1) เรียนรู้และปรับปรุงองค์กรเพื่อรับมือวิกฤตครั้งต่อไป 2) สร้างความมั่นใจต่อผู้มีส่วนได้ส่วนเสียในเรื่องศักยภาพขององค์กรในการรับมือกับภาวะวิกฤต 3) ตรวจสอบให้แน่ชัดว่าวิกฤตได้จบลงแล้วอย่างแท้จริง

หมายเหตุ. ดัดแปลงจาก *"ตารางเปรียบเทียบแนวทางการจัดการวิกฤต (Comparison of Staged Approached to Crisis Management)"* จาก *Ongoing Crisis Communication: Planning, Managing, and Responding* (3rd ed.) (p. 10) โดย Coombs, 2012, California, CA: SAGE Publications. (Coombs, 2012, p. 10)

แม้ว่าหลักการจัดการวิกฤตถูกคิดและพัฒนาขึ้นมาครั้งแรกในยุคภูมิทัศน์สื่อดั้งเดิม แต่ได้มีการพัฒนาเรื่อยมาเพื่อให้สอดรับกับการเปลี่ยนแปลงของเทคโนโลยีการสื่อสารในยุคภูมิทัศน์สื่อดิจิทัลปัจจุบัน ทำให้หลักการและแนวคิดการจัดการวิกฤตมีศักยภาพ และบทบาทในการจัดการวิกฤตทั้งในพื้นที่สื่อดั้งเดิมและพื้นที่สื่อใหม่ของการสื่อสารออนไลน์ โดยการศึกษาเกี่ยวกับหลักการจัดการวิกฤตตั้งแต่แรกเริ่มจนถึงปัจจุบันยังยืนยันว่า กุญแจสำคัญของการจัดการวิกฤต คือ การสร้างความเชื่อมั่นต่อสาธารณชน (public trust) ด้วยการเปิดเผยข้อมูลที่องค์กรมีเกี่ยวกับภาวะวิกฤตหรือการให้ข้อมูลที่เป็นความจริง ประกอบกับการนำเสนอแนวปฏิบัติในภาวะวิกฤตแก่สาธารณชนและผู้มีส่วนได้ส่วนเสีย

อย่างไรก็ตาม ในทางปฏิบัติยังมีข้อผิดพลาดที่มักพบในการจัดการวิกฤตที่สวนทางกับหลักการทางวิชาการอยู่ คือ หลายหน่วยงานยังคงใช้การแถลงการณ์ต่อสาธารณะว่า สามารถควบคุมปัญหาได้ ทั้งที่ในความเป็นจริงยังจัดการไม่ได้ หรือการให้ข้อมูลชี้นำว่า ปัญหาที่เกิดไม่ใช่เรื่องใหญ่ ทั้งที่เป็นเรื่องใหญ่ (Clemmitt, 2015, pp. 6-8) แต่แนวทางจัดการวิกฤตไม่มีแนวทางใดที่ถูกต้องตายตัว เนื่องจากวิกฤตไม่สามารถคาดเดาได้ และมีรูปแบบเฉพาะเจาะจงขึ้นอยู่กับลักษณะธรรมชาติของวิกฤตและองค์กร การศึกษาการจัดการวิกฤตจึงเป็นได้เพียงแนวทางการรับมือในภาพกว้าง ส่วนการรับมือหรือการดำเนินงานในเชิงลึกของการปฏิบัติองค์กรต่างต้องทำการรวบรวมข้อมูล ศึกษา ตัดสินใจดำเนินการด้วยวิธีการต่างๆ ด้วยตนเองและฝึกซ้อมรับมือกับวิกฤตอย่างสม่ำเสมอ ฉะนั้น การถอดบทเรียนการจัดการวิกฤตจึงยังคงมีประโยชน์ในการเพิ่มองค์ความรู้ และนำเสนอหลักการที่สามารถนำไปปรับใช้กับวิกฤตและองค์กรที่อยู่ในบริบทใกล้เคียงกันได้อย่างมีประสิทธิภาพมากที่สุด

นอกจากกรอบแนวคิดที่ใช้จัดการวิกฤตจะมีการปรับตัวตามการเปลี่ยนแปลงของบริบทสังคมในแต่ละช่วงสมัยแล้ว การศึกษาทบทวนงานศึกษาวิจัยจำนวนหนึ่งให้ผลยืนยันตรงกันถึงบทบาทสื่อสังคมออนไลน์โดยเฉพาะ Facebook ในการจัดการวิกฤตที่เพิ่มขึ้น เช่น งานวิจัยจำนวนหนึ่งที่ชี้ให้เห็นว่า Facebook ได้รับความไว้วางใจทั้งในระดับองค์กร และระดับปัจเจกบุคคลในฐานะช่องทางการสื่อสารที่ใช้ในการจัดการภาวะวิกฤตที่มีประสิทธิภาพ (ปรีดิ์เปรม ชัยกิจ, 2559; เอกภพ จึงกุล, 2558; Eriksson & Olsson, 2016; Szymczak, Kuecuekbalaban, Lemanski, & Knuth, 2016) งานวิจัยอีกจำนวนหนึ่งชี้ให้เกิดความสนใจเรื่องตัวชี้วัดต่างๆ ที่เกี่ยวข้อง เช่น งานวิจัยที่มุ่งเน้นการศึกษาจุดต่างเรื่องเวลาในการจัดการ

วิกฤตออนไลน์และออฟไลน์ ผลการศึกษาเผยให้เห็นการหน่วงเวลาในการตอบสนองต่อวิกฤตที่ยอมรับได้ลดลงจากช่วงเวลา 1-2 วัน ในภูมิทัศน์สื่อดั้งเดิม เป็น ภายใน 1 ชั่วโมง หรือไม่เกิน 1 วัน ของสื่อออนไลน์[5] (Stríteský et al., 2015) และในมุมของผู้ใช้สื่อในฐานะผู้มีส่วนได้ส่วนเสีย มีงานวิจัยที่สะท้อนให้เห็นว่า ประชาชนคาดหวังให้มีการตอบสนองต่อวิกฤตเร็วขึ้นตามเทคโนโลยีในยุคดิจิทัลที่เอื้อให้การสื่อสารเป็นไปอย่างรวดเร็ว (Clemmitt, 2015; Roshan, Warren, & Carr, 2015) เป็นต้น

อย่างไรก็ตาม ข้อค้นพบของงานวิจัยเรื่องระยะหน่วงเวลายังมีข้อจำกัดอยู่ คือ ด้วยธรรมชาติของวิกฤตที่มีรายละเอียดแตกต่างกันไปในแต่ละกรณี และด้วยลักษณะทางประชากรในแต่ละประเทศที่ต่างกัน ข้อค้นพบนี้จึงยังไม่สามารถนำมาใช้เป็นข้อสรุปในทุกพื้นที่ได้ แต่ในภาพรวมยังสามารถสรุปได้ว่า หน่วงเวลาการตอบสนองวิกฤตในบริบทของการสื่อสารออนไลน์ถูกบีบให้สั้นลง

งานศึกษาที่ผ่านมามีการนำแนวคิดการจัดการวิกฤตไปใช้วิเคราะห์การจัดการวิกฤตที่มี Facebook เข้ามาเกี่ยวข้องในวิกฤตหลากหลายประเภท เช่น งานวิจัยที่ศึกษาการใช้ Facebook ของธุรกิจโรงแรมในการจัดการภาวะวิกฤตที่เกิดจากภัยธรรมชาติ (Möller, Wang, & Nguyen, 2018) งานวิเคราะห์การใช้ Facebook ในภาวะวิกฤตที่เกิดจากการแพร่ระบาดของไวรัสซิกา (Zika outbreak) ในสาธารณรัฐสิงคโปร์ (Lwin, Lu, Sheldenkar, & Schulz, 2018) งานวิจัยเชิงทดลองที่ทดสอบกลยุทธ์การตอบสนองวิกฤตที่ใช้บน Facebook เพื่อศึกษาผลกระทบต่อชื่อเสียง ความน่าเชื่อถือ และความวางใจที่ผู้มีส่วนได้ส่วนเสียของโรงพยาบาล (DiStaso, Vafeiadis, & Amaral, 2015) และนอกเหนือกรอบแนวคิดเรื่องการจัดการวิกฤตยังมีบทความวิชาการจำนวนหนึ่งศึกษาวิกฤตเกี่ยวกับการละเมิดข้อมูลส่วนตัวผู้ใช้ขององค์กรต่างๆ รวมถึงหนึ่งในวิกฤตที่ Facebook ประสบในมิติด้านกฎหมาย การกำกับดูแล และนโยบาย (Bennett, 2018; Isaak & Hanna, 2018; Marcus, 2018; Tuttle, 2018) ในส่วนของ Yahoo มีบทความวิชาการที่ศึกษาในเชิงนโยบายและกฎหมาย (Trautman & Ormerod, 2017) สำหรับ Google+ เนื่องจากเหตุการณ์พึ่งตกเป็นข่าวเมื่อเดือนตุลาคมที่ผ่านมา จึงอาจเร็วเกินไปที่จะมีบทความวิชาการที่ศึกษาเรื่องนี้

[5] ข้อค้นพบนี้ได้จากงานวิจัยที่สำรวจความเห็นของกลุ่มตัวอย่างในสาธารณรัฐเช็กในช่วงเดือนมิถุนายน-ตุลาคม ปี ค.ศ. 2014 (Stříteský, Stránská, & Drábik, 2015)

นอกจากนี้ หากมองในภาพรวมจะเห็นว่า มีงานวิจัยที่มุ่งเจาะลึกเฉพาะเรื่องการจัดการวิกฤตเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลของผู้ใช้ที่น่าสนใจ งานดังกล่าวอธิบายว่าเนื่องจากวิกฤตเกี่ยวกับการจัดการข้อมูลเป็นเรื่องเฉพาะทาง จึงต้องมีการดำเนินการจัดการวิกฤตที่แตกต่างจากการจัดการวิกฤตในโลกออนไลน์ชนิดอื่นๆ และวิธีการที่มีอยู่อาจใช้ได้ไม่เต็มศักยภาพ จึงเสนอแนวทางใหม่ในการจัดการวิกฤตชนิดนี้ ซึ่งผลการศึกษาชี้ว่าภาพลักษณ์และชื่อเสียงขององค์กรเป็นตัวแปรสำคัญที่จะบ่งชี้ว่า ผลของวิกฤตเรื่องข้อมูลจะรุนแรงหรือไม่ ในกรณีที่เป็นองค์กรที่มีชื่อเสียงมาก การเปิดเผยว่าข้อมูลถูกละเมิดจะมีผลกระทบทางลบต่อองค์กรน้อยว่าองค์กรที่มีระดับชื่อเสียงที่ต่ำกว่า และสำหรับองค์กรที่มีชื่อเสียงมาก กลยุทธ์การตอบสนองวิกฤตไม่ถือเป็นตัวแปรสำคัญ แต่กลยุทธ์เหล่านี้ถือเป็นตัวแปรสำคัญสำหรับองค์กรที่มีชื่อเสียงในระดับต่ำกว่า นอกจากนี้ เนื่องจากงานศึกษาก่อนหน้ายังไม่มีการนำเสนอแนวทางเฉพาะสำหรับจัดการวิกฤตเรื่องการละเมิดข้อมูล งานชิ้นนี้จึงได้นำเสนอกลยุทธ์การตอบสนองวิกฤตสำหรับจัดการวิกฤตที่เกิดจากการละเมิดข้อมูลที่เน้นการรักษาและฟื้นฟูภาพลักษณ์ (image restoration) ไว้ รายละเอียดตาม**ตารางที่ 2** (Gwebu, Wang, & Wang, 2018) แต่ด้วยธรรมชาติของวิกฤตที่มีความแตกต่างกันในแต่ละกรณีอย่างเห็นได้ชัด เพราะบริบททั้งภายในและนอกองค์กรแต่ละแห่งแตกต่างกัน การเสนอแนวคิดใหม่นี้ จึงยังต้องผ่านการนำไปพิสูจน์ต่อยอดเพื่อให้เกิดความเที่ยงและตรงต่อไป

ตารางที่ 2 แสดงกลยุทธ์การจัดการวิกฤตเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลของผู้ใช้

รูปแบบกลยุทธ์	กลยุทธ์	คำอธิบาย
กลยุทธ์การผ่อนปรน (accommodative strategy)	การขอโทษ (apology)	กล่าวขอโทษอย่างตรงไปตรงมาสำหรับเหตุการณ์การละเมิดข้อมูลที่เกิดขึ้น
	การแก้ไขข้อผิดพลาด หรือ การเยียวยา (remedial actions)	ดำเนินการแก้ไขและควบคุมความเสียหายที่เกิดขึ้น เช่น จ่ายค่าชดเชย หรือพัฒนาระบบความปลอดภัยที่ดูแลรักษาข้อมูล
กลยุทธ์การใช้เหตุผล (moderate strategy)	การประจบ (ingratiation)	พยายามทำให้ผู้มีส่วนได้ส่วนเสียชอบองค์กร โดยการยกข้อดีขึ้นมา
	การให้เหตุผล (justification)	พยายามลดระดับความเสียหายด้วยเหตุผล เช่น แถลงว่าข้อมูลที่ถูกละเมิดไปมีการเข้ารหัสป้องกันไว้ หรือ เชื่อว่าข้อมูลจะไม่ถูกนำไปใช้ในทางมิชอบ
กลยุทธ์การป้องกัน (defensive strategy)	การปฏิเสธ (denial)	วางกรอบการให้ข้อมูล ว่าไม่มีการละเมิดเกิดขึ้น
	การแก้ตัว (excuse)	พยายามปัดหรือลดความรับผิดชอบขององค์กรต่อเหตุละเมิดข้อมูล เช่น ให้ข้อมูลว่าการละเมิดเกิดจากมือที่สาม
กลยุทธ์กอบกู้ภาพลักษณ์ (image renewal)	การให้คำมั่นเพื่อแก้ไข (correction commitment)	สร้างความมั่นใจกับผู้มีส่วนได้ส่วนเสียว่าจะไม่เกิดเหตุการณ์ซ้ำ
	การให้คำมั่นต่อผู้มีส่วนได้ส่วนเสีย (stakeholder commitment)	สร้างความเชื่อมั่นต่อผู้มีส่วนได้ส่วนเสียว่า ต่อไปจะได้รับสินค้า/บริการที่ดีที่สุด
	การให้คำมั่นเรื่องค่านิยม (value commitment)	สร้างความเชื่อมั่นต่อผู้มีส่วนได้ส่วนเสียว่าองค์กรจะยึดมั่นค่านิยมองค์กร ในการรักษาข้อมูลส่วนบุคคลของผู้ใช้อย่างดีที่สุด

วิเคราะห์ข้อมูล

งานศึกษาที่ผ่านมาแสดงให้เห็นว่า มีการพัฒนากรอบแนวคิด แนวทาง และหลักการทั้งในมุมของการจัดการวิกฤตในภาพรวม และในอีกมุมที่มุ่งเน้นการจัดการวิกฤตที่เจาะจงเรื่องการจัดการข้อมูลส่วนตัวของผู้ใช้ในสื่อออนไลน์อีกด้วย ในส่วนการวิเคราะห์ข้อมูลของบทความนี้ จึงมุ่งเน้นการศึกษาและถอดบทเรียนการจัดการวิกฤตการละเมิดข้อมูลส่วนบุคคล รวมถึงเหตุข้อมูลหลุดขององค์กรยักษ์ใหญ่ที่เก็บข้อมูลส่วนบุคคลของผู้ใช้จำนวนมหาศาลเอาไว้ โดยใช้แนวคิดการจัดการวิกฤตเป็นกรอบแนวคิดในการวิเคราะห์ การนำเสนอผลการวิเคราะห์ข้อมูลจะแบ่งออกเป็น 3 ส่วน: ส่วนที่ 1 จะเป็นการวิเคราะห์ข้อมูลและถอดบทเรียนการจัดการวิกฤตของ Facebook ส่วนที่ 2 จะเป็นของ Yahoo และส่วนที่ 3 เป็นของ Google+ รายละเอียดดังต่อไปนี้

1. Facebook

เหตุการณ์ครั้งที่ 1: ในช่วงเดือนมีนาคม ค.ศ. 2018 สำนักข่าวต่างรายงานเรื่องเหตุข้อมูลผู้ใช้ Facebook ถูกละเมิด ต้นตอของเรื่อง คือ แอปพลิเคชันที่ชื่อ *"thisisyourdigitallife"* พัฒนาโดย Aleksandr Kogan นักวิชาการจาก Cambridge University ที่ทำงานวิจัย[6] ภายใต้สังกัด Global Science Research (GSR) ซึ่งร่วมมือกับ Cambridge Analytica ในการเก็บข้อมูลอาสาสมัครผู้ใช้แอปพลิเคชัน จำนวน 350,000 คน ที่ได้รับค่าตอบแทนให้เข้าร่วมโครงการนี้ และยินยอมให้มีการเก็บข้อมูลส่วนตัวไปใช้ศึกษา แต่แอปพลิเคชันดึงข้อมูลเพื่อนใน Facebook ของกลุ่มตัวอย่างไปด้วย เนื่องจากค่าอัตโนมัติเบื้องต้นที่ผู้ใช้เลือกเพื่อเข้าใช้งานแอปพลิเคชัน หรือเกมทั่วไป ถูกตั้งไว้เป็นการอนุญาตให้เข้าถึงข้อมูลโพรไฟล์—ชื่อ อีเมล เพศ วันเกิด เมืองที่อยู่ สิ่งที่ชอบ (Likes) และเนื้อหาอื่นๆ ที่จัดอยู่ในหมวดนี้ ที่มีการตั้งค่าเป็นสาธารณะไว้

[6] งานวิจัยชิ้นนี้จัดทำในช่วงปี ค.ศ. 2013 โดยมีวัตถุประสงค์เพื่อวิเคราะห์โพรไฟล์ โดยใช้วิธีเชิงจิตวิทยาที่เรียกว่า "*OCEAN*" ซึ่งประกอบไปด้วยการวิเคราะห์ 5 ด้าน ได้แก่ ความเปิดรับ (ประสบการณ์) (openness to experience) ความพิถีพิถัน/ความรอบคอบ (conscientiousness) ความสนใจต่อสิ่งภายนอก (extraversion) ความยินยอมเห็นใจ (agreeableness) และความไม่เสถียรทางอารมณ์ (neuroticism) เพื่อศึกษาความสัมพันธ์กับพฤติกรรมการไลก์และแชร์ (like and share) ใน Facebook (Isaak & Hanna, 2018, p. 57)

รวมถึง *"เพื่อน"* ด้วย เท่ากับว่ามีข้อมูลที่เก็บไปได้มากกว่า 50 ล้านคน หากมองแบบผิวเผิน การได้ข้อมูลเหล่านี้ไป อาจดูเหมือนไม่อันตราย แต่ชุดข้อมูลนี้สามารถนำไปพัฒนาต่อยอดเพื่อระบุพฤติกรรมของผู้ใช้ที่แม่นยำได้ ภายหลัง SCL องค์กรในเครือของ Cambridge Analytica ได้ทำสัญญาซื้อขายข้อมูลกับ GSR ลงวันที่ 4 มิถุนายน ค.ศ. 2014 เพื่อนำข้อมูลชุดนี้ไปใช้ออกแบบโปรแกรมช่วยในโครงการโฆษณารณรงค์หาเสียงเลือกตั้งประธานาธิบดีของ Donald Trump ในปี ค.ศ. 2016 จำนวนข้อมูลกว่า 50 ล้านชุดที่ได้ไป เป็นข้อมูลที่ตรงกับผู้มีสิทธิ์เลือกตั้งในสหรัฐฯ ถึง 1 ใน 4 แต่ด้วยความที่ไม่มีกฎหมายห้ามการซื้อ ขาย หรือใช้ข้อมูลผู้มีสิทธิ์เลือกตั้งในประเทศสหรัฐอเมริกา จุดนี้จึงเป็นเหมือนพื้นที่สีเทา (Badshah, 2018; Cadwalladr & Graham-Harrison, 2018; Carr, 2018; Channel NewsAsia, 2018; Isaak & Hanna, 2018; Keach, 2018; Winston, 2018)

ก่อนวิกฤต: ในขั้นก่อนวิกฤต Facebook ไม่มีการนำหลักการจัดการวิกฤตมาใช้ ทำให้องค์กรตกอยู่ในภาวะวิกฤตในที่สุด หลังการซื้อขายข้อมูลชุดดังกล่าว ในปี ค.ศ. 2015 Facebook ทราบเรื่อง จึงแถลงถึงเหตุละเมิดข้อมูลดังกล่าว แต่ไม่มีการแจ้งเตือนผู้ใช้ มีเพียง *"การดำเนินการด้านความปลอดภัยไม่กี่ขั้นตอนเท่านั้น"* (Badshah, 2018; Cadwalladr & Graham-Harrison, 2018) ณ จุดนี้ หากมองด้วยกรอบคิดการจัดการวิกฤต เรียกได้ว่า ยังอยู่ในขั้นก่อนวิกฤตในแบบจำลอง 3 ขั้นตอน เพราะมีเพียงการตรวจจับสัญญาณได้จากการทราบเรื่องการซื้อขายข้อมูลเท่านั้น ยังไม่เกิดวิกฤต หากพิจารณาความเคลื่อนไหวของ Facebook แล้ว จะเห็นได้ว่ายังไม่มีการดำเนินการป้องกันและเตรียมรับวิกฤตอย่างจริงจังเท่าที่ควร อาทิ การแจ้งเตือนผู้ใช้หรือการแจ้งเตือนวงกว้าง (mass notification) ที่ถือเป็นรูปแบบการสื่อสารตามหลักการจัดการวิกฤตที่พึงกระทำ (Coombs, 2009, pp. 100-102; 2012, pp. 25-114) ต่อมารายงานข่าวแจ้งว่าในเดือนสิงหาคมปี ค.ศ. 2016 Facebook ได้ส่งจดหมายถึง GSR เพื่อขอให้ลบชุดข้อมูลดังกล่าวทิ้ง แต่ก็ไม่มีกระบวนการติดตามผลว่ามีการลบข้อมูลตามคำขอหรือไม่ จากการให้สัมภาษณ์สื่อของ Chirstopher Wylie ผู้ที่เคยทำงานในทีมวิจัยกับ Aleksandr Kogan ที่กล่าวว่า *"สองปี แต่ไม่ทำอะไรเลย ไม่มีแม้แต่การตรวจสอบว่าได้ลบข้อมูลจริงหรือไม่ที่ให้ทำก็แค่ให้ทำเครื่องหมายในฟอร์มและส่งกลับแค่นั้น"* (Cadwalladr & Graham-Harrison, 2018) การดำเนินการของ Facebook ตอกย้ำว่า องค์กรยังไม่จริงจังกับการติดตามผลการลบข้อมูลหลังการส่งจดหมายถึง GSR และหากมองในส่วนของการเตรียมรับวิกฤต จะเห็นได้ว่า

ยังขาดการประเมินวิกฤต หรือหากมีการประเมินอาจเรียกได้ว่า ประมาท เพราะในความเป็นจริงควรตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลของผู้ใช้ที่เป็นเหมือนเส้นเลือดใหญ่ของบริการที่หล่อเลี้ยงองค์กรอยู่ และควรจะมีการเตรียมการที่น่าจะทำได้ เช่น ใช้ระบบแจ้งเตือนวงกว้างพร้อมระบุขั้นตอนการเปลี่ยนการตั้งค่าที่จำเป็นเพื่อให้ผู้ใช้รักษาสิทธิ์เหนือข้อมูลของตนตั้งแต่ตอนทราบเรื่อง (Coombs, 2009, pp. 100-102; 2012, pp. 25-114) หรือติดตามและพิสูจน์ผลการลบข้อมูลกับ GSR เป็นต้น

ภาวะวิกฤต: เมื่อเริ่มเข้าสู่ภาวะวิกฤต Facebook เลือกที่จะปฏิเสธวิกฤต ทำให้สถานการณ์เลวร้ายลง แต่มีการปรับกลยุทธ์การตอบสนองวิกฤตเพื่อกู้สถานการณ์ในภายหลัง ในช่วงต้นเดือนมีนาคม ปี ค.ศ. 2018 มีการรายงานข่าวเปิดเผยรายละเอียดต้นตอของเหตุการณ์นี้ โดยทีมข่าว Observer ของ The Guardian ที่ได้ข้อมูลมาจาก Wylie และหลังจากรายงานข่าว 4 วัน คือ ในวันที่ 16 มีนาคม Facebook ได้ประกาศว่า *“ต้นตอของข้อมูลรั่วน่าจะเป็น Cambridge Analytica”* และทนายของบริษัทยังได้ตอบกลับทีมข่าวว่า การรายงานข่าวว่า *“ถูกเจาะข้อมูล”* เป็นเท็จ ทำให้องค์กรเสื่อมเสียชื่อเสียง เพราะข้อมูลที่ได้ไปเป็นข้อมูลที่ได้รับความยินยอมจากผู้ใช้ (Cadwalladr & Graham-Harrison, 2018; Grewal, 2018; Winston, 2018) หากพิจารณาเรื่องของช่วงเวลาในการตอบสนองวิกฤตของ Facebook เทียบกับระดับหน่วงเวลาที่ยอมรับได้ต่อการตอบสนองวิกฤตในงานวิจัยของ Stríteský และคณะที่ได้กล่าวถึงไปก่อนหน้า จะเห็นได้ว่า ในภูมิทัศน์สื่อดิจิทัลปัจจุบัน หน่วงเวลาที่ยอมรับได้ลดลงเหลือเพียงภายใน 1 วันเท่านั้น และความคาดหวังของคนยุคนี้ตั้งอยู่บนพื้นฐานของความเร็ว เรียกได้ว่า การตอบสนองวิกฤตของ Facebook ในครั้งนี้ที่ใช้เวลาจำนวน 4 วัน ซึ่งค่อนข้างเร็ว ถึงแม้ว่าจะไม่เป็นไปตามความคาดหวังที่อ้างอิงจากข้อค้นพบที่ระบุว่า ต้องตอบสนองภายใน 1 วัน ทั้งนี้ อาจเนื่องด้วยปัจจัยที่เกี่ยวข้องในกรณีของ Facebook ต่างจากบริบทในการศึกษาของงานดังกล่าว (Stríteský et al., 2015) ระดับความคาดหวังนี้ จึงอาจมีความคลาดเคลื่อนอยู่บ้าง แต่ในภาพรวมการดำเนินงานล่าช้ากว่าจุดอ้างอิงถึง 3 วัน สภาพการณ์นี้มีส่วนส่งผลให้วิกฤตลุกลามในวงกว้างขึ้นอีกด้วย เพราะแม้จะตอบสนองเร็วแต่ก็ยังถือว่าไม่เป็นไปตามคาดและยังขาดการป้องกันกับการเตรียมการในขั้นก่อนวิกฤตอยู่

ในภาวะวิกฤต Facebook เลือกตอบสนองวิกฤตด้วยกลยุทธ์การปฏิเสธ (denial posture) ซึ่งงานวิจัยของ Gwebu และคณะ (2018) ที่เจาะลึกเรื่อง

การจัดการวิกฤตที่เกิดจากการละเมิดข้อมูลตามที่เกริ่นไว้ข้างต้น เผยให้เห็นว่า เนื่องจากวิกฤตชนิดนี้มักสร้างความเสียหายด้านการเงิน ส่วนแบ่งการตลาด ยอดขาย ภาพลักษณ์ และยังทำลายความเชื่อมั่นของลูกค้าที่มีต่อองค์กรอีกด้วย ฉะนั้น วิกฤตด้านข้อมูลนี้จึงจำเป็นต้องมีกลไกการจัดการวิกฤตที่เฉพาะเจาะจง แต่ด้วยงานศึกษาที่เจาะลึกด้านนี้โดยเฉพาะยังมีไม่มากนัก ที่ผ่านมาองค์กรที่ประสบเหตุจึง *"ยังคงใช้หลักการจัดการวิกฤตทั่วไปในการรับมืออยู่"* ซึ่งหลักการทั่วไปที่ว่านี้จะเน้นการป้องกันภาพลักษณ์ชื่อเสียงขององค์กรเป็นหลัก กลยุทธ์การปฏิเสธจึงมักถูกหยิบมาใช้ ในบางกรณีอาจถึงขั้นใช้เพื่อปัดความรับผิดชอบหรือหาตัวผู้รับผิด (Gwebu et al., 2018, pp. 684-686)

แต่อย่างไรก็ดี งานวิชาการอีกจำนวนหนึ่งแสดงให้เห็นว่า หลักการจัดการวิกฤตมีการพัฒนาเรื่อยมาเพื่อรองรับความเปลี่ยนแปลงต่างๆ จึงยังคงสามารถใช้เป็นแนวทางพื้นฐานเพื่อรับมือกับวิกฤตในยุคดิจิทัลได้ แต่จะได้ประสิทธิภาพมากน้อยเพียงใดนั้น ขึ้นอยู่กับปัจจัยทั้งภายในและภายนอกองค์กร (Clemmitt, 2015, pp. 6-8) ในกรณีของ Facebook หากมีการประเมินที่รอบคอบกว่านี้ องค์กรควรใช้กลยุทธ์การผ่อนปรน (accommodative strategy) โดยเลือกที่จะยอมรับวิกฤตและใช้กลยุทธ์การขอโทษผนวกกับการชดเชยหรือแก้ไข (rebuilding posture: apology and compensation /remedial actions) เพื่อแสดงตัวยอมรับความผิดพลาดและแสดงความพร้อมในการรับผิดชอบต่อเรื่องที่เกิดขึ้น อันจะเป็นการเอื้อต่อการจำกัดความเสียหายที่อาจเกิด และพลิกฟื้นความเชื่อมั่นที่มีต่อองค์กรแทน (Coombs, 2012, pp. 154-157; Gwebu et al., 2018, p. 687 ซึ่งน่าจะช่วยบรรเทาความเสียหายจากหนักเป็นเบาได้มากพอสมควร แต่ Facebook ใช้กลยุทธ์การปฏิเสธจึงทำให้เกิดกระแสความไม่พอใจในวงกว้างจากหลายภาคส่วน เช่น รัฐมนตรีกระทรวงยุติธรรมที่ทวีตข้อความ (tweet) เรียกร้องให้ทั้ง Facebook และ Cambridge Analytica รีบออกมาชี้แจงเพิ่มเติมโดยด่วน และยังเสนอให้มีการเพิ่มกฎหมายกำกับดูแลเรื่องการโฆษณาหาเสียงเพื่ออุดช่องโหว่อีกด้วย

นอกจากการปฏิเสธในครั้งก่อนแล้ว Facebook ยังคงยึดติดกับกลยุทธ์การปฏิเสธวิกฤตเช่นเดิม Simon Milner ตัวแทนองค์กรในสหราชอาณาจักรตอบคำถามนักข่าวที่ถามถึงวิกฤตครั้งนี้ โดยให้ข้อมูลว่า *"ข้อมูลที่เอาไปใช้อาจไม่ใช่ที่ Facebook จัดให้ อาจเป็นข้อมูลที่มีการเก็บไปเองก็ได้"* (Cadwalladr & Graham-Harrison, 2018) จากการตอบคำถามนี้จะเห็นได้ว่า Facebook

ยังคงใช้กลยุทธ์การปฏิเสธอยู่ เห็นได้จากการที่ผู้แทนองค์กรออกมาให้ข้อมูลสอดคล้องไปในทางเดียวกัน (Coombs, 2009, 2012) ในวันที่ 21 มีนาคม ค.ศ. 2018 สำนักข่าวต่างรายงานว่า ในสื่อสังคมออนไลน์เกิดกระแสรณรงค์ *"#deletefacebook"* ให้ลบแอปพลิเคชัน และบัญชีผู้ใช้ Facebook กระแสนี้ขึ้นเป็นหัวข้อยอดนิยมใน Twitter บางสำนักข่าวมีการรายงานเพิ่มเติมเรื่องขั้นตอนการลบบัญชีและแอปพลิเคชันด้วย ซึ่งกระแสนี้ผลักดันให้ Mark Zuckerberg ประธานบริหารของ Facebook ออกมาแสดงท่าทีตอบสนองต่อเหตุการณ์ดังกล่าว

ในวันเดียวกันนี้ Zuckerberg ให้สัมภาษณ์สื่อแสดงความตระหนักถึงการเกิดวิกฤตด้านความเชื่อใจของผู้ใช้ต่อองค์กร โดยกล่าวว่า *"การที่ผู้ใช้รู้สึกไม่ดี เป็นเรื่องใหญ่และเป็นเรื่องไม่ดี... เราต้องแสดงความรับผิดชอบ ต้องแก้ไขแล้ว"* (D'Onfro, 2018b) ต่อมาในวันที่ 4 เมษายน ค.ศ. 2018 Facebook ออกแถลงการณ์ชี้แจงว่า ข้อมูลหลุดครั้งนี้มีโอกาสกระทบผู้ใช้ทั่วโลกกว่า 87 ล้านราย[7] ซึ่งมากกว่าที่สำนักข่าวต่างรายงานก่อนหน้าว่ากระทบผู้ใช้ราว 50 ล้านราย จะเห็นได้ว่า Zuckerberg เลือกใช้กลยุทธ์การผ่อนปรนโดยการขอโทษและยอมรับผิด พร้อมเผยข้อมูลอย่างตรงไปตรงมาแทนการปฏิเสธ (Badshah, 2018) ในกรณีนี้ การให้สัมภาษณ์ของประธานบริหารเป็นไปตามหลักการพื้นฐานในการจัดการวิกฤต คือ ในภาวะวิกฤต ผู้บริหาร/ผู้จัดการวิกฤตต้องแสดงตัวในภาวะวิกฤต (be present) และแสดงความจริงใจ (Coombs, 2012, pp. 27-28) ถึงแม้จะมีการแสดงตัวของประธานบริหารแล้วก็ตาม แต่การแสดงตัวที่ไม่ได้ทำในทันทีหลังถูกนำเสนอข่าว จึงเป็นเหตุให้วิกฤตยังคงพา Facebook เข้าสู่กระบวนการพิสูจน์ความจริงตามกฎหมายต่อไป ในวันที่ 11 เมษายน ค.ศ. 2018 ประธานบริหาร Facebook ได้เข้าให้การชี้แจงในการไต่สวนโดยรัฐสภาสหรัฐฯ (Congress) (Time, 2018) ซึ่งหลังจากการให้การนี้ กระแสด้านลบก็ยังคงดำเนินต่อไป

หลังวิกฤต: ในวันที่ 24 กรกฎาคม ค.ศ. 2019 ข่าวรายงานผลการพิจารณาคดีความเรื่อง *"การเก็บข้อมูลส่วนบุคคลของผู้ใช้"* ของ Facebook ใน **"เหตุการณ์ครั้งที่ 1"** ที่เกี่ยวโยงกับ *"การละเมิดโดย Cambridge Analytica"* (Cambridge Analytica data breach) โดยผลการพิจารณาระบุว่า Facebook *"หลอกลวง"*

[7] Facebook คำนวณจากจำนวนเต็มเพื่อนสูงสุดที่ผู้เสียหายแต่ละรายจะสามารถมีได้ (จำนวนตั้งต้นของผู้เสียหายจากแอปพลิเคชัน *"thisisyourdigitallife"* คือ 350,000 ราย) (Badshah, 2018)

(deceiving) ผู้ใช้ ในเรื่องความสามารถในการเก็บดูแลข้อมูลส่วนบุคคลของผู้ใช้เป็นความลับ ในการนี้ Facebook ถูกตัดสินโทษปรับจำนวน 5 พันล้านเหรียญสหรัฐฯ ซึ่งนับเป็นการปรับที่สูงที่สุดในเรื่องเกี่ยวกับการละเมิดความเป็นส่วนตัวของลูกค้า นอกจากนี้ Facebook ยังต้องทำการปรับโครงสร้างองค์กรและแนวทางการดำเนินงานเพื่อให้บริการที่เกี่ยวข้องกับความเป็นส่วนตัวของผู้ใช้มีประสิทธิภาพสูงขึ้น โดย Mark Zuckerberg ได้โพสต์ข้อความใน Facebook ส่วนตัวว่า *"เรามีความตั้งใจจะเปลี่ยนวัฒนธรรมเรื่องความเป็นส่วนตัวใหม่หมดเพื่อลดโอกาสการเกิดการละเมิดอีก... แม้ว่าเราจะตกลงจ่ายค่าปรับครั้งประวัติศาสตร์ แต่ที่สำคัญกว่านั้นคือ เราจะเปลี่ยนโครงสร้างครั้งใหญ่ที่จะเปลี่ยนวิธีการดำเนินการของบริษัทเลยก็ว่าได้"* (Davies & Rushe, 2019) กรณีนี้ หากมองด้วยกรอบคิดเรื่องการจัดการวิกฤตแล้ว จะเห็นได้ว่า Zuckerberg ณ จุดนี้เลือกใช้ *"กลยุทธ์กอบกู้ภาพลักษณ์"* (image renewal) ทั้ง 3 ข้อที่ปรากฏใน **ตารางที่ 1** คือ เป็นการให้คำมั่นเพื่อแก้ไข (correction commitment) ต่อทั้งสาธารณชนและต่อผู้มีส่วนได้ส่วนเสีย (stakeholder commitment) และยังถือเป็นการให้คำมั่นเรื่องค่านิยม (value commitment) ขององค์กร ว่าจะมีการปรับปรุงโครงสร้างครั้งใหญ่เพื่อการรักษาข้อมูลอย่างมีประสิทธิภาพมากขึ้นด้วย

เหตุการณ์ครั้งที่ 2: ช่วงเดือนกันยายน ค.ศ. 2018 ในขณะที่วิกฤตครั้งแรกยังไม่คลี่คลาย ข่าวหลายสำนักรายงานเรื่องเครือข่ายคอมพิวเตอร์ของ Facebook ถูกโจมตีและจารกรรมข้อมูลไป

ก่อนวิกฤต: จากรายงานข่าว Facebook เผยว่า ระบบของตนน่าจะเริ่มถูกโจมตีในวันที่ 14 กันยายน ค.ศ. 2018 เพราะมีจำนวนผู้ลงบันทึกเข้าใช้ (login) ที่สูงผิดปกติ (Rodriguez, 2018; Tynan, 2018) ซึ่งเรียกว่า เป็นการตรวจพบสัญญาณเตือนการเกิดวิกฤตในขั้นก่อนเกิดวิกฤต (Coombs, 2009, 2012) แต่ยังไม่มีการดำเนินการป้องกันหรือการเตรียมการใดๆ เพื่อรับมือกับวิกฤต

ภาวะวิกฤต: เนื่องจากองค์กรยังคงตื่นตัวกับภาวะวิกฤตในครั้งแรก เหตุการณ์ครั้งที่ 2 นี้จึงได้รับการตอบสนองที่ทันท่วงทีขึ้น โดยในช่วงต้น องค์กรยังคงใช้กลยุทธ์การผ่อนปรนเช่นเดียวกับเหตุการณ์แรก แต่ในช่วงท้ายได้เปลี่ยนมาใช้กลยุทธ์การปฏิเสธเพื่อรับมือกับวิกฤตที่ขยายวงกว้างขึ้น Facebook พบว่าระบบถูกเจาะในวันที่ 25 กันยายน ค.ศ. 2018 โดยมีการคาดการณ์ว่า แฮกเกอร์เจาะกลุ่มผู้ใช้ตั้งต้นจำนวนราว 400,000 ราย และขยายจากกลุ่ม *"เพื่อน"* ไปยังบัญชีผู้ใช้อื่นๆ กระทบข้อมูลผู้ใช้กว่า 14 ล้านราย[8] และกระทบเว็บไซต์อื่นที่ผู้ใช้ผูกกับ

การเข้าใช้ Facebook ด้วย (single-sign-in) ซึ่งสาเหตุการโจมครั้งนี้ คาดว่าเกิดจากข้อบกพร่อง 3 ข้อ (bug) ของระบบ Facebook: 2 ข้อ เกิดจากเครื่องมือที่ใช้เพื่อพัฒนาความเป็นส่วนตัวของผู้ใช้ที่เรียกว่า *"View As"*[9] และอีก 1 ข้อบกพร่องจากเครื่องมือช่วยอัปโหลดวิดีโอวันเกิด (birthday video) ผนวกกับการโจมตีที่เกิดขึ้นหลังการปล่อยเครื่องมืออัปโหลดดังกล่าวออกมาให้ใช้ช่วงเดือนกรกฎาคม ค.ศ. 2017 Facebook เชื่อว่าเหล่านี้เป็นสาเหตุให้ข้อมูลผู้ใช้ถูกจารกรรมไปได้ แต่ยังไม่สามารถให้ข่าวหรือระบุตัวแฮกเกอร์ผู้โจมตีได้ เนื่องจากยังอยู่ในกระบวนการสืบสวนของ FBI ที่ขอให้ Facebook ปิดเรื่องนี้ไว้ก่อน (Isaac & Frenkel, 2018; John, 2018; Matsakis & Lapowsky, 2018; O'Flaherty, 2018; Rodriguez, 2018; Tynan, 2018) เนื่องจาก Facebook ยังคงดำเนินการภายใต้ภาวะวิกฤตค้างไว้จากเหตุการณ์ครั้งแรก การตอบสนองวิกฤตในเหตุการณ์ครั้งที่ 2 นี้ จึงมีการป้องกันที่เร็วขึ้นเมื่อเทียบกับเหตุการณ์แรก ในวันที่ 27 กันยายน ค.ศ. 2018 Facebook ทำการตั้งค่า *"access token"* ใหม่สำหรับผู้ใช้ที่เข้าข่ายได้รับผลกระทบ และสร้างเพจแจ้งเตือนความปลอดภัยเพื่อให้ผู้ใช้เข้าตรวจสอบว่า บัญชีของตนอยู่ในกลุ่มเสี่ยงหรือไม่ (Tynan, 2018) ในวันที่ 28 กันยายน Zuckerberg ได้กล่าวในงานแถลงข่าวว่า *"เราให้ความสำคัญกับเรื่องนี้จริงจัง...ผมดีใจที่เราพบปัญหา แต่ปัญหาที่แท้จริง คือการเกิดปัญหานี้ขึ้นตั้งแต่แรก"* (Isaac & Frenkel, 2018)

การตอบสนองวิกฤตครั้งนี้สะท้อนให้เห็นว่า Facebook ยังคงใช้กลยุทธ์การผ่อนปรนเช่นเดียวกับในช่วงหลังของเหตุการณ์แรก (Gwebu et al., 2018) ซึ่งเรียกได้ว่าได้ใช้ *"การเรียนรู้"* บทเรียนจากวิกฤตในครั้งที่ 1 และนำมาใช้ในการจัดการวิกฤตที่ 2

---

[8] Facebook แถลงในตอนต้นว่า คาดว่าจะกระทบผู้ใช้ประมาณ 50 ล้านราย และมีการประเมินโดยละเอียดอีกครั้งจึงแถลงว่า จำนวนผู้เสียหายที่คาดการณ์ คือ 30 ล้านราย แต่ผลการตรวจสอบพบว่าแฮกเกอร์สามารถเจาะข้อมูลไปได้เพียง 14 ล้านรายจากทั้งหมด 30 ล้านราย จึงมีการแถลงผลทดสอบอย่างเป็นทางการอีกครั้งที่ 14 ล้านราย (Rodriguez, 2018; Tynan, 2018)

[9] เป็นเครื่องมือที่อนุญาตให้ผู้ใช้ทำการตรวจสอบดูโพรไฟล์ของตนในมุมมองบุคคลอื่น ซึ่งในกระบวนการตรวจสอบระบบจะใช้ *"access token"* ที่เป็นเหมือนกุญแจในการเข้าถึงบัญชีของผู้ใช้โดยไม่ต้องทำการกรอกรหัสเข้าใช้ซ้ำอีกครั้ง ในกรณีนี้ ผู้โจมตีได้ *"กุญแจ"* ดังกล่าวไปทำให้สามารถเข้ามาล้วงข้อมูลส่วนบุคคลไปได้ (Isaac & Frenkel, 2018; John, 2018; Matsakis & Lapowsky, 2018; O'Flaherty, 2018; Rodriguez, 2018; Tynan, 2018)

(Coombs, 2012) ต่อมาในวันที่ 14 ธันวาคม ค.ศ. 2018 Facebook ได้แถลงเพิ่มเติมเรื่องข้อบกพร่องของระบบที่กระทบผู้ใช้กลุ่มเสี่ยงที่เคยอนุญาตให้แอปพลิเคชันภายนอกเข้าถึงภาพถ่ายของตนไว้ก่อนหน้าว่า จะสามารถเข้าถึงภาพอื่นๆ นอกเหนือจากภาพที่ได้รับอนุญาตเป็นเวลา 12 วัน ตั้งแต่วันที่ 13-25 กันยายนที่ผ่านมา โดยคาดว่ากระทบผู้ใช้กว่า 6.8 ล้านราย ณ จุดนี้ Facebook ยังคงใช้กลยุทธ์การขอโทษร่วมกับการแจ้งเตือนและการป้องกันด้วยการให้ผู้พัฒนาแอปพลิเคชันภายนอกที่เกี่ยวข้อง ลบภาพของผู้ใช้ที่ได้รับผลกระทบออก (Bar, 2018; Panchadar & Moon, 2018) หลังจากนี้เรื่องนี้เข้าสู่กระบวนการสอบสวนตามการร้องเรียนทางกฎหมายทั้งจากกลุ่มผู้มีส่วนได้ส่วนเสียและหน่วยงานกำกับดูแลที่เกี่ยวข้องเพื่อพิจารณาว่า Facebook ได้ละเมิดกฎหมายกำกับดูแลเรื่องสิทธิข้อมูลผู้ใช้อย่างไรบ้าง ซึ่ง Facebook ได้รับโทษปรับ (Sanders & Patterson, 2018) ต่อมาในวันที่ 18 ธันวาคม ค.ศ. 2018 The New York Times ได้เปิดเผยข้อมูลที่ได้จากบันทึกภายในระบบของ Facebook และจากการสัมภาษณ์อดีตพนักงานกว่า 50 คน ว่ามีการแชร์ข้อมูลส่วนบุคคลของผู้ใช้ร่วมกับองค์กรพันธมิตรถึงกว่า 150 องค์กร อาทิ Microsoft's Bing, Amazon, Yahoo, Spotify, Netflix, Huawei, และ Apple ในการนี้ โฆษกตัวแทนของ Facebook และตัวแทนองค์กรที่เกี่ยวข้องต่างเผยว่า การแชร์ข้อมูลดังกล่าวไม่ได้มีการนำไปใช้อย่างมิชอบและยังคงอยู่ภายใต้กฎและการกำกับดูแลอยู่ (Dance, LaForgia, & Confessore, 2018) ซึ่งการตอบสนองวิกฤตครั้งนี้ สำหรับ Facebook เป็นการหวนกลับมาใช้กลยุทธ์การปฏิเสธและให้เหตุผล เพื่อรักษาชื่อเสียงและภาพลักษณ์ขององค์กรเป็นหลัก (Gwebu et al., 2018, p. 687; Ulmer et al., 2007, pp. 59-60) หลังจากนี้ เรื่องนี้ยังคงอยู่ในกระบวนการทางกฎหมายต่อไป[10]

จากกรณีตัวอย่างการจัดการวิกฤตของ Facebook หากไล่เรียงงานศึกษาที่เกี่ยวข้องและเหตุการณ์ที่องค์กรประสบแล้ว จะเห็นว่าก่อนวิกฤตทั้ง 2 เหตุการณ์ Facebook เป็นองค์กรที่มีภาพลักษณ์ค่อนข้างแข็งแกร่งเพราะได้รับความไว้วางใจจากหลายภาคส่วนให้เป็นแพลตฟอร์มการจัดการวิกฤตที่มีประสิทธิภาพดังที่ได้กล่าวไป แต่ในแง่การจัดการวิกฤตขององค์กรเอง ด้วยความที่ Facebook มองข้ามความสำคัญ

[10] ข้อมูลทั้งหมดเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของผู้ใช้ที่ Facebook เผชิญที่กล่าวมาเป็นข้อมูลความคืบหน้าจนถึงวันที่ 30 ธันวาคม ค.ศ. 2018

ของข้อมูลส่วนบุคคลของผู้ใช้ จึงไม่ได้ดำเนินการป้องกันและเตรียมการในขั้นก่อนภาวะวิกฤต ผนวกกับการเลือกใช้กลยุทธ์การปฏิเสธในภาวะวิกฤตส่งผลให้วิกฤตลุกลามมากขึ้น ซึ่งแบบจำลองที่ระบุกลยุทธ์การตอบสนองวิกฤตทั้งของ Benoit, Coombs, และที่พัฒนาขึ้นมาใหม่สำหรับการจัดการวิกฤตข้อมูลโดยเฉพาะที่นำเสนอไปข้างต้น ชี้ให้เห็นผลข้างเคียงในแง่ลบที่อาจตามมาจากการใช้กลยุทธ์นี้ไว้ชัดเจน โดยในกรณีที่เกิดกับ Facebook คือ ถูกฟ้องดำเนินคดีทั้งจากกลุ่มผู้มีส่วนได้ส่วนเสียและหน่วยงานที่เกี่ยวข้อง ราคาหุ้นตก[11] และมีการเรียกร้องให้ประธานบริหารลงจากตำแหน่ง (Dance et al., 2018) ผู้เชี่ยวชาญทั้งในสายวิชาการและวิชาชีพต่างให้ข้อมูลเป็นเอกฉันท์ว่า กลยุทธ์การตอบสนองวิกฤตที่พึงใช้ คือ ควรยอมรับความผิด ขอโทษ การดำเนินการเพื่อจำกัดและลดความเสียหายลง และการสร้างความเชื่อมั่นว่าจะไม่เกิดเหตุการณ์ในลักษณะเดิมซ้ำ (Clemmitt, 2015, pp. 6-8; Ulmer et al., 2007, pp. 57-62)

อย่างไรก็ตาม การที่ Facebook เลือกใช้กลยุทธ์การปฏิเสธเพื่อรักษาภาพลักษณ์ในช่วงต้น ได้กลายเป็นบทเรียนให้มีการปรับกลยุทธ์ รวมถึงมีการปรับนโยบายด้านความปลอดภัยเพื่อป้องกันเหตุละเมิดในอนาคต แต่ในช่วงเดือนธันวาคม ค.ศ. 2018 ที่มีการรายงานข่าวโจมตีองค์กรเพิ่มเติม เรื่องการแชร์ข้อมูลส่วนตัวของผู้ใช้กับองค์กรที่มีความร่วมมือนั้น Facebook ได้กลับมาใช้กลยุทธ์การปฏิเสธอีกครั้ง โดยสังเกตได้ว่าองค์กรพันธมิตรต่างให้ข้อมูลไปในทางเดียวกันกับ Facebook สภาพการณ์นี้สะท้อนภาพความเป็นไปได้ 2 กรณี คือ Facebook น่าจะมีการวางแผนการจัดการวิกฤตที่ครอบคลุมไปถึงองค์กรเหล่านี้ด้วย ทำให้การสื่อสารออกมาเป็นเสียงเดียวตามหลักการตอบสนองวิกฤต (Coombs, 2012, pp. 143-144) หรืออาจเป็นเพียงการให้ข้อมูลตามความเป็นจริงขององค์กรเหล่านี้ที่ไม่ทราบสิทธิ์การเข้าถึงข้อมูลส่วนบุคคลเชิงลึกของผู้ใช้และไม่มีการละเมิดใดๆ ตามที่สำนักข่าวกล่าวอ้าง

หากพิจารณาในรายละเอียดแล้ว จะเห็นได้ว่า รูปแบบธุรกิจของ Facebook อาศัยรายได้จากแชร์ข้อมูลส่วนบุคคลของผู้ใช้กับองค์กรคู่ความร่วมมือกว่า 150 แห่ง ที่เข้ามาทำการโฆษณาเป็นหลัก เพราะฉะนั้นข้อมูลส่วนบุคคลเหล่านี้ จึงเป็นสินทรัพย์ที่สำคัญที่สุดขององค์กรในยุคนี้ (Dance et al., 2018) ปัจจัยสำคัญที่เอื้อให้เกิด

[11] ราคาหุ้น Facebook ตกลง 19% หรือเป็นเงินจำนวน $120,000 ล้าน และถูกปรับคดีที่เกี่ยวพันกับ Cambridge Analytica เป็นเงินจำนวน £500,000 (Sanders & Patterson, 2018)

ธุรกรรมชนิดนี้ คือ ภาพลักษณ์ ชื่อเสียง และความน่าเชื่อถือขององค์กร โดยนัย คือ ภาพลักษณ์และความน่าเชื่อถือขององค์กรเป็นปัจจัยสำคัญที่ช่วยดึงให้องค์กรต่างๆ ลงทุนกับตน ดังนั้น ในภาพรวม กลยุทธ์ที่เน้นรักษาภาพลักษณ์เป็นหลักจึงมักถูกหยิบยกมาใช้ ประธานบริหารบริษัทต้องออกมาเคลื่อนไหวด้วยการขอโทษเมื่อจำเป็นต้องกอบกู้ภาพลักษณ์ เมื่อควบคุมสถานการณ์ได้จึงกลับไปใช้กลยุทธ์ปฏิเสธว่าไม่มีการละเมิดเกิดขึ้น และการแชร์ข้อมูลส่วนบุคคลของผู้ใช้เอื้อประโยชน์ให้คู่ความร่วมมือในเครือข่าย Facebook จึงได้รับความร่วมมือจากพันธมิตรในการตอบสนองวิกฤตไปในทางเดียวกันเพื่อรักษาผลประโยชน์ร่วม ซึ่งงานศึกษาในอนาคตอาจเจาะลึกประเด็นการจัดการวิกฤตของ Facebook โดยผนวกการศึกษาเอกสารเข้ากับการสัมภาษณ์ผู้เกี่ยวข้องในองค์กรเพื่อยืนยันกระบวนการต่อไป

2. Yahoo

จากรายงานข่าวต่างๆ จะเห็นได้ว่า Yahoo ไม่ได้เผชิญวิกฤตเกี่ยวกับการละเมิดข้อมูลส่วนตัวของผู้ใช้เพียงครั้งเดียว แต่เป็นการเกิดวิกฤตซ้ำ 2 ครั้งซ้อน ในช่วง ค.ศ. 2016 โดยเหตุการณ์แรกเป็นการจารกรรมข้อมูลผู้ใช้กว่า 500 ล้านราย โดยแฮกเกอร์ตั้งแต่ช่วงปลายปี ค.ศ. 2014 แต่เหตุการณ์นี้ตกเป็นข่าว 2 ปีให้หลังจากการจารกรรม คือ ในวันที่ 22 กันยายน ค.ศ. 2016 และอีกเหตุการณ์เป็นการจารกรรมข้อมูลตั้งแต่ปี ค.ศ. 2013 ซึ่งแฮกเกอร์ได้ข้อมูลของผู้ใช้ไปมากกว่า 1 พันล้านราย โดยเรื่องนี้ตกเป็นข่าวในเดือนธันวาคมปี ค.ศ. 2016

เหตุการณ์ครั้งที่ 1: ก่อนวิกฤต: การดำเนินการของ Yahoo ในขั้นก่อนวิกฤตสะท้อนให้เห็นว่า ไม่มีการนำหลักการจัดการวิกฤตเข้ามาเป็นส่วนหนึ่งขององค์กร ก่อนที่ Yahoo จะตระหนักว่าตนกำลังเผชิญกับภาวะวิกฤต รายงานข่าวเผยว่า Yahoo ทราบเรื่องช่วงต้นปี ค.ศ. 2016 ว่ามีการจารกรรมข้อมูลจากระบบของตน ต้นตอของเรื่องมาจากกระทู้ใต้ดินที่แฮกเกอร์ชาวรัสเซียที่ใช้นามแฝงว่า *"Tessa88"* โพสต์ตัวอย่างข้อมูลผู้ใช้ที่อ้างว่าเป็นข้อมูลที่ได้ไปจาก Yahoo แต่ด้วยความที่เคยประสบเหตุการณ์ละเมิดข้อมูลแล้วหนึ่งครั้งในปี ค.ศ. 2012 ที่กระทบผู้ใช้จำนวนกว่า 45,000 ราย ทาง Yahoo จึงยังไม่สามารถระบุได้ว่า ข้อมูลที่ได้ไปเป็นชุดที่ถูกละเมิดใน ค.ศ. 2012 หรือไม่ (Perlroth, 2016; Swisher, 2016) ในขั้นนี้เรียกว่า การตรวจพบสัญญาณก่อนเกิดวิกฤต (Coombs, 2009, 2012) เนื่องจากในสายตาขององค์กรยังไม่ทราบถึงเรื่องการละเมิดข้อมูลครั้งใหม่ที่เป็นชุดข้อมูลที่ถูกละเมิดปี ค.ศ. 2013

ภาวะวิกฤต: ภาวะวิกฤตพา Yahoo เข้าสู่การจัดการวิกฤตที่ใช้กลยุทธ์การตอบสนองวิกฤตแบบปฏิเสธเป็นหลัก ในเดือนสิงหาคม ค.ศ. 2016 Yahoo ได้ตรวจพบสัญญาณเตือนวิกฤตจากอีกแหล่ง คือ จากโพสต์ของแฮกเกอร์นามว่า *"Peace of Mind"* ที่นำข้อมูลผู้ใช้ของ Yahoo ออกเผยแพร่ในเว็บไซต์ *"TheRealDeal"* ซึ่งเป็นตลาดซื้อขายข้อมูลเถื่อนที่ทำการแกะรอยจนพบหลักฐานการจารกรรมข้อมูลในปี ค.ศ. 2014 สัญญาณดังกล่าวทำให้ Yahoo ตระหนักรู้ว่า องค์กรเข้าสู่ภาวะวิกฤตเต็มรูปแบบแล้ว Yahoo ตอบสนองวิกฤตด้วยการแถลงว่า ทราบเรื่องที่แฮกเกอร์กล่าวอ้างแล้ว แต่เลือกใช้กลยุทธ์ปฏิเสธ (Coombs, 2012) คือ ยังไม่ยืนยันว่าการกล่าวอ้างของแฮกเกอร์เป็นความจริง ในส่วนของขั้นตอนการจำกัดวิกฤต (Coombs, 2012) Yahoo ไม่ได้ดำเนินการใดๆ *"ไม่แม้แต่แจ้งให้ผู้ใช้เปลี่ยนรหัสผ่าน"* จนทำให้เกิดเสียงวิพากษ์วิจารณ์ในแง่ลบจากหลายทิศทาง สำนักข่าวได้ยกสถิติหน่วงเวลาในการตรวจพบการละเมิดข้อมูลจาก Ponemon Institute ที่เป็นสถาบันที่รวบรวมสถิติเรื่องนี้มานำเสนอว่า หน่วงเวลาโดยเฉลี่ยในการตรวจพบการละเมิดข้อมูลคือ 191 วัน และการจำกัดเหตุอยู่ที่ 58 วันหลังตรวจพบ ซึ่งหากเทียบกับเวลาถึงกว่า 2 ปี ในกรณีของ Yahoo ถือว่านานมาก (Swisher, 2016) หลักจากเหตุการณ์นี้ในขณะที่เรื่องได้เข้าสู่กระบวนการทางกฎหมาย Yahoo ได้เพิ่มมาตรการด้านความปลอดภัยของระบบและกระตุ้นให้ผู้ใช้ทำการเปลี่ยนรหัสเข้าใช้ (Goel & Perlroth, 2016) ซึ่งการดำเนินการนี้ นับเป็นการจำกัดวิกฤตรูปแบบหนึ่ง (Coombs, 2009, 2012)

เหตุการณ์ครั้งที่ 2: ภาวะวิกฤต: ด้วยความที่ Yahoo ไม่เคยใช้หลักการจัดการวิกฤตมาก่อน ส่งผลให้องค์กรตกอยู่ในวิกฤตซ้ำอีกครั้งจากเหตุจารกรรมข้อมูลในอดีต แต่ด้วยภาวะวิกฤตที่รุนแรงขึ้น จึงมีการนำหลักการจัดการวิกฤตเข้ามาใช้ในช่วงหลัง ในวันที่ 14 ธันวาคม ค.ศ. 2016 สำนักข่าวต่างรายงานถึงแถลงการณ์เกี่ยวกับการตรวจพบการละเมิดข้อมูลผู้ใช้ของ Yahoo ที่ปล่อยออกมาในวันเดียวกัน ซึ่งเผยว่าเป็นการจารกรรมข้อมูลที่เกิดตั้งแต่เดือนสิงหาคม ค.ศ. 2013 คาดว่ากระทบผู้ใช้กว่า 1 พันล้านราย โดยในช่วงเดือนพฤศจิกายน ค.ศ. 2016 องค์กรทราบเรื่องจากเจ้าพนักงานด้านกฎหมายที่นำตัวอย่างข้อมูลที่พบว่าถูกจารกรรมและนำไปขายในตลาดมืดมาให้ Yahoo ตรวจสอบเพื่อยืนยัน (Goel & Perlroth, 2016; Merced, 2016) สำหรับเหตุการณ์นี้ Yahoo ยังคงอยู่ในภาวะกฤตก่อนหน้าที่เกิดจากข่าวเมื่อเดือนกันยายนและยังไม่สามารถคลี่คลายวิกฤตได้ แต่กว่าจะพบว่าข้อมูลอีกชุดใหญ่

ถูกจารกรรมไป ก็นับเป็นเวลากว่า 3 ปี ที่สำคัญ Yahoo ไม่ได้เป็นผู้ตรวจพบวิกฤตเอง และไม่ได้ดำเนินการใดๆ เมื่อได้รับเบาะแสมา

สภาพการณ์นี้ นอกจากจะสะท้อนให้เห็นระบบรักษาข้อมูลขององค์กรที่ไม่เข้มแข็งแล้ว ยังสะท้อนให้เห็นว่าระบบการตรวจจับสัญญาณเตือนวิกฤตไม่มีศักยภาพเพียงพอ หรืออาจกล่าวได้ว่า ในขั้นก่อนเกิดวิกฤตไม่มีทั้งการตรวจจับสัญญาณ การป้องกัน หรือการเตรียมรับวิกฤตตามหลักการจัดการวิกฤตแบบ 3 ขั้นตอนอย่างที่ควรจะเป็น แม้จะเคยประสบเหตุมาแล้วใน ค.ศ. 2012 ตามเนื้อข่าว (Coombs, 2012) ในวันเดียวกันนี้ Bob Lord หัวหน้าฝ่ายความปลอดภัยด้านข้อมูลของ Yahoo ได้ออกมาแถลงข้อมูลที่องค์กรใช้ในการคาดการณ์กระบวนการเจาะระบบของแฮกเกอร์ต่อสาธารณะ โดยระบุว่ามีการใช้ระบบคุกกี้[12] (cookies) ปลอมเก็บข้อมูลและล้วงเอาข้อมูลผู้ใช้ไป แต่ก็ยังไม่สามารถระบุตัวแฮกเกอร์หรือวิธีการที่ใช้จริงได้ ซึ่งองค์กรได้แจ้งผู้ใช้ให้ทำการเปลี่ยนรหัสผ่านทั้งบริการของตนและบริการอื่นๆ ที่ใช้รหัสเดียวหรือใกล้เคียงกันด้วย (Goel & Perlroth, 2016)

จากที่กล่าวข้างต้นจะเห็นได้ว่า Yahoo เริ่มมีการนำหลักการจัดการวิกฤตมาใช้ มีการใช้โฆษกที่มีคุณสมบัติตรงตามหลักการ คือ ผู้นำหรือผู้รับผิดชอบต้องแสดงตัวและแสดงความจริงใจด้วยการให้ข้อมูล *"ที่ทราบ ไม่ทราบ และสิ่งที่จะดำเนินการหรือหาคำตอบต่อไป"* ในภาวะวิกฤต (Clemmitt, 2015, p. 6; Ulmer et al., 2007, p. 61) ในที่นี้ หมายถึง การเปิดเผยข้อมูลเท่าที่องค์กรมี และใช้การคาดการณ์ถึงวิธีการเจาะระบบแม้จะยังไม่ได้รับการพิสูจน์อย่างเป็นทางการก็ตาม ต่อมาในวันที่ 1 มีนาคม ค.ศ. 2017 Marissa Mayer ประธานบริหารของ Yahoo แถลงการณ์แสดงความรับผิดชอบต่อเรื่องที่เกิดขึ้น โดยการขอไม่รับเงินปันผลกำไร (bonus) ประจำปี 2016 มูลค่ากว่า 2 ล้านดอลลาร์สหรัฐฯ และกระจายเงินดังกล่าวให้แก่พนักงานแทน (Goel, 2017) ในวันที่ 3 ตุลาคม ค.ศ. 2017 Yahoo แถลงมาตรการบังคับให้ผู้ใช้เปลี่ยนรหัสเข้าใช้ พร้อมยกเลิกคำถามที่ใช้เข้าถึงบัญชีในกรณีที่ลืมรหัสผ่านเพื่อป้องกันวิกฤตซ้ำในอนาคต และเผยการประเมินจำนวนผู้เสียหายจากเหตุการละเมิดข้อมูลฯ ค.ศ. 2013 ที่เดิมระบุว่ากระทบผู้ใช้ 1 พันล้านราย

---

[12] ข้อมูลบางส่วนเกี่ยวกับเว็บไซต์ที่จัดเก็บไว้ในเครื่อง/อุปกรณ์ของผู้ใช้ เพื่อเอื้อให้ทั้งอุปกรณ์ของผู้ใช้และเว็บไซต์เชื่อมต่อกันได้เร็วขึ้นจากข้อมูลชุดดังกล่าว ซึ่งในกรณีนี้แฮกเกอร์ใช้ข้อมูลของผู้ใช้ปลอมตัวเข้าระบบมาล้วงข้อมูล (Goel & Perlroth, 2016)

เป็น 3 พันล้านราย (Haselton, 2017) ซึ่งกลยุทธ์การตอบสนองวิกฤตที่ใช้ คือ การผ่อนปรน (accommodative strategy) โดยใช้การแก้ไขข้อผิดพลาดและการเยียวยา (remedial actions) ด้วยการจ่ายค่าชดเชยให้พนักงาน และให้ผู้ใช้เปลี่ยนรหัสผ่านพร้อมคำถามกู้รหัส

หลังวิกฤต: สุดท้าย Yahoo ได้ขายกิจการส่วนหนึ่งไปด้วยราคาที่ลดลงมากจากราคากิจการที่ตกลงเดิมก่อนเกิดวิกฤต และได้บทเรียนราคาแพงจากการละเลยความสำคัญของการรักษาข้อมูลส่วนบุคคลของผู้ใช้เป็นค่าปรับจากกระบวนการทางกฎหมาย ฐานไม่แจ้งเตือนการจารกรรมข้อมูลเป็นมูลค่ากว่า 35 ล้านดอลลาร์สหรัฐฯ (Global Data Sentinel, 2018) อีกทั้ง Yahoo ยังยอมจ่ายเงินชดเชยให้ผู้ใช้ที่ได้รับผลกระทบจากเหตุละเมิดปี ค.ศ. 2013 ราว 200 ล้านราย เป็นเงินกว่า 50 ล้านดอลลาร์สหรัฐฯ และคืนค่าธรรมเนียมร้อยละ 25 พร้อมการชดเชยอื่นๆ เป็นเวลา 2 ปี (Reints, 2018)

จากข้อมูลข้างต้น เห็นได้ชัดว่า Yahoo ไม่ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลของผู้ใช้ และแนวคิดการจัดการวิกฤต โดยไม่นำเข้ามาเป็นส่วนหนึ่งขององค์กรตั้งแต่ต้น Yahoo ไม่มีการตรวจจับสัญญาณ การป้องกัน และการเตรียมการในภาวะก่อนวิกฤตเลย ทั้งที่องค์กรเคยเผชิญกับวิกฤตตั้งแต่ ค.ศ. 2012 ส่งผลให้ Yahoo ต้องอยู่กับวิกฤตต่อเนื่องมาจนถึง ค.ศ. 2017 แม้จะมีการอัดฉีดเงินลงทุนปรับปรุงระบบรักษาข้อมูลสูงถึง 250 ล้านดอลลาร์สหรัฐฯ เป็นการจัดการหลังเกิดวิกฤต ค.ศ. 2012 ไปแล้ว และยังไม่มีการปรับปรุงเพิ่มเติม (Reuters, 2016) แต่การปรับปรุงระบบครั้งนี้ ก็ไม่สามารถป้องกันวิกฤตอีก 2 ครั้ง ที่ตามมาในปี ค.ศ. 2013 และ 2014 ได้ ซึ่งสะท้อนว่า Yahoo ขาดการจำลองวิกฤตเพื่อทดสอบระบบ ทั้งระบบรักษาข้อมูลและระบบการจัดการวิกฤต

อีกประเด็นสำคัญที่สะท้อนว่า Yahoo ไม่ตระหนักถึงความสำคัญของแนวคิดการจัดการวิกฤต คือ Yahoo ไม่ได้ตรวจพบเหตุละเมิดข้อมูลเอง แต่เป็นบุคคลที่สามที่พบแสดงให้เห็นว่า Yahoo ขาดการวิเคราะห์สภาพแวดล้อม การตรวจจับสัญญาณการป้องกัน การเตรียมการในขั้นก่อนวิกฤต รวมถึงไม่มีแผนการจัดการวิกฤต จึงไม่มีการเตรียมระบบตรวจจับสัญญาณวิกฤตที่ดีพอ และแม้จะมีการตรวจพบว่าเกิดวิกฤตในครั้งแรกแล้ว แต่การดำเนินการมีเพียงการกระตุ้นให้ผู้ใช้เปลี่ยนรหัสเข้าใช้ด้วยตนเองก็สะท้อนว่า องค์กรประเมินความเสียหายที่อาจเกิดตามมาในระดับ

ที่ไม่รุนแรงหรือฉุกเฉินมากเท่าที่ควร หากเทียบกับการที่องค์กรบังคับผู้ใช้เปลี่ยนรหัสในวิกฤตครั้งถัดมาที่องค์กรยอมรับภาวะวิกฤตแล้ว

เมื่อองค์กรเข้าสู่ภาวะหลังวิกฤตและได้ดำเนินการสร้างความเชื่อมั่นต่อผู้มีส่วนได้ส่วนเสียด้วยการชดเชยค่าเสียหาย ซึ่งเป็นหนึ่งในหลักการการจัดการวิกฤตในภาวะหลังวิกฤต (Coombs, 2012, pp. 10-13; Frandsen & Johansen, 2017, pp. 69-87) แต่ในภาพรวมการจัดการวิกฤตของ Yahoo เรียกว่า เป็นการนำแนวคิดมาใช้หลังภาวะวิกฤตซึ่งไม่ช่วยให้องค์กรจำกัดและลดความเสียหายของวิกฤต ทำได้เพียงเยียวยารักษาภาพลักษณ์และชื่อเสียงที่หลงเหลืออยู่ไว้เท่านั้น

3. Google+

Google+ แม้จะไม่ใช่องค์กรเก่าแก่อย่าง 2 องค์กรข้างต้น และถูกมองว่าเป็นไก่รองบ่อน เพราะด้วยเป้าหมายการก่อตั้งที่สร้างมาเพื่อเป็นสังคมออนไลน์คู่แข่งกับยักษ์ใหญ่อย่าง Facebook แต่ไม่ประสบความสำเร็จเท่าที่ควร (Lee, 2018) อย่างไรก็ดี Google+ ก็เป็นอีกหนึ่งแพลตฟอร์มที่ถือข้อมูลส่วนบุคคลของผู้ใช้เป็นจำนวนมากเอาไว้และได้เผชิญกับวิกฤตการละเมิดข้อมูลในช่วงปลายปี ค.ศ. 2018 จนถึงขั้นประกาศปิดตัวในปีถัดไป

ก่อนวิกฤต: Google+ มีการนำหลักการจัดการวิกฤตมาใช้ตั้งแต่ขั้นก่อนวิกฤต ทั้งจากรายงานข่าวและแถลงการณ์ของทาง Google+ เอง ที่เผยแพร่เมื่อวันที่ 8 ตุลาคม ค.ศ. 2018 ระบุว่า องค์กรทราบเรื่องว่ามีข้อมูลส่วนบุคคลของผู้ใช้หลุดตั้งแต่เดือนมีนาคม ค.ศ. 2018 และได้ตรวจสอบชนิดของข้อมูลที่หลุดออกไป การนำไปใช้ และดูว่ามีผู้พัฒนาระบบที่เกี่ยวข้องสามารถเอาข้อมูลไปใช้ในทางมิชอบได้หรือไม่ แต่ไม่พบการนำข้อมูลไปใช้ในทางมิชอบแต่อย่างใด จึงได้แถลงว่า *“ไม่พบหลักฐานที่แสดงว่ามีใครทราบถึงจุดบกพร่อง (bug) ของระบบและไม่มีการใช้ข้อมูลในทางมิชอบ”* (Independent, 2018; Smith, 2018) โดยการทราบเรื่องในเดือนมีนาคมถือเป็นการตรวจจับสัญญาณวิกฤต ซึ่ง Google+ มีการดำเนินการป้องกันและเตรียมการจัดการวิกฤตภายในขั้นตอนนี้ด้วยการตรวจสอบชนิดข้อมูล ตรวจสอบการนำข้อมูลไปใช้ และสำรวจการละเมิดข้อมูลในเดือนตุลาคม (Coombs, 2009, 2012) กล่าวคือ หน่วงเวลาที่ใช้ในการตรวจพบสัญญาณวิกฤตคือ 6 เดือน

ภาวะวิกฤต: การตัดสินใจปฏิเสธการละเมิดข้อมูลขององค์กรในขั้นก่อนวิกฤต ผนวกกับระบบรักษาความปลอดภัยข้อมูลส่วนบุคคลของผู้ใช้ที่ไม่เข้มแข็งพอ เป็นเหตุให้เกิดภาวะวิกฤตที่หนักหน่วงตามมา ในวันที่ 8 ตุลาคม ค.ศ. 2018 สำนักข่าว จำนวนหนึ่งเปิดเผยข้อมูลจากบันทึกภายในของ Google+ ว่า ในความเป็นจริง องค์กรพบข้อบกพร่อง (bug) ของระบบ API ที่อนุญาตให้ผู้พัฒนาแอปพลิเคชัน เข้าถึงข้อมูลส่วนตัวของผู้ใช้และ *"เพื่อน"* แต่เลือกปิดบังข้อมูลเพราะกลัวภาพลักษณ์เสียหายและจงใจไม่แจ้งให้ผู้ใช้ทราบ ทั้งที่ขัดกับกฎหมายกำกับดูแลเรื่องการละเมิดสิทธิ์เหนือข้อมูลส่วนบุคคล (MacMillan & McMillan, 2018; Newman, 2018; Wong & Solon, 2018)

จากรายงานข่าวและการนำกลยุทธ์การป้องกัน (defensive strategy) มาใช้เพื่อทำการปฏิเสธภาวะวิกฤต (denial) วางกรอบการให้ข้อมูลว่าไม่มีการละเมิดเกิดขึ้น เพราะต้องการรักษาภาพลักษณ์และหลีกเลี่ยงการตกเป็นเป้าของสังคม เช่นเดียวกับ Facebook สะท้อนว่าองค์กรตกอยู่ในภาวะวิกฤตแล้ว (Gwebu et al., 2018; Wong & Solon, 2018) ซึ่งทาง Google+ เอง ก็ได้ตอบสนองด้วยการประกาศปิดปรับปรุงระบบเพื่อพัฒนาระบบดูแลความเป็นส่วนตัว ปกป้องผู้ใช้จากแอปพลิเคชันภายนอก (เฉพาะกลุ่มผู้ใช้ระดับธุรกิจเท่านั้น) โดยจะแจ้งเวลาการเปิดใช้ระบบภายหลัง พร้อมเปิดเผยเรื่องข้อมูลรั่ว โดย Ben Smith รองประธานด้านวิศวกรรมขององค์กร ระบุว่า เหตุการณ์นี้อาจกระทบบัญชีผู้ใช้กว่า 500,000 ราย คาดว่าแอปพลิเคชันภายนอก จำนวน 438 รายการ น่าจะสามารถเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้ได้ แต่ทาง Google+ เอง ไม่สามารถตรวจสอบว่าข้อมูลถูกละเมิดหรือไม่ เพราะระบบโดยปกติจะบันทึกความเคลื่อนไหวต่างๆ (activity log for API) ไว้เพียง 2 สัปดาห์เท่านั้น จึงไม่สามารถสืบค้นข้อมูลย้อนหลังได้ครบถ้วนเพื่อยืนยันตัวเลขที่แน่ชัดได้

นอกจากนี้ บทสัมภาษณ์ Yonatan Zunger อดีตวิศวกรผู้ร่วมพัฒนา Google+ ยังตอกย้ำว่า องค์กรไม่ได้ให้ความสำคัญกับการดูแลความปลอดภัยของระบบเท่าที่ควร *"หลังจากที่บริษัทรู้ว่าบริการสื่อสังคมออนไลน์นี้ไม่เป็นที่นิยมดังหวัง จึงโยกงบประมาณไปใช้ในด้านอื่นแทน"* (D'Onfro, 2018a; Smith, 2018; Wong & Solon, 2018) จากแถลงการณ์ เห็นได้ว่า Google+ เลือกใช้กลยุทธ์กอบกู้ภาพลักษณ์ ใช้การให้คำมั่นเพื่อแก้ไขและการให้คำมั่นเรื่องค่านิยม ด้วยการสร้างความเชื่อมั่นต่อผู้มีส่วนได้ส่วนเสีย ซึ่งในที่นี้หมายถึงกลุ่มผู้ใช้ระดับธุรกิจ (enterprise customers) ว่าองค์กรจะยึดมั่นค่านิยมองค์กรในการรักษาข้อมูลส่วนบุคคลของผู้ใช้อย่างดีที่สุด พร้อมกับ

การดำเนินการเพื่อจำกัดวิกฤตด้วยการปิดและปรับปรุงระบบ ดูแลข้อมูลส่วนตัวของผู้ใช้ในระดับนี้ให้ดีขึ้น (Coombs, 2009, 2012; Gwebu et al., 2018) ส่วนบริการสื่อสังคมออนไลน์สำหรับผู้ใช้ทั่วไปจะถูกปิดตัวลงในเดือนสิงหาคม ค.ศ. 2019 โดย Google+ ให้เหตุผลว่า ร้อยละ 90 ของผู้ใช้บริการในส่วนนี้ ลงชื่อเข้าใช้อยู่ในระบบเป็นเวลาเฉลี่ยต่ำว่า 5 วินาทีเท่านั้น จึงไม่ส่งผลกระทบมากเพราะมีเวลาให้เตรียมตัวกว่า 10 เดือน (Smith, 2018) ซึ่งรากของปัญหานี้มาจากการไม่ตระหนักถึงความสำคัญของการปกป้องข้อมูลส่วนบุคคลของผู้ใช้ที่ส่งผลต่อการจัดสรรทรัพยากรขององค์กรไปในด้านอื่น

แต่หลังจากการประกาศปิดตัวเพียง 2 เดือน รายงานข่าวในวันที่ 10 ธันวาคม ค.ศ. 2018 ระบุว่า Google+ พบข้อบกพร่อง (bug) ของระบบ API อีกจุดที่เกิดจากการปรับระบบ (software update) ในวันที่ 7 พฤศจิกายน ค.ศ. 2018 ซึ่งข้อบกพร่องนี้ เปิดช่องโหว่ให้ผู้พัฒนาแอปพลิเคชันสามารถเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้ได้ กระทบผู้ใช้ราว 52.5 ล้านราย โดยองค์กรดำเนินการแก้ไขแล้วเสร็จในวันที่ 13 พฤศจิกายน (Newman, 2018) Google+ ตอบสนองวิกฤตด้วยกลยุทธ์การใช้เหตุผล (moderate strategy) ด้วยการให้เหตุผล (justification) แถลงว่าข้อบกพร่องนี้ *“กระทบผู้ใช้เพียงบางคนเท่านั้น”* และใช้กลยุทธ์การป้องกัน (defensive strategy) ด้วยการปฏิเสธ (denial) วางกรอบการให้ข้อมูลว่า ไม่มีการละเมิดเกิดขึ้นในช่วง 6 วันที่เกิดเหตุ ซึ่งเหตุการณ์นี้ส่งผลให้องค์กรประกาศเลื่อนการปิดบริการสำหรับผู้ใช้ทั่วไปมาเป็นเดือนเมษายน ค.ศ. 2019 แทน เพื่อจำกัดความเสียหายที่อาจเกิดจากวิกฤตในขั้นนี้ของ Google+ (Coombs, 2009, 2012; Gwebu et al., 2018; Newman, 2018)

ในภาพรวม Google+ นำหลักการจัดการวิกฤตมาใช้ตั้งแต่ขั้นก่อนวิกฤต แต่ด้วยการประเมินวิกฤตอย่างประมาท ความไม่พร้อมของระบบที่เกิดจากการไม่ให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลของผู้ใช้ ผนวกกับการใช้กลยุทธ์การปฏิเสธตอบสนองวิกฤตเพื่อรักษาภาพลักษณ์ และปิดบังข้อมูลทั้งต่อผู้มีส่วนได้ส่วนเสียกับองค์กรกำกับดูแล ส่งผลให้วิกฤตลุกลามจนเกินจะรับมือจนในที่สุดองค์กรต้องประกาศปิดบริการส่วนหนึ่ง

สรุปผล อภิปราย และข้อเสนอแนะ

การวิเคราะห์ข้อมูลกรณีตัวอย่างเผยให้เห็นรูปแบบการเกิดวิกฤตการละเมิดข้อมูลส่วนบุคคลของผู้ใช้ และการจัดการวิกฤตขององค์กรที่ดูแลข้อมูลส่วนบุคคลจำนวนมหาศาลในยุคดิจิทัลอย่าง Facebook, Yahoo, และ Google+ โดยผลการวิเคราะห์สะท้อนทั้งจุดเหมือนและต่างในการจัดการวิกฤตของทั้ง 3 องค์กรดังต่อไปนี้ จุดร่วม ได้แก่ การที่ทั้ง 3 องค์กร เผชิญกับวิกฤตที่เกิดขึ้นโดยเจตนา (intentional crises) ทั้งจากบุคคลที่สามที่เป็นผู้พัฒนาแอปพลิเคชันภายนอก แฮกเกอร์ และการรายงานข่าวเปิดเผย ซึ่งวิกฤตลุกลามขึ้นเพราะองค์กรขาดการจัดการวิกฤตในขั้นก่อนวิกฤตแม้จะมีการตรวจพบสัญญาณวิกฤตแล้วก็ตาม

ในภาวะวิกฤต องค์กรเลือกใช้กลยุทธ์การปฏิเสธวิกฤต ซึ่งหากอิงจากหลักคิดที่ได้จากงานศึกษาที่ผ่านมาที่ผู้เชี่ยวชาญต่างชี้ว่า การสร้างความเชื่อใจต่อสาธารณชนด้วยการให้ข้อมูลที่เป็นความจริง พร้อมเสนอแนวปฏิบัติในภาวะวิกฤตแก่สาธารณชนและผู้มีส่วนได้ส่วนเสียเป็นแนวทางที่ดีที่สุด เพราะผู้เกี่ยวข้องไม่ได้ต้องการเพียงความจริง แต่ยังต้องการทางออกด้วย (Clemmitt, 2015, pp. 6-8) พบว่า ทั้ง 3 องค์กรไม่ได้เลือกใช้แนวทางนี้ จึงส่งผลให้เกิดกระแสตอบรับทางลบจากหลายภาคส่วนที่เกี่ยวข้อง และในภาพรวมทั้ง 3 องค์กร ขาดการดำเนินการขั้นหลังวิกฤตจึงทำให้เกิดวิกฤตซ้ำ ส่วนจุดต่าง คือ Facebook และ Google+ มีการนำหลักการจัดการวิกฤตมาใช้ในขั้นวิกฤต ส่วน Yahoo ไม่มีการนำมาใช้ในขั้นนี้ แต่จะนำมาใช้ในขั้นหลังวิกฤตที่เป็นเพียงการชดเชยความเสียหายเท่านั้น ยังขาดการพิสูจน์ศักยภาพการรับมือกับวิกฤตขององค์กร รายละเอียดตาม**ตารางที่ 3**

ทั้งนี้ หากเทียบผลการศึกษาครั้งนี้กับข้อค้นพบในบทความของ Gwebu และคณะ (2018) ที่เน้นเรื่องการจัดการวิกฤตเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลของผู้ใช้ ผลชี้ว่า ชื่อเสียงและภาพลักษณ์ขององค์กรเป็นปัจจัยสำคัญที่ส่งผลต่อความรุนแรงของวิกฤตในระดับที่ต่างกัน คือ องค์กรที่มีชื่อเสียงมากจะได้รับความเสียหายจากการเปิดเผยว่าข้อมูลถูกละเมิดน้อยว่าองค์กรที่มีระดับชื่อเสียงที่ต่ำกว่า และสำหรับองค์กรที่มีชื่อเสียงมากกลยุทธ์การตอบสนองวิกฤตไม่ถือเป็นตัวแปรสำคัญ แต่กลยุทธ์เหล่านี้ถือเป็นตัวแปรสำคัญสำหรับองค์กรที่มีชื่อเสียงในระดับต่ำกว่า (Gwebu et al., 2018) ซึ่งผลการวิเคราะห์ข้อมูลของบทความนี้ ไม่ได้สะท้อนความสำคัญของตัวแปรเดียวกัน เพราะความเสียหายที่เกิดขึ้นเป็นผลจากการขาดการใช้หลักการจัดการวิกฤต

มองข้ามความสำคัญ และขาดความพร้อมของระบบรักษาความปลอดภัยที่ดูแลข้อมูลส่วนบุคคลของผู้ใช้บริการของทั้ง 3 องค์กร อีกทั้งการเลือกใช้กลยุทธ์การตอบสนองวิกฤตด้วยการปฏิเสธวิกฤตของกลุ่มตัวอย่างนั้น นำมาซึ่งความเสียหายไม่ต่างกัน ตัวแปรที่ส่งผลต่อความเสียหายของทั้ง 3 องค์กร คือ ความบกพร่องของระบบรักษาความปลอดภัยที่ดูแลข้อมูลส่วนบุคคลของผู้ใช้

จากผลการวิเคราะห์กรณีตัวอย่างในบทความนี้ สามารถสังเคราะห์ให้เห็นถึงปัจจัยที่เกี่ยวข้องกับวิกฤตการละเมิดข้อมูลส่วนบุคคลในบริบทของสื่อออนไลน์รายละเอียดตาม**แผนภาพที่ 1** จะเห็นได้ว่า ตัวแปรที่ส่งผลต่อประสิทธิภาพการจัดการวิกฤตขององค์กรในเรื่องการละเมิดข้อมูลส่วนบุคคลของผู้ใช้ มีทั้งตัวแปรภายในและภายนอกองค์กร ตัวแปรภายในที่เป็นหัวใจสำคัญ คือ การให้ความสำคัญขององค์กรต่อการปกป้องข้อมูลส่วนบุคคลของผู้ใช้ซึ่งส่งผลถึงการจัดสรรทรัพยากรบุคคลและงบประมาณในการดำเนินการเพื่อพัฒนาระบบรักษาความปลอดภัยข้อมูลส่วนบุคคลของผู้ใช้

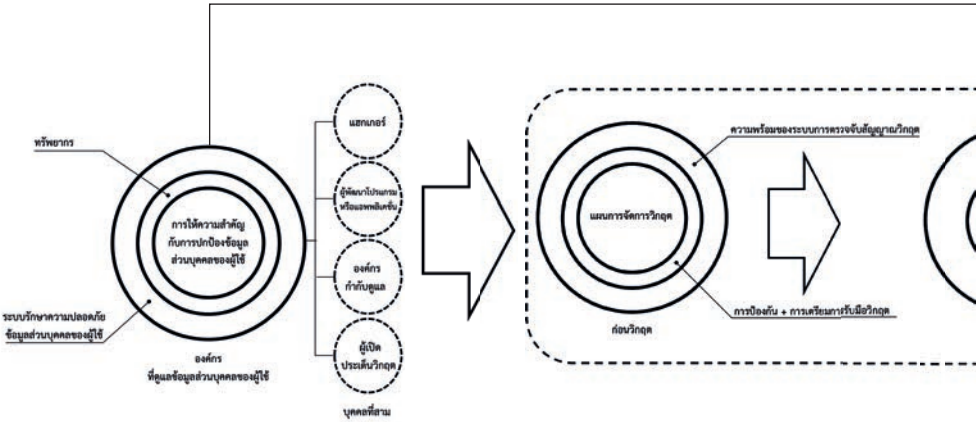
นอกจากตัวแปรภายในแล้ว ยังมีตัวแปรภายนอกที่เกี่ยวข้องกับการเกิดวิกฤต ซึ่งมีทั้งกลุ่ม/องค์กรที่ก่อให้เกิดวิกฤตทางตรง ได้แก่ แฮกเกอร์ผู้พัฒนาโปรแกรมหรือแอปพลิเคชันภายนอก และทางอ้อม ได้แก่ องค์กรกำกับดูแลด้านข้อมูลและสิทธิ์ส่วนบุคคล รวมถึงผู้เปิดประเด็นวิกฤต ในกรณีตัวอย่าง คือ ผู้ให้ข่าวและองค์กรสื่อข่าวที่รายงานข่าวการละเมิดข้อมูลส่วนบุคคลของผู้ใช้ เมื่อเกิดสัญญาณวิกฤต องค์กรจะมีความพร้อมรับมือมากน้อยเพียงใดขึ้นอยู่กับแผนการจัดการวิกฤตขององค์กร หน่วยจัดการวิกฤต ความพร้อมของระบบการตรวจจับสัญญาณวิกฤต รวมถึงการดำเนินการป้องกันและการเตรียมการรับมือ หากองค์กรไม่มีการจัดการในขั้นก่อนวิกฤตนี้ดีพอ จะส่งผลให้ภาวะวิกฤตมีความรุนแรงขึ้น

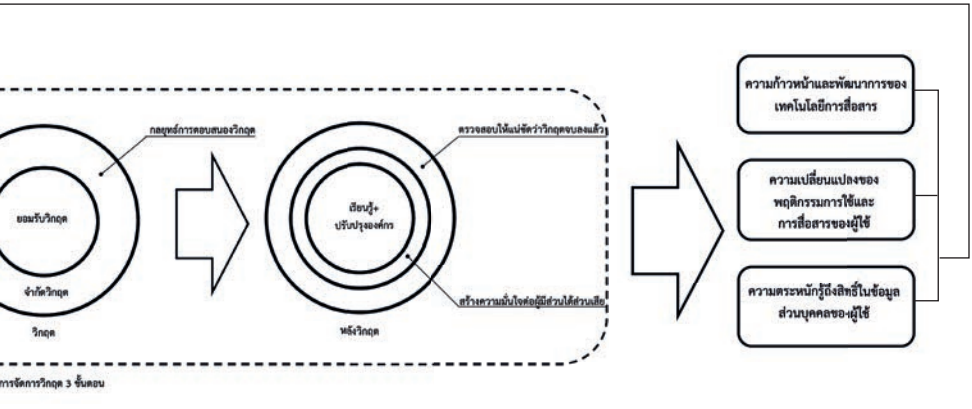
องค์กรควรจะยอมรับภาวะวิกฤต และดำเนินการจำกัดวิกฤตเพื่อแก้สถานการณ์และบรรเทาความรุนแรงของวิกฤตให้ได้มากที่สุด โดยกลยุทธ์การตอบสนองวิกฤตเป็นอีกตัวแปรที่ส่งผลต่อประสิทธิภาพการจำกัดวิกฤตในภาวะวิกฤต กล่าวคือ การเลือกกลยุทธ์ที่เหมาะสมกับสถานการณ์และต้นเหตุของปัญหา จะช่วยลดความรุนแรงและความเสียที่เกิดจากวิกฤตได้ในระดับหนึ่ง ในภาวะหลังวิกฤต องค์กรควรนำสิ่งที่ได้เรียนรู้จากวิกฤตไปพัฒนาระบบรักษาความปลอดภัยข้อมูลส่วนบุคคลของผู้ใช้ พัฒนาระบบตรวจจับสัญญาณวิกฤต และพัฒนาแผนการจัดการวิกฤตต่อไป อย่างไรก็ตาม วิกฤตที่เกิดกับองค์กรไม่ได้ขึ้นอยู่กับการจัดการขององค์กรเพียงฝ่ายเดียว

แต่ยังมีปัจจัยภายนอกที่มีอิทธิพลต่อการเกิดวิกฤตและระดับความรุนแรง คือ พัฒนาการของเทคโนโลยี พฤติกรรมการใช้สื่อและการสื่อสารของผู้ใช้ที่อาจเปลี่ยนไปตามบริบททางสังคม และความตระหนักรู้ถึงสิทธิ์ในข้อมูลส่วนบุคคลของผู้ใช้ที่แตกต่างกันในแต่ละบริบททางสังคมและวัฒนธรรม ดังนั้น ในภาพรวม หลักคิดตามแบบจำลองการจัดการวิกฤต 3 ขั้นตอน และองค์ประกอบต่างๆ ที่เกี่ยวข้องจะเป็นตัวชี้วัดประสิทธิภาพการจัดการวิกฤตขององค์กรตามที่ได้กล่าวไปแล้วข้างต้น

งานวิจัยในอนาคตอาจนำวิกฤตเหล่านี้ไปศึกษาต่อยอดเชิงลึก โดยอาจเปรียบเทียบกับจำนวนองค์กรในลักษณะที่ใกล้เคียงกันมากกว่านี้ และอาจใช้ข้อมูลจากการสัมภาษณ์เชิงลึกถึงแนวทางการจัดการวิกฤตที่องค์กรเหล่านี้ใช้จริง มาวิเคราะห์ประกอบกับผลการวิเคราะห์ด้วยวิธีการศึกษาเอกสาร (documentary research) โดยอาจเก็บข้อมูลจากผู้เกี่ยวข้องกับองค์กรมาเป็นข้อมูลประกอบ

แผนภาพที่ 1 แสดงกรอบแนวคิดการจัดการวิกฤตการละเมิดข้อมูลส่วนบุคคลของผู้ใช้





การจัดการวิกฤต 3 ขั้นตอน

ตารางที่ 3 แสดงรูปแบบการจัดการวิกฤตการละเมิดข้อมูลที่ได้จากการศึกษากรณีตัวอย่างของ Facebook, Yahoo, และ Google+ อิงตามแบบจำลอง 3 ขั้นตอน

Three-stage	Facebook 1	Facebook 2	Yahoo 1	Yahoo 2	Google+
ก่อนวิกฤต (precrisis)					
1) ตรวจจับสัญญาณ (signal detection)	ทราบเรื่องการซื้อขายข้อมูลจากแอปพลิเคชัน *"thisisyourdigitallife"*	จำนวนผู้ลงบันทึกเข้าใช้ (login) สูงผิดปกติ	แฮกเกอร์นามว่า *"Tessa88"* โพสต์ตัวอย่างข้อมูลผู้ใช้ที่อ้างว่าเป็นข้อมูลที่ได้ไปจาก Yahoo	-	ทราบเรื่องข้อมูลส่วนบุคคลของผู้ใช้หลุด
2) ป้องกัน (prevention)	ส่งจดหมายเพื่อขอให้ผู้พัฒนาแอปพลิเคชัน ลบข้อมูล	-	-	-	-
3) เตรียมรับวิกฤต (crisis preparation)	-	-	-	-	-

ตารางที่ 3 แสดงรูปแบบการจัดการวิกฤตการละเมิดข้อมูลที่ได้จากการศึกษากรณีตัวอย่างของ Facebook, Yahoo, และ Google+ อิงตามแบบจำลอง 3 ขั้นตอน (ต่อ)

Three-stage	Facebook 1	Facebook 2	Yahoo 1	Yahoo 2	Google+
ภาวะวิกฤต (crisis)					
1) ยอมรับวิกฤต (crisis recognition)	ช่วงต้น: แถลงการณ์ระบุต้นตอของเหตุละเมิดข้อมูล ช่วงปลาย: แถลงการณ์ชี้แจงว่าข้อมูลหลุดครั้งนี้มีโอกาสกระทบผู้ใช้ทั่วโลกกว่า 87 ล้านราย	แฮกเกอร์เจาะระบบจาก bug กระทบข้อมูลผู้ใช้กว่า 14 ล้านราย	แฮกเกอร์นามว่า “Peace of Mind” นำข้อมูลผู้ใช้ของ Yahoo (ค.ศ. 2014) ออกมาเผยแพร่	นักกฎหมายได้นำตัวอย่างข้อมูลที่ถูกจารกรรมมาให้ Yahoo ตรวจสอบ	บันทึกภายในขององค์กรพบ bug ของระบบ API ที่อนุญาตให้ผู้พัฒนาแอปพลิเคชัน เข้าถึงข้อมูลส่วนตัวของผู้ใช้และ “เพื่อน”
2) จำกัดวิกฤต (crisis containment)	-	ตั้งค่า“access token” ของผู้ใช้กลุ่มเสี่ยงใหม่; สร้างเพจแจ้งเตือนเพื่อให้ผู้ใช้เข้าตรวจสอบว่าบัญชีของตนอยู่ในกลุ่มเสี่ยงหรือไม่	-	บังคับให้ผู้ใช้เปลี่ยนรหัสพร้อมยกเลิกคำถามในการเข้าถึงบัญชีกรณีที่ลืมรหัสผ่าน	-

ตารางที่ 3 แสดงรูปแบบการจัดการวิกฤตการละเมิดข้อมูลที่ได้จากการศึกษากรณีตัวอย่างของ Facebook, Yahoo, และ Google+ อิงตามแบบจำลอง 3 ขั้นตอน (ต่อ)

ภาวะวิกฤต (crisis) (ต่อ)	Facebook 1	Facebook 2	Yahoo 1	Yahoo 2	Google+
หน่วงเวลาในการตอบสนองวิกฤต	2 ปี	2 วัน	2 ปี	3 ปี	6 เดือน
กลยุทธ์การตอบสนองวิกฤต (crisis response strategies)	ช่วงต้น: กลยุทธ์การป้องกัน (defensive strategy) —การปฏิเสธ (denial) ช่วงปลาย: การผ่อนปรน (accommodative strategy)—การขอโทษ (apology)	ช่วงต้น: การผ่อนปรน (accommodative strategy) ช่วงปลาย: กลยุทธ์การป้องกัน (defensive strategy)—การปฏิเสธ (denial)	กลยุทธ์การป้องกัน (defensive strategy) —การปฏิเสธ (denial)	กลยุทธ์การผ่อนปรน (accommodative strategy)—การแก้ไขข้อผิดพลาดหรือการเยียวยา (remedial actions)	ช่วงต้น: กลยุทธ์การป้องกัน (defensive strategy)—การปฏิเสธ (denial) ช่วงปลาย: กลยุทธ์กอบกู้ภาพลักษณ์ (image renewal) —การให้คำมั่นเรื่องค่านิยม (value commitment)

ตารางที่ 3 แสดงรูปแบบการจัดการวิกฤตการละเมิดข้อมูลที่ได้จากการศึกษากรณีตัวอย่างของ Facebook, Yahoo, และ Google+ อิงตามแบบจำลอง 3 ขั้นตอน (ต่อ)

Three-stage	Facebook 1	Facebook 2	Yahoo 1	Yahoo 2	Google+
หลังวิกฤต (postcrisis)					
1) เรียนรู้และปรับปรุงองค์กรเพื่อรับมือวิกฤตครั้งต่อไป	มีการประกาศปรับโครงสร้างองค์กรครั้งใหญ่ในเรื่องเกี่ยวกับการเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้โดยเฉพาะ	-	-	-	-
2) สร้างความมั่นใจต่อผู้มีส่วนได้ส่วนเสียในเรื่องศักยภาพขององค์กรในการรับมือกับภาวะวิกฤต	มีการประกาศปรับโครงสร้างองค์กรครั้งใหญ่ในเรื่องเกี่ยวกับการเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้โดยเฉพาะ	-	-	จ่ายเงินชดเชยให้ผู้ใช้ที่ได้รับผลกระทบแต่ยังขาดการแสดงศักยภาพ	-
3) ตรวจสอบให้แน่ชัดว่าวิกฤตได้จบลงแล้วอย่างแท้จริง	-	-	-	-	-

ตารางที่ 3 แสดงรูปแบบการจัดการวิกฤตการละเมิดข้อมูลที่ได้จากการศึกษากรณีตัวอย่างของ Facebook, Yahoo, และ Google+ อิงตามแบบจำลอง 3 ขั้นตอน (ต่อ)

หลังวิกฤต (postcrisis) (ต่อ)	Facebook 1	Facebook 2	Yahoo 1	Yahoo 2	Google+
ความเสียหายจากวิกฤต	รณรงค์ให้มีการลบแอปพลิเคชัน และบัญชีผู้ใช้ Facebook เป็นหัวข้อยอดนิยมใน Twitter“#deletefacebook”; หุ้นตกลง 19% หรือ $120,000 ล้าน; ถูกปรับ £500,000 (Sanders & Patterson, 2018); ถูกตัดสินปรับข้อหา *“หลอกลวง”* ผู้ใช้ในเรื่องความสามารถในการเก็บดูแลข้อมูลส่วนบุคคลของผู้ใช้เป็นความลับจำนวน $5 พันล้าน (Davies & Rushe, 2019)	หลังเสร็จสิ้นกระบวนการทางกฎหมายจะถูกปรับ 4% ของรายได้ทั้งหมดในรอบปี ประมาณ $1,600 ล้าน (อิงจากรายได้ปี ค.ศ. 2017 ขององค์กร) (O’Sullivan, 2018)	-	ถูกปรับกว่า $35 ล้าน; จ่ายเงินชดเชยให้ผู้ใช้ที่ได้รับผลกระทบราว 200 ล้านรายเป็นเงินกว่า $50 ล้าน; คืนค่าธรรมเนียมร้อยละ 25 พร้อมการชดเชยอื่นๆ เป็นเวลา 2 ปี; กิจการส่วนที่ตกลงขายราคาตก	ปิดบริการสำหรับผู้ใช้ทั่วไป; หลังเสร็จสิ้นกระบวนการทางกฎหมายจะถูกปรับ 4% ของรายได้ทั้งหมดในรอบปี (O’Flaherty, 2019)

รายการอ้างอิง

ภาษาไทย

นิธิมา คณานิธินันท์. (2544). *ความตระหนักรู้ด้านสิทธิข้อมูลส่วนบุคคล ในการสื่อสารผ่านอินเทอร์เน็ตในประเทศไทย* (วิทยานิพนธ์นิเทศศาสตรมหาบัณฑิต). จุฬาลงกรณ์มหาวิทยาลัย, คณะนิเทศศาสตร์, ภาควิชาวารสารสนเทศ.

ปรีดิ์เปรม ชัยกิจ. (2559). *การจัดการภาวะวิกฤตบนสื่อสังคมออนไลน์ของบริษัทผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่* (วิทยานิพนธ์นิเทศศาสตรมหาบัณฑิต). จุฬาลงกรณ์มหาวิทยาลัย, คณะนิเทศศาสตร์, สาขาวิชานิเทศศาสตร์.

เอกพันธ์ พัฒนาวิจิตร. (2559). *ปัจจัยที่ส่งผลต่อการเปิดเผยข้อมูลส่วนบุคคล กรณีศึกษาการลงชื่อเข้าใช้ด้วยรหัสผู้ใช้เฟซบุ๊ก* (การค้นคว้าอิสระวิทยาศาสตรมหาบัณฑิต). มหาวิทยาลัยธรรมศาสตร์, คณะพาณิชยศาสตร์และการบัญชี, สาขาวิชาระบบสารสนเทศเพื่อการจัดการ. สืบค้นเมื่อ 5 มกราคม 2562, จาก http://ethesisarchive.library. tu.ac.th/thesis/2015/TU_2015_5702037135_3915_2778.pdf

เอกภพ จึงกุล. (2558). *การสื่อสารและการจัดการภาวะวิกฤติที่ธนาคารพาณิชย์ประสบบนสื่อสังคมออนไลน์* (วิทยานิพนธ์นิเทศศาสตรมหาบัณฑิต). จุฬาลงกรณ์มหาวิทยาลัย, คณะนิเทศศาสตร์, สาขาวิชานิเทศศาสตร์.

ภาษาอังกฤษ

Armerding, T. (2018). *The 17 biggest data breaches of the 21st century.* Retrieved December 1, 2018, from https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Badshah, N. (2018). *Facebook to contact 87 million users affected by data breach.* Retrieved December 12, 2018, from https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach

Bar, T. (2018). *Notifying our Developer Ecosystem about a Photo API Bug.* Retrieved December 14, 2018, from https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/

Bennett, C. J. (2018). The European General Data Protection Regulation: An instrument for the globalization of privacy standard? *Information Polity, 23*(2), 239-246. doi:10.3233/IP-180002

Bhimani, H., Mention, A.-L., & Barlatier, P.-J. (2018). Social media and innovation: A systematic literature review and future research directions. *Technological Forecasting & Social Change, 144,* 251-269. Retrieved December 14, 2018, from https://doi.org/10.1016/j.techfore.2018.10.007

Cadwalladr, C., & Graham-Harrison, E. (2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* Retrieved December 14, 2018, from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Carr, F. (2018, April 10, 2018). *Facebook Is Telling People Their Data Was Misused by Cambridge Analytica and They're Furious.* Retrieved December 14, 2018, from http://time.com/5234740/ facebook-data-misused-cambridge-analytica/

Channel NewsAsia. (2018). *Facebook says 87 million may be affected by data breach.* Retrieved December 14, 2018, from https://www.channelnewsasia.com/news/world/facebook-says-87-million-may-be-affected-by-data-breach-10105656

Clement, J. (2019). *Number of compromised data records in selected data breaches as of November 2018 (in millions).* Retrieved December 14, 2018, from https://www.statista.com/statistics/290525/ cyber-crime-biggest-online-data-breaches-worldwide/

Clemmitt, M. (2015). Crisis Management. *Sage Business Researcher.* doi:10.1177/2374556814563286

Coombs, W. T. (2009). Conceptualizing Crisis Communication. In R. L. Health & H. D. O'Hair (Eds.), *Handbook of Risk and Crisis Communication* (pp. 99-118). New York, NY: Rouledge.

Coombs, W. T. (2012). *Ongoing Crisis Communication: Planning, Managing, and Responding* (3rd ed.). California, CA: SAGE Publications.

D'Onfro, J. (2018a). *Google+ is shutting down, and the site's few loyal users are mourning.* Retrieved December 14, 2018, from https://www.cnbc.com/2018/10/10/google-plus-users-mourn-shutdown.html

D'Onfro, J. (2018b). *Zuckerberg says he hasn't seen a 'meaningful number of people' deleting Facebook accounts in the wake of data scandal.* Retrieved December 14, 2018, from https://www.cnbc.com/2018/03/21/mark-zuckerberg-on-delete-facebook-push-after-cambridge-analytica-news.html

Dance, G. J. X., LaForgia, M., & Confessore, N. (2018). *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants.* Retrieved December 18, 2018, from https://www.nytimes.com /2018/12/18/technology/facebook-privacy.html?smtyp=cur&smid=tw-nytimes

Davies, R., & Rushe, D. (2019). *Facebook to pay $5bn fine as regulator settles Cambridge Analytica complaint.* Retrieved August 8, 2019, from https://www.theguardian.com/ technology /2019/jul/24/facebook-to-pay-5bn-fine-as-regulator-files-cambridge-analytica-complaint?fbclid =IwAR1p73Fw4kihw23V4Jwziz11fsgkOgiE7A4FCNEFQzVx3iH2RZuUUklNSc

DiStaso, M. W., Vafeiadis, M., & Amaral, C. (2015). Managing a health crisis on Facebook: How the response strategies of apology, sympathy, and information influence public relations. *Public Relations Review, 41*(2), 222-231. doi:10.1016/j.pubrev.2014.11.014

Eriksson, M., & Olsson, E.-K. (2016). Facebook and Twitter in Crisis Communication: A Comparative Study of Crisis Communication Professionals and Citizens. *Journal of Contingencies and Crisis Management, 24*(4), 198-208. doi:https://doi.org/10.1111/1468-5973.12116

Frandsen, F., & Johansen, W. (2017). *Organizational Crisis Communication.* London, LDN: Sage Publications.

Global Data Sentinel. (2018). *Yahoo Data Breach Reaching Conclusion.* Retrieved December 21, 2018, from https://www.globaldatasentinel.com/the-latest/yahoo-data-breach-reaching-conclusion/

Goel, V. (2017). *Yahoo's Top Lawyer Resigns and C.E.O. Marissa Mayer Loses Bonus in Wake of Hack.* Retrieved December 18, 2018, from https://www.nytimes.com/2017/03/01/technology/yahoo-hack-lawyer-resigns-ceo-bonus.html

Goel, V., & Perlroth, N. (2016). *Yahoo Says 1 Billion User Accounts Were Hacked.* Retrieved December 18, 2018, from https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html

Grewal, P. (2018). *Suspending Cambridge Analytica and SCL Group From Facebook.* Retrieved December 14, 2018, from https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/

Gwebu, K. L., Wang, J., & Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *Journal of Management Information Systems, 35*(2), 683-714. doi:10.1080/07421222.2018.1451962

Haselton, T. (2017). *Yahoo just said every single account was affected by 2013 attack — 3 billion in all.* Retrieved December 18, 2018, from https://www.cnbc.com/2017/10/03/yahoo-every-single-account-3-billion-people-affected-in-2013-attack.html

Houser, K. A. & Voss, G. (forthcoming 2018). GDPR: The end of Google and Facebook or a New Paradigm in Data Privacy? *Richmond Journal of Law & Technology,* 25-1. doi:10.2139/ssrn.3212210

Independent. (2018). *Google+ To Shut Down After Data From 500,000 Users May Have Been 'Exposed by Security Bug'.* Retrieved December 21, 2018, from https://www.independent.co.uk/life-style/gadgets-and-tech/google-plus-shut-down-security-bug-personal-data-breach-alphabet-inc-a8574941.html

Isaac, M., & Frenkel, S. (2018). *Facebook Security Breach Exposes Accounts of 50 Million Users.* Retrieved December 18, 2018, from https://www.nytimes.com /2018/09/28/technology/facebook-hack-data-breach.html

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer, 51*(8), 56-59. doi:10.1109/MC.2018.3191268

John, A. S. (2018). *Here's What Makes the Facebook Data Breach so Harmful.* Retrieved December 18, 2018, from https://www.consumerreports.org/digital-security/what-makes-the-facebook-data-breach-so-harmful/

Keach, S. (2018). *SAFE SPACE Facebook data breach explained – what happened with Cambridge Analytica and are you safe?* Retrieved December 18, 2018, from https://www.thesun.co.uk /tech/5843838/facebook-data-scandal-cambridge-analytica-safe/

Kemp, S. (2018). *The State of the Internet in Q4 2018.* Retrieved December 9, 2018, from https://wearesocial.com/blog/2018/10/the-state-of-the-internet-in-q4-2018

Lee, D. (2018). *Google+ shutting down after users' data is exposed.* Retrieved December 18, 2018, from https://www.bbc.com/news/technology-45792349

Lwin, M. O., Lu, J., Sheldenkar, A., & Schulz, P. J. (2018). Strategic Uses of Facebook in Zika Outbreak Communication: Implications for the Crisis and Emergency Risk Communication Model. *International Journal of Environmental Research and Public Health, 15*(9). doi:10.3390/ijerph15091974

MacMillan, D., & McMillan, R. (2018). *Google Exposed User Data, Feared Repercussions of Disclosing to Public.* Retrieved December 21, 2018, from https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194?mod=djemalertNEWS

Marcus, D. J. (2018). The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke Law Journal, 68*(3), 555-593. Retrieved December 21, 2018, from https://scholarship.law.duke.edu/dlj/vol68/iss3/3/

Matsakis, L., & Lapowsky, I. (2018). *Everything We Know About Facebook's Massive Security Breach.* Retrieved December 21, 2018, from https://www.wired.com/story/facebook-security-breach-50-million-accounts/

Merced, M. J. d. l. (2016). *Hacked Yahoo Data Is for Sale on Dark Web.* Retrieved December 21, 2018, from https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html

Möller, C., Wang, J., & Nguyen, H. T. (2018). #Strongerthanwinston: Tourism and crisis communication through Facebook following tropical cyclones in Fiji. *Tourism Management, 69*, 272-284. doi:10.1016/j.tourman.2018.05.014

Newman, I. H. (2018). *A New Google+ Blunder Exposed Data From 52.5 Million Users.* Retrieved December 14, 2018, from https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/

News BTC. (2018). *The 6 Worst Data Breaches In History.* Retrieved December 1, 2018, from https://www.newsbtc.com/press-releases/the-6-worst-data-breaches-in-history/

O'Flaherty, K. (2018). *Facebook Data Breach -- What To Do Next.* Retrieved December 14, 2018, from https://www.forbes.com/sites/kateoflahertyuk/2018/09/29/facebook-data-breach-what-to-do-next/#1dfdb5512de3

O'Flaherty, K. (2019). *Google+ Security Bug -- What Happened, Who Was Impacted And How To Delete Your Account.* Retrieved December 27, 2018, from https://www.forbes.com/sites/kateoflahertyuk/2018/10/09/google-plus-breach-what-happened-who-was-impacted-and-how-to-delete-your-account/#1d4abe886491

O'Sullivan, D. (2018). *Facebook could face billion dollar fine for data breaches.* Retrieved December 27, 2018, from https://edition.cnn.com/2018/12/14/tech/facebook-billion-dollar-fine/index.html

Panchadar, A., & Moon, A. (2018). *Irish regulator investigates Facebook over private photo glitch.* Retrieved December 14, 2018, from https://www.reuters.com/article/us-facebook-cyber/new-facebook-bug-exposed-photos-of-up-to-68-million-users-idUSKBN1OD1UX

Perlroth, N. (2016). *Yahoo Says Hackers Stole Data on 500 Million Users in 2014.* Retrieved December 18, 2018, from https://www.nytimes.com/2016/09/23/ technology/yahoo-hackers.html

Reints, R. (2018). *Yahoo Agrees to $50 Million Settlement for Those Affected by the 2013 Data Breach.* Retrieved December 18, 2018, from http://fortune.com/2018/10/24/ yahoo-settlement-data-breach/

Reuters. (2016). *Why Yahoo's Security Problems Are a Story of Too Little, Too Late.* Retrieved December 21, 2018, from http://fortune.com/2016/12/19/yahoo-hack-cyber-security/

Rodriguez, S. (2018, October 12, 2018). *Facebook says hackers were able to access millions of phone numbers and email addresses.* Retrieved December 18, 2018, from https://www.cnbc.com /2018/10/12/facebook-security-breach-details.html

Roshan, M., Warren, M., & Carr, R. (2015). Understanding Stakeholders' Expectations of Organisational Crisis Communication by Social Media. Paper presented at *the 2nd European Conference on Social Media 2015: ECSM 2015,* Polytechnic Institute of Porto, Portugal.

Sanders, J., & Patterson, D. (2018). *Facebook data privacy scandal: A cheat sheet.* Retrieved December 18, 2018, from https://www.techrepublic.com/article/ facebook-data-privacy-scandal-a-cheat-sheet/

Smith, B. (2018). *Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+.* Retrieved December 21, 2018, from https://www.blog.google/technology/safety-security/project-strobe/

Stríteský, V. c., Stránská, A., & Drábik, P. (2015). Crisis communication on Facebook. *Studia commercialia Bratislavensia, 8*(29), 103-111. doi:10.1515/stcb-2015-0010

Swisher, K. (2016). *Yahoo is expected to confirm a massive data breach, impacting hundreds of millions of users.* Retrieved December 18, 2018, from https://www.recode.net/2016/9/22/13012836 /yahoo-is-expected-to-confirm-massive-data-breach-impacting-hundreds-of-millions-of-users

Szymczak, H., Kuecuekbalaban, P., Lemanski, S., & Knuth, D. (2016). Trusting Facebook in Crisis Situations: The Role of General Use and General Trust Toward Facebook. *Cyberpsychology, Behavior, and Social Networking, 19*(1), 23-27. doi:10.1089/cyber.2015.0450

Techworld. (2018). *The UK's most infamous data breaches.* Retrieved December 14, 2018, from https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

Time (Producer). (2018). *Facebook CEO Mark Zuckerberg testifies on Capitol Hill, where he faces tough questions from senators about Facebook's data-privacy.* Retrieved December 14, 2018, from https://www.facebook.com/time/videos/10155653968751491/

Trautman, L. J., & Ormerod, P. C. (2017). Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. *American University Law Review, 66*(5), 1231-1291. Retrieved December 14, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2883607

Tuttle, H. (2018). Facebook Scandal Raises Data Privacy Concerns. *Risk Management (00355593), 65*(4), 6-9. Retrieved December 14, 2018, from https://eds.a.ebscohost.com/eds/detail /detail?vid=1&sid=e680cd2d-584a-47ee-a41c-4bad2d5357fd%40sdc-v-sessmgr02&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=129484447&db=bft

Tynan, D. (2018). *Facebook says 14m accounts had personal data stolen in recent breach.* Retrieved December 14, 2018, from https://www.theguardian.com/technology /2018/oct/12/facebook-data-breach-personal-information-hackers

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2007). *Effective Crisis Communication: Moving From Crisis to Opportunity.* California, CA: Sage Publications.

Winston, J. (2018). *The Facebook data breach is a scandal of our own making. Legally, there's nothing we can do about it.* Retrieved December 21, 2018, from https://www.nbcnews.com /think/opinion/facebook-data-breach-scandal-our-own-making-legally-there-s-ncna862211

Wong, J. C., & Solon, O. (2018). *Google to shut down Google+ after failing to disclose user data leak.* Retrieved December 21, 2018, from https://www.theguardian.com /technology /2018/oct/08/google-plus-security-breach-wall-street-journal