**รายการตรวจสอบการระบุและจัดลำดับความสำคัญของสินทรัพย์ ไซเบอร์ที่สำคัญ**

จุดประสงค์ของรายการตรวจสอบนี้คือเพื่อช่วยให้ผู้จัดการเหตุฉุกเฉินและผู้มีส่วนได้ส่วนเสียหลักอื่นๆ เตรียมพร้อมที่จะตอบสนองและกู้คืนจากเหตุการณ์ทางไซเบอร์ที่ขัดขวางบริการและการดำเนินงานที่สำคัญอย่างมีประสิทธิภาพ โดยกำหนดกระบวนการทั่วไปในการระบุและจัดลำดับความสำคัญของทรัพย์สินทางไซเบอร์ที่สำคัญของเขตอำนาจ โดยเป็นส่วนหนึ่งของกระบวนการวางแผน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับกระบวนการนี้และการเตรียมพร้อมสำหรับเหตุการณ์ทางไซเบอร์ โปรดดู **ข้อควรพิจารณาในการวางแผนสำหรับเหตุการณ์ทางไซเบอร์: คำแนะนำสำหรับผู้จัดการเหตุฉุกเฉิน** ที่ [fema.gov/plan](https://www.fema.gov/emergency-managers/national-preparedness/plan)

|  |
| --- |
| **การชี้บ่ง (Identificaton)** |
| **รายการตรวจสอบ** | **หมายเหตุ** |
| [ ]  รวบรวมทีมจากหลายสาขาซึ่งรวมถึงผู้เชี่ยวชาญด้านการจัดการเหตุฉุกเฉิน กฎหมาย เทคโนโลยีสารสนเทศ ความปลอดภัยสาธารณะ และผู้เชี่ยวชาญด้านภาคเอกชนที่รับผิดชอบในเขตอำนาจ |  |
| [ ]  ระบุบริการที่สำคัญภายในเขตอำนาจ เริ่มต้นด้วยบริการที่สำคัญที่รู้จัก จากนั้นขยายเพื่อระบุบริการที่เกี่ยวข้อง การใช้ lifelines ชุมชนเป็นจุดเริ่มต้นอาจเป็นประโยชน์ |  |
| [ ]  พัฒนารายการทรัพย์สินโครงสร้างพื้นฐานที่สำคัญที่ครอบคลุมซึ่งสนับสนุนบริการที่สำคัญแต่ละบริการภายในเขตอำนาจร่วมกับเจ้าของและผู้ปฏิบัติงาน ซึ่งรวมถึงทรัพย์สินที่สำคัญ: |  |
| **ตัวอย่างของโครงสร้างพื้นฐานที่สำคัญ*** ศูนย์จัดส่ง / จุดตอบรับความปลอดภัยสาธารณะ (PSAPS) / ศูนย์ปฏิบัติการฉุกเฉิน / โรงพยาบาล
 |
| [ ]  การดำเนินธุรกิจด้านการกำกับดูแล |
| [ ]  การตอบสนองเหตฉุกเฉิน |
| [ ]  เพื่อรักษาความปลอดภัยและความสงบเรียบร้อยของประชาชน |
| [ ]  เพื่อความมั่นคงทางเศรษฐกิจของเขตอำนาจหรือภูมิภาค |
| [ ]  เพื่อให้บริการการรักษาพยาบาลและบริการสาธารณสุข |
| [ ]  สำหรับการให้บริการเครือข่ายการสื่อสารด้วยเสียงและ/หรือข้อมูล |
| [ ]  เพื่อดำเนินการระบบข้อความสาธารณะหรือคำเตือน |
| [ ]  สำหรับการให้บริการที่จำเป็นขั้นพื้นฐาน เช่น น้ำ ไฟฟ้า หรือก๊าซ |
| [ ]  พบปะกับเจ้าของบริการและผู้ปฏิบัติงาน ผู้มีส่วนได้ส่วนเสียด้านบริการ และผู้ให้บริการหรือผู้จำหน่าย เพื่อระบุสินทรัพย์โครงสร้างพื้นฐานที่สำคัญและหารือเกี่ยวกับ: |  |
| [ ]  บริการและการดำเนินงานที่สำคัญ |
| [ ]  การขึ้นต่อกันต้นน้ำ ภายใน และปลายน้ำ |
| [ ]  โครงสร้างพื้นฐานทางไซเบอร์ (ทั้งภายในและภายนอกองค์กร) จำเป็นต่อการรักษาบริการและการดำเนินงานที่สำคัญ |
| **ตัวอย่างของโครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญ*** สวิตช์หลัก / ซอฟต์แวร์ระบบการจัดการบันทึก (RMS) / สกาดาสาธารณูปโภคระบบ (เช่น การส่งน้ำ) / ระบบวิทยุสื่อสาร
 |
| [ ]  ผลที่ตามมาที่อาจเกิดขึ้นจากการหยุดชะงักของบริการ |
| [ ]  วิธีรับทราบสถานการณ์เกี่ยวกับสถานะและความพร้อมในการปฏิบัติงานของบริการที่สำคัญในระหว่างเหตุการณ์ |
| [ ]  พัฒนารายการสินทรัพย์โครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญที่ครอบคลุมซึ่งสนับสนุนบริการและการดำเนินงานที่สำคัญภายในเขตอำนาจ |  |
| [ ]  รวบรวมข้อมูลที่ได้รับและสร้างบริการที่สำคัญและรายการอ้างอิง สินค้าคงคลังจะรวบรวมบริการที่สำคัญ โครงสร้างพื้นฐาน สินทรัพย์ เจ้าของและผู้ปฏิบัติงานที่เกี่ยวข้อง บุคลากรสำคัญอื่นๆ และการพึ่งพาระหว่างระบบ |  |

|  |
| --- |
| **การจัดลำดับความสำคัญ** |
| **รายการตรวจสอบ** | **หมายเหตุ** |
| [ ]  พัฒนาวิธีการและ/หรือกลไกการให้คะแนนเพื่อประเมินความสำคัญของสินทรัพย์โครงสร้างพื้นฐานทางไซเบอร์แต่ละรายการต่อการดำเนินงาน ตัวอย่าง การให้คะแนนสินทรัพย์โครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญมีอยู่ในหน้าต่อไปนี้ |  |
| [ ]  พบปะกับเจ้าของบริการ ผู้ประกอบการ และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องเพื่อ: |  |
| [ ]  ตรวจสอบสินทรัพย์โครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญแต่ละรายการโดยใช้วิธีการที่ระบุ หากใช้กลไกการให้คะแนน ให้ใช้คะแนนวิกฤตกับสินทรัพย์โครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญแต่ละรายการ |
| [ ]  หารือและจัดทำเอกสารว่ามีความซ้ำซ้อนหรือการสำรองข้อมูลใดบ้างสำหรับบริการเหล่านั้นตัวอย่างเช่น บริการบางอย่างอาจสามารถทำงานได้ด้วยตนเองหรือถูกย้ายไปยังตำแหน่งที่ไม่ได้รับผลกระทบ |
| [ ]  จัดอันดับโครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญโดยใช้วิธีการหรือคะแนนวิกฤตที่ระบุ อย่าลืมพิจารณาความซ้ำซ้อนและการสำรองข้อมูลเป็นปัจจัยบรรเทา |  |
| [ ]  ใช้ข้อมูลนี้เพื่อจัดลำดับความสำคัญในการใช้ทรัพยากรที่มีจำกัด และกำหนดลำดับของความพยายามในการเผชิญเหตุ |  |

**ตัวอย่างกลไกการให้คะแนนโครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญ**

กลไกการให้คะแนนตัวอย่างนี้เป็นแนวทางตัวอย่างในการประเมินความสำคัญของโครงสร้างพื้นฐานทางไซเบอร์

ในตัวอย่างนี้ ตัวเลขในวงเล็บแสดงถึงคะแนนที่เกี่ยวข้องสำหรับแต่ละคำตอบ คะแนนรวมจะถูกคำนวณหลังจากตอบคำถามทุกข้อเสร็จแล้ว หมายเหตุ: โครงสร้างพื้นฐานที่มีคะแนนสูงกว่าแสดงถึงโครงสร้างพื้นฐานที่อาจได้รับการพิจารณาว่ามีลำดับความสำคัญสูงกว่า

เมื่อสร้างหรือใช้กลไกการให้คะแนนโครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญ แต่ละเขตอำนาจจะกำหนดระบบการให้คะแนนสำหรับการประเมินผลกระทบที่เหมาะสมสำหรับชุมชนของตน เพื่อให้สามารถประมาณผลกระทบที่สอดคล้องกันตลอดกระบวนการจัดลำดับความสำคัญของสินทรัพย์ ด้านล่างนี้เป็นคำจำกัดความสำหรับระบบการให้คะแนนที่เป็นไปได้ซึ่งดัดแปลงมาจากมาตรฐาน

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) สำหรับการจัดหมวดหมู่ความปลอดภัยของระบบสารสนเทศและข้อมูลของรัฐบาลกลาง

**ผลกระทบเล็กน้อย:** ผลกระทบเชิงลบอย่างจำกัดที่อาจ: (i) ทำให้เกิดความเสื่อมโทรมในความสามารถภารกิจในขอบเขตและระยะเวลาที่เขตอำนาจสามารถปฏิบัติหน้าที่หลักได้ แต่ประสิทธิผลของหน้าที่จะลดลงอย่างเห็นได้ชัด; (ii) ส่งผลให้เกิดความเสียหายน้อยที่สุดต่อทรัพย์สินของเขตอำนาจ; (iii) ส่งผลให้เกิดการสูญเสียทางการเงินน้อยที่สุด; หรือ (iv) ส่งผลให้เกิดอันตรายต่อบุคคลน้อยที่สุด

**ผลกระทบปานกลาง:** ผลกระทบร้ายแรงที่อาจ: (i) ทำให้เกิดความเสื่อมโทรมอย่างมีนัยสำคัญในความสามารถภารกิจในขอบเขตและระยะเวลาที่เขตอำนาจสามารถปฏิบัติหน้าที่หลักได้ แต่ประสิทธิผลของหน้าที่จะลดลงอย่างมีนัยสำคัญ; (ii) ส่งผลให้เกิดความเสียหายอย่างมีนัยสำคัญต่อทรัพย์สินของเขตอำนาจ; (iii) ส่งผลให้เกิดการสูญเสียทางการเงินอย่างมีนัยสำคัญ; หรือ (iv) ส่งผลให้เกิดอันตรายร้ายแรงต่อบุคคลที่ไม่เกี่ยวข้องกับการสูญเสียชีวิตหรือการบาดเจ็บสาหัสถึงชีวิต

**ผลกระทบรุนแรง:** ผลกระทบเชิงลบที่เป็นหายนะที่อาจ: (i) ทำให้ความสามารถภารกิจเสื่อมโทรมลงอย่างรุนแรงในขอบเขตและระยะเวลาที่สามารถปฏิบัติหน้าที่หลักได้ แต่ประสิทธิผลของการปฏิบัติหน้าที่จะลดลงอย่างรุนแรง; (ii) ส่งผลให้เกิดความเสียหายอย่างใหญ่หลวงต่อทรัพย์สินของเขตอำนาจ; (iii) ส่งผลให้เกิดการสูญเสียทางการเงินครั้งใหญ่; หรือ (iv) ส่งผลให้เกิดอันตรายร้ายแรงหรือภัยพิบัติต่อบุคคลที่เกี่ยวข้องกับการสูญเสียชีวิตหรือการบาดเจ็บสาหัสถึงชีวิต

**การหยุดชะงักโดยสมบูรณ์:** ผลกระทบเชิงลบที่เป็นหายนะที่ทำให้เกิดการเสื่อมโทรมอย่างรุนแรงหรือสูญเสียขีดความสามารถของภารกิจในขอบเขตและระยะเวลาที่เขตอำนาจไม่สามารถปฏิบัติหน้าที่หลักได้อย่างน้อยหนึ่งอย่าง

|  |
| --- |
| **กลไกการให้คะแนนโครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญ** |
| **รายการตรวจสอบ** | **หมายเหตุ** |
| 1. ประมาณระดับของผลกระทบที่การสูญเสียหรือการด้อยค่าของโครงสร้างพื้นฐานนี้จะมีต่อความสามารถของเขตอำนาจในการควบคุมดูแล

[ ]  ไม่มีผลกระทบ (0)[ ]  เล็กน้อย (1)[ ]  ปานกลาง (2)[ ]  รุนแรง (3)[ ]  การหยุดชะงักโดยสิ้นเชิง (4) |  |
| 1. ประมาณระดับผลกระทบที่การสูญเสียหรือการด้อยค่าของโครงสร้างพื้นฐานนี้จะมีต่อความสามารถในการตอบสนองเหตุฉุกเฉินของเขตอำนาจ

[ ]  ไม่มีผลกระทบ (0)[ ]  เล็กน้อย (1)[ ]  ปานกลาง (2)[ ]  รุนแรง (3)[ ]  การหยุดชะงักโดยสิ้นเชิง (4) |  |
| 1. ประมาณระดับของผลกระทบที่การสูญเสียหรือการด้อยค่าของโครงสร้างพื้นฐานนี้จะมีต่อความสามารถของเขตอำนาจในการให้บริการทางการแพทย์และบริการสาธารณสุข

[ ]  ไม่มีผลกระทบ (0)[ ]  เล็กน้อย (1)[ ]  ปานกลาง (2)[ ]  รุนแรง (3)[ ]  การหยุดชะงักโดยสิ้นเชิง (4) |  |
| 1. ประมาณระดับของผลกระทบที่การสูญเสียหรือการด้อยค่าของโครงสร้างพื้นฐานนี้จะมีต่อความสามารถของเขตอำนาจในการจัดหาความปลอดภัยสาธารณะ

[ ]  ไม่มีผลกระทบ (0)[ ]  เล็กน้อย (1)[ ]  ปานกลาง (2)[ ]  รุนแรง (3)[ ]  การหยุดชะงักโดยสิ้นเชิง (4) |  |
| 1. ประมาณระดับของผลกระทบทางเศรษฐกิจต่อการสูญเสียหรือการด้อยค่าของโครงสร้างพื้นฐานนี้ที่จะมีต่อเขตอำนาจ

[ ]  ไม่มีผลกระทบ (0)[ ]  เล็กน้อย (1)[ ]  ปานกลาง (2)[ ]  รุนแรง (3)[ ]  การหยุดชะงักโดยสิ้นเชิง (4) |  |
| 1. ประมาณระดับของผลกระทบที่การสูญเสียหรือการด้อยค่าของโครงสร้างพื้นฐานนี้จะมีต่อความสามารถของเขตอำนาจในการให้บริการที่จำเป็นขั้นพื้นฐาน เช่น น้ำ ไฟฟ้า หรือก๊าซ

[ ]  ไม่มีผลกระทบ (0)[ ]  เล็กน้อย (1)[ ]  ปานกลาง (2)[ ]  รุนแรง (3)[ ]  การหยุดชะงักโดยสิ้นเชิง (4) |  |
| 1. การสูญเสียหรือการด้อยค่าของโครงสร้างพื้นฐานนี้จะส่งผลให้เกิดการหยุดชะงักต่อโครงสร้างพื้นฐานอื่น ๆ หรือทรัพยากรหลักหรือไม่?

[ ]  ไม่ (0)[ ]  ใช่ (1) |  |
| 1. ความรู้เกี่ยวกับการสูญเสียหรือการด้อยค่าของโครงสร้างพื้นฐานนี้จะบ่อนทำลายขวัญและกำลังใจของประชาชนหรือความเชื่อมั่นต่อสถาบันของรัฐและ/หรือเศรษฐกิจหรือไม่?

[ ]  ไม่ (0)[ ]  ใช่ (1) |  |
| 1. ประมาณระยะเวลาในการสูญเสียโครงสร้างพื้นฐานนี้ก่อนที่จะเกิดผลกระทบรุนแรง

[ ]  สามารถเลื่อนหรือดำเนินการในลักษณะอื่นได้ตั้งแต่ 7 วันขึ้นไป (1)[ ]  อาจหยุดชะงักหรือไม่พร้อมใช้งานเป็นเวลา 1-7 วันโดยไม่มีผลกระทบที่สำคัญ (2)[ ]  จะต้องได้รับการฟื้นฟูภายใน 24 ชั่วโมงเพื่อหลีกเลี่ยงผลกระทบร้ายแรง (3)[ ]  จะต้องได้รับการฟื้นฟูภายใน 12 ชั่วโมงเพื่อหลีกเลี่ยงผลกระทบร้ายแรง (4) |  |
| คะแนนรวม: กรอกคะแนนรวม |