Data Breach Response

โครงการอบรมและ
ลงทะเบียนผู้ประกอบธุรกิจที่
ให้บริการแก่ผู้ให้บริการ
แพลตฟอร์มอีคอมเมิร์ซ

#DP102

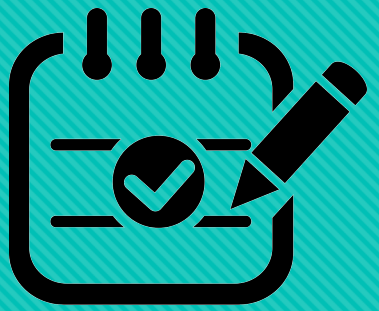
ข้อแนะนำในการเตรียมพร้อมกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Breach Preparation)

สามารถเป็นส่วนหนึ่งของ

แผนการรับมือสถานการณ์ข้อมูลส่วนบุคคลรั่วไหล

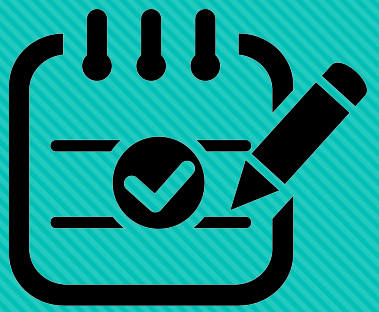
(Data Breach Response Plan)

Data Breach Preparation Checklist



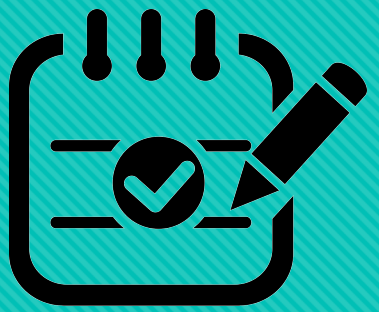
- ควรจัดทำ**แผนการรับมือสถานการณ์ข้อมูลส่วนบุคคลรั่วไหล (Data Breach Response Plan) รวมถึงแผนการสื่อสาร (Communication Plan) ในกรณีที่เหตุการณ์ดังกล่าวเกิดขึ้น**
- จัดตั้ง**ทีมเผชิญเหตุ**ที่เกี่ยวข้องกับสถานการณ์ทั้งจากภายในองค์กร และผู้เชี่ยวชาญที่มาจากภายนอก ควรประกอบไปด้วยผู้เชี่ยวชาญด้าน
  - ตรวจพิสูจน์พยานหลักฐานทางดิจิทัล
  - กฎหมาย
  - สารสนเทศ
  - ความมั่นคงปลอดภัยไซเบอร์
  - ทรัพยากรบุคคล
  - ประชาสัมพันธ์

Data Breach Preparation Checklist



- **จัดเตรียมช่องทางประสานงาน สำหรับภายในองค์กร และภายนอกกับคู่ค้า/ลูกค้า**
- การเตรียมพร้อมด้านระบบสารสนเทศ
  - จัดทำหรือทบทวน**ทะเบียนสินทรัพย์ (inventory of asset)** รวมถึงข้อมูลที่สำคัญในการให้บริการ
  - จัดทำหรือทบทวน**แผนผังการเชื่อมต่อเครือข่าย และระบบสารสนเทศ**ที่ให้บริการ ควร**แยกเครือข่ายส่วนที่ให้บริการกับระบบหลัก และจาก Thrid party ที่มาเชื่อมต่อ**
  - จัดทำหรือทบทวน**ข้อมูลการติดต่อสำหรับผู้ดูแลหรือผู้ให้บริการสินทรัพย์ และเครือข่าย** เพื่อเตรียมความพร้อมในกรณีที่ต้องการประสานการแก้ไขปัญหา หรือรับมือสถานการณ์ที่อาจเกิดขึ้น
  - จัดเตรียม**ช่องทางสำรองสำหรับให้บริการ กรณีที่ช่องทางหลักได้รับผลกระทบ**
  - ทบทวนการ**กำหนดสิทธิการเข้าถึงเครือข่าย และระบบสารสนเทศ ตามความจำเป็นและหน้าที่** (need to know, least privilege, separation of duties) อยู่เสมอ หรือเมื่อมีการเปลี่ยนแปลงผู้เกี่ยวข้อง

Data Breach Preparation Checklist (Additional)



- มี**ช่องทางการรับแจ้งเหตุ**เกี่ยวกับปัญหาด้านความมั่นคงปลอดภัยไซเบอร์
- มี**ช่องทางการประชาสัมพันธ์กับคู่ค้า/ลูกค้า**ภายนอก และ**ดำเนินการประชาสัมพันธ์ให้ข้อมูล**ที่อาจเกิดความเสี่ยง**อย่างสม่ำเสมอ**
- การเตรียมพร้อมด้านระบบสารสนเทศ
  - **จัดเก็บบันทึกกิจกรรม (log)** ไปยังพื้นที่จัดเก็บในส่วนกลางที่มีการควบคุมการเข้าถึงอย่างรัดกุม เพื่อให้แน่ใจว่าข้อมูลดังกล่าวจะไม่ถูกทำลายหรือเปลี่ยนแปลง ครอบคลุม
    - ข้อมูลการใช้งานระบบสารสนเทศ เช่น application log
    - ข้อมูลการเชื่อมต่อทางเครือข่ายหรือระบบป้องกันการโจมตีทางเครือข่าย เช่น firewall log, intrusion protection system (ips) log
    - ข้อมูลบันทึกกิจกรรมของระบบปฏิบัติการ เช่น event log, system log, security log, audit log

ข้อแนะนำในการรับมือสถานการณ์การรั่วไหลของข้อมูลส่วนบุคคล (Data Breach Response)

1. ทำให้ธุรกิจเดินได้อย่างต่อเนื่อง พร้อมลดความสับสนและความเสียหาย
2. วิเคราะห์ปัญหาและแก้ไขปัญหาตามแนวทางที่เหมาะสม
3. การแจ้งเตือนกับผู้ได้รับผลกระทบ

ควรมีการดำเนินการตามแผนการรับมือสถานการณ์ข้อมูลส่วนบุคคลรั่วไหล (Data Breach Response Plan) และอาจพิจารณาเพิ่มเติมตามรายละเอียดในส่วนนี้

๑) “ทำให้ธุรกิจเดินได้อย่างต่อเนื่อง พร้อมลดความสับสนและความเสียหาย”

- **เรียกประชุมทีมเผชิญเหตุ**ที่เกี่ยวข้องกับสถานการณ์ เพื่อเริ่มกระบวนการในการประเมินความเสียหาย การวิเคราะห์ความเสียหาย ช่องทางการโจมตี พร้อมหาแนวทางแก้ไข และตัดสินใจเพื่อเลือกมาตรการที่จะใช้รับมือการรั่วไหลของข้อมูลส่วนบุคคล
- ลดความเสียหายของระบบ อย่างน้อย**ตัดการเชื่อมต่อทางเครือข่ายของระบบที่ได้รับผลกระทบทันที** แต่ให้ระมัดระวังเรื่องการปิดเครื่องหรือเข้าดำเนินการใด ๆ เพิ่มเติม ซึ่งอาจส่งผลทำให้หลักฐานถูกเปลี่ยนแปลงไป
  - หากเป็นไปได้ให้ปรับไปใช้ระบบสำรองเพื่อดำเนินงานก่อน
  - เปลี่ยนรหัสผ่านที่สำคัญของผู้ดูแลระบบ เนื่องจากข้อมูลสำคัญอาจถูกขโมยไปก่อนหน้านี้
- ประสาน**นำเนื้อหาที่มีข้อมูลส่วนบุคคลออกจากเว็บไซต์ที่เกี่ยวข้อง** เช่น กรณีโดนโพสต์ข้อมูลขาย
- **เผยแพร่/ให้ข้อมูลส่วนงานที่ต้องประสานกับคู่ค้า/ลูกค้าผ่านช่องทางที่เตรียมไว้** หรือเป็นช่องทางที่ข้อมูลเผยแพร่ไปยังผู้เกี่ยวข้องได้รวดเร็วและครบถ้วนที่สุด พร้อม**จัดเตรียมช่องทางการสื่อสารกับประชาชนที่อาจมีคำถาม** พร้อมคำตอบในมิติต่าง ๆ อย่างชัดเจน ไว้ในพื้นที่ที่เข้าถึงง่าย เช่น เว็บไซต์ เพจสื่อสังคมออนไลน์

๒) “วิเคราะห์ปัญหาและแก้ไขปัญหาตามแนวทางที่เหมาะสม”

- ทีมผู้เชี่ยวชาญพร้อมผู้ปฏิบัติงานเข้า**พิจารณาข้อมูลที่หลุด เพื่อประเมินว่าข้อมูลหลุดมาจากส่วนไหน**
- ทีมผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐาน ดำเนินการ**จัดเก็บหลักฐานและตรวจพิสูจน์พยานหลักฐาน เพื่อประเมินสภาพปัญหา พร้อมประเมินช่องทางการโจมตี**
  - ตรวจสอบว่าในระหว่างที่ถูกโจมตีนั้น เครือข่ายใดบ้างที่สามารถเชื่อมต่อกับเครื่องที่ถูกโจมตีสำเร็จ ซึ่งอาจแสดงให้เห็นถึงความเสี่ยงที่อาจมีเพิ่มเติม และจำเป็นต้องนำมาวิเคราะห์เพิ่มเติม
- ภายหลังจากการวิเคราะห์เสร็จสิ้น**ดำเนินการตามแผนสื่อสาร**ที่จัดเตรียมไว้อย่างเหมาะสม**ไปยังผู้เกี่ยวข้องทั้งภายในองค์กรและภายนอกกับคู่ค้า/ลูกค้า** (โดยเฉพาะคู่ค้าและลูกค้าที่เกี่ยวข้องกับการรั่วไหลของข้อมูล)
  - เนื้อหาของการสื่อสารควรชัดเจน ตรงประเด็นว่าเกิดอะไร และต้องการให้ผู้รับสารทราบและดำเนินการอะไรบ้าง
  - พึงระวังข้อมูลที่สื่อสารซึ่งอาจก่อให้เกิดความเสี่ยงเพิ่มเติมได้ เช่น การแชร์ข้อมูลลิงก์ข้อมูลที่รั่วไหลลงในสื่อ

๓) “การแจ้งเตือนกับผู้ได้รับผลกระทบ” ***

- แจ้ง**หน่วยงานหลักตามกฎหมาย**ที่เกี่ยวข้อง เช่น พรบ.คุ้มครองข้อมูลส่วนบุคคล (ภายใน 72 ชั่วโมง) พรบ.ไซเบอร์
- แจ้ง**หน่วยงานบังคับใช้กฎหมาย** เพื่อให้เข้าร่วมกระบวนการในการตรวจพิสูจน์พยานหลักฐานและการดำเนินคดี
- แจ้ง**คู่ค้า/ลูกค้าที่อาจได้รับผลกระทบ**จากข้อมูลรั่ว เช่น กรณีที่มีบัญชีธนาคารรั่วไหลให้แจ้งธนาคารที่เกี่ยวข้อง เพื่อให้ช่วยเฝ้าระวังความเสี่ยงที่อาจเกิดจากการนำข้อมูลไปใช้งาน
- แจ้ง**ผู้เสียหายหรือเจ้าของข้อมูล**โดยตรง พร้อมข้อแนะนำในการลดความเสี่ยงจากการที่ข้อมูลผู้ใช้งานรั่วไหล
  - **ปรึกษาทีมกฎหมายเกี่ยวกับช่วงเวลาที่ควรจะแจ้งเหตุไปยังผู้เสียหายหรือเจ้าของข้อมูล**โดยตรง โดยพิจารณาให้สอดคล้องกับช่วงเวลาที่ได้ผลของการตรวจพิสูจน์พยานหลักฐาน
  - **จัดเตรียมผู้ประสานงานของหน่วยงานไว้เพื่อแจ้งและรับการประสานจากผู้เกี่ยวข้อง** เพื่อติดตามสถานการณ์และการดำเนินการที่เกี่ยวข้อง
  - **พิจารณาแนวทางการแจ้งผู้เสียหายเพิ่มเติมตามบทความสั้น** "ข้อแนะนำแนวทางการประกาศแจ้งเตือนต่อสาธารณะในกรณีเหตุการณ์ข้อมูลรั่วไหล” https://www.thaicert.or.th/newsbite/2020-05-26-03.html

References

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
  - http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF
- Data breach preparation and response
  - https://www.oaic.gov.au/assets/privacy/guidance-and-advice/data-breach-preparation-and-response.pdf
- DATA BREACH RESPONSE: A GUIDE FOR BUSINESS
  - https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

ข้อแนะนำใน
การแจ้งเตือนกับผู้ได้รับ
ผลกระทบ

1. จุดประสงค์ในการแจ้งเตือน
2. องค์ประกอบในการแจ้งเตือน
3. Workshop

จุดประสงค์ของการแจ้งเตือน

- เพื่อให้สอดคล้องตามแนวทางที่กฎหมายได้ระบุไว้
- เพื่อให้การสื่อสารนั้นชัดเจนและตรงตามข้อเท็จจริง และผู้เกี่ยวข้องนำไปดำเนินงานต่อได้อย่างเหมาะสม
- ลดความเสี่ยงและความเสียหายที่เกิดขึ้นจากผู้เกี่ยวข้อง ทั้งคู่ค้า และผู้เป็นเจ้าของข้อมูลที่อาจได้รับผลกระทบ
- สร้างความเชื่อมั่นให้กับผู้เกี่ยวข้องในแนวทางการดำเนินการที่มี
- สร้างบรรทัดฐานในการแจ้งข้อมูลที่เป็นแนวทางปฏิบัติที่ดี

องค์ประกอบที่จำเป็นของการแจ้งเตือน

เขียนแจ้งเตือน ต้องรู้อะไรบ้าง !!!

- **ช่องทางการสื่อสาร** (อีเมล เว็บไซต์ call center chatbot โทรศัพท์ อื่นๆ)
- **ความต้องการในการแจ้งเตือน** (แจ้งต่อเจ้าของข้อมูลที่ได้รับผลกระทบ แจ้งภาพรวม ออกเป็นรายงาน)
- **ชื่อหัวข้อที่จะสื่อสาร**
- **เนื้อหาหลักที่เกี่ยวข้อง**
  - วันเวลา ข้อมูลที่บ่งชี้ถึงเหตุการณ์ที่คนที่รับข้อมูลทราบ
  - ประเมินจำนวนรายการของข้อมูลที่รั่วไหล หรือจำนวนของผู้ที่คาดว่าจะได้รับผลกระทบ
  - ระบุประเภทของข้อมูลที่รั่วไหล เช่น ชื่อนามสกุล หมายเลขโทรศัพท์ อีเมล ข้อมูลด้านการเงิน อื่น ๆ
  - ประเมินความเสี่ยงว่าข้อมูลที่รั่วไหลนั้นอาจถูกนำไปใช้ประโยชน์ในทางมิชอบในลักษณะใดได้บ้าง
  - ระบุแนวทางการแก้ไขปัญหาหรือเยียวยาผู้ที่ได้รับผลกระทบ
  - ระบุช่องทางการติดต่อผู้ที่รับผิดชอบเรื่องการคุ้มครองข้อมูลส่วนบุคคลทั้งนี้

เริ่มต้น Workshop