



CYBERSECURITY AWARENESS

**การอบรมเชิงปฏิบัติการ
แผนการตอบสนองต่อภัยคุกคาม
(Incident Response Plan: IRP)**



อบรมรุ่นที่ 1: Cybersecurity Awareness_ การอบรมเชิงปฏิบัติการแผนการตอบสนองต่อภัยคุกคาม (Incident Response Plan: IRP)

ระยะเวลาการอบรม: 1 วัน วันที่ 24 มิถุนายน 2568 เวลา 09:00 – 16:00 น.

ผู้เข้าอบรม: ผู้บริหารและเจ้าหน้าที่สารสนเทศ (IT)

กำหนดการอบรม:

ช่วงเวลา	หัวข้อการอบรม (Agenda)
09:00 - 10:30	ความรู้พื้นฐานเกี่ยวกับภัยคุกคามและแนวทางการตอบสนอง - ประเภทของภัยคุกคามที่พบบ่อย - ผลกระทบต่อองค์กร: ความเสียหาย การหยุดชะงักของบริการ อันตรายต่อชีวิต - ความแตกต่างระหว่าง Emergency Response, Incident Response และ Business Continuity
10:30 - 10:45	พักเบรกช่วงเช้า
10:45 - 12:00	บทบาทหน้าที่ของทีมตอบสนองเหตุการณ์ (IRT) - โครงสร้างทีมตอบสนองเหตุการณ์ (IRT) - บทบาทหน้าที่ของทีมย่อย - การบริหารสถานการณ์: การตัดสินใจ การสื่อสารภายใน การประสานงานภายนอก
12:00 - 13:15	พักกลางวัน
13:15 - 14:30	การจัดทำแผนตอบสนองเหตุการณ์และการทดสอบ - การจัดทำแผนตอบสนองเหตุการณ์ (IRT) - รูปแบบการทดสอบ
14:30 - 14:45	พักเบรกช่วงบ่าย
14:45 - 16:00	Workshop: การทดสอบแผนตอบสนองต่อเหตุการณ์ภัยคุกคาม (IRP Testing) และสรุปประเด็นจากการซักซ้อม และแนวทางปรับปรุงในอนาคต
	จบการอบรม

ประวัติวิทยากร

ประวัติวิทยากร

หลักสูตรเชิงปฏิบัติการ แผนปฏิบัติการตอบสนองต่อเหตุการณ์ (Incident Response Plan) และ
หลักสูตรเชิงปฏิบัติการ การบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (BCP)

นายบรรณกิจ ศรีสว

ตำแหน่ง: Senior Consultant

สังกัด: บริษัท เอซีอินโฟเทค จำกัด

อีเมล: bannakit@acinfotec.com

โทรศัพท์: +66(0)2-670-8980 ต่อ 308



คุณวุฒิการศึกษา

- วิศวกรรมศาสตรบัณฑิต (วิศวกรรมคอมพิวเตอร์) มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
- วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยเกษตรศาสตร์

Professional Certifications / ใบรับรองวิชาชีพ

IRCA Certified ISO/IEC 27001:2022 – Principal Auditor

ผู้ตรวจประเมินระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูลระดับหัวหน้าผู้ตรวจประเมิน (ตามมาตรฐาน ISO/IEC 27001:2022) ที่ได้รับการรับรองจากสถาบัน IRCA – International Register of Certificated Auditors

PECB Certified ISO/IEC 22301 – Lead Implementer and Lead Auditor

ผู้วางระบบและผู้ตรวจประเมินระบบบริหารความต่อเนื่องทางธุรกิจระดับหัวหน้า (ตามมาตรฐาน ISO/IEC 22301) ที่ได้รับการรับรองจากสถาบัน PECB – Professional Evaluation and Certification Board

PECB Certified ISO/IEC 27701 – Lead Implementer

ผู้วางระบบการจัดการข้อมูลส่วนบุคคลระดับหัวหน้า (ตามมาตรฐาน ISO/IEC 27701) ที่ได้รับการรับรองจากสถาบัน PECB

ISACA Certified Information Security Manager (CISM)

ผู้จัดการด้านความมั่นคงปลอดภัยสารสนเทศที่ได้รับการรับรองจาก ISACA – Information Systems Audit and Control Association

ISACA Certified Data Privacy Solutions Engineer (CDPSE)

วิศวกรด้านโซลูชันการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจาก ISACA

ISC² Certified in Cybersecurity (CC)

ผู้ผ่านการรับรองความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์จาก ISC² – International Information System Security Certification Consortium

PECB Certified Trainer

วิทยากรผู้ได้รับการรับรองจาก PECB ให้สามารถฝึกอบรมหลักสูตรมาตรฐานสากลต่าง ๆ อย่างเป็นทางการ

ประสบการณ์ในสายงาน

นายบรรณกิจ มีประสบการณ์มากกว่า 17 ปีในด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการบริการ (ITSM) การวางแผนความต่อเนื่องทางธุรกิจ (BCM) และการจัดการข้อมูลส่วนบุคคล โดยมีความเชี่ยวชาญด้านมาตรฐานสากล เช่น ISO/IEC 27001, ISO/IEC 22301, ISO/IEC 27701, ISO/IEC 20000 และกฎหมาย PDPA

ประสบการณ์ฝึกอบรมและให้คำปรึกษาที่เกี่ยวข้องกับหลักสูตร

1. Incident Response Plan Training and Workshop

- ดำเนินการจัดอบรมเชิงปฏิบัติการด้านแผนตอบสนองเหตุการณ์ด้านไซเบอร์ (Cyber Incident Response) ให้แก่หน่วยงานรัฐและเอกชน
- เชี่ยวชาญในกระบวนการวางแผน เตรียมความพร้อม การจำลองสถานการณ์ (Cyber Drill) การสรุปผลและข้อเสนอแนะภายหลังการฝึกซ้อม
- มีบทบาทเป็นผู้นำในการจัดทำคู่มือ Incident Response Plan, playbook, และแผนฟื้นฟูระบบงานจากภัยคุกคาม

2. Business Continuity Plan Training and Workshop

- ให้คำปรึกษาและจัดฝึกอบรมในหลักสูตร BCP อย่างครบวงจร ตั้งแต่การประเมินความเสี่ยงและผลกระทบเชิงธุรกิจ (BIA), การวางแผนและทดสอบแผน BCP ไปจนถึงการปรับปรุงอย่างต่อเนื่อง
- เชี่ยวชาญการออกแบบและพัฒนาแผนความต่อเนื่องทางธุรกิจที่สอดคล้องกับมาตรฐาน ISO/IEC 22301
- มีประสบการณ์จริงในการจัดทำและฝึกอบรมให้กับหน่วยงานภาครัฐและรัฐวิสาหกิจจำนวนมาก

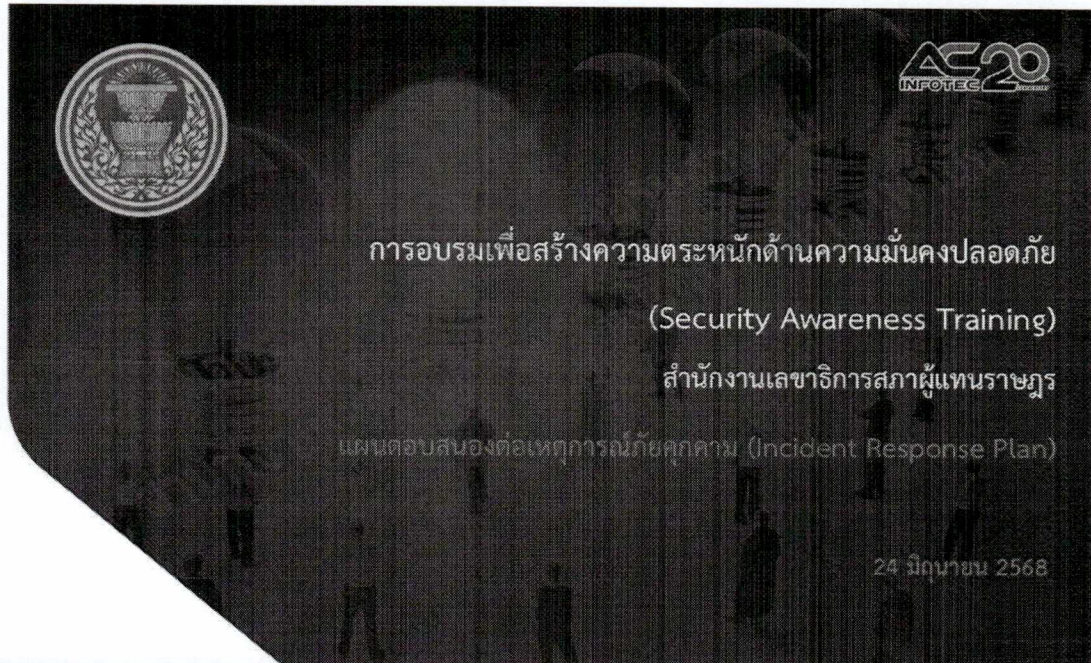
ประสบการณ์ในโครงการที่แสดงถึงศักยภาพความรู้ความสามารถที่เกี่ยวข้องกับการอบรม

- เป็นที่ปรึกษาและผู้จัดอบรมหลักสูตร Incident Response Plan Training and Workshop และ Business Continuity Plan Training and Workshop ให้แก่หน่วยงานภาครัฐและเอกชนหลายแห่ง อาทิ บริษัท เอ็มซีโอที จำกัด (มหาชน), บริษัท เบทาโกร จำกัด (มหาชน), บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน), บริษัท เมืองไทยประกันชีวิต จำกัด (มหาชน) และบริษัท อีซี บาย จำกัด (มหาชน) โดยครอบคลุมตั้งแต่การประเมินช่องว่าง (Gap Assessment) การจัดทำแผนรับมือเหตุการณ์และแผนความต่อเนื่องทางธุรกิจ การฝึกอบรมเชิงปฏิบัติการ (Workshop) และการทดสอบแผน (Plan Testing)
- ดำรงตำแหน่ง ผู้จัดการโครงการ (Project Manager) ในการให้คำปรึกษาด้านมาตรฐาน ISO/IEC 27001:2022 แก่หน่วยงานสำคัญ ได้แก่ ธนาคารกรุงไทย จำกัด (มหาชน), สำนักงานสลากกินแบ่งรัฐบาล, บริษัท ท่าอากาศยานไทย จำกัด (มหาชน) และ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) เพื่อยกระดับระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับมาตรฐานสากล ครอบคลุมการวิเคราะห์ช่องว่าง (Gap Analysis), การวางระบบควบคุม (Control Implementation), การประเมินความเสี่ยง (Risk Assessment) และการเตรียมความพร้อมสำหรับการตรวจประเมินภายนอก

ผลงานและความเชี่ยวชาญอื่นที่เกี่ยวข้อง

- เคยให้คำปรึกษาแก่หน่วยงานขนาดใหญ่ เช่น ธนาคารแห่งประเทศไทย, กรมสรรพากร, ตลาดหลักทรัพย์แห่งประเทศไทย, บริษัท ไทยประกันชีวิต จำกัด (มหาชน), ธนาคารออมสิน และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)
- มีประสบการณ์ในการฝึกอบรมและประเมินผลกระบวนการด้าน Incident Response, Business Continuity และ Cybersecurity Framework ให้หน่วยงานระดับชาติ

เอกสารประกอบการอบรม Cybersecurity Awareness รุ่นที่ 1

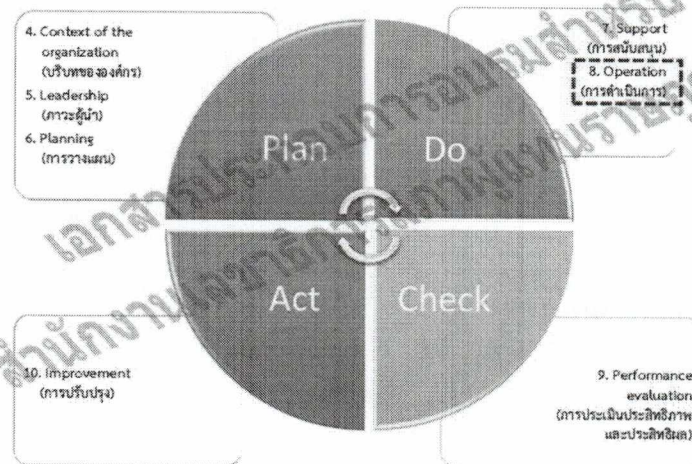


Purpose

- เพื่อเสริมสร้างความรู้ความเข้าใจสำหรับขั้นตอนในการตอบสนองต่อเหตุการณ์ภัยคุกคาม
- เพื่อพัฒนาทักษะในการรับมือและจัดการเหตุการณ์ ให้สามารถรับมือเหตุการณ์ได้อย่างมีประสิทธิภาพและทันเวลา
- เพื่อให้เกิดความเข้าใจร่วมกันในการประสานงานระหว่างตอบสนองเหตุการณ์ ทั้งในด้านการสื่อสารและการดำเนินการ



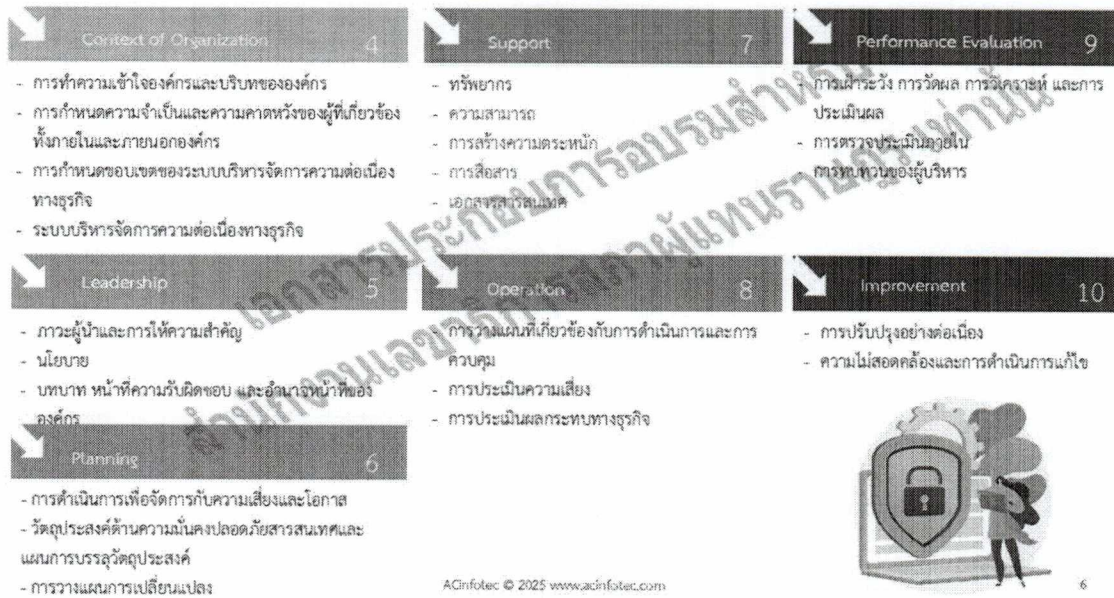
ISO 22301 PDCA Model



ACInfotec © 2025 www.acinfotec.com

5

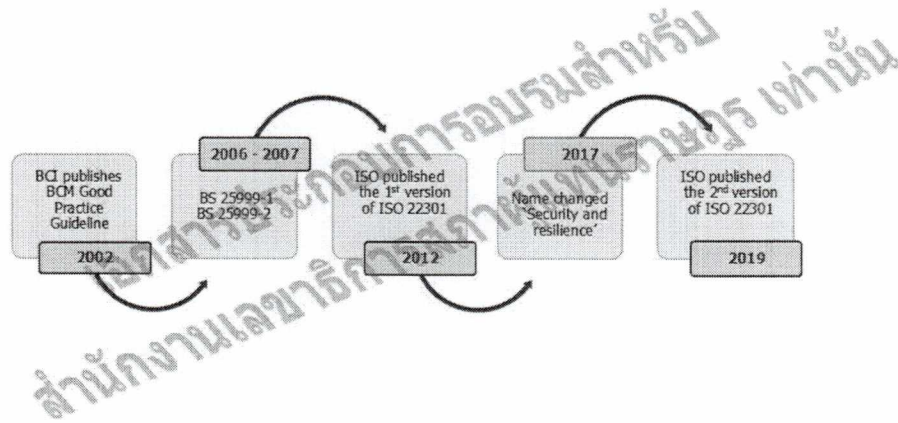
ISO 22301 Clause 4-10



ACInfotec © 2025 www.acinfotec.com

6

BCMS ISO 22301



ACinfotec © 2025 www.acinfotec.com

7



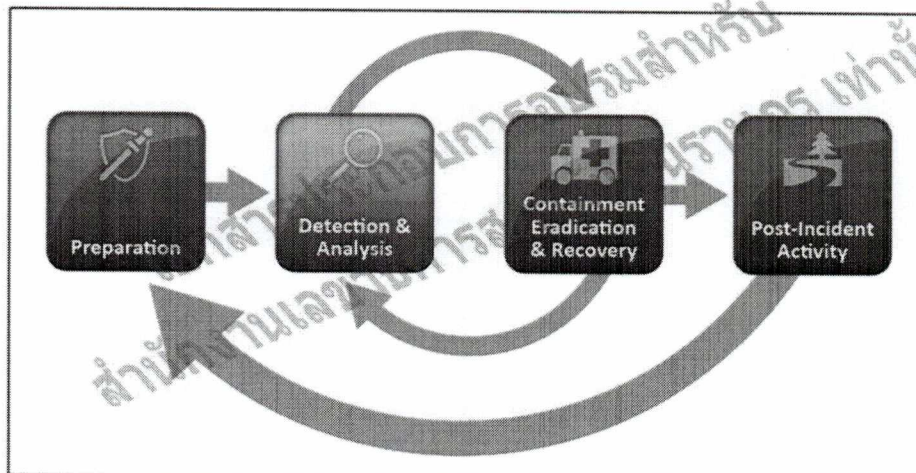
NIST
National Institute of
Standards and Technology

มาตรฐาน NIST

ACinfotec © 2025 www.acinfotec.com

8

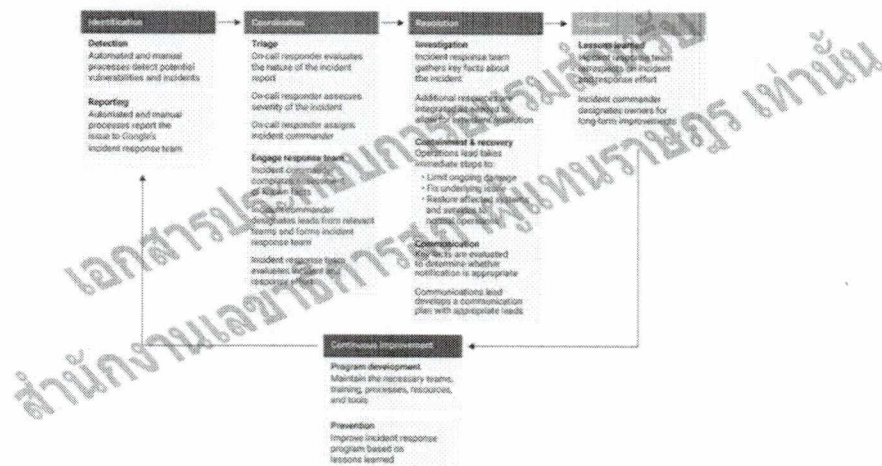
NIST SP 800-61



ACinfotec © 2025 www.acinfotec.com

9

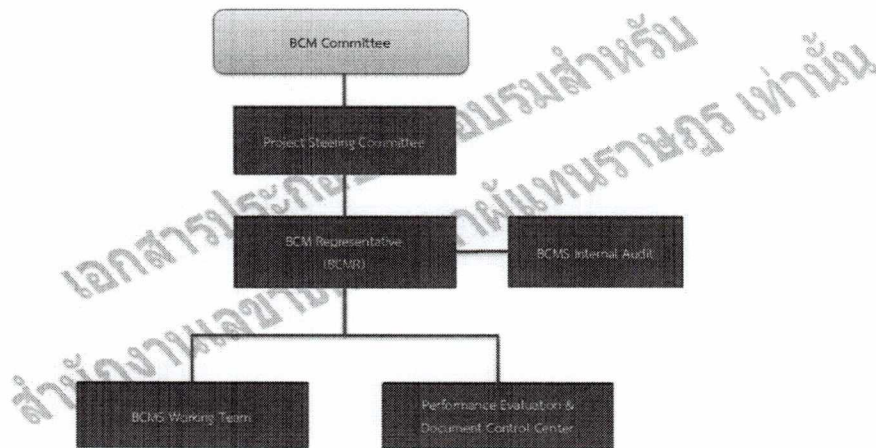
NIST SP 800-61



ACinfotec © 2025 www.acinfotec.com

10

BCM Organization



ACinfotec © 2025 www.acinfotec.com

11

BCM Organization

Working groups	Activities
Project Steering Committee คณะผู้บริหารการดำเนินงานระบบบริหารความเสี่ยงทางธุรกิจ	เข้าร่วม Kick-off Meeting ของโครงการ และการฝึกอบรม BCM Executive Awareness สำหรับผู้บริหาร, เข้าร่วมการประชุมทบทวนการดำเนินงานของระบบ BCMS, ตรวจสอบความคืบหน้าของโครงการ ให้อยู่ในแผนที่ และการสนับสนุนเพื่อแก้ไขปัญหาดังกล่าว (ถ้ามี)
BCM Representative (BCMR) ผู้แทนคณะผู้บริหารในการจัดการดูแลระบบบริหารความเสี่ยงทางธุรกิจ	กำกับดูแลกิจกรรมการดำเนินงานของระบบ BCMS ทั้งหมด และรายงานผลการดำเนินงานของระบบ BCMS ต่อ Project Steering Committee
BCMS Internal Auditor คณะผู้ตรวจสอบประเมินภายในระบบบริหารความเสี่ยงทางธุรกิจ	วางแผนและดำเนินการตรวจสอบตามข้อกำหนด ISO 22301 รวมถึงรายงานผลการตรวจสอบประเมินภายในและการปรับปรุงแก้ไขข้อบกพร่องที่เกี่ยวข้อง และผู้บริหาร
BCMS Working Team คณะทำงานระบบบริหารความเสี่ยงทางธุรกิจ	Core Team : เข้าร่วมการฝึกอบรมและดำเนินงานของระบบ BCMS อย่างต่อเนื่อง Support Team : ทีมอื่น ๆ ที่ให้การสนับสนุนการดำเนินงานของระบบ BCMS เช่น ฝ่ายบุคคล, ฝ่ายอาคารสถานที่
Performance Evaluation & Document Control Center ผู้ติดตามการประเมินผลการปฏิบัติงานและควบคุมเอกสาร	Performance Evaluation : ประเมินผลการดำเนินงานของระบบ BCMS Document Control Center : ควบคุมดูแลเอกสารของระบบ BCMS

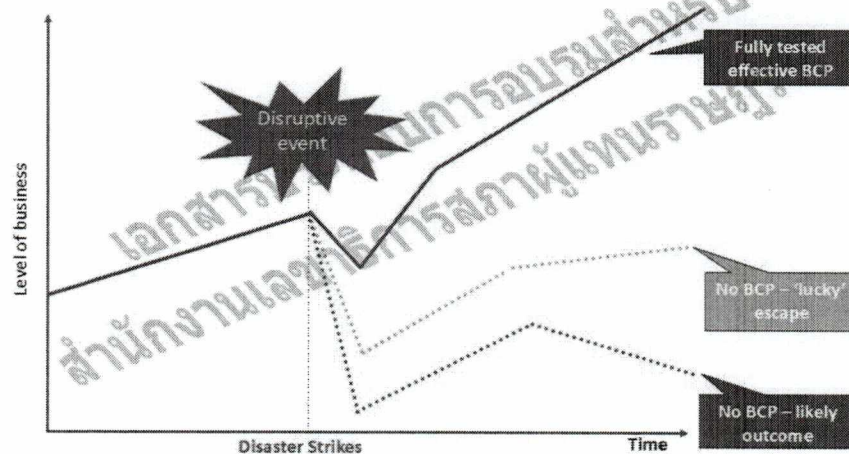
ACinfotec © 2025 www.acinfotec.com

12

From Incident to Emergency

คำศัพท์	ความหมาย
Event	เหตุการณ์ต่างๆ ที่เกิดขึ้นในแต่ละช่วงเวลา
Incident	เหตุการณ์ที่อาจจะส่งผลให้การดำเนินงานขององค์กรหยุดชะงัก ไม่สามารถดำเนินงานต่อไปได้ มีการสูญเสีย มีเหตุฉุกเฉิน หรือภาวะวิกฤติ
Disruption	เหตุการณ์ที่กระทบความตั้งใจที่คาดหมายได้ เช่น แอพลิเคชัน และไม่สามารถคาดหมายได้ อาทิเช่น แผ่นดินไหว ไฟฟ้าดับ ซึ่งส่งผลให้การดำเนินงานขององค์กรหยุดชะงัก
Crisis	เหตุการณ์ที่คุกคามต่างๆ ที่มีสาเหตุจากคนหรือธรรมชาติ ซึ่งมีความจำเป็นเร่งด่วนที่ต้องทำการปกป้องชีวิตมนุษย์ ทรัพย์สิน หรือสภาพแวดล้อม
Disaster	สถานการณ์ที่ส่งผลกระทบในวงกว้าง ทำให้เกิดความสูญเสียต่อทรัพย์สิน สภาพเศรษฐกิจ หรือสิ่งแวดล้อมอย่างมาก ซึ่งเกินกว่าความสามารถขององค์กร ชุมชน หรือสังคม ที่จะตอบสนองและกู้คืนด้วยทรัพยากรที่ตนมีกับเหตุการณ์นั้นได้
Emergency	ภาวะเร่งด่วน โดยทั่วไปจะเป็นเหตุการณ์ที่เกิดขึ้นโดยไม่คาดคิด หรือเหตุการณ์ที่มีความจำเป็นเร่งด่วนในการแก้ไข

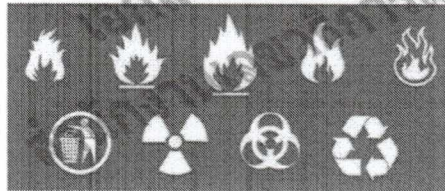
Objective of Business Continuity Plan (BCP)



Type of Disaster

ภัยพิบัติหรือวิกฤตการณ์อาจเกิดขึ้นจาก

1. ภัยธรรมชาติ
2. ภัยจากมนุษย์
3. ภัยทางเทคนิค



ให้โดยองค์กรผู้ทำงาน ซึ่งผลให้ทรัพย์สินเสียหาย

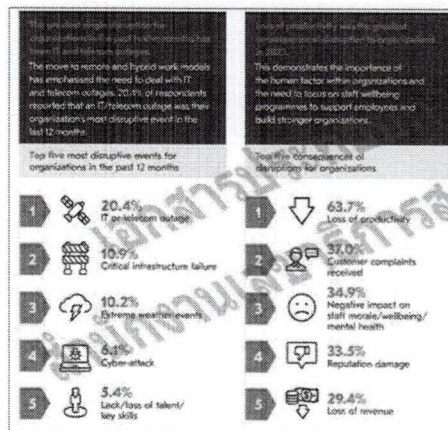
ระบบทั้งเชิงระบบหรือตัวทำงานเสียไป สิ้นเปลือง
คอมพิวเตอร์ภายในองค์กรเสียหาย

การขาดการดูแลและส่งผลให้ต้องทำการอพยพออก
จากอาคาร

ผู้บริหารและพนักงานจำนวนมากต้องเข้าโรงพยาบาล
เนื่องจากอาหารเป็นพิษ ส่งผลให้ไม่สามารถปฏิบัติงานได้

- Hacker ลักลอบเข้าระบบงานขององค์กร และปิดกั้นการ
ทำงานของพนักงานในองค์กร

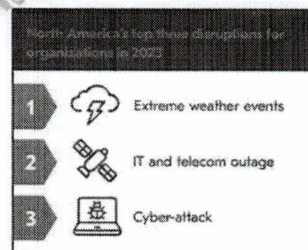
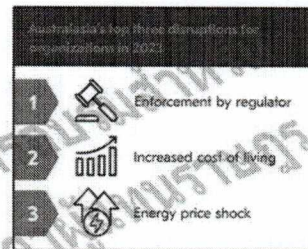
Business Disruption Landscape



Incident assessment past 12 Months

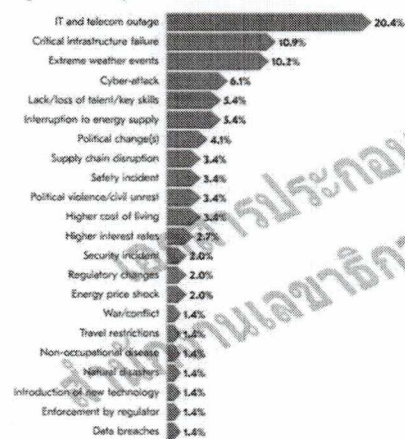
Rank	Event	Frequency	Impact	Total Index
1	Health incidents (unemployment, disease, chronic health conditions, etc.)	8.43	1.91	16.34
2	Safety incidents (unemployment, safety, reportable incident)	7.25	1.85	14.22
3	Financial cost of living	6.12	2.22	13.36
4	Supply chain disruption	6.00	2.22	13.34
5	Non-communicable diseases (e.g. pandemic)	5.95	1.92	13.29
6	Interruption to energy supply	6.26	2.09	13.16
7	Security incidents	6.88	1.83	12.47
8	Exposure to other risks (e.g. climate change, fires, etc.)	5.90	2.00	12.09
9	Financial impact (e.g. unemployment, etc.)	6.80	1.84	12.08
10	Cyber-attacks	6.14	1.96	12.06
11	IT and telecom outages	5.92	2.04	12.05
12	Political violence/instability	5.51	2.16	11.96
13	Natural disasters (e.g. hurricanes, tsunamis, etc.)	5.89	2.08	11.60
14	Environmental impact (e.g. climate change)	4.72	2.27	10.69
15	Exchange rate volatility	4.71	2.39	10.69
16	Higher interest rates	4.52	2.25	10.28
17	Energy price shock	4.44	2.25	10.09
18	Product safety recall	4.08	1.64	9.91
19	Critical infrastructure failure	4.10	2.25	9.99
20	Introduction of new technology (e.g. AI, Big Data)	4.41	1.96	9.03
21	Issues arising from remote/hybrid working	3.42	1.64	8.88
22	Financial institutions (e.g. banks)	3.81	2.14	8.37
23	Political change(s)	3.95	2.14	8.34
24	Workforce	3.41	2.20	7.93
25	Regulatory changes	3.90	2.09	7.63
26	Data breaches	3.27	1.87	7.03
27	Taxation restrictions	4.04	1.34	7.03
28	Loss of effective disaster incident	3.00	1.78	5.34

** bci-horizon-scan-report-2023

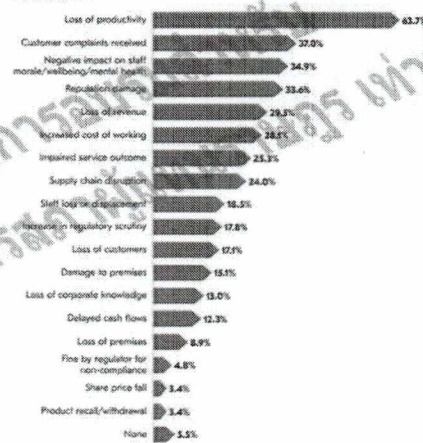


** bci-horizon-scan-report-2023

Which of the following events produced the biggest disruption to your organization in the past 12 months?



What impacts or consequences arose from the disruptions experienced in the last 12 months?



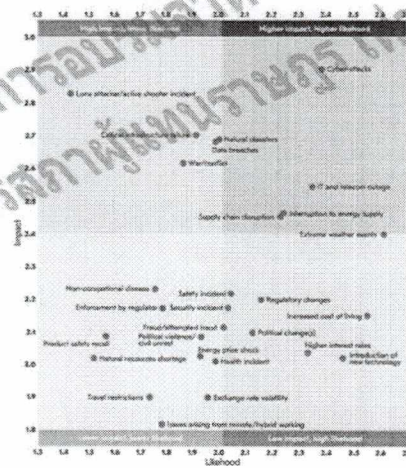
** bci-horizon-scan-report-2023

Risk and Threat Assessment

Rank	Event	Unlikely	Impact	Risk Index
1	Cyberattacks	2.38	2.90	6.92
2	Extreme weather events (e.g. floods, storms, fires, etc.)	2.44	2.60	6.36
3	IT and telecom outage	2.34	2.54	5.95
4	Increased cost of living	2.57	2.18	5.50
5	Interruption to energy supply	2.23	2.44	5.46
6	Supply chain disruption	2.21	2.43	5.42
7	Natural disasters (earthquakes, tsunamis, etc.)	1.99	2.46	4.94
8	Data breaches	1.98	2.48	4.91
9	Critical infrastructure failure	1.90	2.70	5.14
10	Introduction of new technology (IoT, AI, Big data)	2.43	2.02	4.93
11	Higher interest rates	2.35	2.04	4.74
12	Regulatory changes	2.14	2.20	4.72
13	War/conflict	1.75	2.61	4.57
14	Safety incidents (personnel injury, safety asset damage, dangerous occurrences, etc.)	2.03	2.32	4.52
15	Political changes	2.11	2.10	4.43
16	Security incidents	2.02	2.18	4.40
17	Fraud/unintended fraud	2.03	2.11	4.32
18	Political violence/turbulence	1.93	2.09	4.04
19	Lone attacker/active shooter incidents	1.62	2.82	4.00
20	Health incidents (COVID-19, influenza, measles, etc.)	2.01	1.97	3.97
21	Health incidents (COVID-19, influenza, measles, etc.)	1.74	2.23	3.87
22	Supply chain disruption	1.91	2.02	3.86
23	Enforcement by regulator	1.77	2.17	3.85
24	Exchange rate volatility	1.94	1.90	3.68
25	Travel restrictions	1.72	1.90	3.28
26	Product safety recall	1.83	2.09	3.23
27	Issues arising from remote/hybrid working (the new working environment)	1.78	1.81	3.22
28	Natural resources shortage	1.81	2.02	3.04

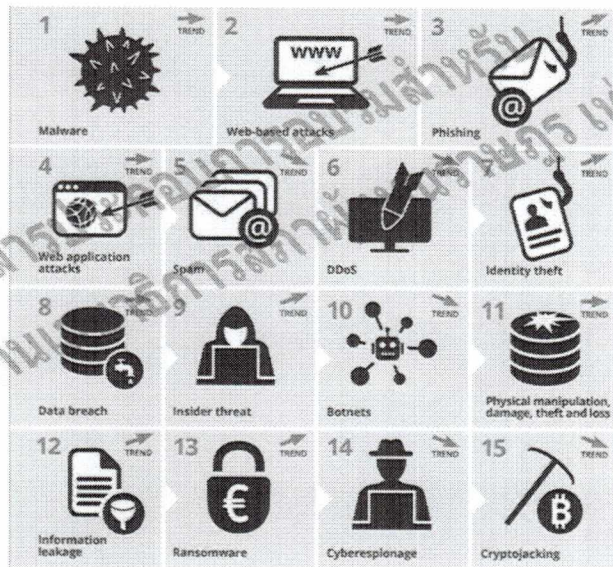
** bci-horizon-scan-report-2023

The likelihood and impact levels for incidents occurring in respondent organizations in the next twelve months



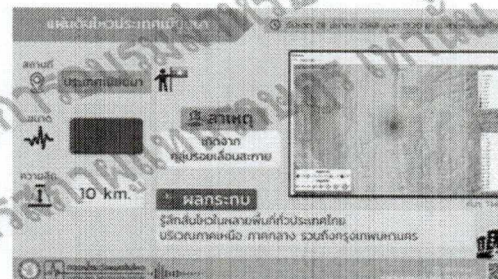
ENISA Threat Landscape

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

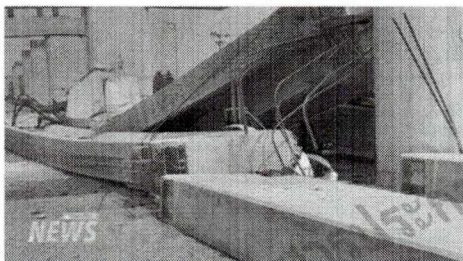


20

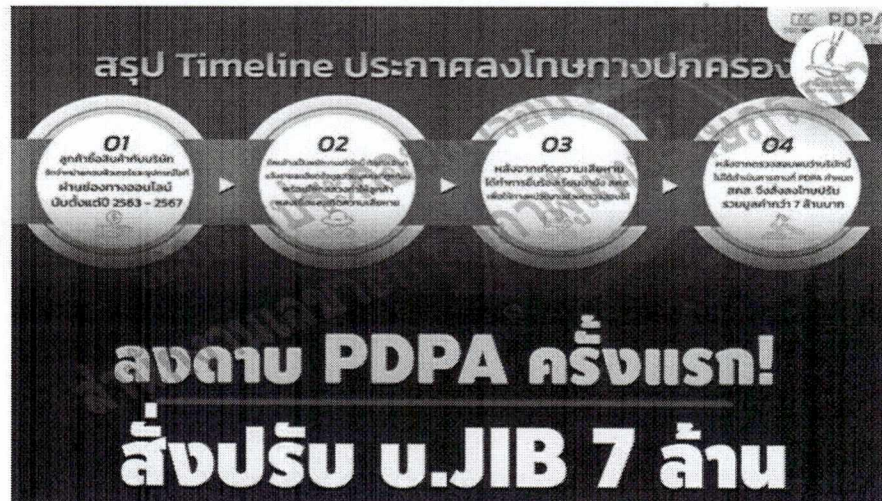
ตัวอย่างภัยคุกคาม (Threat)



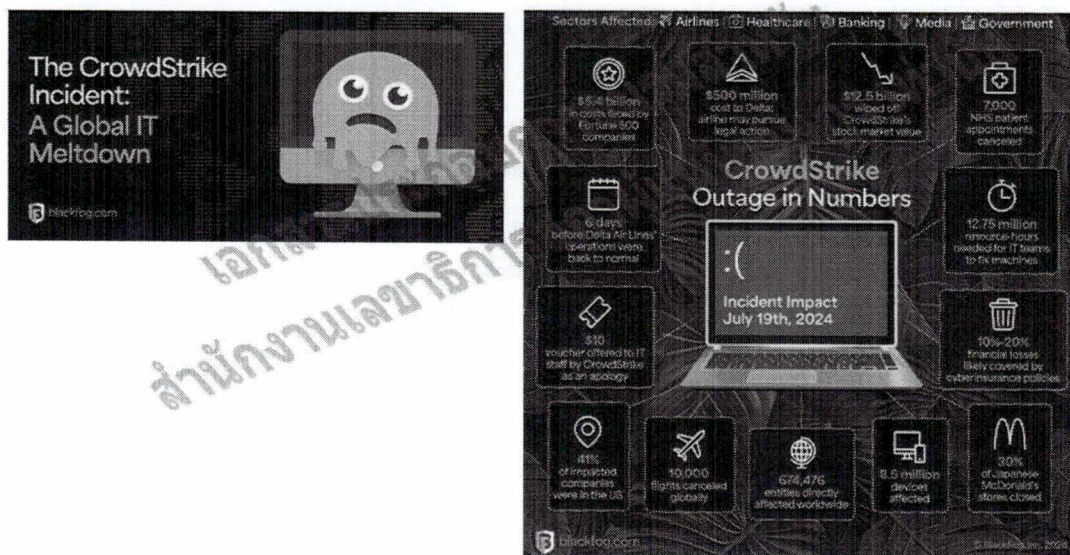
ตัวอย่างผลที่ตามมา (Consequence)



ตัวอย่างภัยคุกคาม (Threat) และผลกระทบที่ตามมา (Consequence)



ตัวอย่างภัยคุกคาม (Threat) และผลกระทบที่ตามมา (Consequence)





2. ภาพรวมและคำนิยามเกี่ยวกับเหตุการณ์

R I S K

Concept of Business Continuity

Business continuity

- ความสามารถขององค์กรในการที่จะรับมือผลิตภัณฑ์หรือบริการให้อยู่ในระดับที่ลูกค้ายอมรับได้เมื่อองค์กรต้องเผชิญกับภาวะวิกฤติ หรือภัยพิบัติ

Business continuity management

- กระบวนการจัดการแบบองค์รวม โดยกำหนดจุดความที่อาจก่อให้เกิดภัยพิบัติและผลกระทบจากภัยคุกคามเหล่านั้น หากเกิดขึ้นจริง โดยกำหนดกรอบสำหรับการสร้างความยืดหยุ่นขององค์กรในแง่ของตอบสนองต่อภัยคุกคามต่างๆ อย่างมีประสิทธิภาพ เพื่อปกป้องผลประโยชน์ขององค์กรส่วนได้ส่วนเสีย (Stakeholder) อาทิเช่น ชื่อเสียง แบรนด์ และกิจกรรมที่สร้างมูลค่าขององค์กร

Business continuity plan

- แผนหรือกระบวนการเชิงขั้นตอนทางขององค์กรสำหรับ การตอบสนอง (Response) ฟื้นฟู (Recover) ปักปันมา (Resume) และฟื้นฟู (Restore) การดำเนินงานขององค์กรในขณะที่ยังคงเผชิญกับภาวะวิกฤติให้อยู่ในระดับที่องค์กรทนได้

Business continuity management system

- ระบบบริหารจัดการที่จัดทำโดยองค์กรซึ่งดำเนินการ ตรวจสอบ ติดตาม บำรุงรักษา และปรับปรุงกระบวนการด้านความต่อเนื่องทางธุรกิจ

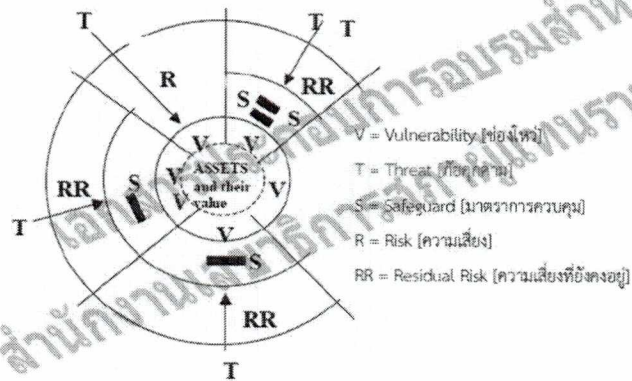
From Incident to Emergency

คำศัพท์	ความหมาย
Event	เหตุการณ์ต่างๆ ที่เกิดขึ้นในแต่ละช่วงเวลา
Incident	เหตุการณ์ที่อาจจะส่งผลให้การดำเนินงานขององค์กรหยุดชะงัก ไม่สามารถดำเนินงานต่อไปได้ มีการสูญเสียเงิน เหตุฉุกเฉิน หรือภาวะวิกฤติ
Disruption	เหตุการณ์เกี่ยวกับความถี่ที่คาดหมายได้ เช่น แอฉิน และไม่สามารถคาดหมายได้ อาทิเช่น แผ่นดินไหว ไฟฟ้าดับ จึงส่งผลทำให้การดำเนินงานขององค์กรหยุดชะงัก
Crisis	เหตุการณ์เกี่ยวกับความถี่ต่างๆ ที่มีสาเหตุจากคนหรือธรรมชาติ ซึ่งมีความจำเป็นเร่งด่วนที่ต้องหาวิธีการป้องกันชีวิตมนุษย์ ทรัพย์สิน หรือสภาพแวดล้อม
Disaster	สถานการณ์ที่ส่งผลกระทบต่อในวงกว้าง ทำให้เกิดความสูญเสียต่อทรัพย์สิน สภาพเศรษฐกิจ หรือสิ่งแวดล้อมอย่างมาก ซึ่งเกินกว่าความสามารถขององค์กร ชุมชน หรือสังคม ที่จะตอบสนองและกู้คืนด้วยทรัพยากรที่มีกับเหตุการณ์นั้นได้
Emergency	ภาวะเร่งด่วน โดยทั่วไปจะเป็นเหตุการณ์ที่เกิดขึ้นโดยไม่คาดคิด หรือเหตุการณ์ที่มีความจำเป็นเร่งด่วนในการแก้ไข

Business Impact Analysis and Business Continuity Risk Management



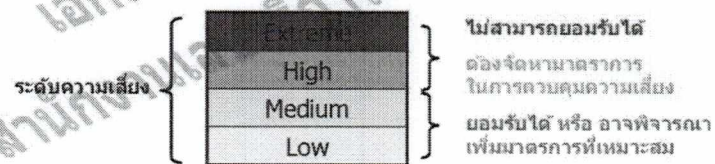
Business Continuity Risk Management



Risk Management Process

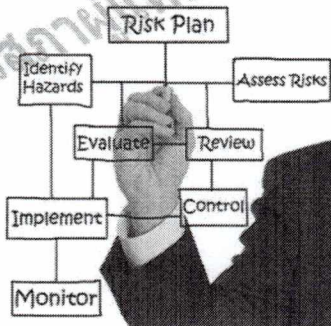
ระดับของความเสียหาย (Risk Level)

- เป็นไปไม่ได้ที่ทุกความเสี่ยงจะถูกยอมรับ
- ทุกความเสี่ยงจะยังมีความเสี่ยงคงเหลืออยู่ (Residual risk)
- ระดับความเสี่ยงที่องค์กรยอมรับได้อยู่ที่ระดับอะไร



Risk Management aspect of BCP

- ผลลัพธ์ของการประเมินความเสี่ยงซึ่งเป็นส่วนประกอบในการจัดทำแผน BCP ขององค์กร
 - ผลลัพธ์ที่ตามมา (Consequence) ของความเสี่ยงที่องค์กรให้ความสำคัญ
 - กลยุทธ์ในการกู้คืนธุรกิจ

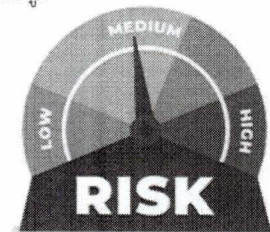


Risk

Risk (ความเสี่ยง) คืออะไร

- ผลของความไม่สอดคล้องกับวัตถุประสงค์
- ผลที่ตามมาของความไม่แน่นอนอาจเป็นบวกหรือลบก็ได้
- แต่ผลเชิงลบเท่านั้นที่เกี่ยวข้อง ที่ต้องหามาจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล

เหตุการณ์ที่ไม่แน่นอนต่างๆ ซึ่งหากเกิดขึ้นแล้วส่งผลกระทบเชิงลบต่อการดำเนินงาน ทั่วไองค์กร ไม่สามารถบรรลุวัตถุประสงค์ที่กำหนด



Risk Management Criteria

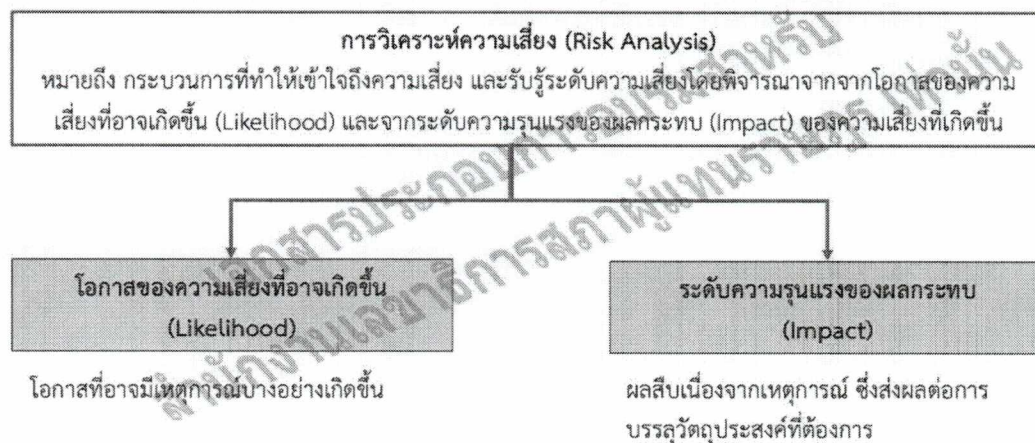
หลักเกณฑ์ประเมินความเสี่ยง คือ การประเมินความเสี่ยงด้านต่างๆ พิจารณาจากโอกาสของความเสี่ยงที่อาจเกิดขึ้น (Likelihood) และจากระดับความรุนแรงของผลกระทบ (Impact) ของความเสี่ยงที่เกิดขึ้น จะทำให้ทราบความเสี่ยงดังกล่าวตกอยู่ในตารางประเมินความเสี่ยง (Risk Matrix) ที่มีความเสี่ยงอยู่ในระดับใด ซึ่งหน่วยงานจะต้องหามาตรการในการบริหารความเสี่ยง เพื่อจัดการ ควบคุม และลดความเสี่ยงดังกล่าว เพื่อให้โอกาสที่จะเกิดความเสี่ยงนั้นๆ น้อยลงหรือระดับความรุนแรงของผลกระทบบรรเทาลง โดยความเสี่ยงที่ยังคงเหลืออยู่ (Residual Risk) จะต้องอยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite/Risk Acceptable level)



ACinfotec © 2025 www.acinfotec.com

33

Risk Analysis



ACinfotec © 2025 www.acinfotec.com

34

Risk Analysis

โอกาสของความเสี่ยงที่อาจเกิดขึ้น (Likelihood)

โอกาสที่อาจมีเหตุการณ์บางอย่างเกิดขึ้น เช่น

- ภัยทางธรรมชาติ
- ภัยจากการกระทำของมนุษย์ทั้งตั้งใจและไม่ตั้งใจ



ACinfotec © 2025 www.acinfotec.com

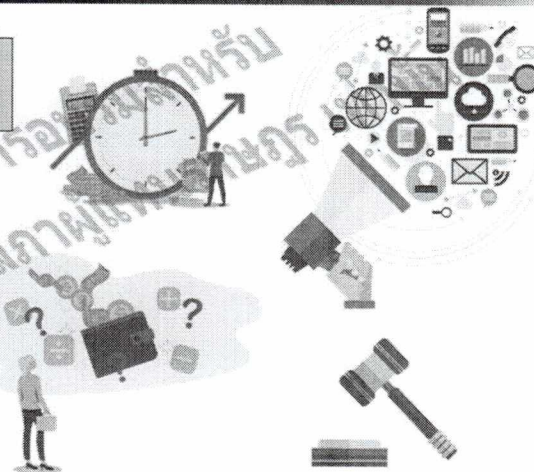
35

Risk Analysis

ระดับความรุนแรงของผลกระทบ (Impact) ทั้ง 3 ด้าน

การวิเคราะห์และระบุเหตุการณ์เสี่ยง สามารถพิจารณาจากประเด็นในแต่ละประเภทความเสี่ยง ดังนี้

- ความเสี่ยงด้านปฏิบัติการ (Operation Risk)
- ความเสี่ยงด้านการเงิน (Financial Risk)
- ความเสี่ยงด้านกฎระเบียบ (Regulatory Risk)



ACinfotec © 2025 www.acinfotec.com

36

Business Impact Analysis and Business Continuity Risk Management

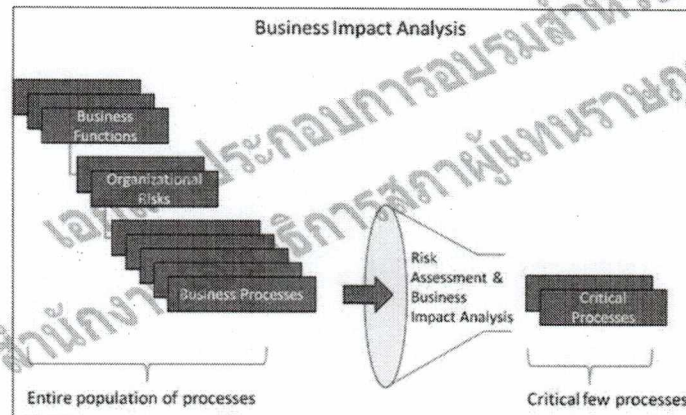


Image source: enaxisconsulting.com

Business Impact Analysis (BIA)

วัตถุประสงค์ของการจัดทำ Business Impact

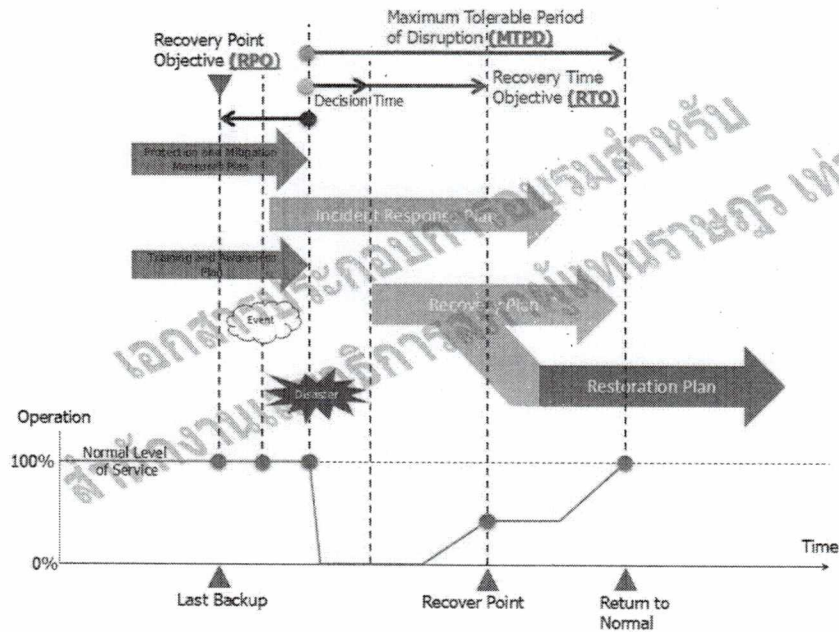
Analysis (BIA) เพื่อระบุ:

- กระบวนการที่สำคัญในการดำเนินธุรกิจ
- ผลกระทบที่อาจเกิดขึ้น หรือความเสี่ยงขององค์กรจากเหตุการณ์ร้ายแรงต่างๆ

BIA ช่วยกำหนดข้อมูลที่สำคัญดังต่อไปนี้:

- กรอบระยะเวลาในการนำกระบวนการทางธุรกิจกลับขึ้นมาในระดับต่ำสุดที่องค์กรกำหนดไว้
- กรอบระยะเวลาที่ต้องมีการกำหนดจนถึงการกลับมาดำเนินงานธุรกิจเพื่อชดเชยการดำเนินงานปกติ
- จุดของข้อมูลที่สามารถนำกลับมาได้เมื่อองค์กรประสบกับภาวะวิกฤติ





Business Impact Analysis

- Recovery Time Objective (RTO)

- ระยะเวลาที่การดำเนินงานของธุรกิจหยุดชะงัก ก่อนที่จะกลับมาดำเนินการอีกครั้ง

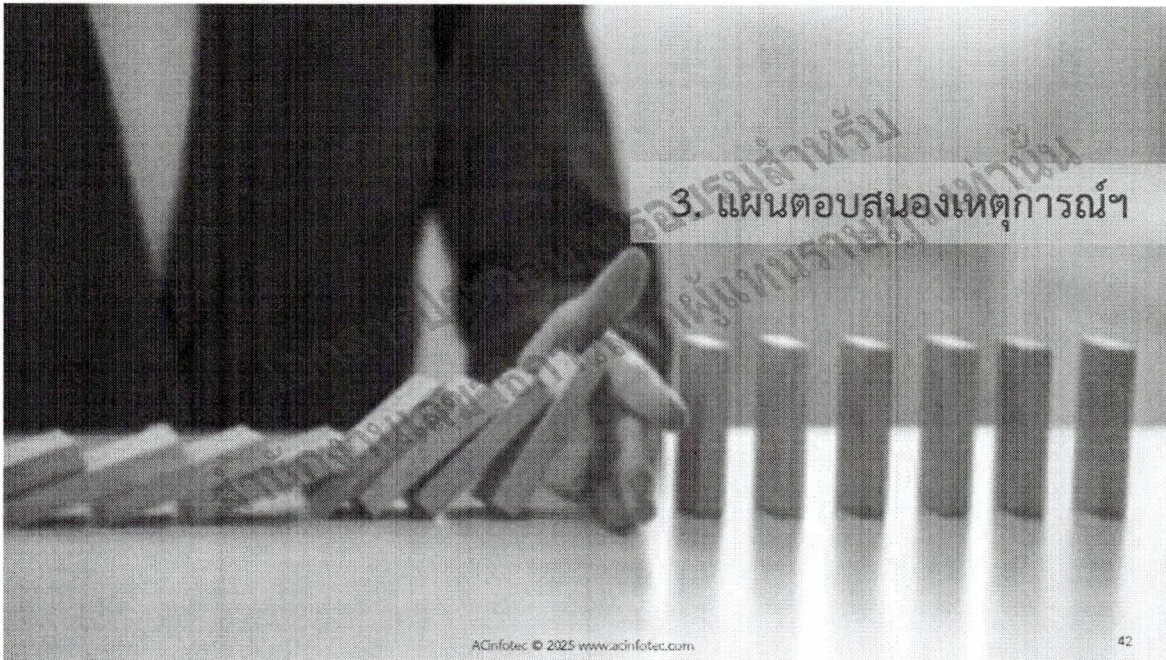
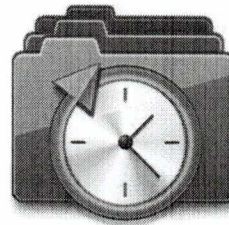
Item	Required Recovery Time following a disaster (RTO)	Maximum Tolerable Period of Disruption (MTPD)
Non-essential	15 days	30 days
Normal	3 days	7 days
Important	24 hours	72 hours
Urgent	8 hours	24 hours
Critical / Essential	Minutes to hours	Minutes to hours



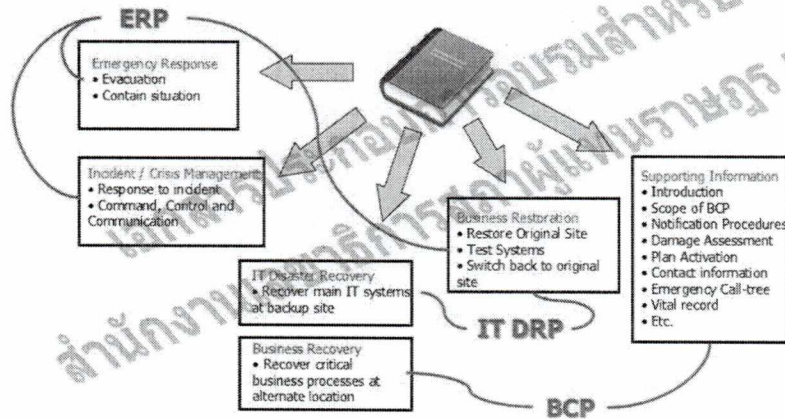
Business Impact Analysis

- Recovery Point Objective (RPO)

- ระดับสูงสุดที่องค์กรยอมรับได้สำหรับข้อมูลที่สูญหายจากเหตุการณ์ภัยคุกคาม
- จุดชี้วัดของข้อมูลที่สามารถกู้คืนได้ก่อนที่จะมีการหยุดชะงักของระบบ



Types of Plan & Components



Incident Response Plan (IRP)

- การตรวจหาและบันทึกเหตุการณ์ภัยคุกคาม (Incident)
- การประเมินและการแบ่งประเภทเหตุการณ์ภัยคุกคาม (Incident)
- การสืบสวนและการวินิจฉัยเหตุการณ์
- การส่งต่อเรื่องไปยังผู้ที่เกี่ยวข้อง Incident escalation (หากจำเป็น)
- การควบคุม การกำจัดเหตุการณ์ภัยคุกคาม และการกู้คืนให้เป็นสถานะปกติ
- การเปิดเผยข้อมูลและติดตามผลของเหตุการณ์ การเรียนรู้จากสิ่งที่เกิดขึ้น

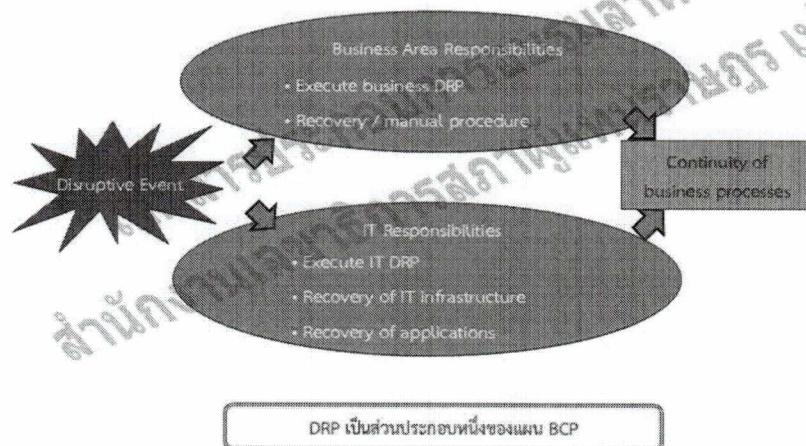
IRP อาจจะเป็น 'ส่วนประกอบ' หรือ
'ไม่เป็น' ส่วนประกอบของแผน BCP

Disaster Recovery Plan (DRP)

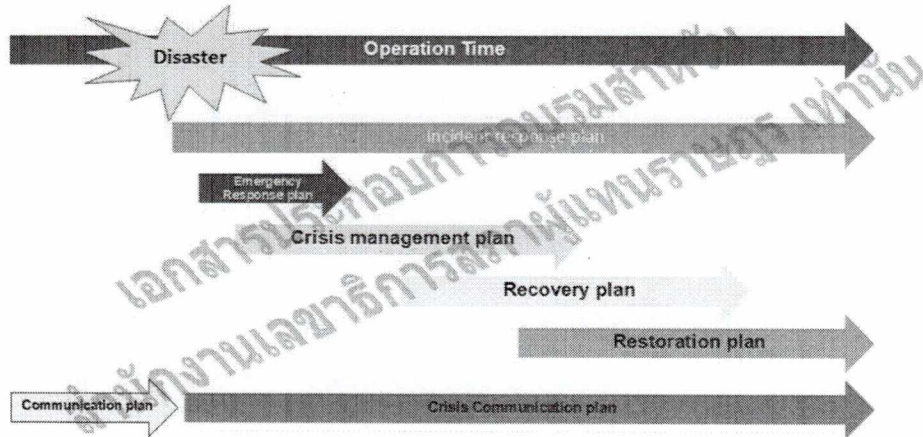
- เป็นแผนสำหรับตอบสนองกับเหตุการณ์ภัยพิบัติซึ่งจะให้ความสำคัญในการกู้คืนกระบวนการทางธุรกิจที่สำคัญ ระบบ IT หรือระบบทางวิศวกรรม
- แผนการกู้คืนจะถูกเขียนขึ้นโดยอ้างอิงข้อมูล ผลที่ตามมา (consequence) ของเหตุการณ์ภัยพิบัตินั้น (ข้อมูลอ้างอิง: จากการประเมินความเสี่ยง)
- กิจกรรมส่วนใหญ่ของการกู้คืนมักจะเกิดขึ้นที่สถานที่ปฏิบัติงานสำรอง



Disaster Recovery Plan

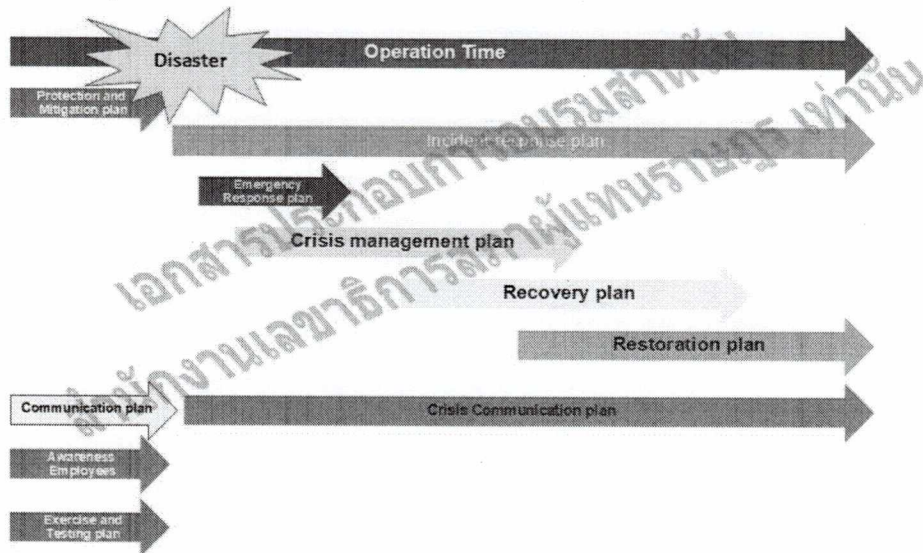


BCM dealing with Disaster Situation



ACInfosec/Client Confidential

BCM dealing with Disaster Situation



ACInfosec/Client Confidential

4. การจัดทำแผนตอบสนองเหตุการณ์

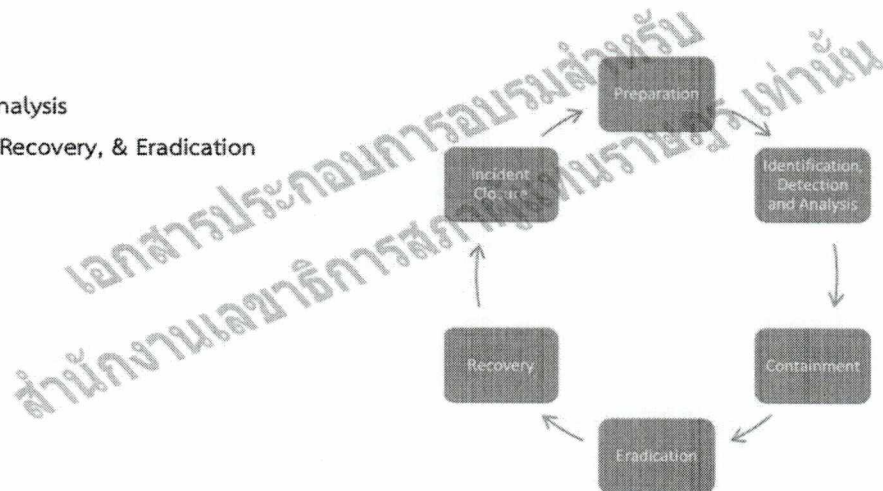
Incident Response Plan

Preparation

Detection & Analysis

Containment, Recovery, & Eradication

Case Studies



Incident Response Plan

- ทำความเข้าใจและจัดทำเอกสารเกี่ยวกับทรัพย์สินของโครงการ/องค์กร และภัยคุกคามและช่องโหว่ที่ต่อทรัพย์สินเหล่านั้น หรือที่เรียกว่า **การประเมินความเสี่ยง**
- ระบุนโยบายด้านความปลอดภัยและนโยบายที่เกี่ยวข้อง
- พัฒนาแผนการรักษาความปลอดภัยทางไซเบอร์เพื่อป้องกันความเสี่ยงเหล่านั้น
- พัฒนาแผนการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์

ACInfotec © 2025 www.acinfotec.com

51

Incident Response Policy

- ชุดของกฎและข้อกำหนดที่จัดทำเป็นเอกสารอย่างเป็นทางการซึ่งต้องปฏิบัติตาม
- ระบุสิ่งที่สำคัญต่อองค์กรหรือโครงการโดยการระบุทรัพย์สินหลักและความจำเป็นในการปกป้องหรือบริหารจัดการทรัพย์สินเหล่านั้น
- อาจมีนโยบายโครงการ, นโยบายองค์กร/แผนก, นโยบายสถาบัน และนโยบายที่ควบคุมโดยหน่วยงานกำกับ

ACInfotec © 2025 www.acinfotec.com

52

Incident Response Policy

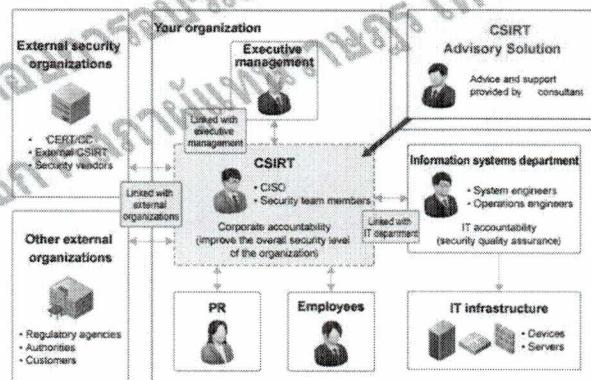
- วัตถุประสงค์ของนโยบายคืออะไร?
- เป้าหมายของนโยบาย IR (และการ IR โดยทั่วไป)
- นโยบายนี้ใช้กับใคร?
- อภิธานศัพท์
- การสื่อสารกับองค์กรของคุณอย่างไร?
- ฝ่ายใดบ้างที่ทำหน้าที่ IR และได้รับการแต่งตั้ง
- หน้าที่ทั่วไปใน IR (การรวบรวมหลักฐาน, ความสามารถในการปิดกั้น/บล็อก, ฯลฯ)
- วิธีการติดต่อ เช่น ความปลอดภัยสาธารณะ, สำนักงานความปลอดภัย, ฝ่ายรับเรื่องร้องเรียน

ACinfotec © 2025 www.acinfotec.com

53

การจัดตั้ง IR Team

- การตัดสินใจว่าใครอยู่ในทีม
 - ผู้ที่นำการสอบสวน
 - ผู้เชี่ยวชาญด้านเครือข่าย
 - ผู้เชี่ยวชาญแอปพลิเคชันหลัก
 - ความรู้และความรับผิดชอบด้านความมั่นคงปลอดภัย
- กำหนดบทบาทและความรับผิดชอบ
 - ใครเป็นผู้นำ
 - นักวิเคราะห์
 - การจำกัดผลกระทบ
 - การกู้คืน
 - ทรัพยากรที่เกี่ยวข้องทั้งภายในและภายนอก
 - ระบุผู้เชี่ยวชาญเฉพาะ



54

IR Team Skills

ทีมรับมือเหตุการณ์ภัยคุกคาม ควรมีความพร้อมในการจัดการกับภัยคุกคามเมื่อได้รับการแจ้งเหตุที่อาจเกิดขึ้น ต่อความมั่นคงปลอดภัยจากบุคคลภายในองค์กรเสมอ ควรมีการจัดโครงสร้างและขนาดของทีมรับมือเหตุการณ์ภัย คุกคามให้เหมาะสมกับลักษณะและขนาดขององค์กร และควรคำนึงถึงการประสานงานหรือขอความร่วมมือกับฝ่ายงาน อื่นภายในองค์กรที่เกี่ยวข้องกับการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้น

ทีมรับมือเหตุการณ์ภัยคุกคามสามารถแบ่งได้ 3 ประเภท ดังนี้

1. ทีมรับมือเหตุการณ์ภัยคุกคามที่เป็นบุคลากรภายในทั้งหมด (Insource)
2. ทีมรับมือเหตุการณ์ภัยคุกคามที่มีทั้งบุคลากรภายใน และบุคลากรจากภายนอก (Co-Source)
3. ทีมรับมือเหตุการณ์ภัยคุกคามที่เป็นบุคลากรจากภายนอกทั้งหมด (Fully Outsourced)

ทีมรับมือเหตุการณ์ภัยคุกคาม และตอบสนองฯ ควรประกอบด้วยบุคลากร ดังนี้

1. บุคลากรที่ทำหน้าที่รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัย ทางเทคโนโลยีสารสนเทศจากผู้ที่เกี่ยวข้องว่ามีเหตุภัยคุกคามเกิดขึ้นภายในองค์กร และ
2. บุคลากรที่ทำหน้าที่รับผิดชอบในการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

55

IR Team Skills

Team Leader

- ✓ Communication skills
- ✓ Diplomacy
- ✓ Organized
- ✓ Integrity
- ✓ Coping with Stress
- ✓ Problem Solving
- ✓ Time Management

Team Members

- ✓ Networking Expertise
- ✓ Knowledge of Key Applications and Services
- ✓ Host & System Expertise
- ✓ Malicious Code (Viruses, Worms, Trojan Horse programs)
- ✓ Programming Skills

56

การติดต่อประสานงานภายในองค์กร (IR Team)

- ระบุผู้นำเหตุการณ์
 - กำหนดความรับผิดชอบและบทบาท
 - มอบหมายบทบาท
- ระบุผู้มีอำนาจในการตัดสินใจ
 - ระบบต้องหยุดทำงานหรือไม่?
 - ระบบทั้งหมดจำเป็นต้องล้างข้อมูลและติดตั้งใหม่หรือไม่?
 - เริ่มต้นแผนปฏิบัติการทันทีหรือไม่? (การกำหนดเส้นทางแบบ black-hole)
- กำหนดแผนการสื่อสารและการทำงานร่วมกัน
 - การเข้าถึงระยะไกล
 - องค์กรภายนอก
 - สภาพแวดล้อมการทำงานร่วมกัน
- ระบุผู้ที่ประสานงานกับกลุ่มภายนอก

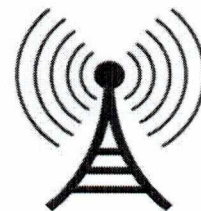
การประสานงานเพื่อดำเนินการร่วมกับหน่วยงานอื่นทั้งภายในและภายนอก จึงเป็นสิ่งจำเป็นในการรับมือและตอบสนองต่อภัยคุกคาม โดยผู้พิจารณาเป็นส่วนหนึ่งของแผนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งได้รับการฝึกฝนทักษะที่จำเป็นตามตำแหน่งและหน้าที่ในการรับมือและตอบสนองต่อภัยคุกคามด้วยบุคคลอย่างน้อยดังต่อไปนี้

- ผู้บริหาร (Top Management)
- ฝ่ายงานเทคโนโลยีสารสนเทศ (IT)
- ฝ่ายงานกฎหมายและควบคุมการปฏิบัติตามกฎหมาย (Legal & Compliance Officer)
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)
- ฝ่ายสื่อสารองค์กร (Public Affairs/Media Relations)
- ฝ่ายทรัพยากรบุคคล (Human resources)
- ทีมบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Team)
- ฝ่ายรักษาความปลอดภัย (Physical Security)

57

การติดต่อประสานงานภายนอกองค์กร (External Team)

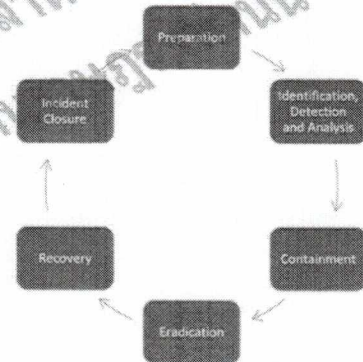
- การประสานงาน
 - CERT team
 - ISP
 - Related projects
 - Vendors
 - Legal advisors
 - Law enforcement
 - Trust groups
- การแบ่งปันข้อมูล
 - ปริมาณเท่าไร
 - วิธีการแบ่งปัน
 - การพิจารณา Security, privacy, and legal
 - ข้อตกลงการแบ่งปันข้อมูล



58

Incident Response Plan

- การระบุ ตรวจสอบ และการวิเคราะห์ ที่ดำเนินการเพื่อตรวจจับ ตรวจสอบ ยืนยัน และวิเคราะห์เหตุการณ์ที่มีความสำคัญต่อการพัฒนากลยุทธ์การจำกัดและกำจัดที่มีประสิทธิภาพ เมื่อเหตุการณ์ได้รับการยืนยันแล้ว สามารถจัดสรรทรัพยากรเพื่อสอบสวนขอบเขต ผลกระทบ และการตอบสนองที่จำเป็นได้ ระยะเวลาตรวจจับและการวิเคราะห์จะระบุที่มาของเหตุการณ์และเก็บรักษาหลักฐาน
- ระบบตรวจสอบและแจ้งเตือน
 - การให้ข้อมูลที่เพียงพอสำหรับการสอบสวนเหตุการณ์ที่เกิดขึ้น
 - ในสภาพแวดล้อมแบบเปิด การตรวจสอบเป็นแกนหลักด้านความปลอดภัยที่สำคัญ
 - เครือข่ายและไฟร์วอลล์
 - การบันทึกโฮสต์และแอปพลิเคชัน
 - ระบบตรวจจับการบุกรุก
 - การสแกน
 - รายการภัยคุกคามด้านความปลอดภัยและฟีดข้อมูล



ACInfotec © 2025 www.acinfotec.com

59

Common Categories of Cyber Incidents

ประเภทเหตุการณ์ (Incident Type)	คำอธิบาย (Description)
การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access)	เมื่อบุคคลหรือหน่วยงานได้รับการเข้าถึงเซิร์ฟเวอร์หรือทางกายภาพโดยไม่ได้รับอนุญาตไปยังเครือข่ายของมหาวิทยาลัย, ระบบ, แอปพลิเคชัน, ข้อมูล หรือทรัพยากรอื่น ๆ
การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service - DoS)	การโจมตีที่สามารถป้องกันหรือทำให้การทำงานของบริการที่ได้รับอนุญาตของเครือข่าย, ระบบ หรือแอปพลิเคชันบนพร่องลงได้สำเร็จ โดยการใช้ทรัพยากรทั้งหมด กิจกรรมที่รบกวนถึงกันเป็นเหยื่อหรือการมีส่วนร่วมในการโจมตี DoS
โค้ดประสงค์ร้าย (Malicious Code)	การติดตั้งซอฟต์แวร์ประสงค์ร้ายได้สำเร็จ (เช่น ไวรัส, เวิร์ม, โทรจัน หรือสแปนที่ประสงค์ร้ายที่ใช้โค้ดอื่น ๆ) ที่ติดเชื้ระบบปฏิบัติการหรือแอปพลิเคชัน หน่วยงานไม่จำเป็นต้องรายงานเหตุการณ์ประเภทนี้ที่ถูกกักกันโดยซอฟต์แวร์ป้องกันไวรัส (AV) สำเร็จแล้ว
การใช้งานที่ไม่เหมาะสม (Improper or Inappropriate Usage)	เมื่อบุคคลละเมิดนโยบายการใช้คอมพิวเตอร์ที่ยอมรับได้
การละเมิด PII ที่ต้องสงสัย (Suspected PII Breach)	หากเหตุการณ์เกี่ยวข้องกับข้อมูลที่ระบุตัวบุคคลได้ (PII) การละเมิดจะต้องถูกรายงานเพียงแต่ ต้องสงสัย (เหตุการณ์ PII ที่ต้องสงสัยสามารถแก้ไขได้โดยการยืนยันว่าไม่มีการละเมิด PII)
การสูญเสียบข้อมูลที่จะมีผลอันต้องสงสัย (Suspected loss of Sensitive Information)	เหตุการณ์ที่เกี่ยวข้องกับการสูญเสียบข้อมูลที่จะมีผลอันต้องสงสัย (ไม่ใช่ PII) ซึ่งเกิดขึ้นจากผลของการเข้าถึงโดยไม่ได้รับอนุญาต, โค้ดประสงค์ร้าย หรือการใช้งานที่ไม่เหมาะสม โดยไม่ทราบสาเหตุหรือขอบเขต

ACInfotec © 2025 www.acinfotec.com

60

Detection & Analysis

ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น 2 ประเภท

- Precursor เป็นข้อมูลที่ยังบ่งบอกว่า Incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลที่ยังบ่งบอกว่า Incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

ตัวอย่างแหล่งข้อมูลการแจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่าย

แหล่งข้อมูล	คำอธิบาย
ประเภท Alert	
IDPS	ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีโดยเฉพาะ ทั้งในระดับเครือข่าย และ Endpoint วิธีการตรวจจับมีหลายแบบแตกต่างกันไป ระบบประเภทนี้จะมีการแจ้งเตือนเมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก
SIEM	ทำหน้าที่คล้าย IDPS แต่จะตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่นๆ เพื่อนำมาวิเคราะห์ โดยปกติ SIEM จะมีประสิทธิภาพได้ต้องมีการตั้งค่า Rule set ที่ดีโดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่ SIEM ดูแลอยู่
Anti-Malware Software	ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ปัจจุบันทำงานได้ทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ถึงความพยายามในการโจมตีหรือการโจมตีได้สำเร็จแล้ว
File Integrity Monitoring	ระบบที่ทำหน้าที่สอดส่องดูแลการเปลี่ยนแปลงแก้ไขของไฟล์สำคัญๆ และจะแจ้งเตือนเมื่อมีการเปลี่ยนแปลงของไฟล์โดยไม่ได้รับอนุญาต

61

Detection & Analysis

ตัวอย่างแหล่งข้อมูลการแจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่าย

แหล่งข้อมูล	คำอธิบาย
Third-Party Monitoring Service	บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบของเรา โดยเฉพาะเมื่อระบบของเราถูกนำไปใช้โจมตีระบบอื่นๆ ภายนอกองค์กร ถึงแม้ตัวบ่งชี้ได้จากระบบได้ถูกยึดครองโดยผู้ไม่หวังดีและนำไปใช้ในการสร้างความเสียหาย
ประเภท Log	
Operating System and Application Log	ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยบันทึกเหตุการณ์หลากหลายประเภท สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์
Network Device Log	อุปกรณ์เครือข่ายที่มีบันทึกข้อมูลผ่านเข้าออกเครือข่ายก็สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้เช่นเดียวกัน ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์
ข้อมูลจากแหล่งสาธารณะ	
Vulnerability and Exploit Database	ข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่ สามารถถูกใช้เป็นเครื่องบ่งชี้ภัยคุกคามได้ หากการโจมตีที่ออกมาใหม่นั้นสามารถโจมตีระบบที่เราดูแลอยู่ได้
บุคคลเป็นผู้แจ้งเตือน	
บุคคลภายในองค์กร	บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝนเพื่อช่วยสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศได้
บุคคลภายนอกองค์กร	บุคคลภายนอก เช่น ลูกจ้างสามารถเป็นแหล่งข้อมูลการทำงานผิดปกติของระบบได้ นอกจากนี้ยังมี CERT ต่างๆ รวมถึง White Hat Hacker

62

เทคนิค	คำอธิบาย
Profiling (Baselining) Networks and Systems & Understand Normal Behavior	ข้อมูลสถานการณ์การทำงาน การตั้งค่า และการใช้งานปกติของระบบ จะทำให้ทราบได้เร็วขึ้นเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้นในระบบ
Log Retention Policy	Log จากอุปกรณ์ต่างๆ เช่น iPDS, Workstation, Servers, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์ต่อไปเพื่อหลักฐานทางกฎหมายหรือเรียกดูในอนาคต จึงต้องมีการเก็บรักษาและป้องกันอย่างดี รวมถึงเก็บไว้เป็นระยะเวลาที่เหมาะสม ตอบโจทย์ในด้านของการตอบสนองและเป็นไปตามกฎหมายข้อบังคับ
Perform Event Correlation	การเชื่อมโยงข้อมูลเข้าๆ ออกๆ ระหว่างการเข้ามีระบบเป้าหมายที่ผ่านอุปกรณ์ต่างๆ บนเครือข่าย ดังนั้นการวิเคราะห์จึงจำเป็นต้องใช้ข้อมูลจากทุกอุปกรณ์ที่คาดว่าจะเกี่ยวข้องร่วมกัน (Correlation) เพื่อให้เห็นถึงเส้นทางการโจมตี และสาเหตุที่แท้จริงที่ทำการบุกรุกประสบความสำเร็จ
Clock Synchronization	อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ตรงกันอยู่เสมอ ไม่เช่นนั้นแล้วการ Correlate Event จะทำได้ยากหรือไม่สามารถทำได้
Sniff and Analyze Network Data	ในหลาย ๆ กรณีการดักจับข้อมูลทางเครือข่ายขณะเกิดเหตุเพื่อนำมาวิเคราะห์วิเคราะห์สามารถที่จะให้ข้อมูลเบาะแสที่สำคัญได้
Seek Assistance	เมื่อใดที่ทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ Incident เพื่อหาสาเหตุที่แท้จริงเพื่อกำจัดผู้บุกรุกออกจากระบบได้ ก็สามารถใช้บริการให้คำแนะนำปรึกษาจากภายนอกสมาคมควรได้ เช่น CERT ต่าง ๆ หรือบริการจากที่ปรึกษาภายนอก เป็นต้น

Detection & Analysis

[illegible]

แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคาม			
ชื่อเหตุการณ์ภัยคุกคาม		หมายเลขของเหตุการณ์ภัยคุกคาม	
วันที่บันทึกเหตุการณ์ภัยคุกคาม		หมายเลขของเหตุการณ์ภัยคุกคามอื่นๆ ที่เกี่ยวข้องกับเหตุการณ์นี้	
ข้อมูลของแจ้งเหตุการณ์ภัยคุกคาม		ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม	
ชื่อ - นามสกุล		ชื่อ - นามสกุล	
หน่วยงาน		โทรศัพท์	
โทรศัพท์	อีเมล	อีเมล	
วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม			
วันที่และเวลาพบเหตุภัยคุกคาม			
วันที่และเวลารายงานเหตุภัยคุกคาม			

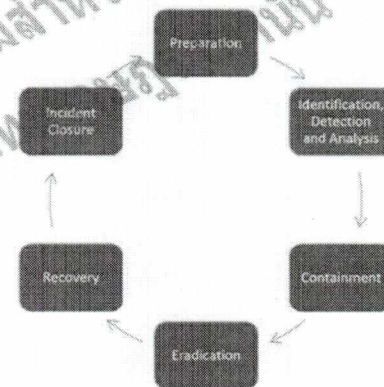
หน้า 37 จาก 50

[illegible][illegible]

รายละเอียดเหตุการณ์ภัยคุกคาม	
- สิ่งที่เกิดขึ้น - เกิดขึ้นอย่างไร - ทำไมจึงเกิดขึ้น - การประเมินทรัพย์สินสารสนเทศที่เกี่ยวข้อง - ผลกระทบทางธุรกิจ - ช่องโหว่ที่พบ/ปัจจัยของเหตุการณ์ภัยคุกคาม	
การดำเนินการทั้งหมดของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้	การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้
คำใช้จ่ายในการฟื้นฟูคืนสู่สภาพปกติ	รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์ภัยคุกคาม
สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม	

- การควบคุมผลกระทบ (Containment) ขั้นตอนการควบคุมผลกระทบ พยายามจำกัดขอบเขตและขนาดของการโจมตีอย่างเข้มข้น ช่องโหว่ในสถาปัตยกรรมคอมพิวเตอร์บางอย่างสามารถใช้ประโยชน์ได้อย่างรวดเร็ว การจำกัดวงเกี่ยวข้องกับการรวบรวม การเก็บรักษา การรักษาความปลอดภัย และการจัดทำเอกสารหลักฐานทั้งหมด
- การควบคุมผลกระทบมีสองเป้าหมายหลัก ดังนี้
 - ป้องกันไม่ให้ข้อมูลออกจากเครือข่ายผ่านเครื่องที่ได้รับผลกระทบ
 - ป้องกันไม่ให้ผู้โจมตีสร้างความเสียหายเพิ่มเติมต่อทรัพย์สินเทคโนโลยีสารสนเทศ

- **การควบคุมผลกระทบ (Containment)** ขั้นตอนการควบคุมผลกระทบ พยายามจำกัดขอบเขตและขนาดของกรโคมต้อย่างแข็งขัน ช่องโหว่ในสถาปัตยกรรมคอมพิวเตอร์บางอย่างสามารถถูกใช้ประโยชน์ได้อย่างรวดเร็ว การจำกัดวงเกี่ยวข้องกับกรรวบรวมการเก็บรักษา การรักษาความปลอดภัย และการจัดทำเอกสารหลักฐานทั้งหมด
- **การควบคุมผลกระทบมีสองเป้าหมายหลัก ดังนี้**
 - ป้องกันไม่ให้ข้อมูลออกจากเครือข่ายผ่านเครื่องที่ได้รับผลกระทบ
 - ป้องกันไม่ให้ผู้โจมตีสร้างความเสียหายเพิ่มเติมต่อทรัพย์สินเทคโนโลยีสารสนเทศ



Containment

การควบคุมความเสียหายมีความจำเป็นอย่างยิ่งที่จะป้องกันไม่ให้ความเสียหายกระจายออกไปเป็นวงกว้าง สร้างผลกระทบต่อการดำเนินงานธุรกิจอื่นๆ และยังเป็นกัมปัดพั้นที่เพิ่มระยะเวลาให้ทีมที่รับมือ Incident มีเวลาในการคิดหาสาเหตุ และวิธีการแก้ปัญหาที่ถาวรได้

ข้อสำคัญของการควบคุมความเสียหาย คือ การตัดสินใจเลือกใช้อุปกรณ์ที่เหมาะสม โดยวิธีการทั่วไปมีดังต่อไปนี้

- ปิดระบบ (Shut Down)
- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมีข้อยกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่ผิดปกติใดๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- Redirect Network Traffic และ/หรือการส่งข้อมูลของผู้บุกรุกไปยัง Blackhole / Sandbox / Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้อุปกรณ์ควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่ต้องกรำงำลงเพื่อระบุประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

67

Containment

การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือ เพื่อให้การแก้ไข Incident ส่งผลกระทบท่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการตามขั้นตอนทาง กฎหมาย ดังนี้ การดำเนินการจัดเก็บ

หลักฐานทางดิจิทัล องค์กรสามารถดำเนินการโดยพิจารณาตามหลักการดังต่อไปนี้

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวข้องกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ได้ทันเวลา
- เมื่อหลักฐานมีบันทึกการเข้าถึงและการกระทำใดๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม
- การเปลี่ยนตัวผู้ดูแลจำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody)

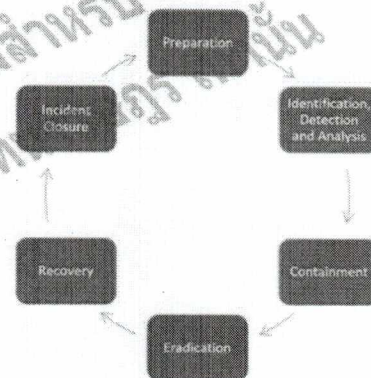
รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

- 1) ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น
- 2) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident
- 3) สถานที่จัดเก็บหลักฐาน

68

Incident Response Plan

- **การกำจัด (Eradication)** การกำจัดคือการลบภัยคุกคามร้าย บัณชี หรือการเข้าถึงที่ไม่เหมาะสม การกำจัดยังรวมถึงการซ่อมแซมช่องโหว่ที่อาจเป็นสาเหตุหลักของการถูกบุกรุก เราขอแนะนำอย่างยิ่งให้ทำการติดตั้งระบบปฏิบัติการและแอปพลิเคชันใหม่ทั้งหมด
- ขั้นตอนทั่วไปที่เกี่ยวข้องกับระยะการกำจัดของการตอบสนองต่อเหตุการณ์คือ:
 - กำหนดเกณฑ์มาตรฐานการกำจัดบริการรายการตรวจสอบต่างๆ สำหรับการถูกบุกรุก
 - ระบุและบรรเทาช่องโหว่ทั้งหมดที่ถูกใช้ประโยชน์
 - ลบมัลแวร์ เนื้อหาที่ไม่เหมาะสม และส่วนประกอบอื่นๆ
 - หากพบโฮสต์ที่ได้รับผลกระทบเพิ่มเติม เช่น การติดมัลแวร์ใหม่ ให้ทำซ้ำขั้นตอนการตรวจจับและวิเคราะห์เพื่อระบุโฮสต์ที่ได้รับผลกระทบอื่นๆ ทั้งหมด จากนั้นจึงทำการจำกัดวงและกำจัดเหตุการณ์สำหรับโฮสต์เหล่านั้น
 - ติดตั้งระบบปฏิบัติการใหม่ ติดตั้งแอปพลิเคชันใหม่ ติดตั้งแพทช์ทั้งหมด



ACInfotec © 2025 www.acinfotec.com

69

Eradication

หากพิจารณา Incident Response Life Cycle จะพบว่า เมื่อมีการควบคุมความเสียหายและมีการเก็บ หลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้ว ข้อมูลทั้งหมดจะต้องนำกลับมารวบรวมวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “การตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และ ช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามาในระบบทั้งหมดได้เรียบร้อยแล้ว

ตัวอย่างของการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ เช่น

- การปิดช่องโหว่ของระบบ
- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
- การลบโปรแกรมประเภท Backdoor ออกจากระบบ
- การใช้ข้อมูล IoC ในการสแกนหา Malware หรือร่องรอยอื่นๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

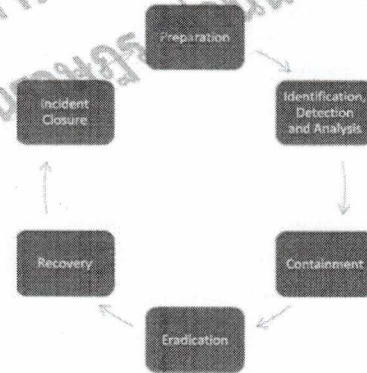
หลังจากดำเนินการควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว องค์กรจึงจะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ โดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควรเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่างๆ จาก Master Image ที่ปลอดภัย
- การ Restore ข้อมูลกลับเข้าสู่ระบบจาก Back Up Storage

70

Incident Response Plan

- การกู้คืน (Recovery) เมื่อเหตุการณ์ถูกจำกัดวงและกำจัดเรียบร้อยแล้ว การกู้คืนสามารถเริ่มต้นได้ ระยะนี้ช่วยให้กระบวนการทางธุรกิจที่ได้รับผลกระทบจากเหตุการณ์สามารถกู้คืนและกลับมาดำเนินการได้ตามปกติ
- ขั้นตอนทั่วไปในการกู้คืนมีดังนี้
 - หากมีข้อมูลที่ละเอียดอ่อนอยู่ในเครื่องที่ได้รับผลกระทบให้พิจารณาประเมินผลกระทบต่อข้อมูล
 - ติดตั้งและอัปเดต OS และแอปพลิเคชันใหม่ เปลี่ยนข้อมูลรับรองของผู้ใช้และระบบทั้งหมด
 - กู้คืนข้อมูลกลับสู่ระบบ
 - นำระบบที่ได้รับผลกระทบกลับสู่สถานะที่พร้อมใช้งาน
 - ยืนยันว่าระบบที่ได้รับผลกระทบทำงานได้ตามปกติ
 - หากจำเป็น ให้ใช้การตรวจสอบเพิ่มเติมเพื่อค้นหากิจกรรมหลังเหตุการณ์ที่เกี่ยวข้องในอนาคต

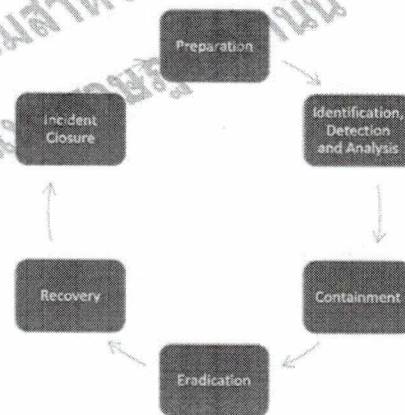


ACinfotec © 2025 www.acinfotec.com

71

Incident Response Plan

- รายงานติดตามผลจะบันทึกเหตุการณ์และรวมถึงบทเรียนที่ได้รับเพื่อรักษาและขยายความรู้ รายงานจัดทำโดยทีม CIRT รายงานควรประกอบด้วย
 - ข้อมูลเกี่ยวกับประเภทของเหตุการณ์
 - คำอธิบายว่าเหตุการณ์ถูกค้นพบได้อย่างไร
 - ข้อมูลเกี่ยวกับระบบที่ได้รับผลกระทบ
 - ข้อมูลเกี่ยวกับผู้รับผิดชอบระบบและข้อมูลของระบบนั้น
 - คำอธิบายสาเหตุของเหตุการณ์
 - คำอธิบายการตอบสนองต่อเหตุการณ์และประสิทธิภาพของการตอบสนองนั้น
 - ข้อเสนอแนะเพื่อป้องกันเหตุการณ์ในอนาคต
 - การหารือเกี่ยวกับบทเรียนที่ได้รับซึ่งจะช่วยปรับปรุงการตอบสนองในอนาคต
 - ลำดับเหตุการณ์ ตั้งแต่การตรวจจับจนถึงการปิดเหตุการณ์



ACinfotec © 2025 www.acinfotec.com

72

Lessons Learned

- Critical aspect of IR process
- Closes gaps in processes
 - monitoring
 - communication
 - processes

การเรียนรู้เพื่อปรับปรุงการดำเนินการหลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post-Incident Activity) ทีมรับมือและผู้ที่เกี่ยวข้องทั้งหมดควรมีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูลความคิดเห็น ในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งการใช้ข้อมูลจาก Issue Tracking System เพื่อประกอบการพิจารณาปรับปรุงและพัฒนา

73

Lessons Learned

- ตัวอย่างประเด็นคำถาม ที่องค์กรสามารถพิจารณาปรับใช้ประกอบการประชุมแลกเปลี่ยนข้อมูลหลังจากการรับมือ ภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์โดยองค์กรสามารถพิจารณาเพิ่มเติมได้จากตัวอย่างที่ระบุไว้ใน BCP เช่น
- การดำเนินงานเสร็จสิ้นตามกำหนด และได้ผลลัพธ์ตามที่ระบุไว้หรือไม่
 - ขั้นตอนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้ดำเนินการครบถ้วนถูกต้องตามที่กำหนดหรือไม่
 - การใช้ทรัพยากรเพื่อรับมือและตอบสนองเป็นไปตามที่วางแผนไว้หรือไม่ มีส่วนใดบ้างที่ต้องได้รับการจัดสรรเพิ่มเติม
 - ข้อมูลที่จำเป็นต้องใช้ในการตอบสนอง มีข้อมูลจากส่วนใดบ้างที่ทีมรับมือ คิดว่ายังได้รับเข้าไป
 - การปฏิบัติงานในขั้นตอนใดที่ทำให้การกู้คืนข้อมูลหรือระบบช้าลง
 - การติดต่อสื่อสารระหว่างทีมรับมือและตอบสนองต่อเหตุการณ์ทั้งภายในและภายนอกองค์กร มีประเด็นปัญหา อุปสรรคอะไรบ้าง ที่ต้องได้รับการทบทวนเพื่อนำไปพัฒนาและปรับปรุงต่อไป
 - เหตุการณ์ภัยคุกคามลักษณะนี้มีแนวทางในการป้องกันไม่ให้เกิดซ้ำในอนาคตได้อย่างไรบ้าง
 - สัญญาณตรวจจับทั้ง Precursor และ Indicator ใดบ้างที่ควรเพิ่มเติมเพื่อเพิ่มประสิทธิภาพและความเร็วในการ รับมือและตอบสนอง
 - การแลกเปลี่ยนข้อมูลกับหน่วยงานอื่น มีประเด็นปัญหาหรืออุปสรรคอะไรบ้าง และสามารถปรับปรุงให้ดีขึ้นอย่างไร

74

Thank you



Follow us on:



www.acinfotec.com



[ACinfotecthailand](#)



[ACinfotec Co., Ltd.](#)



Email : sales@acinfotec.com
training@acinfotec.com

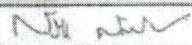
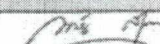
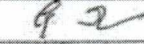
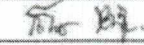
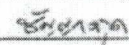
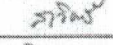
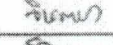
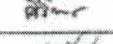
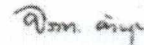
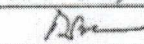
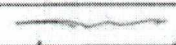
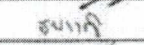
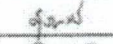
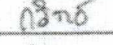
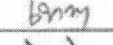
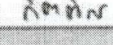
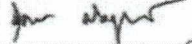
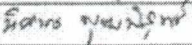


Tel. : 081-668-9014
02-670-8980-3 ext. 406

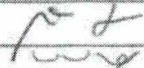
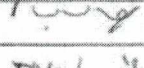
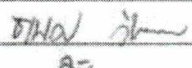
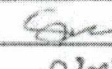
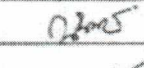
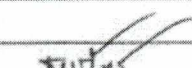
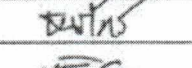
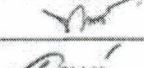
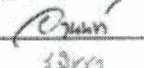
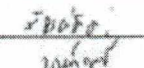
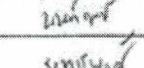
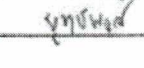
รายชื่อผู้เข้าร่วมอบรมหลักสูตร Cybersecurity Awareness รุ่นที่ 1

รายชื่อผู้เข้าร่วมอบรมหลักสูตร Cybersecurity Awareness รุ่นที่ ๑
 วิชาแผนตอบสนองภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan)
 วันอังคารที่ ๒๔ มิถุนายน ๒๕๖๔ ระหว่างเวลา ๐๙.๐๐ - ๑๖.๐๐ นาฬิกา

ณ ห้องประชุม/สัมมนา ๖๐๖ ชั้น ๖ สำนักงานเลขาธิการสภาผู้แทนราษฎร อาคารรัฐสภา

ลำดับ	ชื่อ - สกุล	ตำแหน่ง	ลายเซ็น
๑	นางสาวสิริธร ลิ้มปทยอม	ผู้อำนวยการสำนักสารสนเทศ	
กลุ่มงานบริหารทั่วไป			
๒	นางณภกัษ สุวรรณภกุล	ผู้บังคับบัญชากลุ่มงานบริหารทั่วไป	
๓	นางอุไร วัชราม	เจ้าพนักงานคอมพิวเตอร์ทั่วไปอาวุโส	
๔	ว่าที่ร้อยตรี รณยุทธ หงษ์ภู	เจ้าพนักงานคอมพิวเตอร์ทั่วไปอาวุโส	
๕	นางสาวชญานุกาญจน์ เนื่องโคตะ	เจ้าพนักงานคอมพิวเตอร์ทั่วไปอาวุโส	
๖	นางสาวสาวตรี จิตมั่น	เจ้าพนักงานคอมพิวเตอร์ทั่วไปอาวุโส	
๗	นางสาวจินตนา ศิลาเดช	เจ้าพนักงานคอมพิวเตอร์ทั่วไปอาวุโส	
๘	นางสาวศิริพร พรหมวาส	เจ้าพนักงานคอมพิวเตอร์ทั่วไปชำนาญงาน	
๙	นางสาวบุปผาชาติ กลางประพันธ์	เจ้าพนักงานคอมพิวเตอร์ทั่วไปชำนาญงาน	
กลุ่มงานวิทยาการคอมพิวเตอร์			
๑๐	นางสาวจรรยา คำพูน	ผู้บังคับบัญชากลุ่มงานวิทยาการคอมพิวเตอร์	
๑๑	นางนทียา แก้วประทุม	นักวิชาการคอมพิวเตอร์เชี่ยวชาญ	
๑๒	นางณัชชา ศรีเพลิง	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๑๓	พันจ่าเอก กิตติ ดุษฎี	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๑๔	นายเทอดศักดิ์ สีนสมบูรณ์ทอง	นักวิชาการคอมพิวเตอร์ชำนาญการ	
๑๕	นายธนาวุฒิ จันทิมา	นักวิชาการคอมพิวเตอร์ชำนาญการ	
๑๖	นายธนยศ สุวรรณ	นักวิชาการคอมพิวเตอร์ชำนาญการ	
๑๗	นายสุรพงษ์ รัตนมณี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	
๑๘	นายกรัณย์ รักวิชา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	
๑๙	สิบเอก เทวา เพ็งพันธ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	
๒๐	นายกิตติกร บุญมาดย์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	
กลุ่มงานพัฒนาระบบงานคอมพิวเตอร์			
๒๑	นายณัฐวัชร มังคละคุปต์	ผู้บังคับบัญชากลุ่มงานพัฒนาระบบงานคอมพิวเตอร์	
๒๒	นางนิตากร พุฒิสุทธิ	นักวิชาการคอมพิวเตอร์เชี่ยวชาญ	

ลำดับ	ชื่อ - สกุล	ตำแหน่ง	ลายเซ็น
๒๓	นางบัญญัติพร พวงมะลัย	นักวิชาการคอมพิวเตอร์เชี่ยวชาญ	
๒๔	นางสาวผดุง เหลืองประมวส	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๒๕	นางสาวพัฒนา ชมภู	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๒๖	นางสาววิภาวดี อ่วมเจริญ	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๒๗	นายอาทิตย์ ธนวงษ์	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๒๘	นายสมศักดิ์ เกิดหล้า	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๒๙	นางสาววันเพ็ญ ชูเมือง	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๓๐	นางนุจรินทร์ ธรรมะโกมินทร์	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๓๑	นายชาคริต วิมานรัตน์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	
กลุ่มงานบริหารระบบเครือข่ายคอมพิวเตอร์			
๓๒	สืบเอก โชคชัย สุฤทธิ	ผู้บังคับบัญชากลุ่มงานบริหารระบบเครือข่ายคอมพิวเตอร์	
๓๓	นายธีรวิทย์ วงษ์วิจิตร	นักวิชาการคอมพิวเตอร์เชี่ยวชาญ	
๓๔	นางสมคิด แซ่ว่อง	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๓๕	นายสุธี ยืนนานอน	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๓๖	นายมนินทร์ รัตนานพวงศ์	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๓๗	นายวิชณู แก้วประทุม	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๓๘	นางธีราพร สอดส่องเกษ	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๓๙	นางสาวเหนือฝัน พิมพ์วงศ์	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๔๐	นายชัยวัฒน์ ปันคำ	นักวิชาการคอมพิวเตอร์ชำนาญการ	
๔๑	นายจิรภัทร์ เต็มวุฒิโรจน์	นักวิชาการคอมพิวเตอร์ชำนาญการ	
๔๒	นายพัชรณัฐ สิริสานต์สกุล	นักวิชาการคอมพิวเตอร์ชำนาญการ	
๔๓	นางสาวลดาพรรณ สิงคณิกา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	
กลุ่มงานบริการระบบคอมพิวเตอร์			
๔๔	นางสาวฐิตาภรณ์ ไชยชมภู	ผู้บังคับบัญชากลุ่มงานบริการระบบคอมพิวเตอร์	
๔๕	นางสัณญา เงินเล็ก	นักวิชาการคอมพิวเตอร์เชี่ยวชาญ	
๔๖	นางสุธาวี อนุญาหงษ์	นักวิชาการคอมพิวเตอร์เชี่ยวชาญ	
๔๗	นางเสาวนีย์ สุกใส	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๔๘	นายนำพล นัยยติ	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
๔๙	นายรัตนพล บัณฑล	นักวิชาการคอมพิวเตอร์ชำนาญการ	

ลำดับ	ชื่อ - สกุล	ตำแหน่ง	ลายเซ็น
๕๐	นายสุทธิพงษ์ พุทธิสลาต	เจ้าพนักงานเครื่องคอมพิวเตอร์อาวุโส	
๕๑	นายเศรษฐบุตร บุญชุ่ม	เจ้าพนักงานเครื่องคอมพิวเตอร์อาวุโส	
๕๒	นายธเนศ วิไลจิตต์	เจ้าพนักงานเครื่องคอมพิวเตอร์อาวุโส	
๕๓	นายวสันต์ ปุ่มา	เจ้าพนักงานเครื่องคอมพิวเตอร์อาวุโส	
๕๔	นายชนาเทพ มั่นนาไส	เจ้าพนักงานเครื่องคอมพิวเตอร์อาวุโส	
๕๕	นางสาวณัฐณพัชรา เอกกนกพัฒน์	เจ้าพนักงานเครื่องคอมพิวเตอร์อาวุโส	
๕๖	นายธนกฤต รอดสำราญ	เจ้าพนักงานเครื่องคอมพิวเตอร์อาวุโส	
๕๗	นายธนภัทร ศรีหาลัง	เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน	
๕๘	นายศักดิ์ชาย ชูดวงจันทร์	เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน	
๕๙	นายสาธิต ใจห้าว	เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน	
๖๐	นายสุเมธ หงษาคระประเสริฐ	เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน	
๖๑	นายทรงฤทธิ์ ทองคำ	เจ้าพนักงานเครื่องคอมพิวเตอร์ชำนาญงาน	
๖๒	นายอานนท์ บติบระกุล	เจ้าพนักงานเครื่องคอมพิวเตอร์ปฏิบัติงาน	
	น.ส. ศุภิษา สว่างฉาย	นักศึกษานิเทศน์	
	นาย ธีรภัทร สิงห์	นักศึกษานิเทศน์	
	นาย ธีรภัทร จันทะลา	นักศึกษานิเทศน์	
	ร.ร. นนทอนันต์ บุรณศิริ	ผู้ฝึกสอน อ.ท. ทบ. ๖๓	
	นาย ธีรภัทร สิงห์	..	

ผลการประเมินการอบรมหลักสูตร Cybersecurity Awareness รุ่นที่ 1

คำถามสำหรับการอบรมหลักสูตร Cybersecurity Awareness รุ่นที่ 1

1. แผนการตอบสนองต่อภัยคุกคาม (Incident Response Plan) มีประโยชน์อย่างไร?

- ก. ช่วยให้องค์กรสามารถหยุดการทำงานของระบบได้ทันที
 - ข. ช่วยให้เจ้าหน้าที่รับมือกับการละเมิดความปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพ ลดความเสียหายที่อาจเกิดขึ้น
 - ค. ช่วยให้องค์กรสามารถหลีกเลี่ยงการเกิดเหตุการณ์ด้านความปลอดภัยได้ทั้งหมด
- เฉลย: ข. ช่วยให้เจ้าหน้าที่รับมือกับการละเมิดความปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพ ลดความเสียหายที่อาจเกิดขึ้น

2. ขั้นตอนแรกในวงจรของการบริหารจัดการเหตุการณ์ภัยคุกคาม (Incident Response Lifecycle) คืออะไร?

- ก. การควบคุม (Containment)
- ข. การตรวจจับ (Detection)
- ค. การเตรียมความพร้อม (Preparation)

เฉลย: ค. การเตรียมความพร้อม (Preparation)

3. การกระทำใดที่จัดเป็นการ "ควบคุม" (Containment) ในแผนตอบสนองต่อเหตุการณ์ภัยคุกคาม?

- ก. การถอดปลั๊กอุปกรณ์ที่ติดมัลแวร์ออกจากเครือข่าย
- ข. การติดตั้งโปรแกรมป้องกันไวรัส
- ค. การแจ้งเตือนผู้ใช้งานเกี่ยวกับเหตุการณ์ที่เกิดขึ้น

เฉลย: ก. การถอดปลั๊กอุปกรณ์ที่ติดมัลแวร์ออกจากเครือข่าย

4. ข้อใดคือความแตกต่างระหว่าง "เหตุการณ์ด้านความปลอดภัย" (Security Event) และ "เหตุการณ์ภัยคุกคามด้านความปลอดภัย" (Security Incident)?

- ก. เหตุการณ์ด้านความปลอดภัยคือกิจกรรมที่ทำให้เกิดการแจ้งเตือน ส่วนเหตุการณ์ภัยคุกคามด้านความปลอดภัยคือเหตุการณ์ที่คุกคามความปลอดภัยอย่างแท้จริง
- ข. เหตุการณ์ด้านความปลอดภัยคือสิ่งที่องค์กรควบคุมได้ ส่วนเหตุการณ์ภัยคุกคามด้านความปลอดภัยคือสิ่งที่ควบคุมไม่ได้
- ค. ไม่มีข้อแตกต่าง ทั้งสองคำมีความหมายเดียวกัน

เฉลย: ก. เหตุการณ์ด้านความปลอดภัยคือกิจกรรมที่ทำให้เกิดการแจ้งเตือน ส่วนเหตุการณ์ภัยคุกคามด้านความปลอดภัยคือเหตุการณ์ที่คุกคามความปลอดภัยอย่างแท้จริง

5. องค์ประกอบสำคัญของแผนรับมือเหตุการณ์ภัยคุกคามที่ดีควรมีอะไรบ้าง?

ก. เพียงแค่รายชื่อผู้ติดต่อทีมกฎหมาย

ข. ซอฟต์แวร์ป้องกันไวรัสที่ทันสมัยที่สุด

ค. แผนการสื่อสาร, ขั้นตอนการรายงานเหตุการณ์ภัยคุกคาม, และแผนการกู้คืนระบบ

เฉลย: ค. แผนการสื่อสาร, ขั้นตอนการรายงานเหตุการณ์ภัยคุกคาม, และแผนการกู้คืนระบบ

6. ข้อใดต่อไปนี้เป็นตัวอย่างของ "เหตุการณ์ภัยคุกคามด้านความปลอดภัย" ทั้งหมด?

ก. การเปลี่ยนรหัสผ่านตามปกติ

ข. การติดมัลแวร์เรียกค่าไถ่ (Ransomware)

ค. การอัปเดตซอฟต์แวร์ประจำวัน

เฉลย: ข. การติดมัลแวร์เรียกค่าไถ่ (Ransomware)

7. "บทเรียนที่ได้" (Lessons Learned) ในวงจรการบริหารจัดการเหตุการณ์ภัยคุกคามมีความสำคัญอย่างไร?

ก. เพื่อลงโทษผู้ที่ทำให้ผิดพลาด

ข. เพื่อวิเคราะห์เหตุการณ์ที่เกิดขึ้น ระบุจุดอ่อน และปรับปรุงการรับมือในอนาคต

ค. เพื่อบันทึกข้อมูลสำหรับการฟ้องร้องทางกฎหมายเท่านั้น

เฉลย: ข. เพื่อวิเคราะห์เหตุการณ์ที่เกิดขึ้น ระบุจุดอ่อน และปรับปรุงการรับมือในอนาคต

8. หน้าที่หลักของ "ผู้รับมือต่อเหตุการณ์ภัยคุกคาม" (Incident Responder) คืออะไร?

ก. การตรวจสอบระบบความปลอดภัย, การสืบสวนเหตุการณ์, การควบคุมและกำจัดภัยคุกคาม

ข. การขายผลิตภัณฑ์รักษาความปลอดภัยใหม่ ๆ

ค. การออกแบบเว็บไซต์ขององค์กร

เฉลย: ก. การตรวจสอบระบบความปลอดภัย, การสืบสวนเหตุการณ์, การกักกันและกำจัดภัยคุกคาม

9. การ "กำจัด" (Eradication) ในแผนตอบสนองต่อเหตุการณ์ภัยคุกคาม หมายถึงอะไร?

ก. การลบข้อมูลทั้งหมดออกจากระบบ

ข. การนำภัยคุกคามออกจากระบบ เช่น มัลแวร์ หรือบัญชีที่ถูกบุกรุก

ค. การเปลี่ยนผู้ดูแลระบบทั้งหมด

เฉลย: ข. การนำภัยคุกคามออกจากระบบ เช่น มัลแวร์ หรือบัญชีที่ถูกบุกรุก

10. เหตุใดการทดสอบและฝึกซ้อมแผนรับมือเหตุการณ์ภัยคุกคามจึงมีความสำคัญ?

ก. เพื่อให้ทีมงานได้พักผ่อนจากการทำงานปกติ

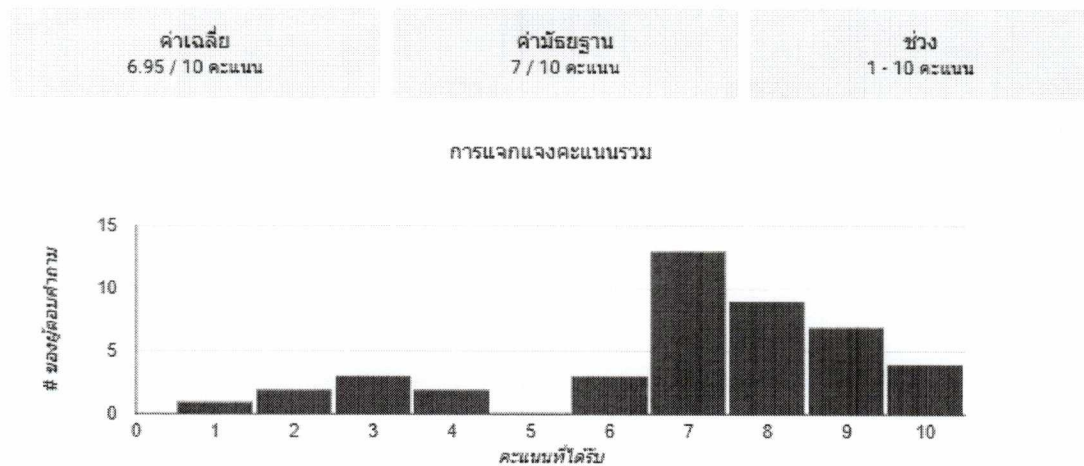
ข. เพื่อให้แน่ใจว่าแผนมีประสิทธิภาพและสมาชิกในทีมคุ้นเคยกับบทบาทหน้าที่ของตน

ค. เพื่อแสดงให้เห็นว่าองค์กรมีอุปกรณ์ที่ทันสมัย

เฉลย: ข. เพื่อให้แน่ใจว่าแผนมีประสิทธิภาพและสมาชิกในทีมคุ้นเคยกับบทบาทของตน

ผลการประเมินก่อนการฝึกอบรม (Pre Test)

จากการตอบคำถามก่อนการฝึกอบรม พบว่าผู้เข้าอบรมส่วนใหญ่ตอบคำถามได้อยู่ในช่วงคะแนน 7/10 ขึ้นไป ซึ่งสามารถวิเคราะห์ได้ว่าผู้เข้ารับการอบรมส่วนใหญ่ มีความรู้ความเข้าใจในเรื่องของ Cybersecurity Awareness พอสมควร ทั้งนี้ พบว่า ในข้อคำถามที่ 3 และ 6 พบการตอบผิดบ่อยครั้ง



ผลการประเมินภายหลังการฝึกอบรม (Post Test)

จากการตอบคำถามภายหลังการฝึกอบรม พบว่าผู้เข้าอบรมส่วนใหญ่ตอบคำถามได้อยู่ในช่วงคะแนน 10/10 ซึ่งสามารถวิเคราะห์ได้ว่าหลังจากผู้เข้ารับการอบรมผ่านการฝึกอบรม ทำให้มีความรู้ความเข้าใจในเรื่องของ Cybersecurity Awareness มากยิ่งขึ้น

