สำนักงานทะเบียนนักศึกษา
OFFICE OF THE REGISTRAR

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

หลักสูตร เตรียมความพร้อมสำหรับ

ระบบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

ตามแนวทาง ISO/IEC 27001

25 กรกฎาคม 2567, เวลา 9:30 - 16:00

สำนักงานทะเบียนนักศึกษา มหาวิทยาลัยธรรมศาสตร์

MYSURACHET.COM

Surachet Suchaiya, PhD.
Director of
Cyber Innovation Promotion
Association of Technology (CIPAT)

CIPAT

สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์

Cyber Innovation Promotion Association of Technology

Cyber Innovation Promotion Association of Technology

สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ลงนามความร่วมมือทางวิชาการ (MOU)กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

25
JUN 2024

by cpadmin | posted in: News | 0

เมื่อวันที่ 25 มิถุนายน พ.ศ. 2567 สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ลงนามความร่วมมือทางวิชาการ (MOU) กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดย พลอากาศตรีอมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ คุณอดิศร นิลวิสุทธิ์ นายกสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (CIPAT) นอกจากนั้น ยังมีพลตรีธีรวุฒิ วิทยากรณ์ รองเลขาธิการ สกมช. และ ดร.สุรเชษฐ์ สุชัยยะ ผู้อำนวยการสมาคม CIPAT ร่วมเป็นสักขีพยานในการลงนามความร่วมมือครั้งนี้

บันทึกความเข้าใจความร่วมมือทางวิชาการดังกล่าวมีวัตถุประสงค์ เพื่อสนับสนุนและส่งเสริมการพัฒนาทักษะความรู้และความตระหนักทราบต่อภัยคุกคามไซเบอร์จากการใช้เทคโนโลยีดิจิทัล ให้แก่ทุกภาคส่วน การพัฒนากำลังคนด้านความมั่นคงปลอดภัยไซเบอร์รวมถึงการส่งเสริมความร่วมมือทางวิชาการงานวิจัยตลอดจนโครงการพัฒนา นวัตกรรมและเทคโนโลยีต่างๆ

สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ลงนามความร่วมมือทางวิชาการ (MOU)กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

สกมช. ผนึกกำลังพันธมิตร เร่งผลิตบุคลากรผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

27 OCT 2023

by cpadmin | posted in: News | 0

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ผนึกกำลังพันธมิตร เร่งผลิตบุคลากรผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับ Cloud Security First ให้ได้ 10,000 คน ในปี 2567

เมื่อวันที่ 25 ตุลาคม 2566 พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นประธานในการประชุมหารือ การพัฒนาบุคลากรผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับ Cloud Security First ร่วมกับ นายอดิศร นิลวิสุทธิ์ นายกสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ ดร.สุรเชษฐ์ สุชัยยะ ผู้อำนวยการสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ และผู้แทนจาก บริษัท FORTINET SECURITY NETWORK (THAILAND) LTD. บริษัท GOOGLE (THAILAND) COMPANY LIMITED บริษัท หัวเว่ย เทคโนโลยี (ประเทศไทย) จำกัด และ EC-Council Global Services โดยเลขาธิการฯ ได้กล่าวต่อที่ประชุม ซึ่งมีใจความสำคัญตอนหนึ่งว่า "สกมช. ได้ตระหนักและเล็งเห็นถึงความสำคัญในการพัฒนาบุคลากรของประเทศด้าน Cloud Security และ Cloud Engineer และมีเป้าหมายไปสู่การสร้าง Cloud

CIPAT ร่วมกับคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และ พันธมิตรด้านเทคโนโลยี พัฒนาบุคลากรผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รองรับ Cloud Security First

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

CIPAT MOU สถาบันอุดมศึกษาเอกชนแห่งประเทศไทยฯ (สสอท.) และมหาวิทยาลัยเอกชน

20
APR 2023

by cpadmin | posted in: News | 0

เมื่อวันพฤหัสบดีที่ 20 เมษายน 2566 สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ CIPAT โดย คุณเอดิศร นิลวิสุทธิ์ อุปนายกสมาคม ลงนามความร่วมมือวิชาการ ร่วมกับ สถาบันอุดมศึกษาเอกชนแห่งประเทศไทยฯ (สสอท.) และมหาวิทยาลัยเอกชน สมาคมต่างๆ ลงนามบันทึกข้อตกลงความร่วมมือทางวิชาการ (MOU) ร่วมกับ คณะอนุกรรมการสาขาวิชาบริหารธุรกิจ สมาคมสถาบันอุดมศึกษาเอกชนแห่งประเทศไทยฯ กับ สมาคมดิจิทัลเพื่อการศึกษาไทย สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ สมาคมผู้สอบบัญชีภาษีอากรแห่งประเทศไทย สมาคมนักบัญชีไทย สมาคมการค้าส่ง-ปลีกไทย สมาคมเจ้าหน้าที่ความปลอดภัยในการทำงาน จังหวัดสมุทรปราการ บริษัท ศาลาแดง จำกัด บริษัท พี ยู ยู เอ็น อินเทลลิเจนท์ จำกัด และบริษัท เอด้า ซอฟท์ จำกัด ณ หอประชุม SBU Hall มหาวิทยาลัยเซาธ์อีสท์บางกอก

การลงนามบันทึกข้อตกลงความร่วมมือครั้งนี้ เพื่อพัฒนาและปรับปรุงกระบวนการเรียนการสอนให้ตรงกับความต้องการของอุตสาหกรรมอย่างต่อเนื่อง ในการสร้างผลงานทางวิชาการระหว่างคณะบัญชีและวิทยาการจัดการ กับ คณะอนุกรรมการสาขาวิชาบริหารธุรกิจ สมาคมสถาบันอุดมศึกษาเอกชนแห่งประเทศไทย ฯ เพื่อนำไปสู่การจัดกิจกรรมพัฒนานักศึกษาร่วมกัน เช่น การประกวด Startup, การสร้างบทเรียนออนไลน์ เพื่อพัฒนาการเรียนการสอน ที่ส่งเสริมการเรียนรู้โดยการลงมือปฏิบัติ (Active Learning) แนวความคิดใหม่ๆ การศึกษาเชิงบูรณาการและการเป็นผู้ประกอบการ เพื่อสร้างเครือข่ายและความสัมพันธ์อันดีกับองค์กรระดับประเทศและสากล




CIPAT MOU สถาบันอุดมศึกษาเอกชนแห่งประเทศไทยฯ (สสอท.) และมหาวิทยาลัยเอกชน

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

CIPAT MOU สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

16
FEB 2023

by cpadmin | posted in: News | 0

วันที่ 16 กุมภาพันธ์ 2566 ทางสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ หรือ CIPAT ได้ร่วมทำข้อตกลงความร่วมมือกับคณะวิศวกรรมศาสตร์โทรคมนาคม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยข้อตกลงความร่วมมือนี้จะนำไปสู่การพัฒนาบุคคลากรในสาขาที่ขาดแคลนทักษะใหม่ ไม่ว่าเป็นด้าน Cybersecurity ในกลุ่มอุตสาหกรรม ICS/OT และด้านอื่นในเชิงวิชาการอันเป็นประโยชน์สาธารณะต่อไป








CIPAT MOU สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

พิธีลงนามความร่วมมือ CIPAT กับ มหาวิทยาลัยศรีปทุม

16
NOV 2021

by cpadmin | posted in: News | 0

เมื่อวันที่ 15 พฤศจิกายน 2564 ที่ผ่านมา

จัดพิธีลงนามบันทึกข้อตกลงความร่วมมือทางวิชาการ (MOU) ผนึกกำลังร่วมมือกัน 3 องค์กร ระหว่าง คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม ร่วมกับ บริษัท โค้ดดิ้ง ฮับ จำกัด และ สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (CIPAT) ในรูปแบบออนไลน์ ผ่านโปรแกรม ZOOM โดยมี ผู้ช่วยศาสตราจารย์ ดร.วิรัช เลิศไพฑูรย์พันธ์ รองอธิการบดี พร้อมด้วยผู้ช่วยศาสตราจารย์ ดร.ธนา สุขวารี คณบดีคณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม ร่วมลงนามบันทึกข้อตกลงความร่วมมือ MOU ร่วมกับ นายจีรวุฒิ วงศ์พิมลพร CEO, Founder บริษัท โค้ดดิ้ง ฮับ จำกัด และ นายนนทวัตต์ สาระมาน นายกสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ CIPAT

โดยทาง CIPAT ร่วมมือด้านวิชาการ Cybersecurity for Business ที่ได้จัดทำร่วมกับมหาวิทยาลัยศรีปทุมอย่างต่อเนื่อง ในหลักสูตรบัณฑิตพันธุ์ใหม่ เป็นเวลา 3 รุ่น โดยได้รับเสียงตอบรับได้ดีมาโดยตลอด ในความร่วมมือกันนี้จะเป็นการสร้างสรรค์หลักสูตร Cybersecurity และโครงการที่เกิดขึ้นให้เป็นรูปธรรมยิ่งขึ้นต่อไปในอนาคต

CIPAT ร่วม MOU กับ มหาวิทยาลัยศรีปทุม

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

CIPAT ร่วมเปิดโครงการ หลักสูตร Cybersecurity for Online Business ในโครงการบัณฑิตพันธุ์ใหม่ (Non-degree) มหาวิทยาลัยศรีปทุม

27
SEP 2023

by cpadmin | posted in: News | 0

สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ CIPAT ร่วมเปิดโครงการ หลักสูตร Cybersecurity for Online Business เป็นการอบรมในโครงการบัณฑิตพันธุ์ใหม่ (Non-degree) โดยมี ผศ.ดร.ปราลี มณีรัตน์ รักษาการคณบดีคณะเทคโนโลยีสารสนเทศ และ ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง ที่ปรึกษาโครงการฯ ร่วมให้เกียรติต้อนรับผู้เข้าอบรม ที่ มหาวิทยาลัยศรีปทุม เมื่อวันที่ 24 กันยายน 2566 ที่ผ่านมา

สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ CIPAT ร่วมกับ Fortine

CIPAT ร่วมเปิดโครงการ หลักสูตร Cybersecurity for Online Business ในโครงการบัณฑิตพันธุ์ใหม่ (Non-degree) มหาวิทยาลัยศรีปทุม

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

พิธีบันทึกข้อตกลงความร่วมมือระหว่าง RMUTSB และ CIPAT

11
FEB 2021

by cpadmin | posted in: News | 0

ในวันที่ 10 กุมภาพันธ์ 2564 เวลา 16:30 ได้มีพิธีบันทึกข้อตกลงความร่วมมือเพื่อการพัฒนากำลังคนดิจิทัลด้านความมั่นคงปลอดภัยทางไซเบอร์
ระหว่าง คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ
กับ สมาคมสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ CIPAT

เพื่อส่งเสริมและสนับสนุนการยกระดับความรู้และทักษะการใช้เทคโนโลยีดิจิทัลพื้นฐานที่จำเป็นและการใช้เทคโนโลยีดิจิทัลขั้นสูง ให้แก่ นิสิต นักศึกษา
ครู อาจารย์ รวมทั้งบุคลากรทั้งภายในและภายนอกของ RMUTSB ให้สามารถในการใช้งานเทคโนโลยีดิจิทัลได้อย่างมีประสิทธิภาพในระดับมาตรฐาน

CIPAT MOU กับ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

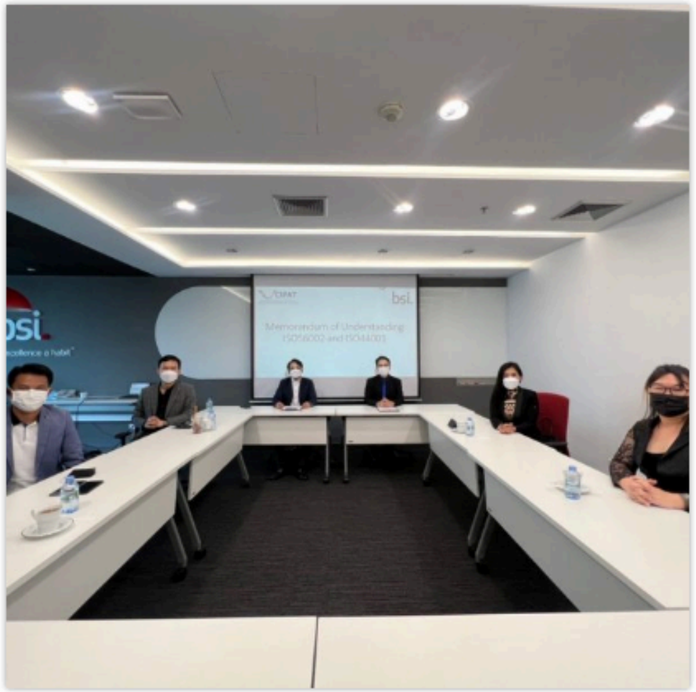
CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

สมาคม CIPAT ร่วม MOU กับบริษัท BSI

17
MAY 2022

by cpadmin | posted in: News | 0

เมื่อวันที่ 17 พฤษภาคม 2565 การลงนามความร่วมมือระหว่างสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (CIPAT) กับสถาบันมาตรฐานอังกฤษ (ประเทศไทย) หรือ BSI เพื่อการส่งเสริมและขับเคลื่อนมาตรฐานสากลด้านนวัตกรรม (ISO56002) และระบบการจัดการความมือทางธุรกิจ (ISO44001) โดยมีท่านนายกสมาคม คุณเนนทวัตต์ สาระมาน และกรรมการบริหาร ร่วมงาน



CIPAT ร่วม MOU กับบริษัท BSI Group สถาบันมาตรฐานอังกฤษ

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MOU ระหว่าง CIPAT กับ Fortinet บริษัทชั้นนำด้านความปลอดภัย

อ่านรายละเอียด

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ CIPAT ร่วมกับ Fortinet ประเทศไทย ดอบรมเชิงปฏิบัติการ ในหลักสูตร Fortinet Network Security

4
OCT 2023

by cpadmin | posted in: News | 0

สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ CIPAT ร่วมกับ Fortinet ประเทศไทย ในการขับเคลื่อนการพัฒนากำลังคน ด้าน Cybersecurity จัดอบรมเชิงปฏิบัติการ ในหลักสูตร Fortinet Network Security ให้กับน้องๆที่กำลังจะจบการศึกษาสู่ตลาดงาน ที่ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง KMITL

สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ CIPAT ร่วมกับ Fortinet ประเทศไทย อบรมเชิงปฏิบัติการ ในหลักสูตร Fortinet Network Security

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MOU ระหว่าง CIPAT กับ TRIS ในการจัดทำงานวิชาการและที่ปรึกษากฎหมาย PDPA

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Surachet Suchaiya, PhD.

ประวัติการศึกษา ประวัติการทำงาน ความเชี่ยวชาญ ประสบการณ์ ประกาศนียบัตรการฝึกอบรมที่ได้รับ และงานวิจัยของอาจารย์

หลักสูตร เตรียมความพร้อมสำหรับระบบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

Agenda

1. ภัยคุกคามทางไซเบอร์ในยุค **AI**
2. ประเภทของภัยคุกคาม
3. กรณีศึกษาภัยคุกคามทางไซเบอร์ที่สร้างผลกระทบต่อระบบเศรษฐกิจ
4. การสร้างมั่นคงปลอดภัยระบบสารสนเทศตามแนวทาง **ISO/IEC 27001**
5. กลยุทธ์ความพร้อมรับมือภัยไซเบอร์
6. บทบาทหน้าที่และการมีส่วนร่วม
7. **Workshop**
8. สรุปและตอบคำถาม

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

1 ภัยคุกคามทางไซเบอร์ในยุค AI

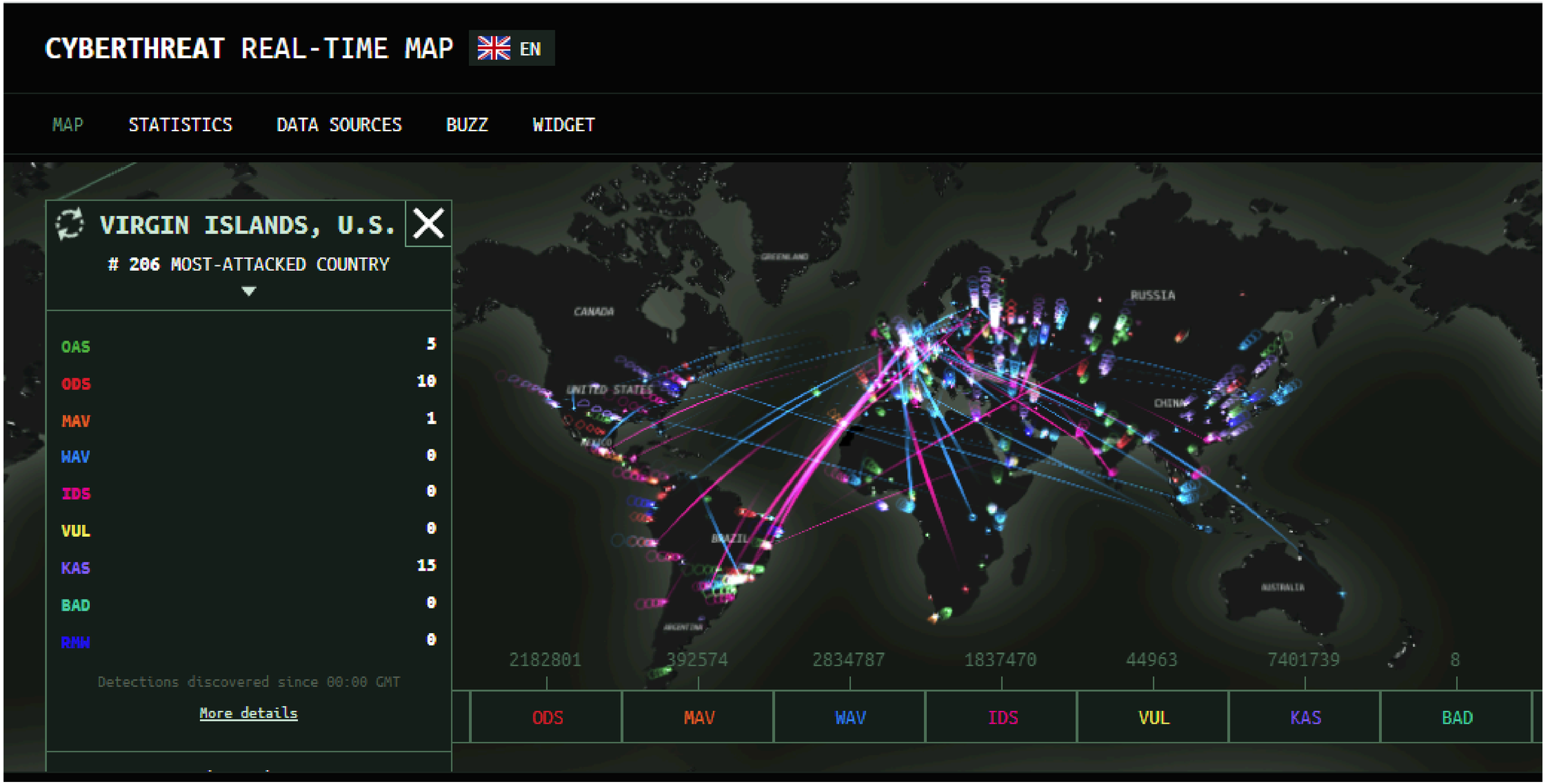
CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

1 ภัยคุกคามทางไซเบอร์ในยุค AI

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

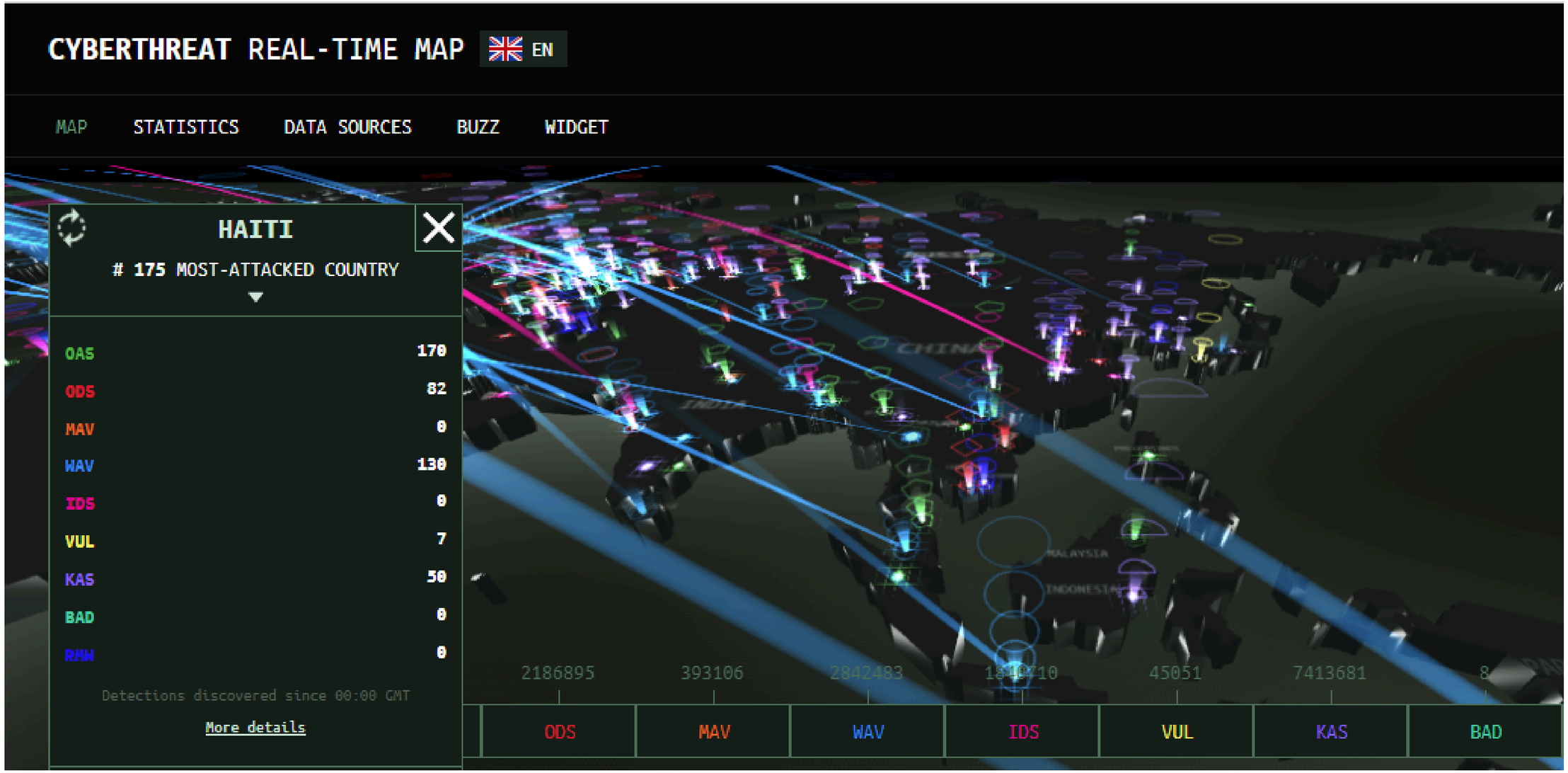
MYSURACHET.COM



1 ภัยคุกคามทางไซเบอร์ในยุค AI

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

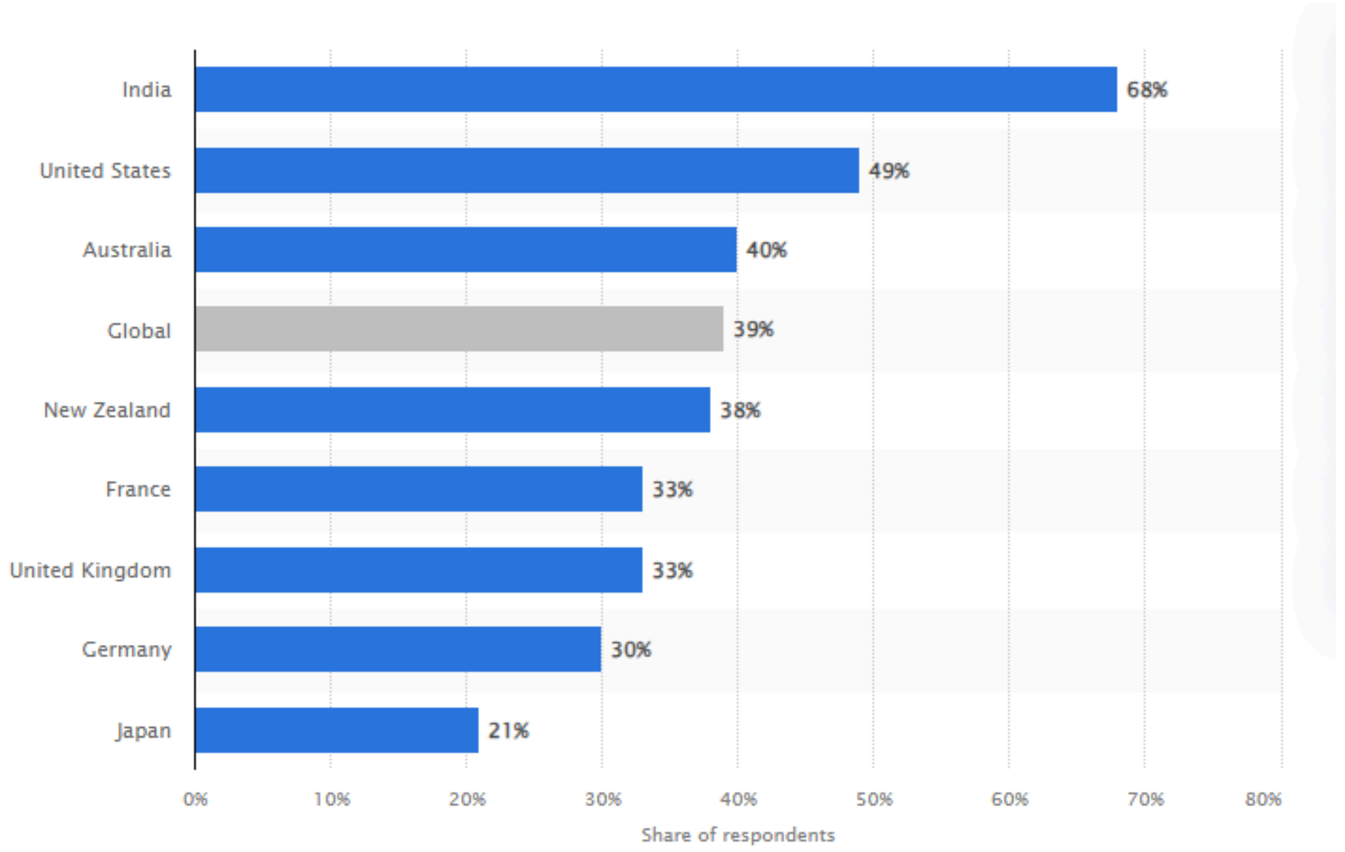
MYSURACHET.COM



1 ภัยคุกคามทางไซเบอร์ในยุค **AI : Economic Review**

แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์

Percentage of internet users in selected countries who have ever experienced any cybercrime in 2022



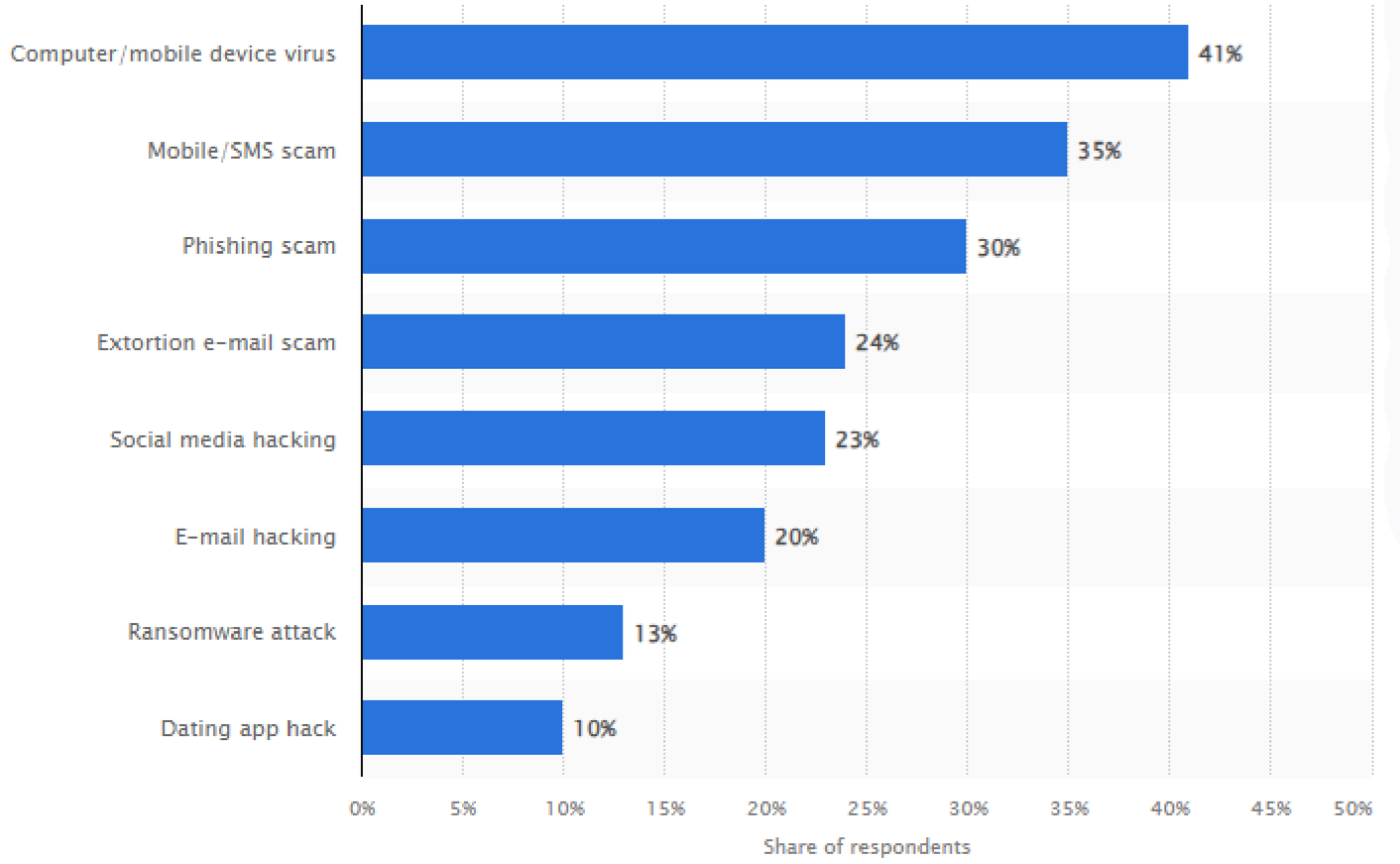
CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลจาก https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

1 ภัยคุกคามทางไซเบอร์ในยุค AI : Economic Review

แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์

Share of adults worldwide who have experienced cyber crime as of January 2023

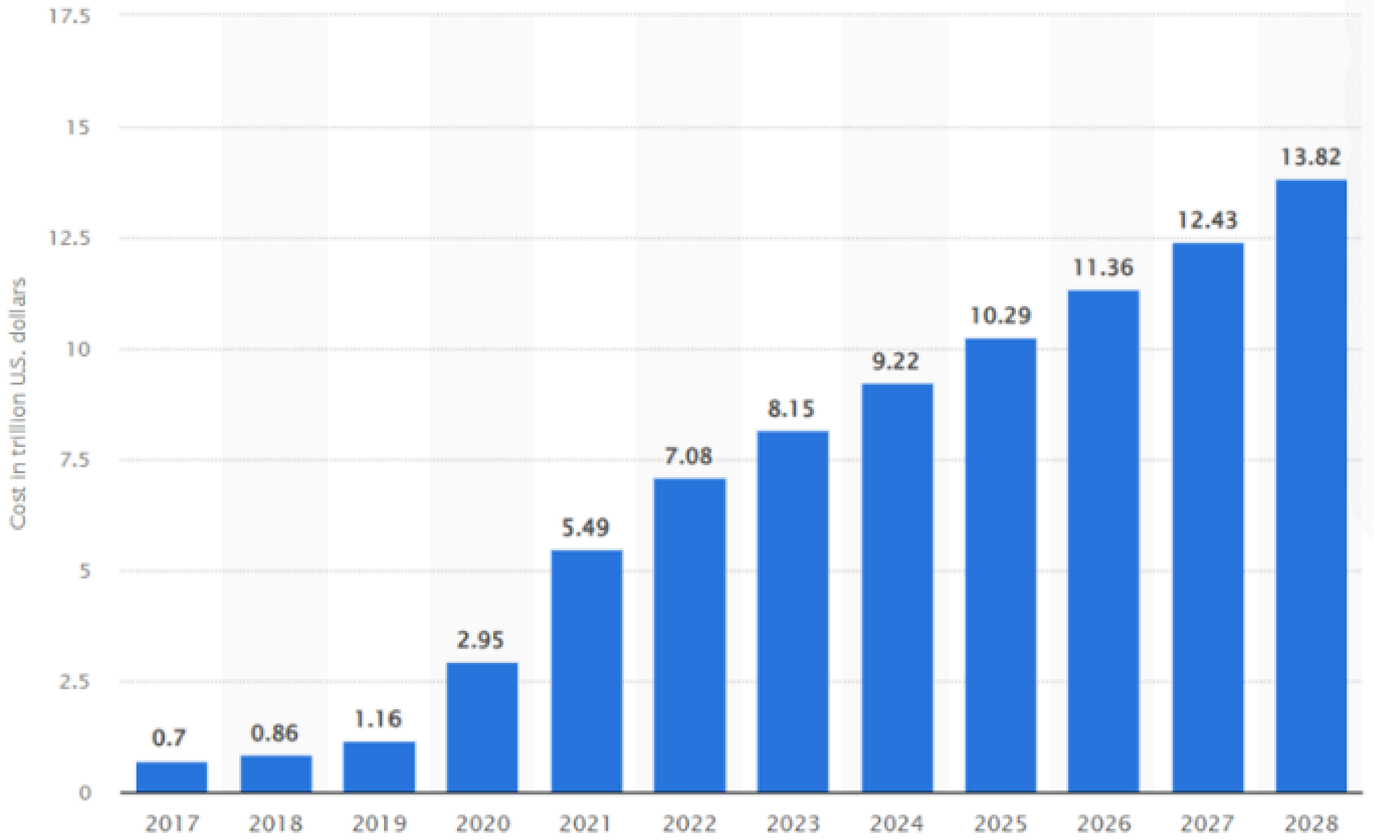


ข้อมูลจาก https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

1 ภัยคุกคามทางไซเบอร์ในยุค **AI : Economic Review**

แนวโน้มและอันตรายที่เกิดขึ้นจากภัยคุกคามทางโลกไซเบอร์

Estimated cost of cybercrime worldwide 2017-2028(in trillion U.S. dollars)



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลจาก https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

1 ภัยคุกคามทางไซเบอร์ในยุค **AI : Economic Review**

งบประมาณด้านความมั่นคงปลอดภัยไซเบอร์แต่ละประเทศ

Percentage of IT budget allocated to security, by country.

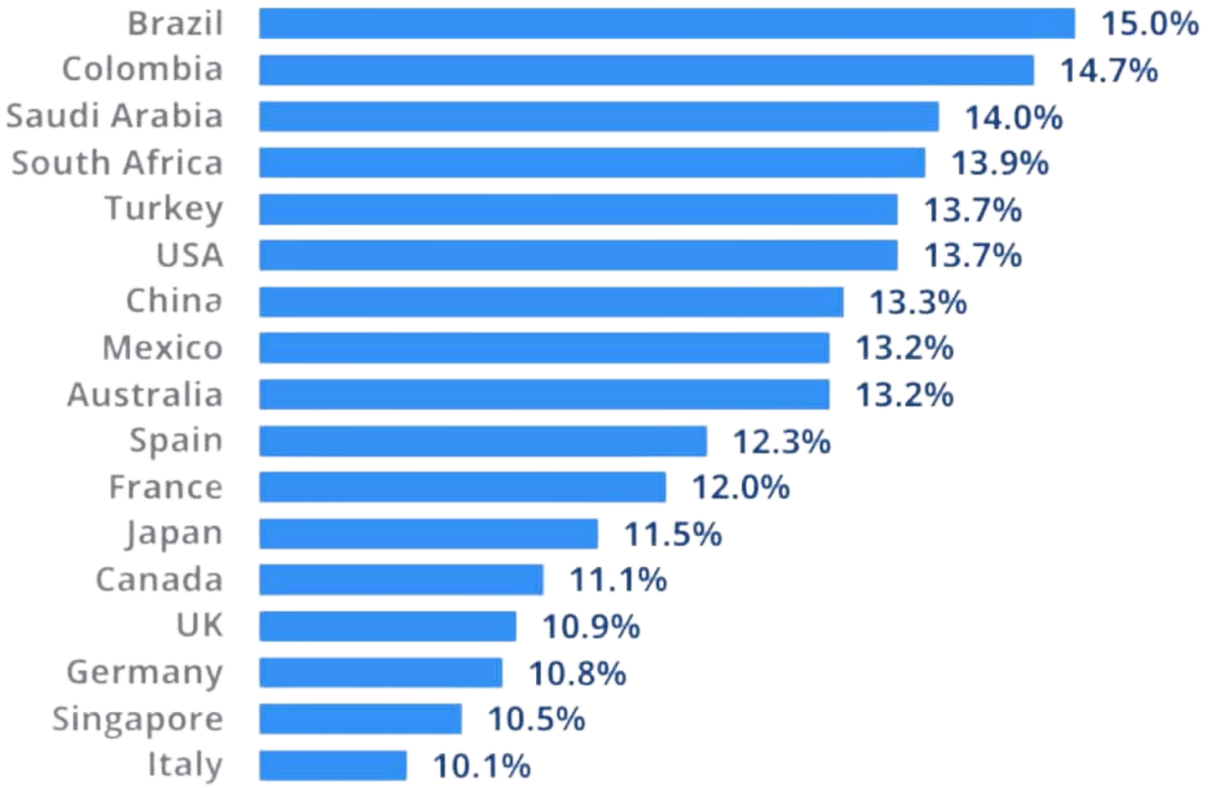


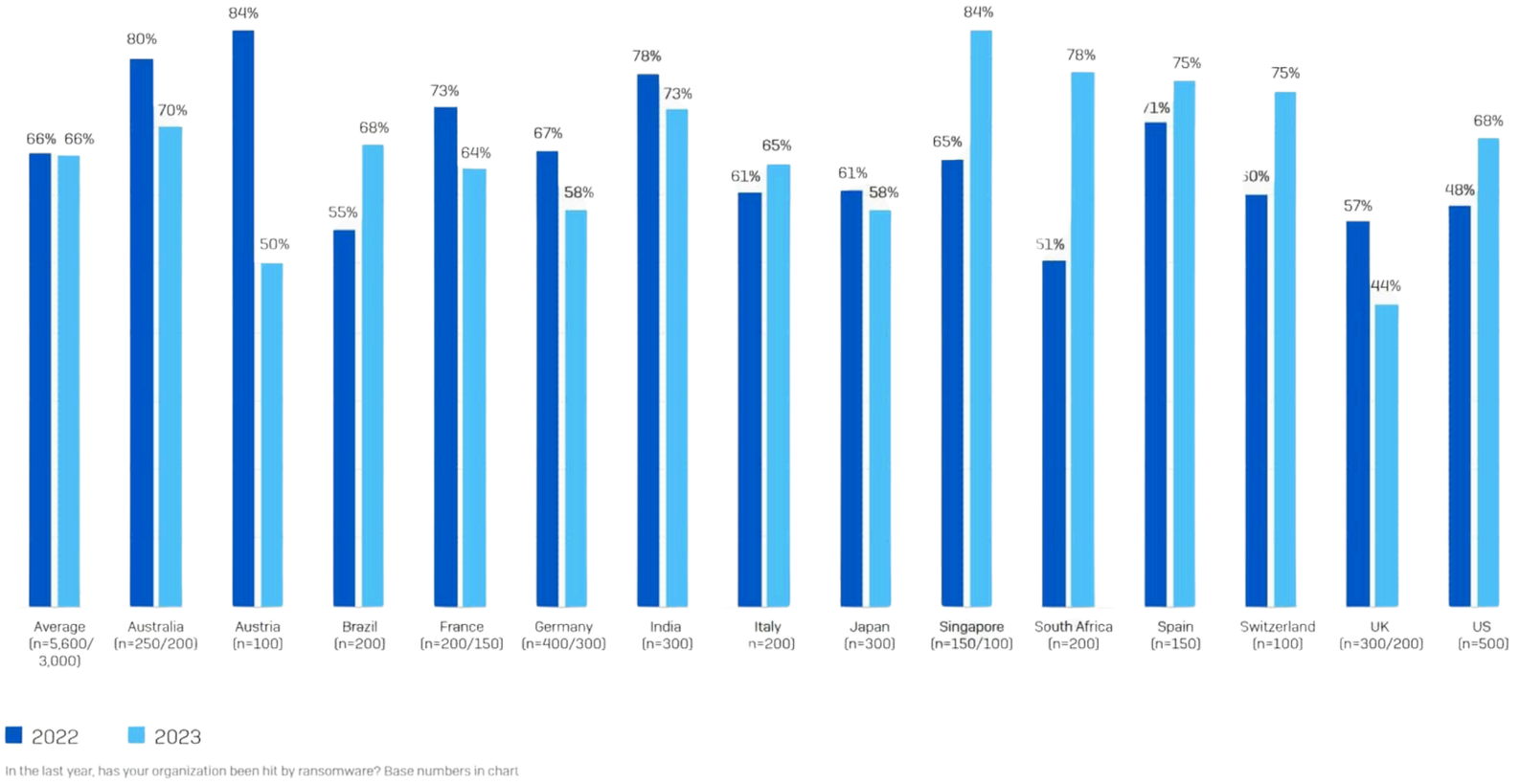
Figure 24: Percentage of IT budget allocated to security, by country.

ข้อมูลจาก https://www.comparitech.com/blog/information-security/italy-cyber-security-statistics/

1 ภัยคุกคามทางไซเบอร์ในยุค **AI : Economic Review**

อัตราการโจมตีจากการเรียกค่าไถ่ข้อมูลในปี **2022** และ ปี**2023**

Rate of Ransomware Attacks by Country : 2022 vs 2023



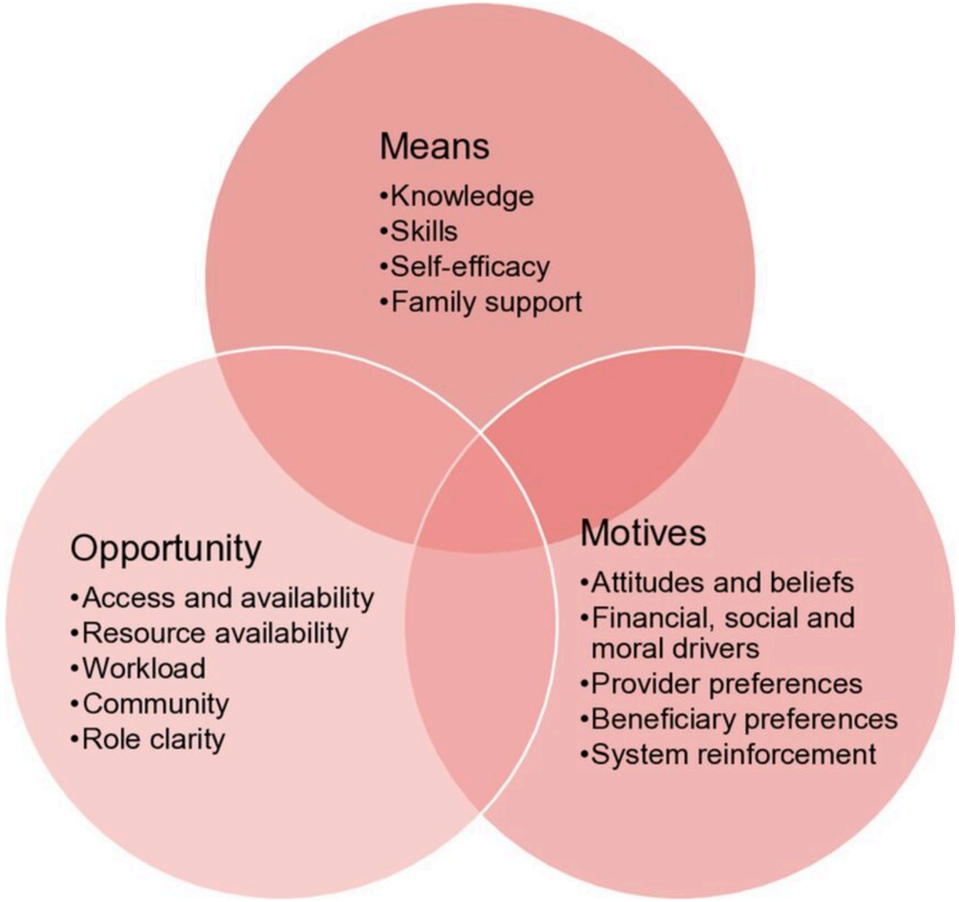
In the last year, has your organization been hit by ransomware? Base numbers in chart

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลจาก https://www.comparitech.com/blog/information-security/italy-cyber-security-statistics/

1 ภัยคุกคามทางไซเบอร์ในยุค AI : Economic Review

ปัจจัยที่ก่อให้เกิดอาชญากรรมทางไซเบอร์ (Cyber Crime)

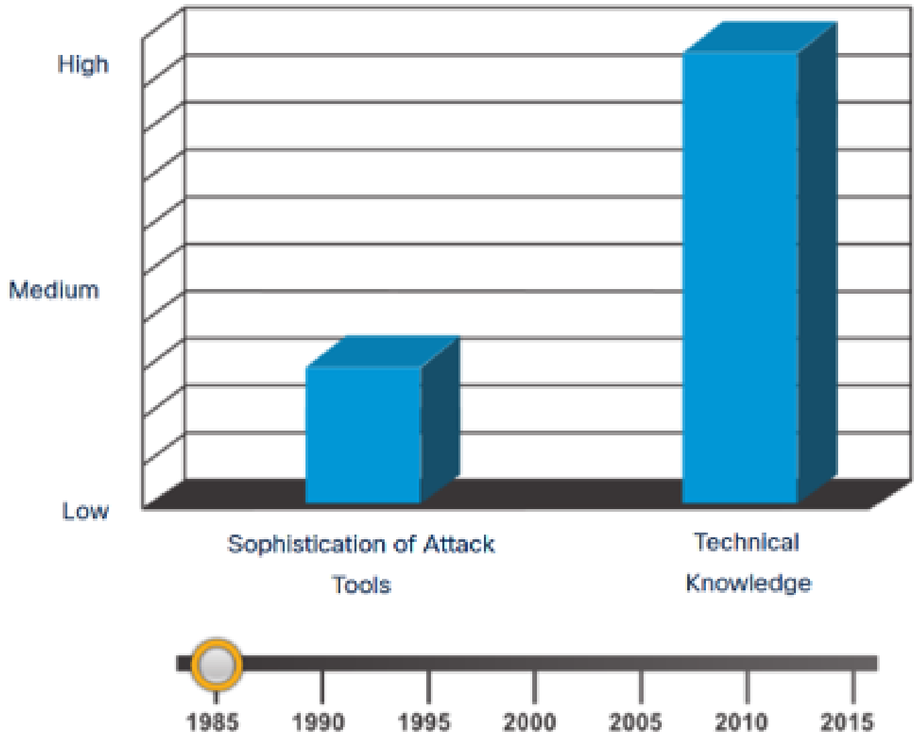


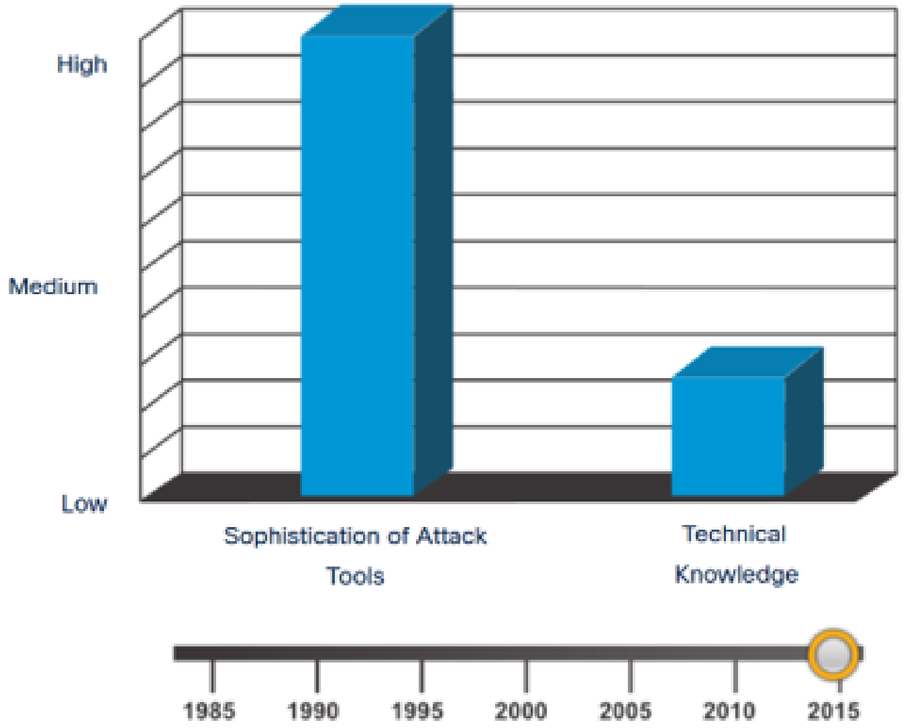
CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลจาก https://www.secnia.go.th/2018/07/21/เครือข่ายสาธารณสุขสิงตโปร์/

1 ภัยคุกคามทางไซเบอร์ในยุค AI

Attack Tools (เครื่องมือที่ใช้ในการโจมตี)





CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

2 ประเภทของภัยคุกคาม

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

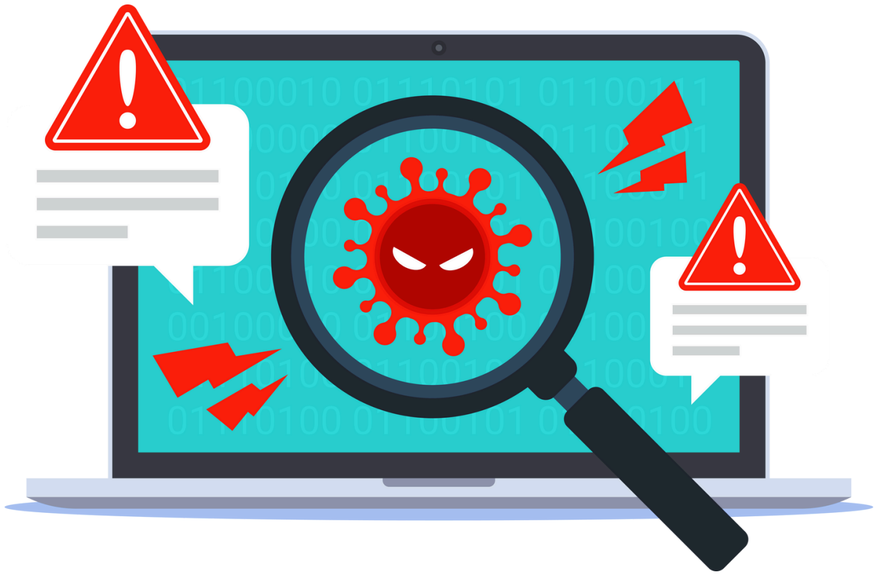
MYSURACHET.COM

Threat Landscape

2 ประเภทของภัยคุกคาม

1.Malware (มัลแวร์)

- **Virus:** โค้ดที่แฝงตัวในโปรแกรมอื่นๆ และแพร่กระจายไปยังโปรแกรมอื่นๆ เมื่อถูกเรียกใช้งาน
- **Worms:** มัลแวร์ที่แพร่กระจายไปทั่วเครือข่ายโดยไม่ต้องพึ่งพาโฮสต์โปรแกรม
- **Trojans:** มัลแวร์ที่ปลอมตัวเป็นซอฟต์แวร์ที่ไม่เป็นอันตราย แต่ทำการโจมตีเมื่อถูกติดตั้ง
- **Ransomware:** มัลแวร์ที่เข้ารหัสไฟล์ของผู้ใช้และเรียกค่าไถ่เพื่อปลดล็อกไฟล์
- **Spyware:** มัลแวร์ที่คอยสอดส่องและเก็บข้อมูลของผู้ใช้โดยไม่ได้รับอนุญาต



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

2

ประเภทของภัยคุกคาม

2.Phishing (ฟิชชิ่ง)

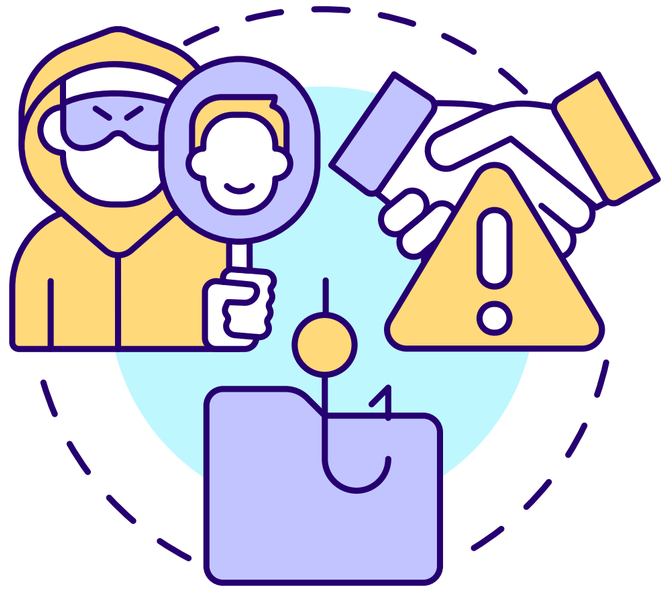
- การส่งอีเมลหรือข้อความที่ปลอมแปลงเป็นแหล่งข้อมูลที่น่าเชื่อถือเพื่อหลอกให้ผู้ใช้เปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่านหรือข้อมูลบัตรเครดิต

2

ประเภทของภัยคุกคาม

3.Social Engineering (วิศวกรรมสังคม)

- การใช้วิธีทางจิตวิทยาในการหลอกลวงบุคคลให้เปิดเผยข้อมูลที่เป็นความลับหรือดำเนินการที่ไม่ปลอดภัย



2 ประเภทของภัยคุกคาม

4.Denial of Service (DoS) and Distributed Denial of Service (DDoS)

- การโจมตีที่พยายามทำให้บริการออนไลน์ไม่สามารถให้บริการได้โดยการส่งปริมาณการใช้งานจำนวนมากไปยังเซิร์ฟเวอร์เป้าหมาย

2 ประเภทของภัยคุกคาม

5.Advanced Persistent Threats (APTs)

- การโจมตีที่พยายามทำให้บริการออนไลน์ไม่สามารถให้บริการได้โดยการส่งปริมาณการใช้งานจำนวนมากไปยังเซิร์ฟเวอร์เป้าหมาย

2 ประเภทของภัยคุกคาม

6.Insider Threats (ภัยคุกคามจากคนในองค์กร)

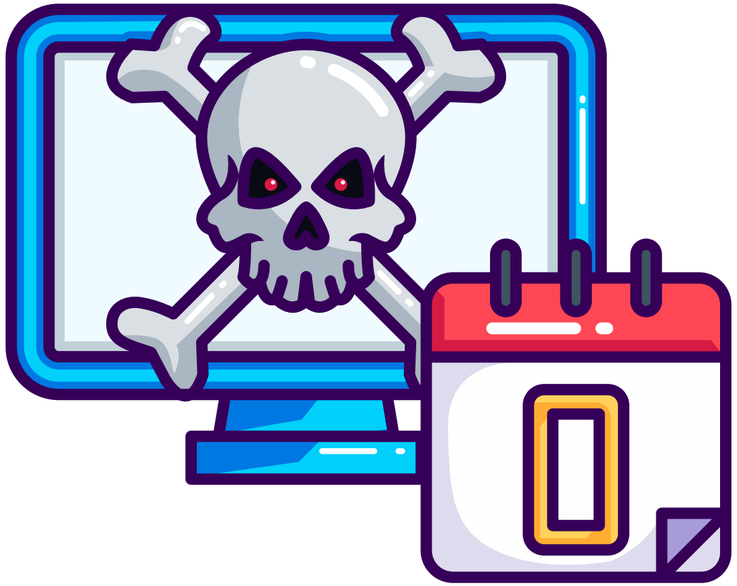
- การคุกคามที่มาจากบุคคลภายในองค์กร เช่น พนักงานที่มีความประสงค์ร้ายหรือทำการกระทำที่ไม่ปลอดภัยโดยไม่ได้ตั้งใจ

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

2 ประเภทของภัยคุกคาม

7.Zero-Day Exploits

- การโจมตีที่ใช้ช่องโหว่ที่ยังไม่มีการแก้ไขหรือประกาศต่อสาธารณะ ซึ่งทำให้การป้องกันเป็นไปได้ยาก ผู้บริหารด้านความมั่นคงปลอดภัยควรมีการแลกเปลี่ยนข้อมูลกับหน่วยงานที่ดูแลด้านความมั่นคงปลอดภัย เช่น **Thai CERT , CSIRT** ของหน่วยงานต่างๆ เพื่อทราบถึงภัยคุกคามเป็นต้น



2 ประเภทของภัยคุกคาม

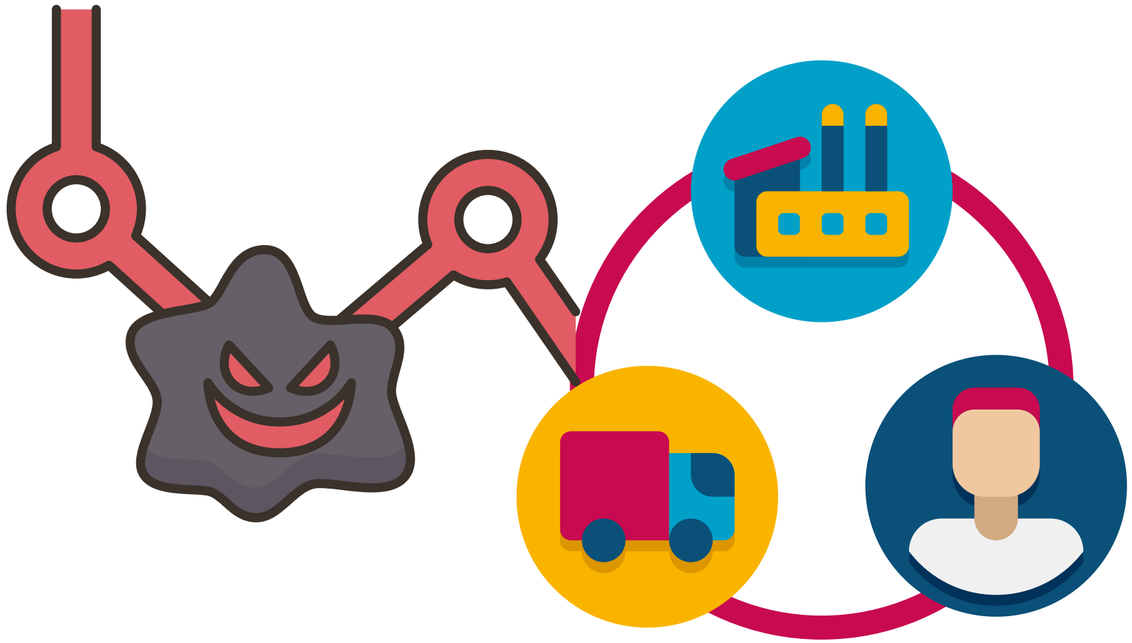
8.IoT Attacks (การโจมตีอุปกรณ์ IoT : Internet of Things)

- การโจมตีที่มุ่งเป้าไปยังอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ต เช่น กล้องวงจรปิด, อุปกรณ์สมาร์ทโฮม, ระบบ **OT (Operational Technology)**ในภาคอุตสาหกรรม, ระบบ **Automation System**, อุปกรณ์ **PLC**, ระบบ **SCADA**, ระบบ **Industrial Internet of Things**

2 ประเภทของภัยคุกคาม

9.Supply Chain Attacks (การโจมตีห่วงโซ่อุปทาน)

- การโจมตีที่มุ่งเป้าไปที่ผู้ให้บริการหรือซัพพลายเออร์เพื่อเข้าถึงระบบขององค์กรผ่านการโจมตีช่องโหว่ในห่วงโซ่อุปทาน



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

2 ประเภทของภัยคุกคาม

10.Cryptojacking (การใช้ทรัพยากรของผู้อื่นในการขุดคริปโต)

- การใช้ทรัพยากรของคอมพิวเตอร์ของผู้อื่นเพื่อขุดคริปโตเคอร์เรนซีโดยไม่ได้รับอนุญาต

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

3

กรณีศึกษาภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

3 ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่1

SingHealth ถูกโจมตีทางไซเบอร์ กรกฎาคม **2018**
โจรกรรมข้อมูลผู้ป่วย **1.5**ล้านคน

SingHealth

Defining Tomorrow's Medicine

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลจาก https://www.secnia.go.th/2018/07/21/เครือข่ายสาธารณสุขสิงตโปร์/

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่1

SingHealth ถูกโจมตีทางไซเบอร์ กรกฎาคม **2018**
โจรกรรมข้อมูลผู้ป่วย **1.5**ล้านคน

SingHealth
Defining Tomorrow's Medicine

รูปแบบการโจมตี

- **Hacker** ใช้ **Advanced Persistent Threat (APT)** โจมตี **Front-End Workstation** เพื่อเข้าสู่ฐานข้อมูลกลาง
- **Hacker** มีเจตนาขโมยข้อมูลนายกรัฐมนตรีสิงคโปร์ ('ลี เซียนลุง')

ผลกระทบ
ข้อมูลผู้ป่วยราว **1.5**ล้านคน ที่เคยเข้ารับบริการที่ **Specialist Outpatient Clinics** และ **Polyclinics** ของ **SingHealth** ตั้งแต่ **1** พฤษภาคม **2015** ถึง **4** กรกฎาคม **2018** ถูกขโมยข้อมูล **Demographic (ID Card,** ชื่อ ที่อยู่ เพศ วันเกิด)

- ถูกขโมยข้อมูลการสั่งยาจาก **OPD**

ข้อมูลจาก https://www.secnia.go.th/2018/07/21/เครือข่ายสาธารณสุขสิงตโปร์/

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่1

ตัวอย่าง **Advanced Persistent Threat (APT)** แยกตามประเทศ

Suspected attribution	APT	Target sectors
Iran	APT33-34,39	The travel industry and IT firms that support it and the high-tech industry,military,commercial
China	APT1-8,10-27,30-31,40-41	government, international financial organization, and aerospace and defense organizations, as well as high tech, construction and engineering, telecommunications, media, and insurance.
North Korea	APT37-38	industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

3 ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่2

กฟภ. ถูกโจมตีทางไซเบอร์ด้วยมัลแวร์เรียกค่าไถ่
จนต้องปิดให้บริการระบบหลายวัน มิถุนายน 2020

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.nia.go.th/cyber/cyberpage/89/

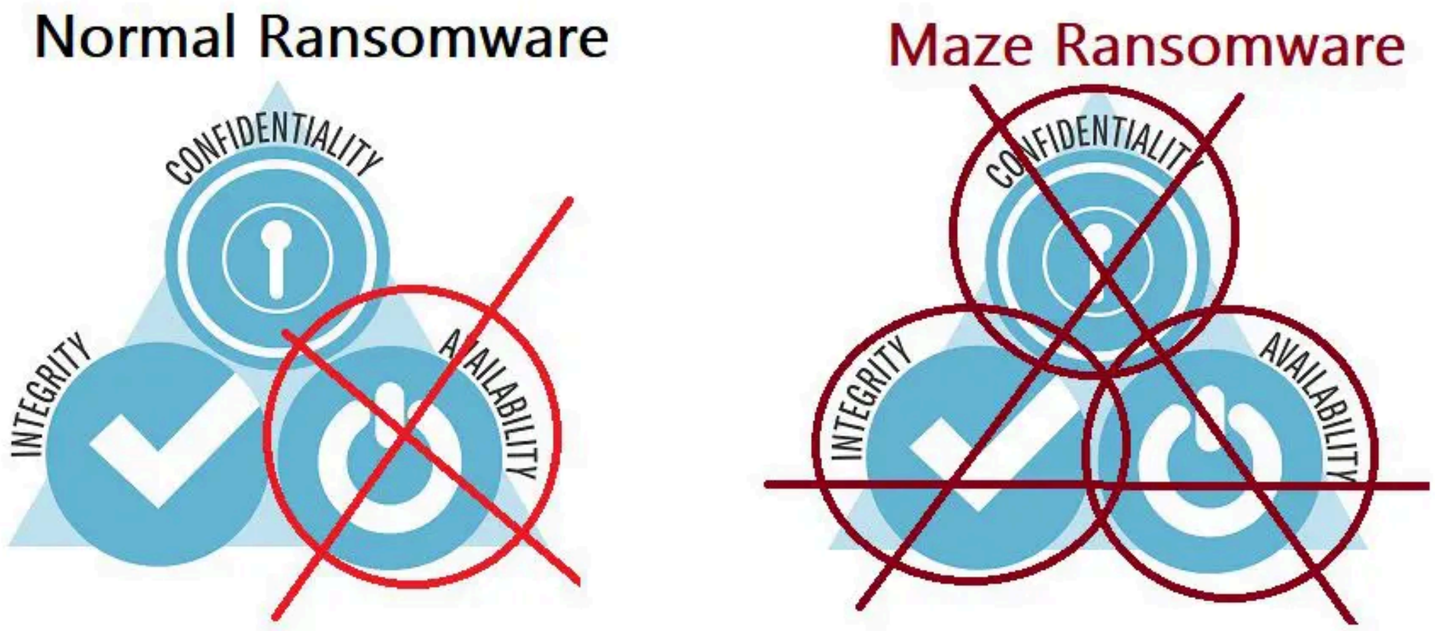
3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่2

กฟภ. ถูกโจมตีทางไซเบอร์ด้วยมัลแวร์เรียกค่าไถ่
จนต้องปิดให้บริการระบบหลายวัน มิถุนายน **2020**

Maze Ransomware Triple Threat



ข้อมูลอ้างอิง https://www.nia.go.th/cyber/cyberpage/89/

3 ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่2

กฟภ. ถูกโจมตีทางไซเบอร์ด้วยมัลแวร์เรียกค่าไถ่ จนต้องปิดให้บริการระบบหลายวัน มิถุนายน 2020

ความเสียหาย

- ไฟล์ถูกบีบอัดและเข้ารหัสเพื่อเรียกค่าไถ่ไฟล์
- **Hacker** เผยแพร่ข้อมูลที่ขโมยมาในโลกออนไลน์

ประชาชนผู้รับบริการได้รับผลกระทบจากการโจมตีทางไซเบอร์ดังนี้

- ต้องปิดระบบเทคโนโลยีสารสนเทศบางส่วน ชั่วคราว
- ปิดบริการระบบชำระค่าบริการแบบออนไลน์ ชั่วคราว
- ปิดบริการแอปพลิเคชัน **PEA Smart Plus** ชั่วคราว

ข้อมูลอ้างอิง https://www.nia.go.th/cyber/cyberpage/89/

3 ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่3

JBS Foods ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**
REvil Ransomware เรียกค่าไถ่ไฟล์

ข้อมูลอ้างอิง https://claroty.com/blog/jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test/

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่3

JBS Foods ถูกโจมตีทางไซเบอร์ พฤษภาคม 2021

JBS Foods ดำเนินธุรกิจเกี่ยวกับแปรรูปเนื้อสัตว์รายใหญ่ที่สุดในโลก ส่งออกเนื้อสัตว์จากบราซิลไปยังสหรัฐอเมริกา มีพนักงาน **230,000**คน ยอดขายมากกว่า **5,200**ล้าน**USD.**

รูปแบบการโจมตี

- **Hacker** ใช้ **REvil Ransomware** เพื่อล๊อคการเข้าถึงระบบของบริษัท เหตุการณ์นี้เกิดขึ้นกว่า **1** เดือน ทำให้ธุรกิจของ **JBS Foods** หยุดชะงัก

ผลกระทบ

- **JBS** ต้องปิดโรงงานหลายแห่งทั่วโลก
- การส่งสินค้าเนื้อสัตว์ล่าช้าหรือหยุดชะงัก
- ราคาเนื้อสัตว์ทั่วโลกเพิ่มสูงขึ้น
- **JBS** สูญเสียรายได้และเสียชื่อเสียง

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://claroty.com/blog/jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test/

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่3

JBS Foods ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**

การตอบสนอง

- **JBS** ตัดสินใจจ่ายค่าไถ่ จำนวน **11** ล้าน**USD** ให้กับกลุ่ม **REvil**
- **JBS** ประสานไปยังหน่วยงานรัฐบาลหลายประเทศร่วมมือกันสืบสวนหาตัวผู้ก่อการ
- เหตุการณ์นี้สร้างความกังวลเกี่ยวกับความมั่นคงทางอาหาร

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://claroty.com/blog/jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test/

3 ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่4

CNA Financial ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**
REvil Ransomware เรียกค่าไถ่ไฟล์

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.insurancejournal.com/news/national/2021/11/29/643569.htm

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่4

CNA Financial ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**

CNA เป็นบริษัทประกันภัยรายใหญ่ในสหรัฐอเมริกา มีพนักงาน **4,500**คน ยอดขายมากกว่า **7,000**ล้าน**USD.**

รูปแบบการโจมตี

- **Hacker** ใช้ **REvil Ransomware** เพื่อล๊อคการเข้าถึงระบบของบริษัท และข้อมูลสำคัญของบริษัท

ผลกระทบ

- **CNA Financial** ต้องหยุดการดำเนินงานบางส่วน
- ลูกค้าของ **CNA Financial** ไม่สามารถเข้าถึงข้อมูลประกันภัยของตน
- บริษัทต้องสูญเสียรายได้และเสียชื่อเสียง

CNA

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.insurancejournal.com/news/national/2021/11/29/643569.htm

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่4

CNA Financial ถูกโจมตีทางไซเบอร์ พฤษภาคม **2021**

การตอบสนอง

- **CNA** ตัดสินใจจ่ายค่าไถ่ จำนวน **40** ล้าน**USD** ให้กับกลุ่ม **REvil**
- **CNA** ประสานไปยังหน่วยงานรัฐบาลหลายประเทศร่วมมือกันสืบสวนหาตัวผู้ก่อการ
- เหตุการณ์นี้สร้างความกังวลเกี่ยวกับความเชื่อมั่น และ ความมั่นคงทางการเงิน

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.insurancejournal.com/news/national/2021/11/29/643569.htm

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่5

Kaseya VSA ถูกโจมตีทางไซเบอร์ กรกฎาคม **2021**

ข้อมูลอ้างอิง https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่5

Kaseya VSA ถูกโจมตีทางไซเบอร์ กรกฎาคม 2021

Kaseya VSA ดำเนินธุรกิจเกี่ยวกับให้บริการซอฟต์แวร์ควบคุมระบบระยะไกล **(Remote Monitoring and Management - RMM)**

กรกฎาคม **2021 Kaseya VSA** ถูก **Hacker** กลุ่ม **REvil** โจมตีช่องโหว่

รูปแบบการโจมตี

- แทรก **code** อันตรายในช่องโหว่ของ **Kaseya VSA** เพื่อควบคุมระบบคอมพิวเตอร์ของลูกค้าที่ใช้บริการ
- ใช้คอมพิวเตอร์ของลูกค้าที่ถูกควบคุมกระจาย **REvil Ransomware** เข้ารหัสไฟล์ข้อมูลเพื่อเรียกค่าไถ่

การตอบสนอง

- เมื่อถูกโจมตีทาง **Kaseya** ปิดระบบ **Server** ของตัวเองทั้งหมด
- แจ้งให้ลูกค้าที่ใช้งาน **VSA** แบบ **On-Premise** ปิด **Server** ด้วยเช่นกัน

ข้อมูลอ้างอิง https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่5

Kaseya VSA ถูกโจมตีทางไซเบอร์ กรกฎาคม **2021**

ผลกระทบ

- ส่งผลกระทบต่อองค์กรทั่วโลกมากกว่า **1,000** แห่ง ถูกเข้ารหัสไฟล์
- สร้างความเสียหายทางการเงินและชื่อเสียงของ **Kaseya VSA** และองค์กรที่ถูกโจมตี

การตอบสนอง

- เมื่อถูกโจมตีทาง **Kaseya** ปิดระบบ **Server** ของตัวเองทั้งหมด
- แจ้งให้ลูกค้าที่ใช้งาน **Kaseya** แบบ **On-Premise** ปิด **Server** ด้วยเช่นกัน
- **Kaseya** ไม่ได้จ่ายค่าไถ่ไฟล์ สามารถถอดรหัสและกู้คืนระบบได้
- **Kaseya update software** เพื่อแก้ไขช่องโหว่
- **Kaseya** ประสานไปยังหน่วยงานของรัฐบาลหลายประเทศ เพื่อร่วมมือกันสืบสวนหาตัวผู้ก่อการในครั้งนี้

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

3 ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่6

ข้อมูลคนไข้ในระบบสาธารณสุขรั้วไหล กันยายน 2021

ข้อมูลอ้างอิง https://www.hfocus.org/content/2024/03/30032

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่6

ข้อมูลคนไข้ในระบบสาธารณสุขรั้วไหล กันยายน 2021

วันที่ 6 กันยายน 2564 มีรายงานข้อมูลพื้นฐานของคนไข้ในระบบสาธารณสุขรั้วไหลกว่า ล้านรายชื่อ

รูปแบบการโจมตี

- แฮกเกอร์โจมตีระบบฐานข้อมูลของโรงพยาบาล เป็นไปได้ทั้งรัฐ-เอกชน
- ขโมยข้อมูลคนไข้กว่า ล้านรายชื่อ
- ข้อมูลที่ถูกขโมย ได้แก่ ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ วันเดือนปีเกิด ชื่อแพทย์เจ้าของไข้ และชื่อโรงพยาบาล

ผลกระทบ

- ผู้ป่วยมีความเสี่ยงต่อการถูกแฮกข้อมูลส่วนบุคคล
- อาจถูกนำไปใช้เพื่อหลอกลวง หรือทำธุรกรรมที่ผิดกฎหมาย
- เสียชื่อเสียงต่อระบบสาธารณสุข
- สร้างความกังวลให้กับประชาชน

ข้อมูลอ้างอิง https://www.hfocus.org/content/2024/03/30032

3

ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

การก่ออาชญากรรมทางไซเบอร์ กรณีศึกษาที่6

ข้อมูลคนไข้ในระบบสาธารณสุขรั้วไหล กันยายน 2021

วันที่ 6 กันยายน 2564 มีรายงานข้อมูลพื้นฐานของคนไข้ในระบบสาธารณสุขรั้วไหลกว่าล้านรายชื่อ

การตอบสนอง

- สธ.-สกมช. ยอมรับว่ามีข้อมูลรั่วไหล เป็นไปได้ทั้งรัฐ-เอกชน
- สั่งปิดระบบฐานข้อมูลที่ถูกโจมตี
- แจ้งความดำเนินคดีกับผู้กระทำผิด
- ตั้งคณะกรรมการสอบสวนหาสาเหตุ
- เตรียมเยียวยาผู้เสียหาย
- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ร่วมตรวจสอบช่องโหว่
- เตรียมเสนอมาตรการป้องกันการโจมตีทางไซเบอร์ในอนาคต

ข้อมูลอ้างอิง https://www.hfocus.org/content/2024/03/30032

3 ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

กรณีศึกษาความผิดพลาดของซอฟต์แวร์

CrowdStrike Software Glitch 19 กรกฎาคม **2024**

ข้อมูลอ้างอิง https://www.techradar.com/news/live/windows-outage-july-2024-live

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

3 ภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ

กรณีศึกษาความผิดพลาดของซอฟต์แวร์

CrowdStrike Software Glitch 19 กรกฎาคม **2024**

สาเหตุ

- เกิดจาก ข้อผิดพลาดของซอฟต์แวร์ **CrowdStrike Falcon** ซึ่งเป็นแพลตฟอร์มรักษาความปลอดภัย ไม่ได้เกิดจากการโจมตีทางไซเบอร์จากภายนอก ทาง **CrowdStrike** ระบุว่าสาเหตุเกิดจาก "การอัปเดตซอฟต์แวร์ที่ผิดพลาด" ส่งผลกระทบต่อระบบของลูกค้าทั่วโลก

ผลกระทบ

- ผู้ใช้ **CrowdStrike** หลายล้านคนทั่วโลกประสบปัญหาระบบล่ม ไม่สามารถใช้งานแพลตฟอร์มรักษาความปลอดภัย ส่งผลกระทบต่อธุรกิจ องค์กร และหน่วยงานต่างๆ เป็นวงกว้าง บางองค์กรต้องหยุดการดำเนินงานชั่วคราว
- เสียหายทางการเงินจากเหตุการณ์ครั้งนี้ **some businesses** สูญเสียรายได้ เสียโอกาสทางธุรกิจ และต้องเสียค่าใช้จ่ายเพิ่มเติมในการแก้ไขปัญหา
- ส่งผลต่อชื่อเสียงของ **CrowdStrike** ความน่าเชื่อถือของบริษัทลดลง ลูกค้าสูญเสียความมั่นใจ อาจสูญเสียลูกค้าบางส่วน

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.techradar.com/news/live/windows-outage-july-2024-live

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง ISO/IEC 27001

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

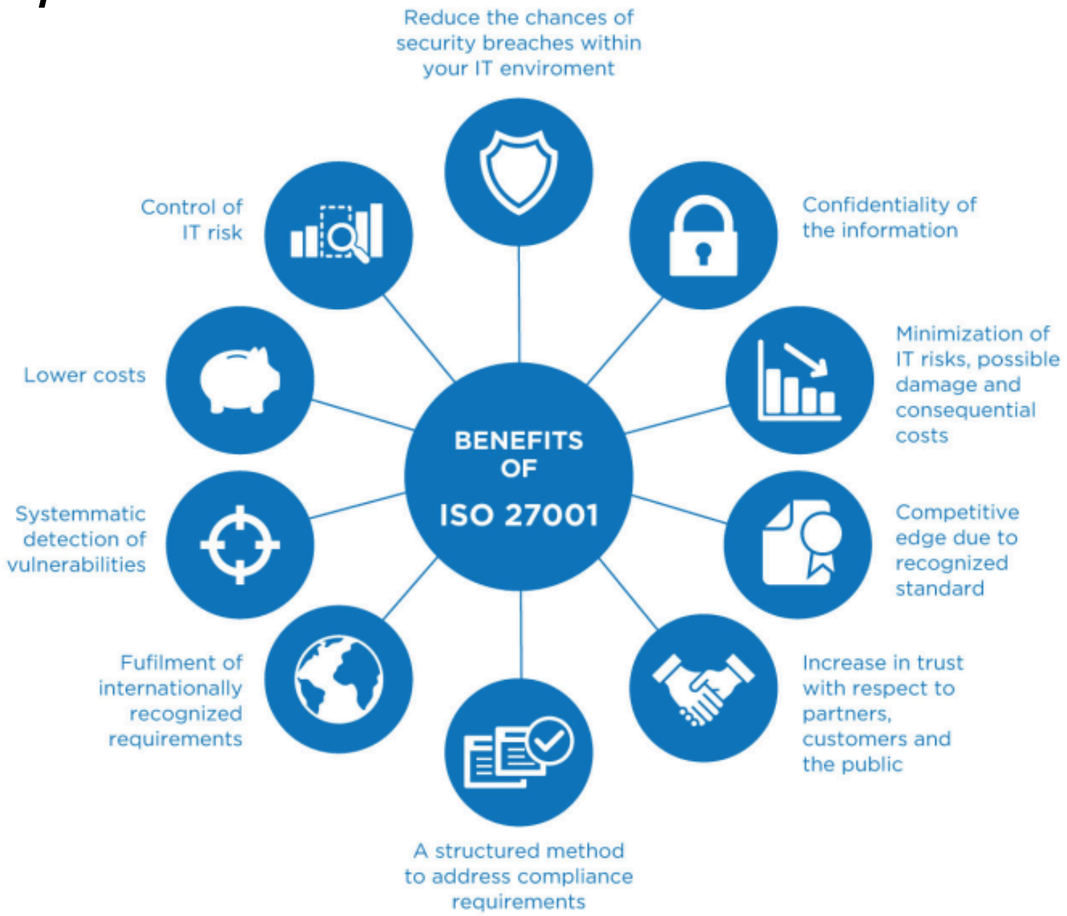
MYSURACHET.COM

Information Security Management System

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

Benefit of ISO/IEC 27001



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://goodtitevs.best/product_details/1338642.html

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

Benefit of ISO/IEC 27001

1.Reduce the chances of security breaches within your IT environment

- ลดโอกาสเกิดเหตุการณ์ละเมิดความปลอดภัยในสภาพแวดล้อม IT ของคุณ

2.Confidentiality of the information

- การรักษาความลับของข้อมูล

3.Minimization of IT risks, possible damage, and consequential costs

- ลดความเสี่ยงด้าน IT ความเสียหายที่อาจเกิดขึ้น และต้นทุนที่ตามมา

4.Competitive edge due to recognized standard

- มีความได้เปรียบในการแข่งขันเนื่องจากการปฏิบัติตามมาตรฐานที่ได้รับการยอมรับ

5.Increase in trust with respect to partners, customers, and the public

- เพิ่มความไว้วางใจจากคู่ค้า ลูกค้า และสาธารณชน

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://goodtitevs.best/product_details/1338642.html

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

Benefit of ISO/IEC 27001

6.A structured method to address compliance requirements

- มีวิธีการที่เป็นระบบในการจัดการตามข้อกำหนดด้านการปฏิบัติตามมาตรฐาน

7.Fulfillment of internationally recognized requirements

- ปฏิบัติตามข้อกำหนดที่ได้รับการยอมรับในระดับสากล

8.Systematic detection of vulnerabilities

- การตรวจหาจุดอ่อนอย่างเป็นระบบ

9.Lower costs

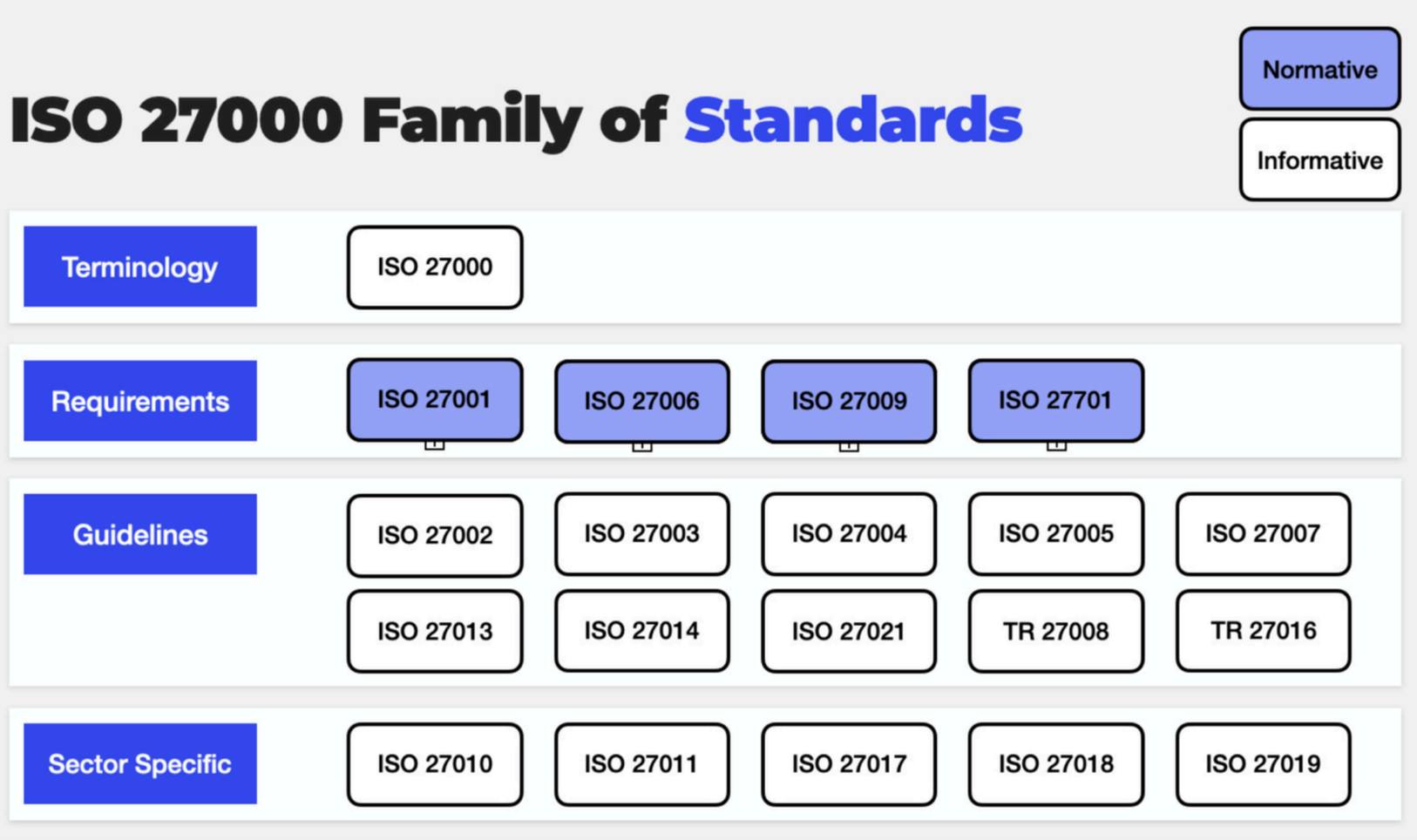
- ลดต้นทุน

10.Control of IT risk

- การควบคุมความเสี่ยงด้าน IT

ข้อมูลอ้างอิง https://goodtitevs.best/product_details/1338642.html

4 การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง ISO/IEC 27001



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

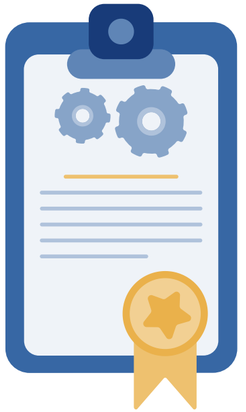
ข้อมูลอ้างอิง https://www.techradar.com/news/live/windows-outage-july-2024-live

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27000 Series

- เป็นชุดของมาตรฐานที่ครอบคลุมหลายด้านของความมั่นคงปลอดภัยของข้อมูล โดยมีเป้าหมายเพื่อช่วยให้องค์กรสามารถปกป้องข้อมูลที่สำคัญจากภัยคุกคามต่างๆ และเพิ่มความมั่นคงปลอดภัยในการดำเนินงาน โดยมาตรฐานในชุดนี้ประกอบไปด้วย



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27000 Series

- ISO/IEC 27001: Information Security Management Systems (ISMS)
- ISO/IEC 27002: Code of Practice for Information Security Controls
- ISO/IEC 27003: Guidelines for the Implementation of an ISMS
- ISO/IEC 27004: Information Security Management Measurement
- ISO/IEC 27005: Information Security Risk Management
- ISO/IEC 27006: Requirements for ISMS Certification
- ISO/IEC 27007: Guidelines for Information Security Management Systems Auditing
- ISO/IEC 27008: Guidelines for Auditors on Information Security Controls
- ISO/IEC 27009: Sector-specific Application of ISO 27001
- ISO/IEC 270010: Information Security Management for Inter-sector and Inter-organizational Communications

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.techradar.com/news/live/windows-outage-july-2024-live

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27000 Series

- ISO/IEC 27011: Information Security Management Guidelines for Telecommunications Organizations
- ISO/IEC 27012: Guidelines for Cybersecurity Information Sharing
- ISO/IEC 27013: Guidance on the Integration and Implementation of ISMS with ISO 20000-1
- ISO/IEC 27014: Governance of Information Security
- ISO/IEC 27015: Information Security Management for Financial Services
- ISO/IEC 27016: Information Security Management for the Banking and Financial Services Sector
- ISO/IEC 27017: Cloud Services Security
- ISO/IEC 27018: Protection of Personally Identifiable Information (PII) in Public Clouds

ข้อมูลอ้างอิง https://www.techradar.com/news/live/windows-outage-july-2024-live

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27000 Series

- ISO/IEC 27019: Information security controls for the energy utility industry
- ISO/IEC 27701: Privacy Information Management System (PIMS) - Requirements and Guidelines
- ISO/IEC 27799: Health Informatics - Information Security Management in Health Using ISO/IEC 27002

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.techradar.com/news/live/windows-outage-july-2024-live

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001 , Information Security Management Systems (ISMS)

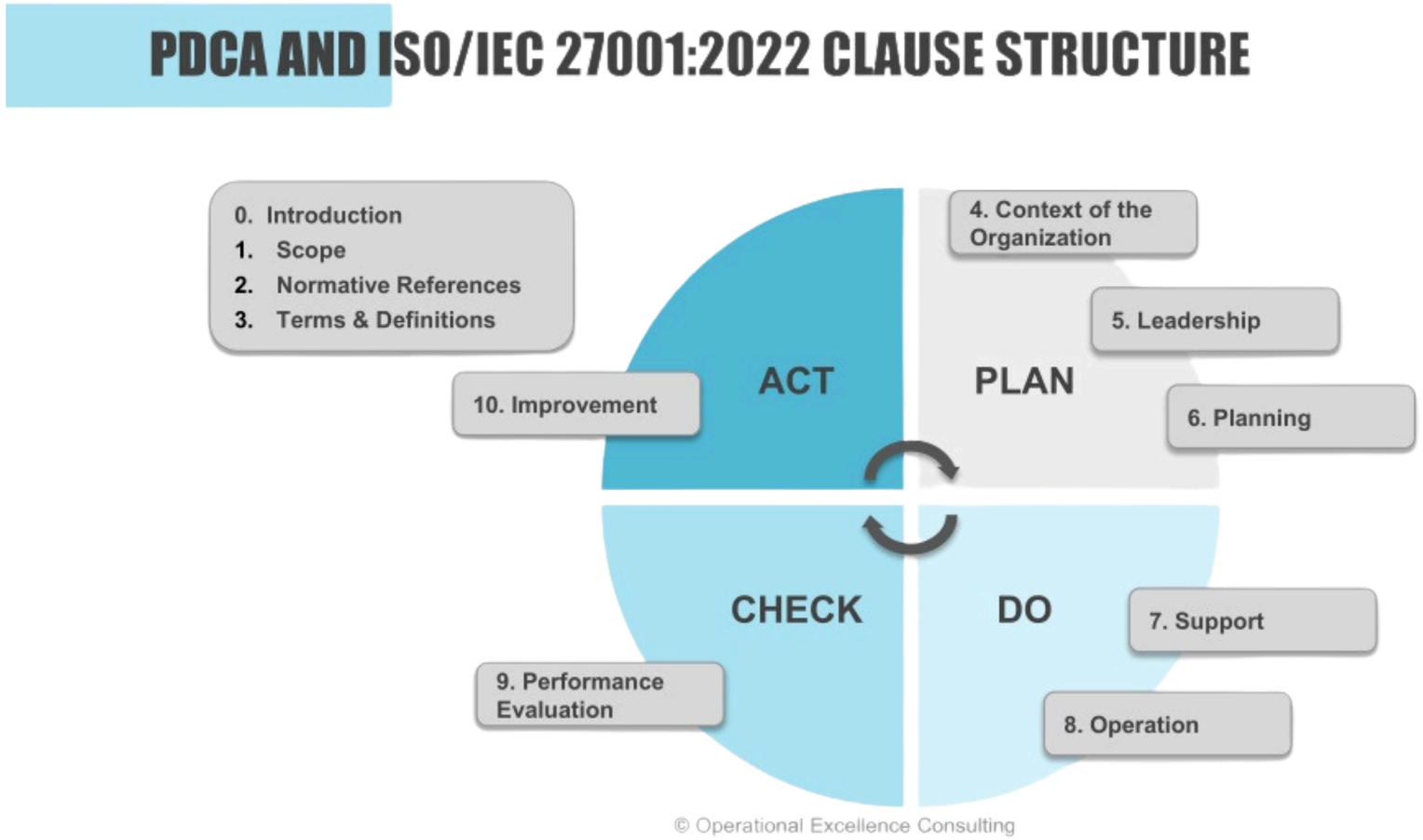
Version	Clause	Control	Category
ISO/IEC 27001:2005	11	133	39
ISO/IEC 27001:2013	10	114	14
ISO/IEC 27001:2022	10	93	4

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001: Information Security Management Systems (ISMS)



ข้อมูลอ้างอิง https://www.slideserve.com/oeconsulting/iso-iec-27001-2022-isms-awareness-training

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , 10ข้อกำหนด (Clause)

- Clause 1: ขอบเขตและการแนะนำ (Scope and Introduction)
- Clause 2: การอ้างอิงเอกสาร (Normative References)
- Clause 3: คำศัพท์และนิยาม (Terms and Definitions)
- Clause 4: บริบทขององค์กร (Context of the Organization)
- Clause 5: ความเป็นผู้นำ (Leadership)
- Clause 6: การวางแผน (Planning)
- Clause 7: การสนับสนุน (Support)
- Clause 8: การดำเนินการ (Operation)
- Clause 9: การประเมินผลการดำเนินงาน (Performance Evaluation)
- Clause 10: การปรับปรุง (Improvement)

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Introduction : Clause 1-3

- Clause 1: ขอบเขตและการแนะนำ (Scope and Introduction)
- Clause 2: การอ้างอิงเอกสาร (Normative References)
- Clause 3: คำศัพท์และนิยาม (Terms and Definitions)

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Information Security Management Systems (ISMS)

ISO/IEC 27001:2022 KEY CLAUSE STRUCTURE (4-10)

PLAN			DO		CHECK	ACT
4. Context of the organization	**5. Leadership**	**6. Planning**	**7. Support**	**8. Operation**	**9. Performance evaluation**	**10. Improvement**
4.1 Understanding the organization and its context	5.1 Leadership and commitment	6.1 Actions to address risks and opportunities	7.1 Resources	8.1 Operational planning and control	9.1 Monitoring, measurement, analysis and evaluation	10.1 Nonconformity and corrective action
4.2 Understanding the needs and expectations of interested parties	5.2 Policy	6.2 Information security objectives and planning to achieve them	7.2 Competence	8.2 Information security risk assessment	9.2 Internal audit	10.2 Continual improvement
4.3 Determining the scope of the ISMS	5.3 Organizational roles, responsibilities and authorities		7.3 Awareness	8.3 Information security risk treatment	9.3 Management review	
4.4 Information Security Management System			7.4 Communication			
			7.5 Documented information			

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.slideserve.com/oeconsulting/iso-iec-27001-2022-isms-awareness-training

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Clause 4-10

- Clause 4: บริบทขององค์กร (Context of the Organization)
  - 4.1 การทำความเข้าใจองค์กรและบริบทขององค์กร (Understanding the organization and its context)
  - 4.2 การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties)
  - 4.3 การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system)
  - 4.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management system)

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Clause 4-10

Clause 4.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management system)

- Effective Implementation of the system
- Internet audit
- Management review

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Clause 4-10

- Clause 5: ความเป็นผู้นำ (Leadership)
  - 5.1 ภาวะผู้นำและการให้ความสำคัญ (Leadership and commitment)
  - 5.2 นโยบาย (Policy)
  - 5.3 บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ขององค์กร (Organizational roles, responsibilities and authorities)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Clause 4-10

- Clause 6: การวางแผน (Planning)
  - 6.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส (Actions to address risks and opportunities)
    - 6.1.1 ภาพรวม (General)
    - 6.1.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment)
    - 6.1.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)
  - 6.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ (Information security objectives and plans to achieve them)
  - 6.3 การวางแผนการเปลี่ยนแปลง (Planning of changes) <New Clause>

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Clause 4-10

- Clause 7: การสนับสนุน (Support)
  - 7.1 ทรัพยากร (Resources)
  - 7.2 สมรรถนะ (Competence)
  - 7.3 การสร้างความตระหนัก (Awareness)
  - 7.4 การสื่อสารให้ทราบ (Communication)
  - 7.5 สารสนเทศที่เป็นลายลักษณ์อักษร (Documented information)
    - 7.5.1 ภาพรวม (General)
    - 7.5.2 การสร้างและปรับปรุงสารสนเทศ (Creating and updating)
    - 7.5.3 การควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร (Control of documented information)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Clause 4-10

- Clause 8: การดำเนินการ (Operation)
  - 8.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม (Operational planning and control)
  - 8.2 การประเมินความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment
  - 8.3 การจัดการกับความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment)

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Clause 4-10

- Clause 9: การประเมินผลการดำเนินงาน (Performance Evaluation)
  - 9.1 การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมินผล (Monitoring, measurement, analysis and evaluation)
  - 9.2 การตรวจประเมินภายใน (Internal audit)
  - 9.3 การทบทวนของผู้บริหาร (Management review)
    - 9.3.1 ทั่วไป (General)
    - 9.3.2 ข้อมูลนำเข้าสำหรับการทบทวนของผู้บริหาร (Management review inputs)
    - 9.3.3 ผลการทบทวนของผู้บริหาร (Management review results)

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Clause 4-10

- Clause 10: การปรับปรุง (Improvement)
  - 10.1 การปรับปรุงอย่างต่อเนื่อง (Continual improvement)
  - 10.2 ความไม่สอดคล้องและการดำเนินการแก้ไข (Nonconformity and corrective action)

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Control Attributes (คุณสมบัติการควบคุม)

Five control attributes	Attribute values
Control type	#Preventative, #Detective, #Corrective
Information security property	#Confidentiality, #Integrity, #Availability
Cybersecurity concepts	#Identify, #Protect, #Detect, #Respond, #Recover
Operational capabilities	#Governance, #Asset_management, #Information_protection, #Human_resource_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Legal_and_compliance, #Information_security_event_management, #Information_security_assurance
Security domains	#Governance_and_Ecosystem, #Protection, #Defence, #Resilience

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Annex A

- ภาคผนวกที่ประกอบด้วยการควบคุมและวัตถุประสงค์ในการควบคุมที่มีความสำคัญสำหรับการจัดการความมั่นคงปลอดภัยของข้อมูล

Category	Control
A5 มาตรการขององค์กร (Organizational controls) : A5.1 - A5.37	37
A6 มาตรการด้านบุคลากร (People controls) : A6.1 - A6.8	8
A7 มาตรการทางกายภาพ (Physical controls) : A7.1 - A7.14	14
A8 มาตรการทางเทคโนโลยี(Technological controls) : A8.1 - A8.34	34

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 , Annex A : 11 New Controls

- A 5.7 Threat intelligence
- A 5.23 Information security for use of cloud services
- A 5.30 Information and Communications Technology readiness for business continuity
- A 7.4 Physical security monitoring
- A 8.9 Configuration management
- A 8.10 Information deletion
- A 8.11 Data masking
- A 8.12 Data leakage prevention
- A 8.16 Monitoring activities
- A 8.23 Web filtering
- A 8.28 Secure coding

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,

Annex A5 มาตรการขององค์กร (Organizational controls) Highlight Control

- A 5.7 Threat intelligence
- A 5.23 Information security for use of cloud services
- A 5.30 Information and Communications (ICT) Technology readiness for business continuity

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

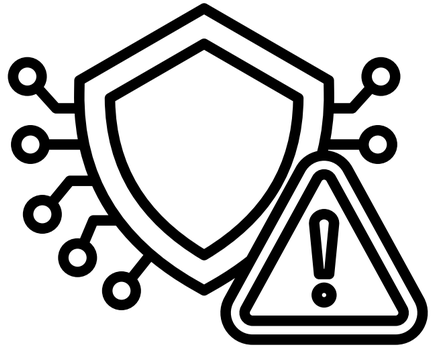
การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,

Annex A5 มาตรการขององค์กร (Organizational controls) Highlight Control

- A 5.7 Threat intelligence (ข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย)
  - Strategic
  - Operational
  - Tactical

Threat intelligence (มาตรการข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย) มีความเกี่ยวข้องกับ Insightful , บริบทและนำไปปฏิบัติได้ โดยให้จัดทำกิจกรรมเพื่อระบุ คัดเลือก รวบรวม ประมวลผล วิเคราะห์ และสื่อสารข้อมูลที่เกี่ยวข้อง เพื่อพิจารณาภัยคุกคามภายในและภายนอก



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,

Annex A5 มาตรการขององค์กร (Organizational controls) Highlight Control

- A 5.23 Information security for use of cloud services (ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการ Cloud)
  - กระบวนการสำหรับการจัดหา การใช้บริการ การบริหารจัดการ และการสิ้นสุดการใช้บริการ Cloud
  - ต้องมีการกำหนดโดยให้เป็นไปตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร
  - ความรับผิดชอบของผู้ให้บริการคลาวด์กับองค์กร
  - จัดการความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลที่สัมพันธ์เชื่อมโยงกับบริการคลาวด์

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,

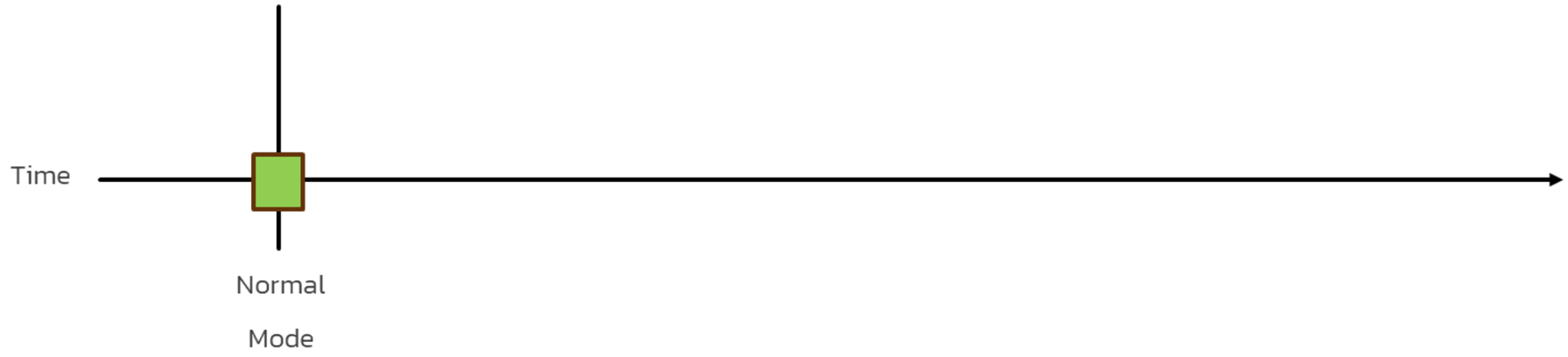
Annex A5 มาตรการขององค์กร (Organizational controls) Highlight Control

- A 5.30 Information and Communications (ICT) Technology readiness for business continuity (ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ)
  - Business Impact Analysis (BIA) กระบวนการวิเคราะห์ปัจจัยเสี่ยงและผลกระทบจากในช่วงเวลาหนึ่งที่ระบบงานขององค์กรถูกทำให้รหยุดชะงัก
  - Recovery Point Objective (RPO) ปริมาณข้อมูลสูญหายที่องค์กรยอมรับได้ในช่วงเวลาหนึ่ง (Acceptable Loss)
  - Recovery Time Objective (RTO) ระยะเวลาที่องค์กรยอมรับได้ในการกู้คืนระบบในกรณีที่เกิดเหตุฉุกเฉินขึ้น ซึ่งเป็นค่าที่ถูกกำหนดโดยเจ้าของระบบ ต้องให้ผู้บริหารระดับสูงรับรู้ และยอมรับในค่า RTO ที่ถูกกำหนดขึ้น
  - Maximum Tolerable Period of Disruption (MTPD) ช่วงเวลานานที่สุดที่ธุรกิจหยุดชะงัก หากเกินก าหนดช่วงเวลา นี้แล้วจะไม่สามารถท าให้ธุรกิจฟื้นคืนสู่สภาพปกติได้

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019

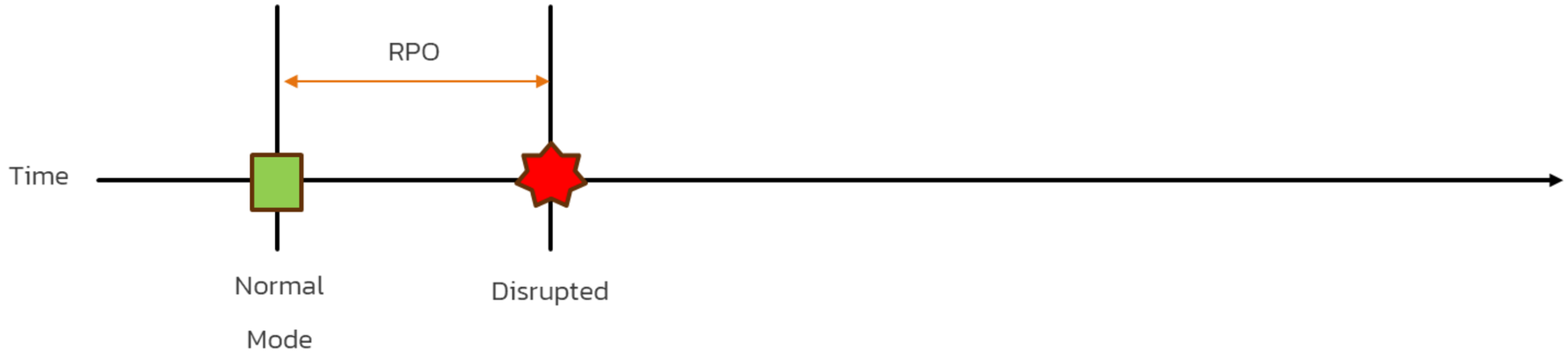


CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

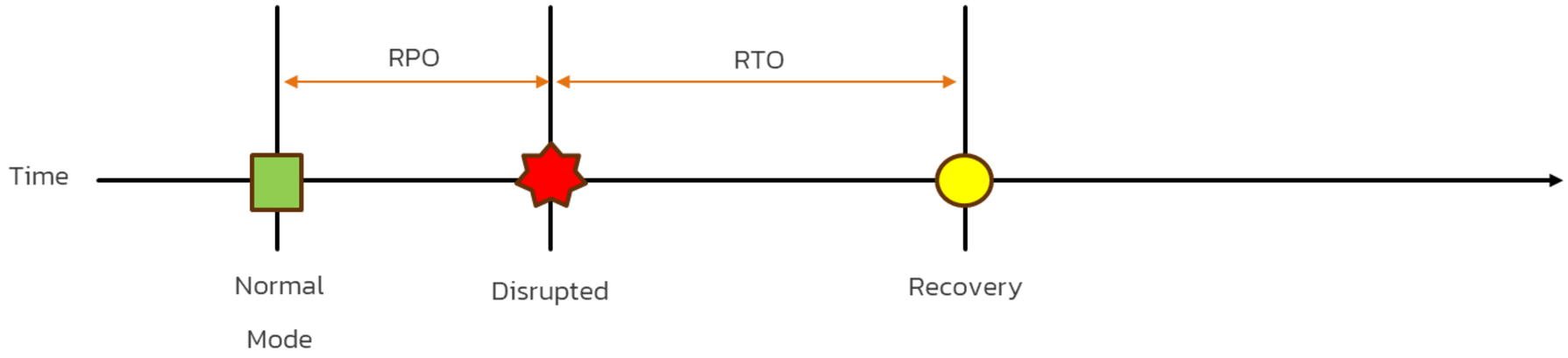
การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4 การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019

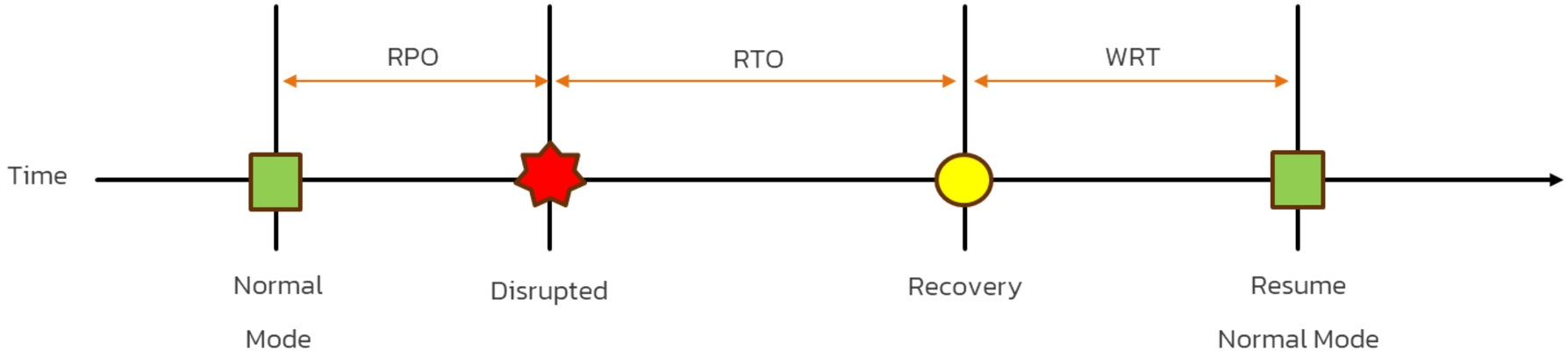


CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

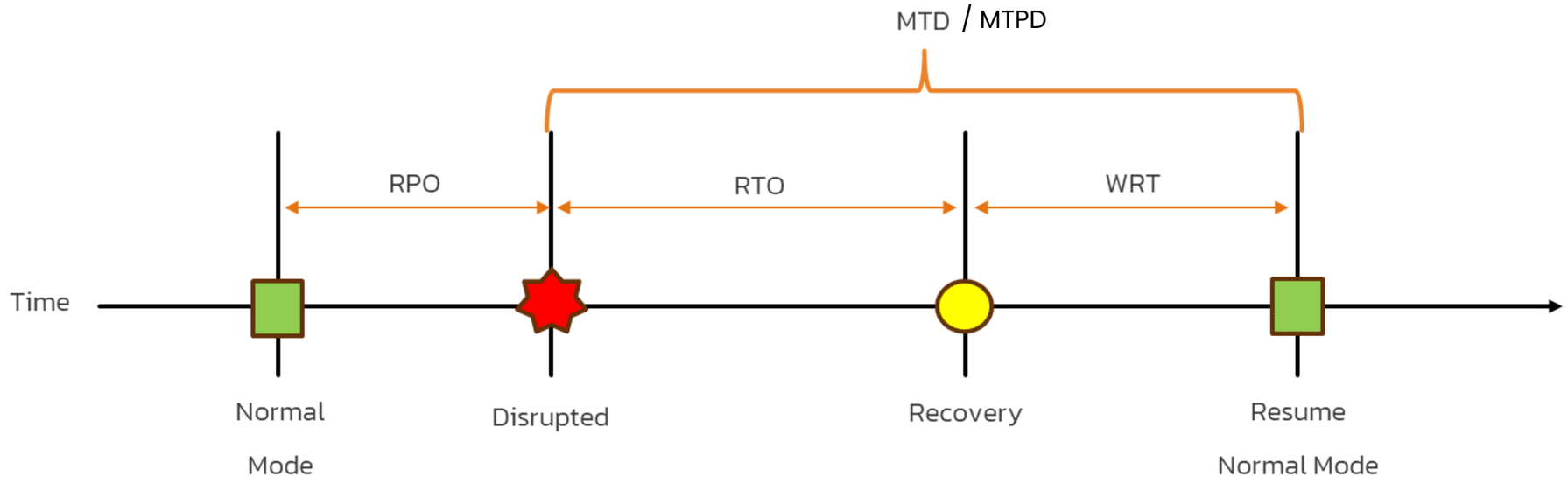
การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019



4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

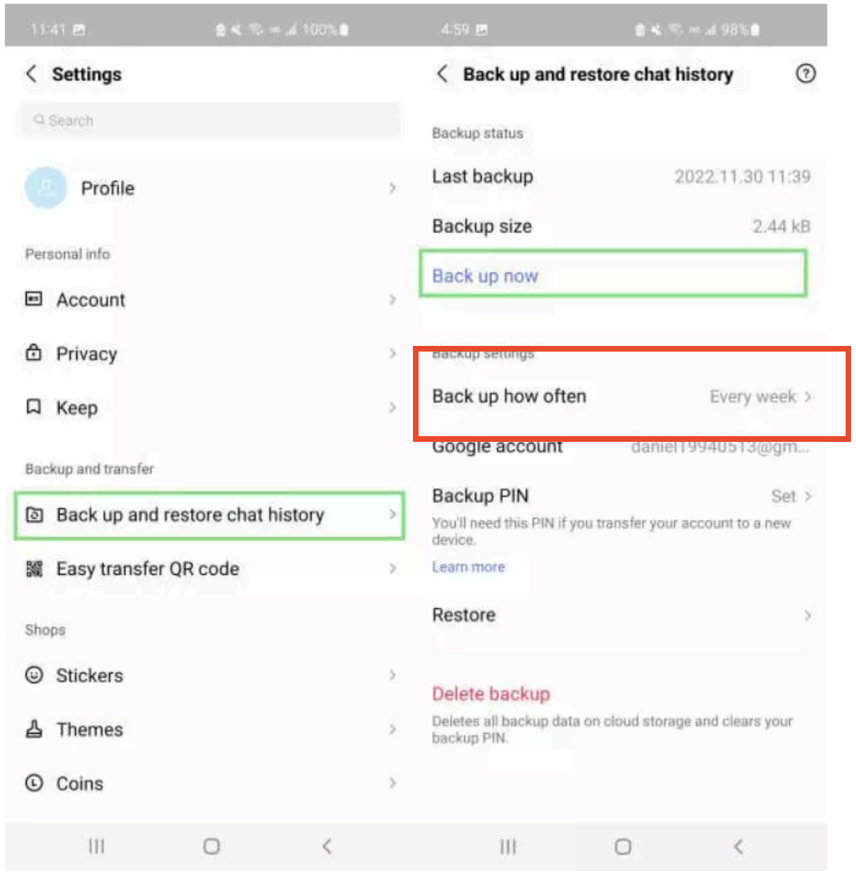
การวิเคราะห์ผลกระทบทางธุรกิจหลัก (BIA : Business Impact Analysis)
อ้างอิง ISO/IEC 22301:2019



4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ตัวอย่าง Back and Recovery Plan บน Digital Device ที่ใกล้ตัวทุกคน



Line : Instat Message

RPO (Recover Point Objective)

- Everyday
- Every 3 day
- Every week
- Every 2 weeks
- Every Month

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,

Annex A7 มาตรการทางกายภาพ (Physical controls) Highlight Control

- A 7.4 Physical security monitoring (การเฝ้าระวังด้านความมั่นคงปลอดภัยทางกายภาพ)

มาตรการนี้ครอบคลุมถึงบริเวณ อาคาร หรือสถานที่ขององค์กรต้องมีการเฝ้าระวังและ ติดตามอย่างต่อเนื่องเพื่อป้องกันการเข้าถึงการกายภาพโดย ไม่ได้รับอนุญาต

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,
Annex A8 มาตรการทางเทคโนโลยี(Technological controls) Highlight Control

- A 8.9 Configuration management
- A 8.10 Information deletion
- A 8.11 Data masking
- A 8.12 Data leakage prevention
- A 8.16 Monitoring activities
- A 8.23 Web filtering
- A 8.28 Secure coding

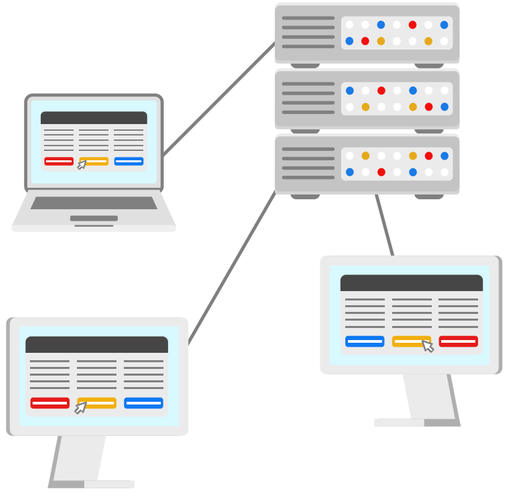
CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,
Annex A8 มาตรการทางเทคโนโลยี(Technological controls) Highlight Control

- A 8.9 Configuration management (การบริหารจัดการการตั้งค่าระบบ)
  - กระบวนการและเครื่องมือในการบังคับใช้การตั้งค่าระบบ ซึ่งรวมถึงการตั้งค่าด้านความมั่นคงปลอดภัยของฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่าย
  - ต้องมีการจัดทำเป็นลายลักษณ์อักษร นำสู่การปฏิบัติ ติดตาม และทบทวน (เพื่อให้เป็นไปตามการตั้งค่าที่กำหนดไว้นั้น)



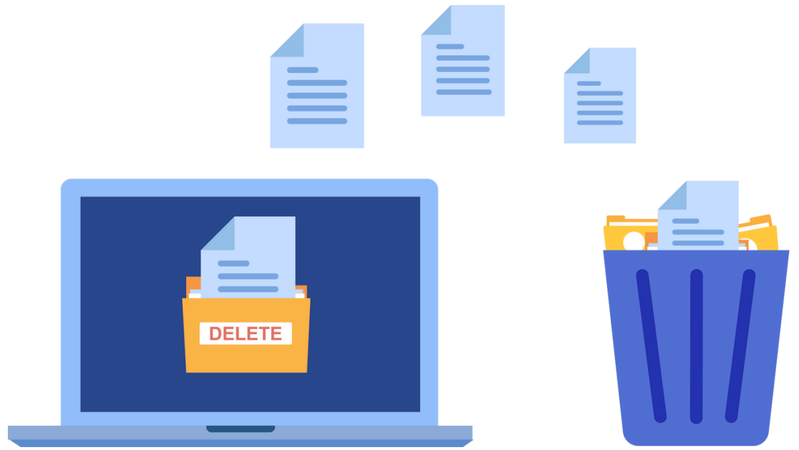
CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,
Annex A8 มาตรการทางเทคโนโลยี(Technological controls) Highlight Control

- A 8.10 Information deletion (การลบข้อมูล)
  - ข้อมูลที่มีการจัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือบนสื่อบันทึกข้อมูลอื่นๆ ต้องมีการลบทำลายเมื่อไม่มีความจำเป็นในการใช้งานอีกต่อไป



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,
Annex A8 มาตรการทางเทคโนโลยี(Technological controls) Highlight Control

- A 8.11 Data masking (การปิดบังข้อมูล)
  - การปิดบังข้อมูล (เพื่อไม่ให้ข้อมูลที่จัดเก็บไว้ในระบบถูกมองเห็น หรือถูกนำไปใช้ประโยชน์ได้) ต้องมีการนำมาใช้งานโดยให้เป็นไปตามนโยบายเฉพาะแยกตามเรื่องที่เกี่ยวข้องกับ
  - การควบคุมการเข้าถึง นโยบายเฉพาะแยกตามเรื่องอื่นๆ ที่เกี่ยวข้องและความต้องการทางธุรกิจขององค์กร
  - โดยต้องพิจารณากฎหมายที่เกี่ยวข้องประกอบด้วย

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,
Annex A8 มาตรการทางเทคโนโลยี(Technological controls) Highlight Control

- A 8.12 Data leakage prevention (การป้องกันการรั่วไหลของข้อมูล)
  - มาตรการการป้องกันการรั่วไหลของข้อมูล
  - ใช้เครื่องมือทางเทคโนโลยีเพื่อป้องกันข้อมูลรั่วไหล
  - ต้องมีการนำมาประยุกต์ใช้กับระบบ เครือข่าย และอุปกรณ์ต่างๆ ที่มีการประมวลผล จัดเก็บ หรือรับส่งข้อมูลสำคัญ
  - ระบุและจำแนกข้อมูล ติดตามช่องทาง และป้องกันข้อมูลรั่วไหล

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,
Annex A8 มาตรการทางเทคโนโลยี(Technological controls) Highlight Control

- A 8.16 Monitoring activities (กิจกรรมการเฝ้าระวังการทำงานของระบบและอุปกรณ์)
  - เครือข่าย ระบบ และแอพพลิเคชั่นต้องมีการเฝ้าระวังการทำงานเพื่อตรวจหาพฤติกรรมที่ผิดปกติ และประเมินเหตุการณ์ด้านความปลอดภัยของข้อมูลที่อาจเกิดขึ้น
  - ใช้เครื่องมือติดตามเพื่อติดตามอย่างต่อเนื่อง
  - เครื่องมือมีความสามารถในการปรับตัวเข้ากับภัยคุกคามที่แตกต่างกัน
  - เครื่องมือมีความสามารถของฟังก์ชั่นแจ้งเตือนเพื่อให้สามารถสื่อสารเหตุการณ์ผิดปกติไปยังผู้มีส่วนได้เสียที่เกี่ยวข้อง

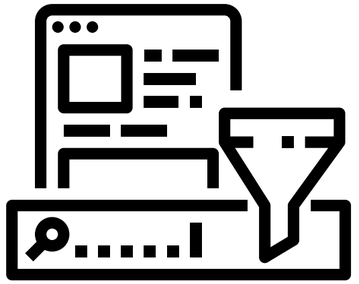
CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,
Annex A8 มาตรการทางเทคโนโลยี(Technological controls) Highlight Control

- A 8.23 Web filtering (การคัดกรองเว็บ)
  - การบริหารจัดการการเข้าถึงเว็บไซต์ภายนอก มีการปกป้องการบุกรุกโดยมัลแวร์และการเข้าถึงทรัพยากรบนเว็บที่ไม่ได้รับอนุญาต
  - ลดโอกาสการเข้าถึงเนื้อหาที่เป็นอันตราย (เช่น โปรแกรมไม่ประสงค์ดี ซอฟต์แวร์ที่เป็นอันตรายต่างๆ)
  - ระบุประเภทของบุคลากรเว็บไซต์ที่ควรหรือไม่ควรเข้าถึง
  - กำหนดกฎเกณฑ์ในการใช้ทรัพยากรออนไลน์อย่างปลอดภัยและเหมาะสม
  - ให้การฝึกอบรมแก่บุคลากรเกี่ยวกับการใช้ทรัพยากรออนไลน์อย่างปลอดภัยและเหมาะสม

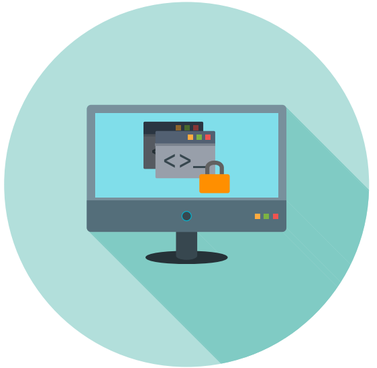


4

การสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง **ISO/IEC 27001**

ISO/IEC 27001:2022 ,
Annex A8 มาตรการทางเทคโนโลยี(Technological controls) Highlight Control

- A 8.28 Secure coding (การเขียนโปรแกรมให้มีความมั่นคงปลอดภัย)
  - ตรวจสอบให้แน่ใจว่าหลักการการเขียนโปรแกรมให้มีความมั่นคงปลอดภัย ต้องมีการนำมาปฏิบัติกับการพัฒนาซอฟต์แวร ร รวมถึงซอฟต์แวร์ 3rd Party และ Open source software
  - ติดตามข่าวสารล่าสุดเกี่ยวกับภัยคุกคามซอฟต์แวร์ในโลกแห่งความเป็นจริง
  - พิจารณา Life cycle การเขียนโค้ดทั้งหมด รวมถึงพิจารณาการนำมาใช้ซ้ำ



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

5 กลยุทธ์ความพร้อมรับมือภัยไซเบอร์

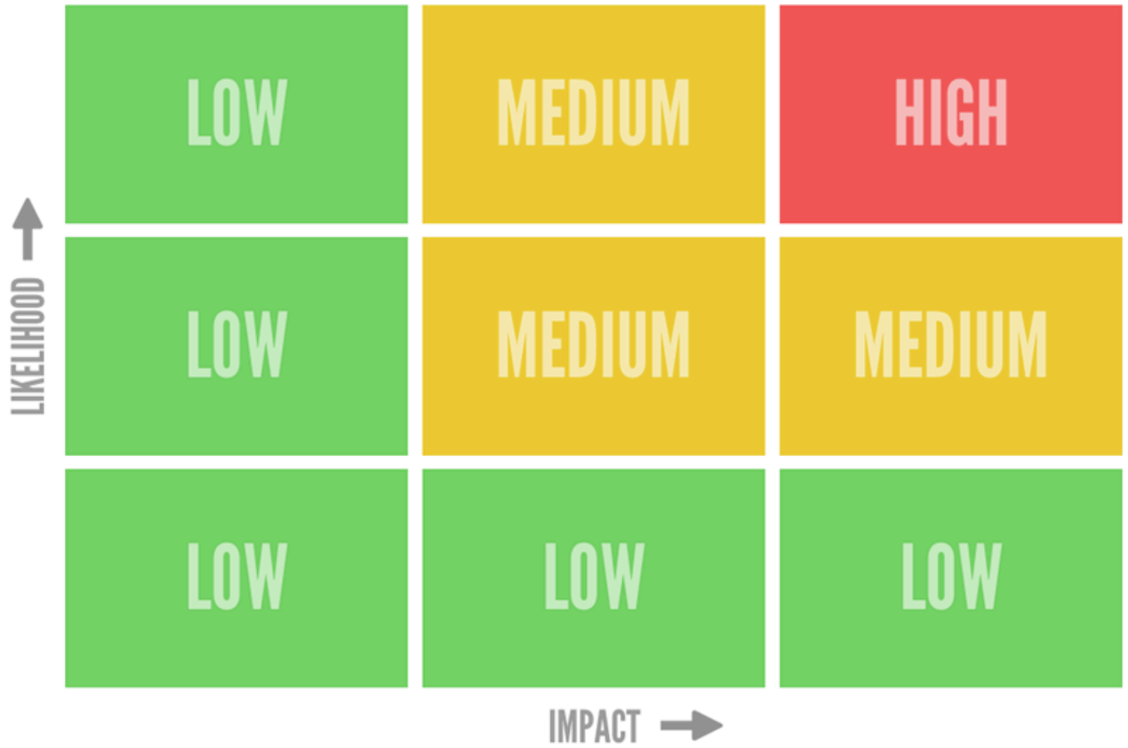
CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

5 กลยุทธ์ความพร้อมรับมือภัยไซเบอร์

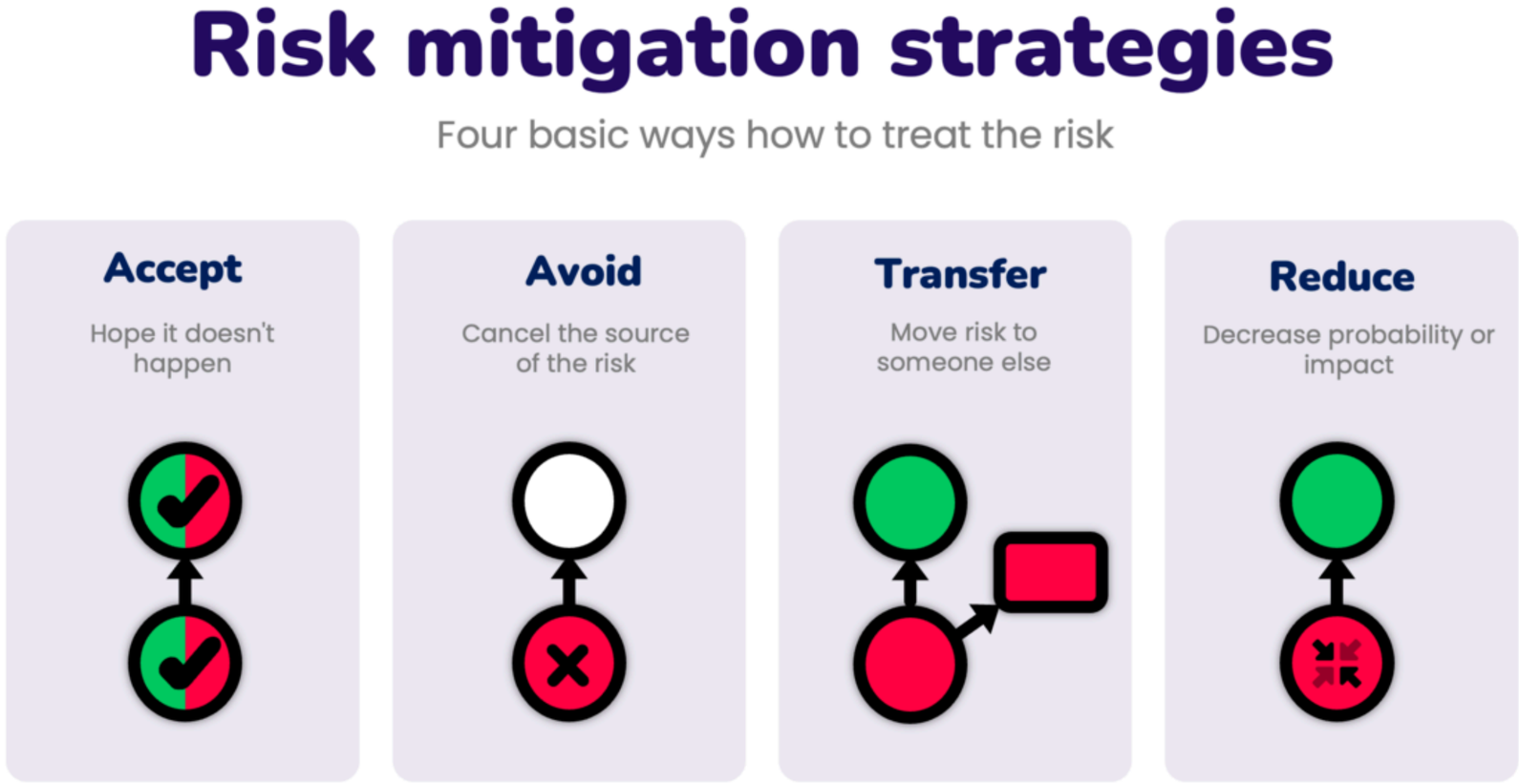
การประเมินความเสี่ยง (Risk Assessment)
พิจารณาระดับความเสี่ยงจาก ผลกระทบ (I) x โอกาสที่จะเกิดภัย (L)

- Impact : ผลกระทบ
- Likelihood : โอกาสที่จะเกิดภัย



5 กลยุทธ์ความพร้อมรับมือภัยไซเบอร์

กลยุทธ์การบรรเทาความเสี่ยง



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://www.insurancejournal.com/news/national/2021/11/29/643569.htm

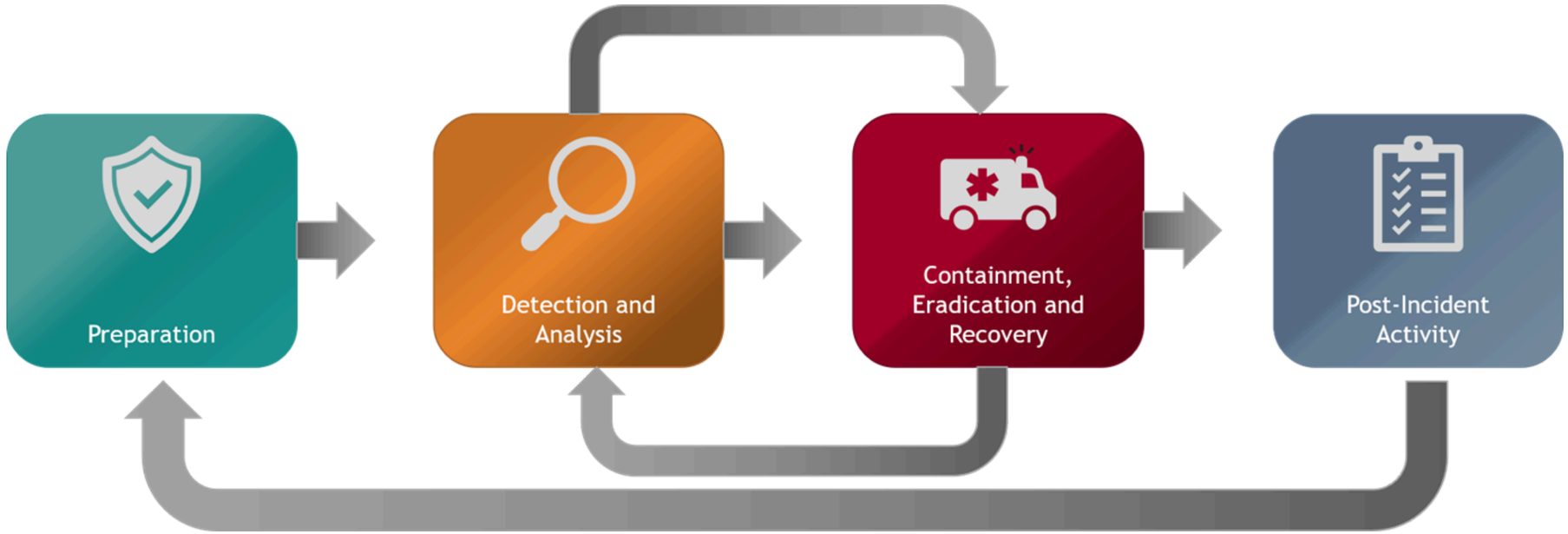
5 กลยุทธ์ความพร้อมรับมือภัยไซเบอร์

การสร้างทีมรับมือเหตุการณ์ ภัยคุกคามทางไซเบอร์

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

5 กลยุทธ์ความพร้อมรับมือภัยไซเบอร์

การกำหนดโครงสร้างการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์
Standard Operation Procedures (SOPs)



5 กลยุทธ์ความพร้อมรับมือภัยไซเบอร์

NIST Cybersecurity Framework v2.0

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลอ้างอิง https://csf.tools/reference/nist-cybersecurity-framework/v2-0/

5 กลยุทธ์ความพร้อมรับมือภัยไซเบอร์

NIST Cybersecurity Framework v2.0

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

- Govern
- Identify
- Protection
- Detect
- Respond
- Recover

ข้อมูลอ้างอิง https://csf.tools/reference/nist-cybersecurity-framework/v2-0/

5 กลยุทธ์ความพร้อมรับมือภัยไซเบอร์

ISO/IEC 22301 (BCMS)

ISO 22301:2019

- กลุ่มการควบคุมระบบการจัดการ (Management Controls)
- กลุ่มการควบคุมการจัดการความเสี่ยง (Risk Management Controls)
- กลุ่มการควบคุมการจัดการสินทรัพย์ (Asset Management Controls)
- กลุ่มการควบคุมการสร้างมูลค่า (Value Creation Controls)
- กลุ่มการควบคุมการจัดการการวัดผล (Measurement and Monitoring Controls)

6 บทบาทหน้าที่และการมีส่วนร่วม

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Roles and Participation

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของผู้บริหาร (Leadership and Commitment)
- บทบาทของทีมงานความมั่นคงปลอดภัยของข้อมูล (ISMS Team)
- บทบาทของพนักงานทุกคน (All Employees)
- การฝึกอบรมและการสร้างความตระหนักรู้ (Training and Awareness)
- การรายงานเหตุการณ์และการตอบสนอง (Incident Reporting and Response)
- การปรับปรุงกระบวนการและการปฏิบัติตามข้อกำหนด (Continuous Improvement and Compliance)

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของผู้บริหาร (Leadership and Commitment)
  - การแสดงความมุ่งมั่นและการสนับสนุน
    - ผู้บริหารระดับสูงต้องแสดงความมุ่งมั่นในการนำระบบ ISO 27001 มาใช้ในองค์กรอย่างชัดเจนและต่อเนื่อง
    - การให้การสนับสนุนด้านทรัพยากรและงบประมาณที่จำเป็นต่อการดำเนินการและการบำรุงรักษาระบบ ISMS

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของผู้บริหาร (Leadership and Commitment)
  - การกำหนดนโยบายและวัตถุประสงค์
    - ผู้บริหารต้องกำหนดนโยบายความมั่นคงปลอดภัยของข้อมูลและวัตถุประสงค์ที่สอดคล้องกับกลยุทธ์และเป้าหมายขององค์กร
    - การสื่อสารนโยบายและวัตถุประสงค์เหล่านี้ให้กับพนักงานทุกคนในองค์กร

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของผู้บริหาร (Leadership and Commitment)
  - การติดตามและประเมินผล
    - ผู้บริหารต้องติดตามและประเมินผลการดำเนินการของระบบ ISMS อย่างต่อเนื่อง เพื่อให้แน่ใจว่ามีการปรับปรุงและพัฒนาอย่างต่อเนื่อง
    - การจัดการทบทวนการบริหาร (Management Review) เพื่อตรวจสอบประสิทธิภาพและความเหมาะสมของระบบ ISMS

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของทีมงานความมั่นคงปลอดภัยของข้อมูล (ISMS Team)
  - การวางแผนและดำเนินการ
    - ทีมงาน ISMS ต้องรับผิดชอบในการวางแผนและดำเนินการตามข้อกำหนดของ ISO/IEC 27001
    - การระบุและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล และการกำหนดมาตรการควบคุมเพื่อป้องกันและลดความเสี่ยง

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของทีมงานความมั่นคงปลอดภัยของข้อมูล (ISMS Team)
  - การจัดทำและปรับปรุงเอกสาร
    - ทีมงานต้องจัดทำและบำรุงรักษาเอกสารที่เกี่ยวข้องกับระบบ ISMS เช่น นโยบาย, ขั้นตอนการดำเนินงาน, บันทึกเหตุการณ์, และรายงานการประเมินความเสี่ยง
    - การปรับปรุงเอกสารอย่างต่อเนื่องเพื่อให้สอดคล้องกับข้อกำหนดและมาตรการความมั่นคงปลอดภัยที่เปลี่ยนแปลงไป

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของทีมงานความมั่นคงปลอดภัยของข้อมูล (ISMS Team)
  - การฝึกอบรมและการสร้างความตระหนักรู้
    - ทีมงาน ISMS ต้องจัดการฝึกอบรมและสร้างความตระหนักรู้ให้กับพนักงานทุกคนเกี่ยวกับความมั่นคงปลอดภัยของข้อมูลและบทบาทของพวกเขาในการปฏิบัติตามข้อกำหนดของ ISO/IEC 27001

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของพนักงานทุกคน (All Employees)
  - การปฏิบัติตามนโยบายและขั้นตอน
    - พนักงานทุกคนต้องปฏิบัติตามนโยบายและขั้นตอนที่กำหนดโดยระบบ ISMS
    - การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลตามขั้นตอนที่กำหนด

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของพนักงานทุกคน (All Employees)
  - การปกป้องข้อมูลและการใช้งานระบบอย่างปลอดภัย
    - พนักงานต้องรับผิดชอบในการปกป้องข้อมูลและใช้งานระบบไอทีขององค์กรอย่างปลอดภัย
    - การระมัดระวังในการจัดการข้อมูลส่วนบุคคลและข้อมูลที่มีความสำคัญ

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- บทบาทของพนักงานทุกคน (All Employees)
  - การมีส่วนร่วมในการปรับปรุงระบบ
    - พนักงานสามารถมีส่วนร่วมในการปรับปรุงระบบ ISMS โดยการเสนอแนะและแบ่งปันความคิดเห็นเกี่ยวกับมาตรการความมั่นคงปลอดภัยของข้อมูล
    - การเข้าร่วมกิจกรรมการฝึกอบรมและการสร้างความตระหนักรู้ที่จัดโดยทีมงาน ISMS

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- การฝึกอบรมและการสร้างความตระหนักรู้ (Training and Awareness)
  - ความสำคัญของการฝึกอบรม
    - การฝึกอบรมเป็นสิ่งสำคัญในการให้ความรู้และทักษะที่จำเป็นสำหรับพนักงานทุกคนในการปฏิบัติตามมาตรฐาน ISO 27001
    - การฝึกอบรมควรครอบคลุมถึงนโยบายและขั้นตอนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูล

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- การฝึกอบรมและการสร้างความตระหนักรู้ (Training and Awareness)
  - การสร้างความตระหนักรู้
    - การสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกันเป็นสิ่งสำคัญในการปกป้องข้อมูลขององค์กร
    - การจัดกิจกรรมและแคมเปญเพื่อสร้างความตระหนักรู้ เช่น การจัดสัมมนา, การแจกใบปลิว, หรือการส่งอีเมลแจ้งเตือน

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- การฝึกอบรมและการสร้างความตระหนักรู้ (Training and Awareness)
  - การฝึกอบรมอย่างต่อเนื่อง
    - การฝึกอบรมควรเป็นกระบวนการที่ต่อเนื่องและมีการอัปเดตอยู่เสมอ เพื่อให้พนักงานทราบถึงภัยคุกคามใหม่ ๆ และวิธีการป้องกันที่มีประสิทธิภาพ

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- การรายงานเหตุการณ์และการตอบสนอง (Incident Reporting and Response)
  - การระบุและรายงานเหตุการณ์
    - พนักงานทุกคนต้องสามารถระบุและรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลได้อย่างรวดเร็ว
    - การรายงานเหตุการณ์ควรมีขั้นตอนที่ชัดเจนและสามารถปฏิบัติตามได้ง่าย

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- การรายงานเหตุการณ์และการตอบสนอง (Incident Reporting and Response)
  - การตอบสนองต่อเหตุการณ์
    - ทีมงานความมั่นคงปลอดภัยของข้อมูลต้องมีแผนการตอบสนองต่อเหตุการณ์ที่มีประสิทธิภาพ เพื่อให้สามารถจัดการกับเหตุการณ์ได้อย่างรวดเร็วและลดผลกระทบที่อาจเกิดขึ้น
    - การตอบสนองควรครอบคลุมถึงการตรวจสอบ, การประเมินความเสี่ยง, และการดำเนินการแก้ไข

6 บทบาทหน้าที่และการมีส่วนร่วม

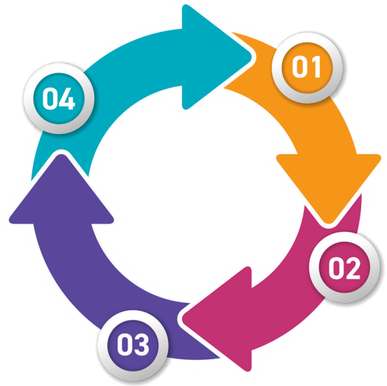
บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- การรายงานเหตุการณ์และการตอบสนอง (Incident Reporting and Response)
  - การสื่อสารภายในองค์กร
    - การสื่อสารภายในองค์กรในระหว่างการจัดการเหตุการณ์เป็นสิ่งสำคัญ เพื่อให้พนักงานทุกคนทราบถึงสถานการณ์และการดำเนินการที่กำลังเกิดขึ้น
    - การสื่อสารควรเป็นไปอย่างโปร่งใสและครอบคลุมทุกฝ่ายที่เกี่ยวข้อง

6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

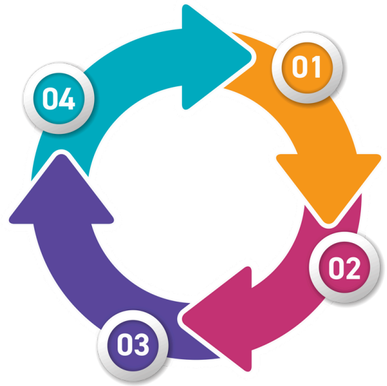
- การปรับปรุงกระบวนการและการปฏิบัติตามข้อกำหนด (Continuous Improvement and Compliance)
  - การปรับปรุงอย่างต่อเนื่อง
    - องค์กรต้องมีการตรวจสอบและปรับปรุงกระบวนการความมั่นคงปลอดภัยของข้อมูลอย่างต่อเนื่อง เพื่อให้แน่ใจว่ามาตรการความปลอดภัยยังคงมีประสิทธิภาพ
    - การใช้ผลการประเมินและการทบทวนเพื่อนำมาปรับปรุงกระบวนการและมาตรการ



6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

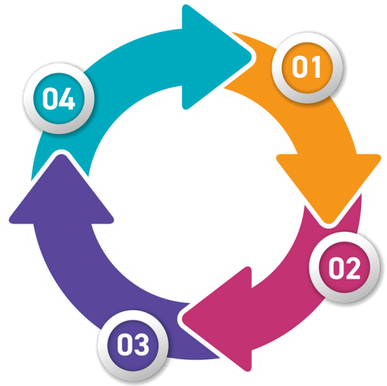
- การปรับปรุงกระบวนการและการปฏิบัติตามข้อกำหนด (Continuous Improvement and Compliance)
  - การปฏิบัติตามข้อกำหนด
    - การปฏิบัติตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 เป็นสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูล
    - การทำการตรวจสอบภายในและการทบทวนการบริหารอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าองค์กรปฏิบัติตามข้อกำหนดทั้งหมด



6 บทบาทหน้าที่และการมีส่วนร่วม

บทบาทหน้าที่การมีส่วนร่วมของผู้บริหารและพนักงานในระบบ ISO/IEC 27001

- การปรับปรุงกระบวนการและการปฏิบัติตามข้อกำหนด (Continuous Improvement and Compliance)
  - การจัดทำรายงานและเอกสาร
    - การจัดทำรายงานและเอกสารที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดและการปรับปรุงกระบวนการ เป็นสิ่งสำคัญในการตรวจสอบและประเมินความสอดคล้องกับมาตรฐาน
    - การจัดทำเอกสารอย่างถูกต้องและครบถ้วนช่วยให้สามารถติดตามและปรับปรุงได้อย่างมีประสิทธิภาพ



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

7 Workshop

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Workshop and Brainstrom

7 Workshop

วัตถุประสงค์การทำ Workshop

เพื่อให้ผู้เข้าร่วมอบรมได้เรียนรู้และฝึกปฏิบัติการจัดการความเสี่ยงตามมาตรฐาน ISO 27001 โดยแต่ละกลุ่มจะได้รับโจทย์ที่แตกต่างกันเพื่อจำลองสถานการณ์และพัฒนามาตรการควบคุมความเสี่ยง

กติกาการทำ Workshop

- ให้ผู้เข้าอบรมแบ่งออกเป็น 5 กลุ่ม
- ให้แต่ละกลุ่มมีหัวหน้ากลุ่มเพื่อประสานงานและกำกับดูแลการดำเนินงานของกลุ่ม
- ให้แต่ละกลุ่มกำหนดหน้าที่สำหรับสมาชิกกลุ่มแต่ละคน เช่น ผู้จดบันทึก, ผู้วิเคราะห์ข้อมูล และผู้นำเสนอ
- สามารถใช้คอมพิวเตอร์ / Tablet / Smartphone การนำเสนอผลงานได้
- ให้เวลาทำโจทย์ Workshop กลุ่มละ 30 นาที หรือตามที่ผู้จัดเห็นสมควร
- นำเสนอกลุ่มละ 5 นาที

7 Workshop

โจทย์ Workshop กลุ่มที่ 1: การโจมตีแบบฟิชชิง (Phishing Attack)

- สถานการณ์: มีรายงานว่ามีอีเมลฟิชชิงถูกส่งไปยังพนักงานในสำนักทะเบียนมหาวิทยาลัย โดยพยายามหลอกให้พนักงานกรอกข้อมูลเข้าสู่ระบบปลอม ซึ่งอาจทำให้ข้อมูลส่วนบุคคลและข้อมูลการเงินถูกขโมย
- การระบุและประเมินความเสี่ยง:
  - ระบุภัยคุกคาม (Threat) ?
  - ผลกระทบ (Impact) ?
  - โอกาสที่เกิด/ความน่าจะเป็น (Likelihood) ของภัยคุกคาม?
  - ระดับความเสี่ยง (RisK) ?
- ออกแบบมาตรการควบคุมความเสี่ยง (Risk control measures design)
- วางแผนการจัดการความเสี่ยง (Risk Management Plan)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

7 Workshop

โจทย์ Workshop กลุ่มที่ 2: การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access)

- สถานการณ์: มีการค้นพบว่ามีบุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงระบบฐานข้อมูลของสำนักทะเบียนมหาวิทยาลัย ซึ่งอาจทำให้ข้อมูลนักศึกษาและบุคลากรถูกเปิดเผยหรือแก้ไข
- การระบุและประเมินความเสี่ยง:
  - ระบุภัยคุกคาม (Threat) ?
  - ผลกระทบ (Impact) ?
  - โอกาสที่เกิด/ความน่าจะเป็น (Likelihood) ของภัยคุกคาม?
  - ระดับความเสี่ยง (RisK) ?
- ออกแบบมาตรการควบคุมความเสี่ยง (Risk control measures design)
- วางแผนการจัดการความเสี่ยง (Risk Management Plan)

7 Workshop

โจทย์ Workshop กลุ่มที่ 3: การโจมตีแบบ DDoS (Distributed Denial of Service)

- สถานการณ์: มีการโจมตีแบบ DDoS ที่ทำให้ระบบเว็บไซต์ของสำนักทะเบียนมหาวิทยาลัย ไม่สามารถให้บริการได้ ทำให้ผู้ใช้งานไม่สามารถเข้าถึงข้อมูลและบริการออนไลน์ได้
- การระบุและประเมินความเสี่ยง:
  - ระบุภัยคุกคาม (Threat) ?
  - ผลกระทบ (Impact) ?
  - โอกาสที่เกิด/ความน่าจะเป็น (Likelihood) ของภัยคุกคาม?
  - ระดับความเสี่ยง (RisK) ?
- ออกแบบมาตรการควบคุมความเสี่ยง (Risk control measures design)
- วางแผนการจัดการความเสี่ยง (Risk Management Plan)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

7 Workshop

โจทย์ Workshop กลุ่มที่ 4: การสูญหายของข้อมูล (Data Loss)

- สถานการณ์: มีการรายงานว่ามีการสูญหายของข้อมูลเนื่องจากฮาร์ดแวร์ที่เก็บข้อมูลเกิดความเสียหาย ซึ่งอาจทำให้ข้อมูลสำคัญสูญหายไป
- การระบุและประเมินความเสี่ยง:
  - ระบุภัยคุกคาม (Threat) ?
  - ผลกระทบ (Impact) ?
  - โอกาสที่เกิด/ความน่าจะเป็น (Likelihood) ของภัยคุกคาม?
  - ระดับความเสี่ยง (RisK) ?
- ออกแบบมาตรการควบคุมความเสี่ยง (Risk control measures design)
- วางแผนการจัดการความเสี่ยง (Risk Management Plan)

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

7 Workshop

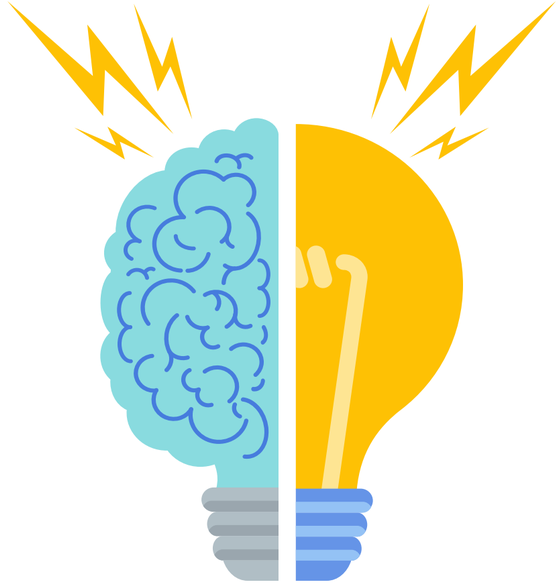
โจทย์ Workshop กลุ่มที่ 5: การใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต (Unauthorized Software Usage)

- สถานการณ์: มีการค้นพบว่ามีพนักงานบางคนติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตลงในคอมพิวเตอร์ของสำนักทะเบียนมหาวิทยาลัย ซึ่งอาจมีความเสี่ยงจากมัลแวร์และการละเมิดลิขสิทธิ์
- การระบุและประเมินความเสี่ยง:
  - ระบุภัยคุกคาม (Threat) ?
  - ผลกระทบ (Impact) ?
  - โอกาสที่เกิด/ความน่าจะเป็น (Likelihood) ของภัยคุกคาม?
  - ระดับความเสี่ยง (RisK) ?
- ออกแบบมาตรการควบคุมความเสี่ยง (Risk control measures design)
- วางแผนการจัดการความเสี่ยง (Risk Management Plan)

7 Workshop

ให้แต่ละกลุ่มระดมสมองทำ Workshop

- ให้เวลาในการทำ Workshop กลุ่มละ 30 นาที



CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

7 Workshop

นำเสนอผลการทำ Workshop รายกลุ่ม

- ให้แต่ละกลุ่มส่งตัวแทนออกมานำเสนอ กลุ่มละ 5 นาที
- วิทยากรผู้ฝึกอบรม และ ผู้บริหารหน่วยงาน/ตัวแทนผู้บริหาร เป็นผู้ให้คะแนนแต่ละกลุ่ม
- สรุปผลการทำ Workshop

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

8 สรุปและตอบคำถาม

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

8 สรุปและตอบคำถาม

สรุปสิ่งที่ได้เรียนในหลักสูตรนี้

- ภัยคุกคามทางไซเบอร์ในยุค AI
- ปัจจัยที่ก่อให้เกิดอาชญากรรมทางไซเบอร์ (Cyber Crime)
- ประเภทของภัยคุกคาม
- กรณีศึกษาภัยคุกคามทางไซเบอร์ ที่สร้างผลกระทบต่อระบบเศรษฐกิจ
- ประโยชน์ของรสร้างมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทาง ISO/IEC 27001
- ISO/IEC 27000 Series
- ISO/IEC27001:2022 10ข้อกำหนด(Clause)
- ISO/IEC27001:2022 Key Clause Structure (Clause 4-10)
- ISO/IEC 27001:2022 , Annex A : 11 New Control (Highlight)
- การความต่อเนื่องทางธุรกิจตามแนวทาง ISO/IEC 22301:2019 เบื้องต้น (BIA,RPO,RTO,MTPD)
- การประเมินความเสี่ยง (Risk Assessment) เบื้องต้น
- กลยุทธ์การบรรเทาความเสี่ยง (Risk mitigation strategies)
- การกำหนดโครงสร้างการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ (SOPs)
- NIST Cybersecurity Framework v2.0
- บทบาทหน้าที่และการมีส่วนร่วม
- ระดมสมองทำโจทย์ Workshop

8 สรุปและตอบคำถาม

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Questions & Answer

www.MySurachet.com

085 636 2551

surachet@catinfonet.com

Thank you

LINE

LINE