

บันทึกข้อความ

ส่วนราชการ กลุ่มพัฒนาระบบบริหาร ทน. โทร ๐ ๒๒๗๑ ๖๑๙๗ โทรสาร ๐ ๒๒๙๘ ๖๖๒๓

ที่ ทส ๐๖๒๒.๑/๒๗๔ **วันที่** ๑๕ กรกฎาคม ๒๕๖๘

เรื่อง ขอส่งรายงานผลการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ ๑ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

เรียน หัวหน้ากลุ่มงานจริยธรรม
หัวหน้าผู้ตรวจราชการกรม
ผู้อำนวยการกอง ศูนย์ กลุ่ม
เลขานุการกรม
ผู้อำนวยการสำนักงานทรัพยากรน้ำที่ ๑-๑๑

ตามบันทึก กลุ่มพัฒนาระบบบริหาร ที่ ทส ๐๖๒๒.๑/๒๓๓ ลงวันที่ ๒๓ มิถุนายน ๒๕๖๘ อธิบดีกรมทรัพยากรน้ำได้รับทราบรายงานผลการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ ๑ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) รายละเอียดตามเอกสารแนบ นั้น

กลุ่มพัฒนาระบบบริหาร ขอส่งรายงานผลการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ ๑ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) มาเพื่อโปรดทราบ

จึงเรียนมาเพื่อโปรดทราบ

(นางสาวชมพูนุช ดลสุขเลิศ)
ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร

การประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ 1

เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

วันที่ 27 พฤษภาคม 2568 ณ ห้องประชุม Warroom ศูนย์เมขลา ชั้น 11
ณ ห้องประชุมสายชล ชั้น 9 กรมทรัพยากรน้ำ และผ่านระบบ ZOOM





ประธานในพิธีเปิดการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ 1 เพื่อเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ แก่บุคลากรในทุกระดับโดยมีผู้บริหารและเจ้าหน้าที่จากทุกหน่วยงาน เข้าร่วมอย่างพร้อมเพรียง

นางสาวอมรรัตน์ พุ่มศรีพักตร์
หัวหน้าผู้ตรวจราชการกรม

ประเด็นสำคัญจากวิทยากร



กล่าวถึงบทบาทของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่ช่วยให้หน่วยงานสามารถรับมือภัยคุกคามได้อย่างเป็นระบบ พร้อม**เสนอแนวทางการจัดลำดับความเสี่ยง จัดตั้งระบบป้องกัน-ตรวจจับ-ตอบสนองภัยไซเบอร์อย่างครบวงจร และเน้นการพัฒนาบุคลากรให้มีความรู้ความเข้าใจด้านนี้อย่างทั่วถึง**



นายกานตพันธุ์ พิศาลสุขสกุล
ผู้ช่วยปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม **DCIO** สป.ทส.



เน้นหลักการพื้นฐาน CIA Triad (Confidentiality, Integrity,Availability) พร้อมให้ภาพรวมกฎหมายไซเบอร์ที่เกี่ยวข้องทั้ง 3 ฉบับ และชี้ให้เห็นแนวโน้มการคุกคามในไทย เช่น Ransomware,Data Theft และ Server Access โดยเสนอแนวทางป้องกัน 10 ข้อ เช่น การอัปเดตระบบการสำรองข้อมูลการใช้ MFA และการจัดตั้ง SOC ตลอดจนการจัดการความเสี่ยงจาก AI และบุคคลภายนอก

นางสาวสายชล แซ่ลี้
ผู้อำนวยการสำนักประสานงาน รักษาการ ผู้อำนวยการสำนักปฏิบัติการ
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ







บริษัท SCP System ย้ำว่า **“ภัยคุกคามไซเบอร์คือเรื่องของทุกคน” โดยชี้ถึงการหลอกลวงแบบ Social Engineering** และความสำคัญของ Multi-Factor Authentication (MFA) รวมถึงบทบาท CISO ที่ทุกหน่วยงานควรมี และเสนอแนวคิด Zero Trust เพื่อเสริมความมั่นคงในการป้องกันภัย





นายสุชญา แสงหาญ
รองกรรมการผู้จัดการใหญ่ สายงาน โทรคมนาคมและความมั่นคงปลอดภัยทางไซเบอร์ บริษัท เอส.ซี.พี.ซิสเท็ม จำกัด



นำเสนอการดำเนินงานของกรมทรัพยากรน้ำ เช่น การติดตั้งระบบ EDR ตรวจจับภัยกว่า 45,000 รายการ การประเมินตนเองตามแนวทาง NIST Framework และการจัดทำแนวทางปฏิบัติที่ประกาศใช้อย่างเป็นทางการ เมื่อ 14 พฤษภาคม 2568 พร้อมชี้ปัญหาสำคัญ เช่น ขาดบุคลากรเฉพาะทาง งบประมาณไม่ต่อเนื่อง และระบบ IT ล้าสมัย



นายสุประภาพ พัฒน์สิงหเสนีย์
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมทรัพยากรน้ำ



การแบ่งปันและถอดบทเรียน

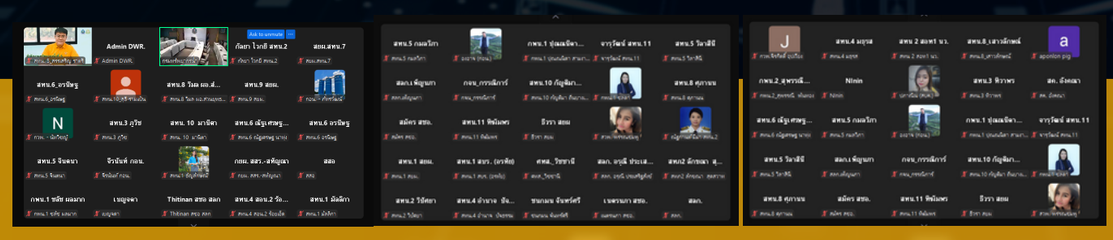
ผู้เข้าร่วมประชุมร่วมแลกเปลี่ยนประสบการณ์การป้องกันภัยไซเบอร์ ทั้งจากชีวิตประจำวันและการทำงาน พร้อม**ตระหนักร่วมกันว่า การรับมือภัยคุกคามไซเบอร์ ไม่ใช่หน้าที่เฉพาะของฝ่าย IT แต่เป็น “ความรับผิดชอบร่วมกันของทุกคนในองค์กร”**











สำนักงานอธิบดี
เลขที่รับ 6339
วันที่ 23 มิ.ย. 2568
เวลา 18.19 น.

สำนักงานรองอธิบดี ๒
เลขที่รับ 1752
วันที่ 23 มิ.ย. 2568
เวลา 10.02 น.

กรมทรัพยากรน้ำ (ภายใน)
ที่ 03469
๒๓ มิ.ย. ๒๕๖๘
09.56

บันทึกข้อความ

ส่วนราชการ กลุ่มพัฒนาระบบบริหาร กรมทรัพยากรน้ำ โทร ๐ ๒๒๗๑ ๖๑๙๗ โทรสาร ๐ ๒๒๙๘ ๖๖๒๓
ที่ ทส ๐๖๒๒.๑/๒๓๓ **วันที่** ๒๓ มิถุนายน ๒๕๖๘
เรื่อง รายงานผลการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ ๑ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

เรียน อธิบดีกรมทรัพยากรน้ำ

ตามบันทึกกลุ่มพัฒนาระบบบริหาร ที่ ทส ๐๖๒๒.๓/๖๔ ลงวันที่ ๒๘ เมษายน ๒๕๖๘ และบันทึกกลุ่มพัฒนาระบบบริหาร ที่ ทส ๐๖๒๒.๓/๘๓ ลงวันที่ ๒๒ พฤษภาคม ๒๕๖๘ ผู้อำนวยการกลุ่มพัฒนาระบบบริหารปฏิบัติราชการแทนอธิบดีกรมทรัพยากรน้ำ ได้อนุมัติจัดประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ ๑ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) ในวันอังคารที่ ๒๗ พฤษภาคม ๒๕๖๘ เวลา ๐๙.๐๐ น. – ๑๕.๓๐ น. ณ ห้องประชุม Warroom ศูนย์เมขลา ชั้น ๑๑ และห้องประชุมสายชล ชั้น ๙ กรมทรัพยากรน้ำ และผ่านสื่ออิเล็กทรอนิกส์ออนไลน์ (ระบบ Zoom) นั้น

กลุ่มพัฒนาระบบบริหาร ขอรายงานผลการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ ๑ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) โดยมี นางสาวอมรรัตน์ พุ่มศรีพักตร์ หัวหน้าผู้ตรวจราชการกรม เป็นประธานเปิดประชุมเชิงปฏิบัติการ มีผู้เข้าร่วมประชุม จำนวนทั้งสิ้น ๑๐๗ คน โดยสรุปผลการประชุม ได้ดังนี้

๑. นายกานตพันธุ์ พิศาลสุขสกุล ผู้ช่วยปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม และ DCIO สป.ทส. กล่าวถึงบทบาทของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่ช่วยให้หน่วยงานสามารถรับมือภัยคุกคามได้อย่างเป็นระบบ พร้อมเสนอแนวทางการจัดลำดับความเสี่ยง จัดตั้งระบบป้องกัน-ตรวจจับ-ตอบสนองภัยไซเบอร์อย่างครบวงจร และเน้นการพัฒนาบุคลากรให้มีความรู้ความเข้าใจด้านนี้อย่างทั่วถึง

๒. นางสาวสายชล แซ่ลี้ ผู้อำนวยการสำนักประสานงาน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เน้นหลักการพื้นฐาน CIA Triad (Confidentiality, Integrity, Availability) พร้อมให้ภาพรวมกฎหมายไซเบอร์ที่เกี่ยวข้องทั้ง ๓ ฉบับ และชี้ให้เห็นแนวโน้มการคุกคามในไทย เช่น Ransomware, Data Theft และ Server Access โดยเสนอแนวทางป้องกัน ๑๐ ข้อ เช่น การอัปเดตระบบ การสำรองข้อมูล การใช้ Multi-Factor Authentication (MFA) และการจัดตั้ง Security Operations center (SOC) ตลอดจนการจัดการความเสี่ยงจาก AI และบุคคลภายนอก

๓. นายสุชญา แสงหาญ รองกรรมการผู้จัดการใหญ่ สายงานโทรคมนาคม และความมั่นคงปลอดภัยทางไซเบอร์ บริษัท เอส.ซี.พี.ซิสเท็ม จำกัด ย้ำว่า “ภัยคุกคามไซเบอร์คือเรื่องของทุกคน” โดยชี้ถึงการหลอกลวงแบบ Social Engineering และความสำคัญของ MFA รวมถึงบทบาท CISO ที่ทุกหน่วยงานควรมี และเสนอแนวคิด Zero Trust เพื่อเสริมความมั่นคงในการป้องกันภัย

๔. นายสุประภาพ พัฒน์สิงหเสนีย์ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร นำเสนอการดำเนินงานของกรมทรัพยากรน้ำ เช่น การติดตั้งระบบ EDR ตรวจจับภัยกว่า ๔๕,๐๐๐ รายการ การประเมินตนเองตามแนวทาง NIST Framework และการจัดทำแนวทางปฏิบัติที่ประกาศใช้อย่างเป็นทางการเมื่อ ๑๔ พฤษภาคม ๒๕๖๘ พร้อมชี้ปัญหาสำคัญ เช่น ขาดบุคลากรเฉพาะทาง งบประมาณไม่ต่อเนื่อง และระบบ IT ล้าสมัย

๕.การแบ่งปัน...

เรืองกลับ กสน.
วันที่ - ๑ ก.ค. ๒๕๖๘
เวลา 09.40น.

๕. การแบ่งปันและถอดบทเรียน

๕.๑ ความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์ กลยุทธ์ที่มีประสิทธิภาพในการสร้างความตระหนักรู้ : องค์กรภาครัฐและเอกชน เริ่มตื่นตัวเรื่องความมั่นคงปลอดภัยไซเบอร์กันมากขึ้น เริ่มมีนโยบาย มีหน่วยงานที่ดูแล มีการฝึกอบรม ทั้งนี้ ควรสร้างความเข้าใจเกี่ยวกับ ภัยคุกคามพื้นฐาน เช่น อีเมลฟิชชิ่ง มัลแวร์ การหลอกลวงผ่านโซเชียลมีเดีย สังเกตแหล่งข้อมูลหลอกลวง มีความตระหนักว่าตัวเราเองและฝ่ายคอมพิวเตอร์เป็นเป้าหมายการโจมตีทางไซเบอร์ โดยกลยุทธ์ที่ได้ผล เช่น การทดสอบ เช่น จำลองอีเมลฟิชชิ่งในองค์กร ปัจจัยสำคัญเพื่อให้ประสบความสำเร็จในการป้องกันภัยคุกคาม คือการให้ความสำคัญต่อภัยคุกคามทั้งระดับผู้บริหารและบุคคล

๕.๒ จุดอ่อนหรือช่องโหว่ที่สำคัญ และความเสี่ยง : บุคคลเป็นจุดอ่อนที่ถูกโจมตีมากกว่าเทคโนโลยี จุดอ่อนที่พบบ่อย ได้แก่ การใช้รหัสผ่านซ้ำ รหัสที่คาดเดาได้ง่าย การมีระบบที่ไม่ได้รับการอัปเดตช่องโหว่ อย่างสม่ำเสมอ และการเปิดสิทธิ์ให้เกินความจำเป็น การดาวน์โหลดไฟล์แนบอันตรายโดยขาดการสังเกต การแบ่งปันรหัสผ่าน การข้ามขั้นตอนความปลอดภัย เช่น MFA

๕.๓ นโยบายและแนวปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ และการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์: ควรมีนโยบายและกรอบการทำงาน แผนการตอบสนองเหตุการณ์ ที่ชัดเจนครอบคลุม การควบคุมการเข้าถึง การประเมินความเสี่ยงองค์กรอย่างสม่ำเสมอ และการฝึกอบรมเจ้าหน้าที่ การอัปเดตเทคโนโลยี และเครื่องมือป้องกันภัยคุกคาม การตรวจสอบและประเมินความเสี่ยงอย่างต่อเนื่องและทดสอบการตอบสนองโดยการจัดทำการจำลองสถานการณ์ ทั้งนี้ ควรจัดสรรงบประมาณทั้งด้านเครื่องมือซอฟต์แวร์และบุคลากร

๕.๔ การรับมือและตอบสนองต่อเหตุการณ์ภัยคุกคามไซเบอร์ที่มีประสิทธิภาพ : ประกอบด้วย การเตรียมความพร้อม การตรวจจับและการระบุเหตุการณ์ การตอบสนองต่อเหตุการณ์ การวิเคราะห์เพื่อเรียนรู้จากการถูกโจมตี การวิเคราะห์ช่องโหว่ของระบบ การตรวจสอบแผนการตอบสนองเพื่อปรับปรุงมาตรการป้องกัน

๕.๕ ผู้เข้าร่วมประชุมร่วมแลกเปลี่ยนประสบการณ์การป้องกันภัยไซเบอร์ ทั้งจากชีวิตประจำวันและการทำงาน พร้อมตระหนักร่วมกันว่า การรับมือภัยคุกคามไซเบอร์ไม่ใช่หน้าที่เฉพาะของฝ่าย IT แต่เป็น “ความรับผิดชอบร่วมกันของทุกคนในองค์กร”

๖. สรุปผลการประเมินความคิดเห็นจากผู้เข้าร่วมการประชุม แบ่งเป็น ๓ ด้าน

๖.๑ ด้านวิทยากร ค่าเฉลี่ยรวมอยู่ในระดับความพึงพอใจมากที่สุด คิดเป็นร้อยละ ๙๔.๓๐

๖.๒ ด้านความเข้าใจ มีค่าเฉลี่ยรวมอยู่ในระดับความพึงพอใจมาก คิดเป็นร้อยละ ๘๗.๗๔

๖.๓ ด้านการนำความรู้ไปใช้ มีค่าเฉลี่ยรวมอยู่ในระดับความพึงพอใจมาก คิดเป็นร้อยละ ๘๙.๘๐

ทั้งนี้ รายงานผลการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ ๑ รายละเอียดตามเอกสารแนบ

จึงเรียนมาเพื่อโปรดทราบ และกลุ่มพัฒนาระบบบริหารจะได้เผยแพร่รายงานผลการประชุมฯ เพื่อให้ทุกหน่วยงานนำองค์ความรู้ไปใช้ประโยชน์ด้านความมั่นคงปลอดภัยไซเบอร์ต่อไป

เรียน ท่าน อทช.
เพื่อโปรดทราบ

(นางสาวชมพูนุช ดลสุขเลิศ)
ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร

- ทราบ
-

(นายเวสารัช โสภณดิเรกรัตน์)
รองอธิบดีกรมทรัพยากรน้ำ
๓ มิ.ย. ๒๕๖๘

(นายธีระชุณ บุญสิทธิ์)
อธิบดีกรมทรัพยากรน้ำ
30 มิ.ย. 2568



รายงานผลการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ 1

เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

(Cyber Security Awareness)

วันอังคารที่ 27 พฤษภาคม 2568

ณ ห้องประชุม Warroom ศูนย์เมขลา ชั้น 11 และ ห้องประชุมสายชล ชั้น 9 กรมทรัพยากรน้ำ

และผ่านระบบสื่ออิเล็กทรอนิกส์ออนไลน์

สารบัญ

	หน้า
1. หลักการและเหตุผล	1
2. วัตถุประสงค์	1
3. กลุ่มเป้าหมาย	1
4. สรุปผลการประชุม	1
5. ผลการประเมินความคิดเห็นจากผู้เข้าร่วมการประชุม	6
6. ประโยชน์ที่ได้รับ	9
7. ข้อเสนอแนะ	9
ภาคผนวก ก รายชื่อวิทยากรและผู้เข้าร่วมประชุม	10
ภาคผนวก ข ประเด็นการแบ่งปันความรู้	14

รายงานผลการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ 1
เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)
วันอังคารที่ 27 พฤษภาคม 2568
ณ ห้องประชุม Warroom ศูนย์เมขลา ชั้น 11 และ ห้องประชุมสายชล ชั้น 9 กรมทรัพยากรน้ำ
และผ่านระบบสื่ออิเล็กทรอนิกส์ออนไลน์

---

1. หลักการและเหตุผล

รัฐบาลได้กำหนดยุทธศาสตร์ด้านการพัฒนาเทคโนโลยีดิจิทัลไว้ในนโยบายและยุทธศาสตร์ชาติ อาทิ ยุทธศาสตร์ชาติระยะ 20 ปี (พ.ศ. 2561-2580) ที่มุ่งเน้นอุตสาหกรรมและบริการดิจิทัล ข้อมูล และปัญญาประดิษฐ์ ภายใต้ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขัน ตลอดจนแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561-2580) ซึ่งเป็นแผนแม่บทหลักในการส่งเสริมโครงสร้างพื้นฐานการพัฒนาเศรษฐกิจดิจิทัล การสร้างสังคมคุณภาพ การส่งเสริมรัฐบาลดิจิทัล ตลอดจนการพัฒนากำลังคนและเสริมสร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล ทั้งนี้ ภัยคุกคามไซเบอร์ รวมทั้งภัยคุกคามจากสารสนเทศรูปแบบต่างๆ มีการพัฒนาและเปลี่ยนแปลงรูปแบบอย่างต่อเนื่อง ดังนั้น การเตรียมความพร้อมเพื่อรับมือ ด้วยการเสริมสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเพิ่มความสามารถของบุคลากรในการรักษาความมั่นคงปลอดภัย ในการป้องกันตนเองและหน่วยงาน เพื่อลดความเสี่ยงและผลกระทบจากการถูกโจมตีหรือภัยคุกคามไซเบอร์ เป็นบริบทที่เป็นความท้าทายและโอกาสของกรมทรัพยากรน้ำ

เพื่อตอบสนองยุทธศาสตร์ดังกล่าว และแผนขับเคลื่อนการพัฒนาคุณภาพการบริหารจัดการภาครัฐสู่ระบบราชการ 4.0 ประจำปีงบประมาณ พ.ศ. 2568 หมวดที่ 4 การวัด วิเคราะห์ และการจัดการความรู้ กิจกรรมที่ 3 การจัดการความรู้ และการสร้างองค์ความรู้ ซึ่งกำหนดให้มีการจัดกิจกรรมการจัดการองค์ความรู้เพื่อปรับปรุงและเพิ่มประสิทธิภาพในการดำเนินการ กลุ่มพัฒนาระบบบริหาร กรมทรัพยากรน้ำ จึงได้จัดโครงการประชุมสัมมนาแลกเปลี่ยนเรียนรู้ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

2. วัตถุประสงค์

1. เพื่อเสริมสร้างความรู้ความเข้าใจ และความตระหนักถึงความเสี่ยงในการถูกโจมตีไซเบอร์
2. เพื่อเสริมสร้างความรู้ความเข้าใจในการป้องกันตนเองและหน่วยงานจากภัยคุกคามไซเบอร์

3. กลุ่มเป้าหมาย

บุคลากรในสังกัดกรมทรัพยากรน้ำ รวม 120 ราย ส่วนกลาง จำนวน 65 ราย และสำนักงานทรัพยากรน้ำที่ 1-11 จำนวน 55 ราย

4. สรุปผลการประชุม

กลุ่มพัฒนาระบบบริหาร ได้จัดการประชุมเชิงปฏิบัติการ KM-COP ครั้งที่ 1 เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) โดยมีนางสาวอมรรัตน์ พุ่มศรีพักตร์ หัวหน้าผู้ตรวจราชการกรม เป็นประธานเปิดประชุมเชิงปฏิบัติการ ณ ห้องประชุม Warroom ศูนย์เมขลา ชั้น 11 กรมทรัพยากรน้ำ และผ่านสื่ออิเล็กทรอนิกส์ โดยมีผู้บริหารและเจ้าหน้าที่ทุกหน่วยงานเข้าร่วมการประชุมสัมมนาแลกเปลี่ยนเรียนรู้ จำนวนทั้งสิ้น 107 คน การประชุมครั้งนี้ฯ เพื่อการสร้างความตระหนักรู้ด้านความมั่นคง

ปลอดภัยไซเบอร์ ซึ่งไม่ใช่ภารกิจของฝ่ายเทคโนโลยีสารสนเทศเท่านั้น แต่เป็นหน้าที่ร่วมกันของทุกคนในองค์กร ที่ต้องมีความเข้าใจในการป้องกันตนเอง โดยมีประเด็นสาระที่สำคัญ ดังนี้

นายกานตพันธุ์ พิศาลสุขสกุล ผู้ช่วยปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) สป.ทส. ได้นำเสนอว่า ปัจจุบันโลกเปลี่ยนแปลงไป รัฐบาลจึงประกาศพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อให้เมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม (สป.ทส.) มีผู้รับผิดชอบดูแลแต่ละระบบของหน่วยงานที่แตกต่างกัน ส่งผลให้เกิดความเสี่ยงที่จะเกิดภัยคุกคามด้านไซเบอร์ เนื่องจากแต่ละระบบผู้รับผิดชอบตั้งรหัสผ่านเข้าระบบเอง ทำให้บุคคลภายนอกเข้าถึงระบบได้ง่าย อีกทั้งหน่วยงานมีปัญหาในเรื่องของมัลแวร์ (Malware) และการแฮคเข้ามาโจมตีในรูปแบบต่างๆ สป.ทส. จึงได้ขับเคลื่อนในเรื่องความปลอดภัยไซเบอร์ ดังนี้

1. ทำความเข้าใจ และสร้างความตระหนักรู้กับบุคลากรภายในหน่วยงานที่เป็นผู้รับผิดชอบดูแลระบบ โดยศึกษาจากการดำเนินงานเรื่องความปลอดภัยไซเบอร์จากหน่วยงานภาคเอกชน ซึ่งมีการทำงานในรูปแบบ Check and Balance รวมทั้งให้ความรู้กับบุคลากรทุกคนในเรื่องความปลอดภัยไซเบอร์

2. จัดลำดับความสำคัญระบบที่มีความสุ่มเสี่ยงต่อการโดนคุกคามทางด้านไซเบอร์

3. จัดสรรงบประมาณเพื่อจัดตั้งระบบการรักษาความปลอดภัยให้ครอบคลุมทุกขั้นตอนตั้งแต่ระบบป้องกัน ระบบตรวจจับ ระบบวิเคราะห์ และระบบตอบสนอง

4. กำหนดผู้รับผิดชอบดูแลระบบการรักษาความปลอดภัย

5. เชื่อมต่อระบบต่างๆ ของหน่วยงานกับระบบการรักษาความปลอดภัย ตามนโยบายการใช้คลาวด์ภัยคุกคามทางไซเบอร์ เป็นหลัก (Cloud First Policy)

การเลือกใช้วิธีการแก้ปัญหาด้านความปลอดภัยไซเบอร์ที่มีประสิทธิภาพประกอบด้วย 4 ขั้นตอนหลัก ได้แก่ (1) การประเมินความเสี่ยงและความต้องการ โดยวิเคราะห์ภัยคุกคามเฉพาะของหน่วยงานรวมถึงทรัพยากรที่มีและข้อจำกัดด้านงบประมาณ (2) พัฒนาแผนงานความปลอดภัย (3) การนำไปใช้และบูรณาการตามลำดับความสำคัญควบคู่กับการฝึกอบรมบุคลากร และ (4) การติดตามผลเพื่อปรับปรุงอย่างต่อเนื่อง สิ่งสำคัญที่สุดในเรื่องความปลอดภัยไซเบอร์ คือ การพัฒนาบุคลากรของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารและบุคลากรของทั้งหน่วยงานให้มีความรู้ ความเข้าใจ และความตระหนักรู้

นายสุชญา แสงหาญ รองกรรมการผู้จัดการใหญ่ สายงาน โทรคมนาคม และ ความมั่นคงปลอดภัยทางไซเบอร์ บริษัท เอส.ซี.พี.ซิสเท็ม จำกัด ได้นำเสนอว่า ปัญหาความปลอดภัยไซเบอร์ คือ ปัญหาของทุกคน เพราะประชาชนมีความรู้เท่าทันและความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ไม่เท่ากัน ปัจจุบันประชาชนโดนคุกคามทางไซเบอร์เป็นจำนวนมาก เนื่องจาก Social Engineering หรือวิศวกรรมสังคม เป็นศิลปะในการหลอกลวง ล่อหลอกผู้อื่น โดยใช้หลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล เพื่อให้ได้ผลประโยชน์ตามที่แฮกเกอร์ต้องการ โดยอาศัยจุดอ่อน ความรู้เท่าไม่ถึงการณ์ ความไม่รู้ ความประมาท ซึ่งจุดอ่อนต่างๆ มาจากการเข้าถึงข้อมูลบุคคล ข้อมูลหน่วยงาน ผ่านช่องทาง Social Media เพราะฉะนั้นความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ของบุคคลจึงเป็นสิ่งสำคัญ ซึ่งความตระหนักรู้ต้องเริ่มต้นจากตัวบุคคลก่อนที่จะไม่เป็นภัยคุกคามทางไซเบอร์ต่อหน่วยงาน ปัจจุบันหน่วยงานใช้การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication : MFA) เป็นกระบวนการเข้าสู่ระบบบัญชีแบบหลายขั้นตอนที่กำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน และมีการตรวจสอบและกำหนดให้ผู้ดูแลระบบเปลี่ยนรหัสผ่านเป็นประจำทุก 3 – 6 เดือน อีกทั้งภัยคุกคามทางไซเบอร์ยังมาจากบุคคลที่สามที่หน่วยงานภาครัฐและรัฐวิสาหกิจจ้างมาบริหารจัดการ ดูแลระบบ ซึ่งบุคคลที่สามไม่มีความตระหนักด้านความปลอดภัยไซเบอร์เนื่องจากเมื่อเกิดภัยคุกคามทางไซเบอร์จะไม่ส่งผล

ต่อหน่วยงานของตัวเองโดยตรง เพราะฉะนั้นบุคลากรด้านเทคโนโลยีสารสนเทศของหน่วยงานต้องเข้ามามีบทบาทในการกำหนดการตั้งชื่อผู้ใช้งานและรหัสผ่านในการเข้าสู่ระบบ รวมทั้งกำหนดนโยบายเพื่อให้เกิดดำเนินการอย่างต่อเนื่อง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้กำหนดให้หน่วยงานแต่งตั้งผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO) ทำหน้าที่พัฒนาและนำระบบรักษาความปลอดภัยมาใช้เพื่อป้องกัน ตรวจจับ และรับมือกับการโจมตีทางไซเบอร์ และขอให้หน่วยงานตรวจประเมินทางไซเบอร์ทุกปี โดยใช้กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ NIST (National Institute of Standards and Technology) เพื่อช่วยให้องค์กรภาครัฐและเอกชนสามารถประเมินจัดการและลดความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพ แบ่งออกเป็น 5 ฟังก์ชันหลัก ดังนี้

1. Identify (ระบุ) การระบุทรัพย์สินดิจิทัลและความเสี่ยง เพื่อเข้าใจบริบทธุรกิจและทรัพยากรที่ต้องปกป้อง

2. Protect (ป้องกัน) การใช้มาตรการป้องกันที่เหมาะสม เพื่อสร้างระบบป้องกันหลายชั้น

3. Detect (ตรวจจับ) ระบบตรวจจับการโจมตีทางไซเบอร์ เพื่อติดตามและวิเคราะห์เหตุการณ์ด้านความปลอดภัยอย่างต่อเนื่อง

4. Respond (ตอบสนอง) แผนตอบสนองต่อเหตุการณ์ไซเบอร์ เพื่อรับมือกับภัยคุกคามอย่างเป็นระบบและลดผลกระทบ

5. Recover (ฟื้นฟู) การกู้คืนและดำเนินการต่อเนื่อง เพื่อฟื้นฟูระบบและบริการให้กลับมาทำงานได้ตามปกติพร้อมทั้งปรับปรุงแผนจากบทเรียนที่ได้รับ

สิ่งที่สำคัญที่สุดของการขับเคลื่อนเรื่องภัยคุกคามทางไซเบอร์ คือ (1) บุคลากรทุกคนต้องมีความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ พร้อมทั้งให้ความร่วมมือในการดำเนินงานขับเคลื่อนการปลอดภัยไซเบอร์ของหน่วยงาน และ (2) ผู้บริหารต้องมีความรู้ ความเข้าใจ เรื่องภัยคุกคามทางไซเบอร์ เพื่อจัดสรรงบประมาณภัยคุกคามทางไซเบอร์ เพื่อดำเนินการเรื่องความปลอดภัยทางไซเบอร์ของหน่วยงาน

นางสาวสายชล แซ่ลี้ ผู้อำนวยการสำนักประสานงาน รักษาการผู้อำนวยการสำนักปฏิบัติการ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้กล่าวถึง ความสำคัญในการสร้างความตระหนักและเสริมทักษะจำเป็นด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งครอบคลุมถึงหลักการพื้นฐานในการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ กฎหมาย สถานการณ์ภัยคุกคามไซเบอร์ระดับโลก ระดับประเทศ และแนวทางในการป้องกันฯ ดังนี้

1. ความหมาย ของ “Cyber Security” คือ ความมั่นคงปลอดภัยทางไซเบอร์ ที่ต้องการป้องกันและการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้อง โดยจุดประสงค์ คือ ป้องกันการเข้าถึง การแก้ไข การเปลี่ยนแปลง หรือการทำลายข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต หรือบุคคลที่ต้องการเข้าถึงข้อมูล เพื่อวัตถุประสงค์ที่ไม่เหมาะสม และ “ภัยคุกคามทางไซเบอร์” คือ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

2. หลักการพื้นฐานการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ CIA Triad ประกอบด้วย



Confidentiality หรือ การรักษาความลับของข้อมูล คือ การรับสิทธิในการเข้าถึงข้อมูลลับผู้ที่สามารถเข้าถึงในแต่ละชุดข้อมูล ตามลำดับและชั้นความลับที่กำหนด Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล

3. กฎหมายที่เกี่ยวข้อง ได้แก่

3.1 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ 2560 ซึ่งเป็นกฎหมายที่ครอบคลุมการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การแฮ็กและการเผยแพร่ข้อมูลเท็จ เป็นกฎหมายพื้นฐานสำหรับการดำเนินคดีกับผู้กระทำผิดทางไซเบอร์

3.2 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.2562 ซึ่งเป็นกฎหมายเพื่อบังคับให้องค์กรในภาคส่วนสำคัญ (เช่น การเงิน พลังงาน คมนาคม และสุขภาพ) ต้องดำเนินมาตรการป้องกันโครงสร้างพื้นฐานสารสนเทศที่สำคัญ และให้สิทธิแก่รัฐบาลในการตรวจสอบและจัดการเหตุการณ์ทางไซเบอร์

3.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยมีเป้าหมายในการคุ้มครองข้อมูลส่วนบุคคลของประชาชน โดยกำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้และจัดเก็บข้อมูล พร้อมทั้งให้สิทธิกับเจ้าของข้อมูลในการควบคุมข้อมูลส่วนตัวและกำหนดบทลงโทษกรณีละเมิด

4. สถานการณ์ภัยคุกคามไซเบอร์ระดับโลก โดย Ransomware ซึ่งเป็นการโจมตีที่มีสัดส่วนสูงสุด ร้อยละ 23 ตามด้วย Data Theft และ Server Access ซึ่งมีสัดส่วน ร้อยละ 13 และร้อยละ 10 ตามลำดับ โดยเหตุการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย เช่น การโจมตีโรงพยาบาลหลายแห่งในประเทศไทยด้วยแรมซัมแวร์ การโจมตีธนาคารไทยทำให้เครื่องเอทีเอ็มจ่ายเงินสดได้โดยไม่ใช้บัตร การแฮกข้อมูลจากหน่วยงานภาครัฐ การแพร่ข่าวสารเท็จ เช่น การเผยแพร่ข่าวสารเท็จเกี่ยวกับการเมือง และการโจมตีโครงสร้างพื้นฐานสำคัญ เช่น การโจมตีระบบโทรคมนาคม กรณีโจมตีระบบโทรคมนาคมและอินเตอร์เน็ตของประเทศไทยทำให้การสื่อสารหยุดชะงัก เป็นต้น

5. แนวทางในการป้องกัน

5.1 อัปเดตซอฟต์แวร์และระบบอยู่เสมอ และหลีกเลี่ยงการดาวน์โหลดและติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ (Software Updates & Patching)

5.2 สำรองข้อมูลอย่างปลอดภัยและเป็นประจำ (Data Backup and Disaster Recovery)

5.3 ยกระดับความปลอดภัยด้วยการยืนยันตัวตน 2 ขั้นตอน

5.4 แต่งตั้งและเสริมบทบาทของ Data Protection Officer (DPO) และ Chief Information Security Officer (CISO)

5.5 จัดตั้ง Security Operation Center (SOC) ตลอดจนตรวจสอบและวิเคราะห์กิจกรรมในเครือข่ายอย่างสม่ำเสมอ

5.6 จัดการความเสี่ยงจากการใช้ AI อย่างมีจริยธรรม (AI Risk Management)

5.7 ส่งเสริมการใช้รหัสผ่านที่ปลอดภัยและนโยบาย Zero-Trust

5.8 มีการกำกับดูแลและคัดเลือกบริษัทที่มีประสบการณ์และมาตรฐานความปลอดภัยและหลีกเลี่ยงการใช้ข้อมูลจริงในขั้นตอนการพัฒนา

5.9 ป้องกัน Insider Threat และจัดการ Offboarding อย่างปลอดภัย

5.10 ให้ความรู้แก่พนักงานและปรับปรุงความรู้

นายสุประภาพ พัฒน์สิงหเสนีย์ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กล่าวอภิปรายเกี่ยวกับ

1. สถานการณ์ปัจจุบันของการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพยากรน้ำ

1.1 แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ : มีการดำเนินการตามแนวทางของ NIST Cybersecurity Framework Version 2.0 และได้ลงนามประกาศ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อวันที่ 14 พฤษภาคม 2568 และได้มีการเวียนให้หน่วยงานภายในกรมฯ รับทราบและถือปฏิบัติ

1.2 การติดตั้ง Endpoint Detection and Response (EDR) เพื่อตรวจจับ ตอบสนอง และวิเคราะห์ภัยคุกคาม : มีการติดตั้ง IBM ReaQta 450 Endpoints ตั้งแต่เดือนเมษายน 2567 - เมษายน 2568 พบภัยคุกคามเริ่มต้น 45,362 รายการ และภัยคุกคามระดับที่เป็นอันตรายต่อระบบภายในองค์กร (Malicious) จำนวน 4,149 รายการ โดยระบบฯ ได้ดำเนินการลบไฟล์ที่ต้องสงสัยเรียบร้อยแล้ว

1.3 การประเมินระดับการเตรียมพร้อมและการปรับตัว (Cyber Resilience Assessment) :

1) การประเมินความเสี่ยงตั้งต้นด้านไซเบอร์ (Inherent Risk Assessment - IRA) : เป็นการประเมินเบื้องต้น ด้านเทคโนโลยีและการเชื่อมต่อ ช่องทางการให้บริการ ลักษณะผลิตภัณฑ์และการให้บริการ ขนาดและลักษณะเฉพาะขององค์กร และประวัติการถูกคุกคามทางไซเบอร์ โดยจากการประเมินตนเอง กรมทรัพยากรน้ำได้ระดับความเสี่ยงปานกลาง

2) การประเมินระดับการจัดการภัยคุกคามทางไซเบอร์ (Maturity Assessment - MA) : เป็นการประเมินการกำกับดูแล การระบุความเสี่ยง การป้องกันความเสี่ยง การตรวจจับ การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ การบริหารความเสี่ยงจากบุคคลภายนอก โดยจากการประเมินกรมทรัพยากรน้ำมีมาตรการดำเนินการที่แล้วเสร็จ 69 รายการ ที่ยังไม่ได้ดำเนินการ 51 รายการ

1.4 การเชื่อมต่อแพลตฟอร์ม Malware Information Sharing Platform (MISP) : มีการเชื่อมต่อแพลตฟอร์ม MISP

1.5 การตรวจสอบและประเมินช่องโหว่ (Vulnerability Assessment) : อยู่ระหว่างดำเนินการ

2. ปัญหา อุปสรรคและผลตอบรับเมื่อดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์

2.1 ขาดบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์ : ส่งผลให้ไม่สามารถตอบสนองต่อภัยคุกคามที่ซับซ้อนและทันสมัยได้อย่างทันท่วงที

2.2 งบประมาณโครงการด้านความมั่นคงปลอดภัยไซเบอร์ไม่ได้รับการจัดสรรอย่างต่อเนื่อง : จำเป็น ต้องสื่อสารให้ผู้บริหารทราบความสำคัญในการใช้งบประมาณในการป้องกัน ซึ่งจะน้อยกว่าการแก้ไขปัญหาเมื่อถูกโจมตี

2.3 ความตระหนักรู้ของบุคลากรภายในองค์กรเกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์ : บุคลากรในองค์กรจำนวนมากยังขาดความเข้าใจและความตระหนักถึงความสำคัญของการรักษาความปลอดภัยไซเบอร์ ทำให้เกิดพฤติกรรมที่เสี่ยงต่อการถูกโจมตี

2.4 ระบบเทคโนโลยีสารสนเทศที่เก่าและมีความล้าสมัย : ทำให้ไม่สามารถรองรับการใช้งานเทคโนโลยีการป้องกันไซเบอร์รุ่นใหม่เข้ามาใช้ได้อย่างเต็มประสิทธิภาพ หรือแม้แต่ข้อจำกัดในการอัปเดตซอฟต์แวร์เพื่อเพิ่มประสิทธิภาพการป้องกันการโจมตี

2.5 พัฒนาการและความหลากหลายของภัยคุกคาม :ภัยคุกคามหรือรูปแบบการโจมตีทางไซเบอร์มีการเปลี่ยนแปลงรวดเร็ว กว่าความรู้ของคนในองค์กรและขีดความสามารถของระบบป้องกัน

ประเด็นการแบ่งปันประสบการณ์

1. ความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์ กลยุทธ์ที่มีประสิทธิภาพในการสร้างความตระหนักรู้ : องค์กรภาครัฐและเอกชน เริ่มตื่นตัวเรื่องความมั่นคงปลอดภัยไซเบอร์กันมากขึ้น เริ่มมีนโยบาย มีหน่วยงานที่ดูแล มีการฝึกอบรม ทั้งนี้ ควรสร้างความเข้าใจเกี่ยวกับ ภัยคุกคามพื้นฐาน เช่น อีเมลฟิชชิ่ง มัลแวร์ การหลอกลวงผ่านโซเชียลมีเดีย สังเกตแหล่งข้อมูลหลอกลวง มีความตระหนักว่า ตัวเราเองและฝ่ายคอมพิวเตอร์เป็นเป้าหมายการโจมตีทางไซเบอร์ โดยกลยุทธ์ที่ได้ผล เช่น การทดสอบ เช่น จำลองอีเมลฟิชชิ่งในองค์กร ปัจจัยสำคัญเพื่อให้ประสบความสำเร็จในการป้องกันภัยคุกคาม คือการให้ความสำคัญต่อภัยคุกคามทั้งระดับผู้บริหารและบุคคล

ส่วนที่ 1 สถานภาพทั่วไป

เพศ	จำนวน (คน)	ร้อยละ
ชาย	29	38.16
หญิง	47	61.84
รวมทั้งสิ้น	**76**	**100.00**

สถานภาพ	จำนวน (คน)	ร้อยละ
ข้าราชการ	46	60.53
พนักงานราชการ	23	30.26
ลูกจ้างประจำ	2	2.63
จ้างเหมาบริการ	5	6.58
รวมทั้งสิ้น	**76**	**100.00**

ส่วนที่ 2 ระดับความพึงพอใจ/ความรู้ ความเข้าใจ/การนำไปใช้ต่อการเข้าร่วมโครงการ

ผลการแสดงความคิดเห็นและความพึงพอใจต่อการประชุม โดยเกณฑ์ใช้ในการวิเคราะห์ข้อมูลระดับความพึงพอใจ/ความรู้ ความเข้าใจ/การนำไปใช้ ต่อการเข้าร่วมโครงการ แบ่งเป็น 5 ระดับ ดังนี้

4.51 - 5.00 หมายถึง มากที่สุด
3.51 - 4.50 หมายถึง มาก
2.51 - 3.50 หมายถึง ปานกลาง
1.51 - 2.50 หมายถึง น้อย
1.00 - 1.50 หมายถึง น้อยที่สุด

ด้านวิทยากร โดยมีค่าเฉลี่ยรวมอยู่ในระดับความพึงพอใจมากที่สุด คิดเป็นร้อยละ 94.34

ข้อ	ด้านวิทยากร	ระดับความคิดเห็น					รวม	ค่าเฉลี่ย	SD	เกณฑ์การประเมิน
		มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด				
		5	4	3	2	1				
1	การเตรียมตัวและความพร้อมของวิทยากร	59	16	1	0	0	76	4.76	0.46	มากที่สุด
2	การถ่ายทอดของวิทยากร	61	15	0	0	0	76	4.80	0.40	มากที่สุด
3	สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น	60	16	0	0	0	76	4.79	0.41	มากที่สุด
4	ใช้ภาษาที่เหมาะสมและเข้าใจง่าย	52	24	0	0	0	76	4.68	0.46	มากที่สุด
5	การตอบคำถามของวิทยากร	54	20	1	1	0	76	4.67	0.57	มากที่สุด
6	เอกสารประกอบการบรรยายเหมาะสม	50	21	5	0	0	76	4.59	0.61	มากที่สุด
							ค่าเฉลี่ยรวม	**4.72**	**0.48**	**มากที่สุด**

ด้านความเข้าใจ โดยมีค่าเฉลี่ยรวมอยู่ในระดับความพึงพอใจมาก คิดเป็นร้อยละ 87.74

ข้อ	ด้านความเข้าใจ	ระดับความคิดเห็น					รวม	ค่าเฉลี่ย	SD	เกณฑ์การประเมิน
		มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด				
		5	4	3	2	1				
1	ความเข้าใจเรื่องนี้ก่อนการเข้าอบรม	23	15	26	12	0	76	3.64	1.07	มาก
2	ความเข้าใจเรื่องนี้หลังการอบรม	44	28	4	0	0	76	4.53	0.60	มากที่สุด
3	สามารถบอกประโยชน์ได้	50	23	3	0	0	76	4.62	0.56	มากที่สุด
4	สามารถบอกข้อดีได้	49	23	4	0	0	76	4.59	0.59	มากที่สุด
5	สามารถอธิบายรายละเอียดได้	37	31	8	0	0	76	4.38	0.67	มาก
6	สามารถจัดระบบความคิด/ประมวลความคิดสู่การพัฒนาอย่างเป็นระบบ	38	32	6	0	0	76	4.42	0.63	มาก
7	บูรณาการทางความคิดสู่การทำงานเป็นทีม/การปรับตัวของบุคลากร/การปฏิรูประบบการทำงานในการปฏิบัติงาน	45	26	5	0	0	76	4.53	0.62	มากที่สุด
							ค่าเฉลี่ยรวม	**4.39**	**0.68**	**มาก**

ด้านการนำความรู้ไปใช้ โดยมีค่าเฉลี่ยรวมอยู่ในระดับความพึงพอใจมาก คิดเป็นร้อยละ 89.80

ข้อ	ด้านการนำความรู้ไปใช้	ระดับความคิดเห็น					รวม	ค่าเฉลี่ย	SD	เกณฑ์การประเมิน
		มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด				
		5	4	3	2	1				
1	สามารถนำความรู้ที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงานได้	50	23	3	0	0	76	4.62	0.56	มากที่สุด
2	สามารถนำความรู้ไปเผยแพร่/ถ่ายทอดแก่เจ้าหน้าที่ภายในหน่วยงานของท่านได้	38	33	4	1	0	76	4.42	0.65	มาก
3	สามารถให้คำปรึกษาแก่เพื่อนร่วมงานได้	38	33	5	0	0	76	4.43	0.61	มาก
4	มีความเข้าใจและสามารถนำความรู้ที่ได้รับไปใช้ได้	42	29	5	0	0	76	4.49	0.62	มาก
							ค่าเฉลี่ยรวม	**4.49**	**0.61**	**มาก**

6. ประโยชน์ที่ได้รับ

1. ผู้เข้าร่วมประชุมสัมมนาได้รับความรู้ความเข้าใจ และตระหนักถึงความเสี่ยงในการถูกโจมตีไซเบอร์

2. ผู้เข้าร่วมประชุมสัมมนาได้รับความรู้ความเข้าใจในการป้องกันตนเองและหน่วยงานจากภัยคุกคามไซเบอร์

7. ข้อเสนอแนะ

1. ได้ความรู้มากๆ
2. อยากให้มีการจัดอบรมแบบนี้อีก
3. เนื้อหามีความเหมาะสมและมีประโยชน์กับหน่วยงาน
4. อยากให้ประชาสัมพันธ์อย่างต่อเนื่อง และต้องมีระบบตรวจสอบสม่ำเสมอ
5. อยากให้กรมมีโปรแกรมแท้ในการใช้งาน เพราะบางทีต้องไปโหลดโปรแกรมในการทำงานแบบฟรีในอินเตอร์เน็ตมาใช้ และอยากให้มีเครือข่ายอินเตอร์เน็ตที่ปลอดภัย
6. อยากให้มีการอัพเดทการเตือนภัยด้านไซเบอร์อย่างสม่ำเสมอเมื่อมีปัญหาใหม่ๆ เข้ามา
7. ควรมีเวลาให้วิทยากรให้ความรู้มากกว่านี้ อย่างน้อยควรเป็นความรู้เกี่ยวกับการลงมือรับมือหรือวิธีแก้ไขปัญหาเบื้องต้น หากโดนเจาะระบบ การปิดระบบหน้าบ้านหลังบ้านเพื่อไม่ให้เกิดความบานปลาย

ภาคผนวก ก

รายชื่อวิทยากรและผู้เข้าร่วมประชุม

รายชื่อวิทยากร

1. นายกานตพันธุ์ พิศาลสุขสกุล	ผู้ช่วยปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) สป.ทส. สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
2. นางสาวสายชล แซ่ลี้	ผู้อำนวยการสำนักประสานงาน รักษาการผู้อำนวยการสำนักปฏิบัติการ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
3. นายสุชญา แสงหาญ	รองกรรมการผู้จัดการใหญ่ สายงาน โทรคมนาคม และความมั่นคงปลอดภัยทางไซเบอร์ บริษัท เอส.ซี.พี.ซิสเท็ม จำกัด
4. นายสุประภาพ พัฒน์สิงหเสนีย์	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

รายชื่อผู้เข้าร่วมประชุม

ณ ห้องประชุม Warroom ศูนย์เมขลา ชั้น 11 และ ห้องประชุมสายชล ชั้น 9 กรมทรัพยากรน้ำ

1. นางสาวอมรรัตน์ พุ่มศรีพักตร์	หัวหน้าผู้ตรวจราชการกรม กตร.
2. นางสาวชมพูนุช ดลสุขเลิศ	ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร กพร.
3. นางรัตน์ดา พัฒน์สิงหเสนีย์	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กพร.
4. นางสาวกมลา มัทธกุลพร	นักวิเคราะห์นโยบายและแผนชำนาญการ กพร.
5. นางสาวกัลยาณี มิ่งประยูร	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กพร.
6. นางสาววิสาขา นิลวัตร	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กพร.
7. นางสาวพัชรี มีเย็น	เจ้าหน้าที่บริหารงานทั่วไป กพร.
8. นางธัญลักษณ์ สิงหเรศร์	เจ้าหน้าที่บริหารงานทั่วไป กพร.
9. นางสาวจารุวรรณ เพชรมั่น	เจ้าหน้าที่วิเคราะห์นโยบายและแผน กพร.
10. นางสาวมัสลิน สิงห์บุญญานุภาพ	เจ้าหน้าที่วิเคราะห์นโยบายและแผน กพร.
11. นางสาวศิรานี เอี่ยมแม้น	ผู้อำนวยการส่วนช่วยอำนวยการ สลก.
12. นางอรุณี ประเสริฐสังข์	ผู้อำนวยการส่วนพัสดุ สลก.
13. นางสาวฐิตินันท์ นพกาศ	เจ้าหน้าที่บริหารงานทั่วไป สลก.
14. นางสาวนาขวัญ เหง้าพรหมมินทร์	เจ้าหน้าที่ส่งเสริมการปฏิบัติงาน สลก.
15. นายอนุพงษ์ ชมภูเอี่ยม	เจ้าพนักงานโสตทัศนศึกษาปฏิบัติการ สลก.
16. นางสาวณัฐชุตา ขุนทอง	เจ้าหน้าที่ส่งเสริมการปฏิบัติงาน สลก.
17. นายชยกร มีศรี	นายช่างเทคนิค สลก.
18. นายศุภกร กิจจรัส	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กตร.
19. นายธนศักดิ์ เดชะอนิวรรตน์	เจ้าหน้าที่บริหารงานทั่วไป กตร.
20. นางสาวกุสุมา แกล้วทนงค์	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กจ.
21. นางสาวสุจิตรา ชูจันทร์	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กจ.

22. นายลภน ดาหาร	นิติกรปฏิบัติการ กนก.
23. นางสาวนันท์นภัส มูลกาศ	เจ้าหน้าที่บริหารงานทั่วไป กตน.
24. นายวรวัฒน์ เมืองชื่น	นักธรณีวิทยาปฏิบัติการ กพน.1
25. นายศรานนท์ วิโรจนวิทย์	เจ้าพนักงานธุรการชำนาญงาน กพน.2
26. นายจักรพันธ์ พันธ์พุทธรัตน์	เจ้าพนักงานธุรการปฏิบัติงาน กพน.2
27. นางสาวปัญจภัสร์ วรเมธพิบูลนนท์	เจ้าหน้าที่บริหารงานทั่วไป กพน.2
28. นายชนะพล พิมเสน	นักวิเทศสัมพันธ์ปฏิบัติการ กยผ.
29. นางสาวสทัญณา ปาลกะวงศ์ ณ อยุธยา	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กยผ.
30. นางสาวรินทร์ลิตา อัครวัชราศิลป์	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กยผ.
31. นายจิระพงศ์ คชเสนีย์	เจ้าหน้าที่วิเคราะห์นโยบายและแผน กยผ.
32. นางสาวเบญจวรรณ แสงทองสกาว	เจ้าพนักงานธุรการชำนาญงาน กยผ.
33. นายอังคาร สุฐิติวนิช	เจ้าหน้าที่บริหารงานทั่วไป กยผ.
34. นายภัทรวัฒน์ เฟื่องเจริญ	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กอน.
35. นางสาวพลาพร สุขมา	นักวิชาการสิ่งแวดล้อมปฏิบัติการ กอน.
36. นางสาวจีรนันท์ เบ็ญชา	นักวิชาการสิ่งแวดล้อมปฏิบัติการ กอน.
37. นางรัตนา สุขลาภวิทยาคุณ	เจ้าพนักงานธุรการชำนาญงาน กอน.
38. นายองอาจ สมชอบ	เจ้าพนักงานธุรการ กอน.
39. นางสาวอัจฉรา แก้วอามาตย์	พนักงานจ้างเหมาบริการ กอน.
40. นายนัทวิชญ์ คุ้มวิจัยรัตน์	นักอุทกวิทยาปฏิบัติการ กวพ.
41. นายจิรกิตติ์ อุปเวียง	นักธรณีวิทยาปฏิบัติการ กวพ.
42. นายณัฐพงศ์ เพียรงูเหลือม	วิศวกรโยธาปฏิบัติการ กวป.
43. นายอำนาจ ราชสิงโห	เจ้าหน้าที่บริหารงานทั่วไป กวป.
44. นายธราดล ชุ่มชื่น	วิศวกรโยธาปฏิบัติการ. กวป.
45. นางสาวณัฐเกตุ อุ่นใจ	เจ้าพนักงานธุรการปฏิบัติงาน กวป.
46. นางสาวนันทิชา ศรีทินนท์	เจ้าพนักงานธุรการปฏิบัติงาน กวป.
47. นางสาววริศรา เรืองบุญญา	เจ้าพนักงานธุรการปฏิบัติงาน กวป.
48. นายคัมภีร์ พงค์ไพศาล	เจ้าพนักงานธุรการ กวป.
49. นางสาวประไพ บรรทัดจันทร์	เจ้าหน้าที่ กวป.
50. นางสาวจิรายุ ศักดาศิริสถาพร	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ ศทส.
51. นางสุรัสวดี บุณยานันต์	ผู้อำนวยการส่วนอำนวยการ ศทส.
52. นางปาริฉัตร วิริยะศิริกุล	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ ศทส.
53. นางสาวนวพร พูลพิพัฒน์	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ ศทส.
54. นางสาวแก้วตา แซ่ลิ้ม	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ ศทส.
55. นายธงไชย สุขสำราญ	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ ศทส.
56. นางสาวชจีวรรณ เบ้าสุวรรณ	นักวิชาการคอมพิวเตอร์ชำนาญการ ศทส.
57. นายธนวัฒน์ เค้าภูไทย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศทส.
58. นางสาวภคนันทน์ พุ่มอรุณ	เจ้าพนักงานธุรการชำนาญงาน ศทส.
59. นายเตย มิลัย	เจ้าหน้าที่วิเคราะห์นโยบายและแผน ศทส.
60.นางสาวสายจุฬา เพ็ชรพันธ์	เจ้าพนักงานธุรการ ศทส.

61. นายฉัตรชัย ภูศรี	เจ้าหน้าที่ Helpdesk ศทส.
62. นายอนุภัทร สินกิจจาทรัพย์	เจ้าหน้าที่ Helpdesk ศทส.
63. นางสาวศิรินันท์ อุตพันธ์	เจ้าหน้าที่วิเคราะห์นโยบายและแผน สลก.

ผู้เข้าร่วมประชุมผ่านระบบสื่ออิเล็กทรอนิกส์ออนไลน์

64. นายชลัช ผลมาก	วิศวกรโยธาปฏิบัติการ กพน.1
65. นางสาวชลดา ดอนแสง	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กพน.1
66. นางสาวปุณณนิดา สามงามยา	นายช่างโยธา กพน.1
67. นายนัทวิชญ์ คุ้มวิจัยรัตน์	นักอุทกวิทยาปฏิบัติการ กวพ.
68. นางสาวพรรณชมพู พงษ์ขาว	เจ้าหน้าที่บริหารงานทั่วไป กวพ.
69. นางสาวเบญจดา พิทักษ์รักษากุล	นักวิเคราะห์นโยบายและแผนปฏิบัติการ กยผ
70. นางสาวกรรณิการ์ สันป่าแก้ว	เจ้าพนักงานธุรการชำนาญงาน กจน.
71. นางสาวฐิตินันท์ นพกาศ	เจ้าหน้าที่บริหารงานทั่วไป สลก.
72. นางสาวปภาณิน ทองบุญเหลือ	เจ้าพนักงานธุรการปฏิบัติงาน สลก.
73. นางสาวชนกมน จันทร์ศรี	เจ้าหน้าที่บริหารงานทั่วไป สลก.
74. นางสาวเพ็ญนภา เทียนสุวรรณ	เจ้าหน้าที่บริหารงานทั่วไป สลก.
75. นายสมัคร สมสุข	นายช่างเทคนิค สลก.
76. นางสาววิชชานี ทรงกิติพิศาล	นักวิเคราะห์นโยบายและแผนชำนาญการ ศทส.
77. นางสาวธัญลักษณ์ ต๊ะวิชัย	ลูกจ้างเหมาบริการ สทน.1
78. นาง มัลลิกา ชัยวรรณ์	เจ้าพนักงานธุรการ สทน.1
79. นางกัลยา ไวกยี	ผู้อำนวยการส่วนยุทธศาสตร์และแผนงาน สทน.2
80. นางสาวลักขณา สุดสวาท	นักวิเคราะห์นโยบายและแผนชำนาญการ สทน.2
81. นางสาววิปัศยา พุ่มเกตุ	เจ้าพนักงานการเงินและบัญชีปฏิบัติงาน สทน.2
82.นางสาวณัฐกานต์ มีมา	วิศวกรโยธาปฏิบัติการ สทน.2
83. นายภูวิช ภูมูลนาธนเดช	เจ้าพนักงานธุรการ สทน.3
84. นางสาวทิวาพร สีอุปลัด	เจ้าพนักงานธุรการ สทน.3
85. นายธนกฤษ ถุวะศรี	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ สทน.4
86. นางสาวมธุรส หมู่ใหญ่	นักวิเคราะห์นโยบายและแผนปฏิบัติการ สทน.4
87. นางสาววณิชชา เชื้อกุณะ	เจ้าหน้าที่บริหารงานทั่วไป สทน.4
88. นาง พรทิวา สมน้อย	เจ้าพนักงานธุรการ สทน.4
89. นายสรรเสริญ ราตรี	นักวิเคราะห์นโยบายและแผนปฏิบัติการ สทน. 5
90. นางสาวจินตนา ศิวเสน	นักวิเคราะห์นโยบายและแผนชำนาญการ สทน. 5
91. นางสาววิลาสินี วัฒนาวงศ์ดอน	นักวิเคราะห์นโยบายและแผนชำนาญการ สทน.5
92. นางสาวกมลวิภา ตรีสาทร	เจ้าหน้าที่วิเคราะห์นโยบายและแผน สทน.5
93. นางสาวธีวรา อุดมธนะธีระ	คนงานสำรวจ สทน.5
94. นางสาวอรนิษฐ มานะสร้าง	นักวิเคราะห์นโยบายและแผนชำนาญการ สทน.6
95. นายณัฐเศรษฐ นาทุ่ง	เจ้าหน้าที่วิเคราะห์นโยบายและแผน สทน.6
96. นางสาวทัศนีย์ พูลผล	ผู้อำนวยการส่วนอำนวยการ สทน. 7
97. นางสาววนิดา แย้มมณี	นักวิเคราะห์นโยบายและแผนปฏิบัติการ สทน. 7

98. นางสาวลัดดา ศรีสวัสดิ์	เจ้าหน้าที่วิเคราะห์นโยบายและแผน สทน. 7
99. นางวิมล โสมสง	ผู้อำนวยการส่วนยุทธศาสตร์และแผนงาน สทน.8
100. นางสาวเสาวลักษณ์ สุดแทน	นักวิเคราะห์นโยบายและแผนชำนาญการ สทน. 8
101. นางสาวศุภานน ไกรวงศ์	นักอุทกวิทยาชำนาการ สทน. 8
102. นายธรรมากร บริหาร	นักวิเคราะห์นโยบายและแผนปฏิบัติการ สทน.9
103. นายสุธี รามแป้น	นักวิเคราะห์นโยบายและแผนชำนาญการ สทน.10
104. นางสาวกัญติมา ถิ่นบางเตียว	ผู้อำนวยการส่วนอำนวยการ สทน.10
105. นางสาวมานิตา สายช่วย	เจ้าหน้าที่บริหารงานทั่วไป สทน.10
106. นายจารุวัฒน์ ฉลาดล้ำ	เจ้าหน้าที่จ้างเหมาบริการ สทน.11
107. นางสาวทิฆัมพร ทากุ	เจ้าหน้าที่บันทึกข้อมูล สทน.11

ภาคผนวก ข

ประเด็นการแบ่งปันความรู้

ที่	ผู้แทนหน่วยงาน	ประเด็นการแบ่งปันความรู้
1.	นางรัตน์ดา พัฒน์สิงหเสนีย์ นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กพร.	กล่าวว่าวิทยากรแบ่งปันความรู้ในการป้องกัน การลดความเสี่ยงทั้งระดับกระทรวง สกมช. มีการแบ่งปันประสบการณ์การการถูกโจมตี ป้องกันแก้ไขเพื่อให้สามารถเรียนรู้และนำมาปรับใช้ในชีวิตประจำวันได้ เช่น การล็อกหน้าจอในช่วงพักกลางวันเพื่อลดความเสี่ยง
2.	นางสาวกุสุมา แกล้วทนงค์ นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กจ.	กล่าวว่ากรมทรัพยากรน้ำมีการรับส่งไฟล์อิเล็กทรอนิกส์จึงควรสำรองข้อมูลมากกว่า 1 แห่ง เพื่อความปลอดภัย การใช้งานผ่านระบบออนไลน์ควรมีการตั้งรหัสผ่านมากกว่า 1 ครั้ง การใช้อีเมลส่วนตัวเพื่อจองที่พักในการทำงาน อาจทำให้เป็นช่องทางที่เกิดภัยคุกคามเข้ามาสู่หน่วยงานได้
3.	นายสุธี รามแป้น นักวิเคราะห์นโยบายและแผนชำนาญการ สทน.10	กล่าวว่า ตัวบุคคลต้องตระหนักและให้ความสำคัญให้รู้จักภัยคุกคามและป้องกันตัวเองในเบื้องต้น ผู้บริหารต้องให้ความสำคัญกับการป้องกันภัยคุกคามทางไซเบอร์ ทั้งนี้ หากไม่มีงบประมาณอาจทำให้การป้องกันภัยคุกคามประสบความสำเร็จได้ยาก
4.	นายสรรเสริญ ราตรี นักวิเคราะห์นโยบายและแผนปฏิบัติการ สทน. 5	กล่าวว่า มีความกังวลด้านไซเบอร์ เคยถูกโจมตี Hard Disk และข้อมูลสูญหาย การป้องกันเบื้องต้นคือไม่ใช้ Flash drive จากบุคคลภายนอก ใช้คอมพิวเตอร์ เป็นเครื่องหลักเชื่อมกับคอมพิวเตอร์เครื่องอื่นผ่านสาย Lan โดยคอมพิวเตอร์เครื่องหลักจะสแกนมัลแวร์ก่อนดาวน์โหลดใช้งาน การเรียนรู้ช่วงเช้าทำให้ทราบแนวโน้มในการดำเนินการในอนาคต หากมีการอบรมด้านไอทีมากขึ้นจะทำให้ป้องกันได้ดีขึ้น
5.	นายวรวัฒน์ เมืองชื่น นักธรณีวิทยาปฏิบัติการ กพน.1	กล่าวว่า ความเสี่ยงในการถูกจู่โจมมักเกิดจากบุคคลจากการตั้งรหัสที่ง่ายเกินไป ไม่ล็อกหน้าจอ การจำพาสเวิร์ดในบราวเซอร์ต่างๆ การขาดการสำรองข้อมูล การละเลยการอัพเดตซอฟต์แวร์เพื่อเพิ่มความปลอดภัยด้านไซเบอร์ ทั้งนี้ภารกิจป้องกันภัยคุกคามไซเบอร์เป็นภารกิจของทุกคน
6.	นายศุภกร กิจจรัส นักวิเคราะห์นโยบายและแผนปฏิบัติการ กตร.	กล่าวว่า ตระหนักถึงความเสี่ยงในการถูกโจมตีทางไซเบอร์ การฟิชชิ่ง การหลอกให้กรอกข้อมูล ภัยทางไซเบอร์ไม่ขึ้นกับเทคโนโลยี แต่ขึ้นกับความตระหนักของบุคคล ควรเปลี่ยนพาสเวิร์ดบ่อยๆ ระวังการดาวน์โหลดลิงก์ที่ไม่ปลอดภัย การใช้ไวไฟสาธารณะ หากเกิดความตระหนักจะลดความเสี่ยงและลดความเสียหายจากภัยคุกคาม

ที่	ผู้แทนหน่วยงาน	ประเด็นการแบ่งปันความรู้
7.	นายธนวัฒน์ เค้าภูไทย นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศทส.	กล่าวว่า ศทส. ได้แจ้งเวียนแนวปฏิบัติและประกาศหน้าเว็บกรมฯ ขั้นต่อไปจะดำเนินตามประกาศ โดยนำซอฟต์แวร์กับฮาร์ดแวร์มาประกอบเพื่อดำเนินการ ทั้งนี้ EDR คล้ายแอนตี้ไวรัส แต่ติดตามตรวจสอบภัยคุกคามได้มากกว่า การลง EDR อาจทำให้การใช้คอมพิวเตอร์ทำงานช้า แต่ ศทส. ได้จัดทำ Wise List ไว้เพื่อให้เกิดการดำเนินการด้านความมั่นคงปลอดภัยได้ดีขึ้น ขณะนี้ได้ลง EDR ที่ส่วนกลาง ต่อไปจะไปลง EDR ที่ส่วนภูมิภาค
8.	นายปัญจภัสร์ วรเมธพิบูลนนท์ เจ้าหน้าที่บริหารงานทั่วไป กพน.2	กล่าวว่า ควรป้องกันตนเองโดยรหัสที่รัดกุม เช่น รหัสผ่านสองชั้น ไม่คลิกลิงก์ประหลาด สนับสนุนรณรงค์แบ่งปันความรู้
9.	นายลภน ดาหาร นิติกรปฏิบัติการ กนก.	กล่าวว่า การล็อกอินอีเมล โซเชียลมีเดียไว้ในอุปกรณ์ต่างๆ โดยไม่ล็อกเอ้าท์จากอุปกรณ์ที่ไม่ใช้งาน อาจมีบุคคลอื่นไปใช้ เกิดอันตรายต่อข้อมูล การทำงานเกี่ยวกับเอกสาร pdf โดยการใช้งานในเว็บไซต์เพื่อส่งผ่านข้อมูล หรือการรวมไฟล์เมื่อไม่มีโปรแกรมแท้ อาจทำให้ข้อมูลรั่วไหล
10.	นางสาวชมพูนุช ดลสุขเลิศ ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร	ในกรณีที่ไม่มีโปรแกรมแท้ ศทส. แนะนำ สนับสนุนได้หรือไม่ จะแจ้งทางใด
11.	นายธนวัฒน์ เค้าภูไทย นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศทส.	กล่าวว่า ศทส. ไม่ได้รับงบประมาณด้านไซเบอร์มา 1 ปี ลิขสิทธิ์บางส่วนหมดลงแล้ว ทั้งนี้ ในปัจจุบัน มี License EDR จาก สกมช. แม้ยังไม่ครอบคลุม โดยจะพยายามให้ครอบคลุมขึ้น ทั้งนี้ จะมีหนังสือแจ้งต่อไป
12.	นายอังคาร สุฐิติวนิช เจ้าหน้าที่บริหารงานทั่วไป กยผ.	กล่าวว่า การป้องกันภัยไซเบอร์ ควรใช้รหัสผ่านที่รัดกุม ใช้ระบบป้องกันสองขั้นตอนในการล็อกอิน อัพเดตซอฟต์แวร์ให้เป็นปัจจุบันอย่างสม่ำเสมอ หลีกเลี่ยงการคลิกลิงก์ที่มาไม่น่าเชื่อถือ ติดตั้งการป้องกันมัลแวร์ แบคอัพข้อมูล ใช้เครือข่ายที่ปลอดภัย ให้ความรู้เจ้าหน้าที่
13.	นายภูวิช ภูมูลนาธนเดช เจ้าพนักงานธุรการ สทน.3	กล่าวว่า การล็อกอินด้วย User Name และรหัสผ่าน จะช่วยป้องกันได้ทางหนึ่ง มีการแนะนำเพื่อนร่วมงานให้ตั้ง User Name และรหัสผ่าน ให้เป็นตัวหนังสืออักขระและตัวเลข ทั้งนี้ เมื่อพบมัลแวร์ หรือ แรมซัมแวร์จะแจ้งส่วนกลางเพื่อ Block User นั้น และลง Window ใหม่
14.	นางกัลยา ไวกยี ผู้อำนวยการส่วนยุทธศาสตร์และแผนงาน สทน.2	กล่าวว่า ต้องสร้างความตระหนักเจ้าหน้าที่อย่างสม่ำเสมอ การทำงานมีระบบป้องกัน เช่น การเข้ารหัสผ่านสำหรับงานสารบัญ สำหรับกลุ่มไลน์นอกจะมีการนำข้อมูลอันตรายออกจากโดยแอดมิน อย่างไรก็ตาม ยังไม่มีข้อมูลสำคัญที่จะโดนแฮก
15.	นายธรรมากร บริหาร นักวิเคราะห์นโยบายและแผนปฏิบัติการ สทน.9	กล่าวว่า พบความเสี่ยงในการทำงาน การแชร์ QR Code ผ่าน Google Drive บางครั้งพบข้อมูลมากกว่าที่แจ้งในหนังสือ ซึ่งอาจทำให้ข้อมูลรั่วไหล ควรมีความตระหนักในเรื่องนี้

ที่	ผู้แทนหน่วยงาน	ประเด็นการแบ่งปันความรู้
17.	นางสาวอรนิษฐ มานะสร้าง นักวิเคราะห์นโยบายและแผนชำนาญการ สทน.6	กล่าวว่า ส่วนตัวถูกมิจฉาชีพ หลอกเรื่องการโอนมัดจำค่าที่พัก เป็นความเสี่ยงการใช้ AI ในการหลอกลวง จากการเรียนรู้ช่วงเช้า จะทำทราบวิธีป้องกัน สำหรับองค์กรไม่พบปัญหา เนื่องจากใช้ระบบ Authentication ของกรมทรัพยากรน้ำ ซึ่งมีระบบป้องกันมัลแวร์
18.	นางสาววนิดา แย้มมณี นักวิเคราะห์นโยบายและแผนปฏิบัติการ สทน.7	กล่าวว่า ได้รับความรู้เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ การป้องกันตนเอง ทั้งนี้ สทน. 7 เคยลงข่าวประชาสัมพันธ์ แต่ปรากฏว่ากลายเป็นเว็บไซต์การพนันออนไลน์ ศทส. จึงช่วยแก้ไขโดยเปลี่ยน User Name และพาสเวิร์ด จากนั้น สทน. 7 จึงตระหนักในการป้องกันดนเองเบื้องต้น โดยลงโปรแกรมกำจัดไวรัสที่ทันสมัย และเจ้าหน้าที่หาความรู้เพิ่มเติมให้ทันภัยคุกคาม
19.	นายภัทรวัฒน์ เฟื่องเจริญ นักวิเคราะห์นโยบายและแผนปฏิบัติการ กอน.	กล่าวว่า มีการใช้เครื่องมือค้นหาทางอินเตอร์เน็ตสืบค้นข้อมูล โดยได้สืบค้นเว็บไซต์กรมทรัพยากรน้ำ และพบว่ามีการป๊อปอัพเว็บไซต์การพนันออนไลน์ จึงแจ้งแอดมินแก้ไข ทั้งนี้ จากการสัมมนาช่วงเช้า ทำให้ทราบว่าแอดมินเว็บไซต์ ต้องบำรุงรักษาและอัพเดตอย่างสม่ำเสมอ เพื่อป้องกันผู้ไม่ประสงค์ดีมาทำให้เกิดความเสียหาย
20.	นายนัทวิชญ์ คุ้มวิจัยรัตน์ นักอุทกวิทยาปฏิบัติการ กวพ.	กล่าวว่า เว็บไซต์ กวพ. เคยโดนแปะลิงก์เว็บไซต์การพนันออนไลน์ อาจเกิดจากไม่ได้การต่อสัญญาการพัฒนาเว็บไซต์ จึงไม่มีการอัพเดต และจากการเรียนรู้ในช่วงเช้าทำให้ทราบว่าควรเปลี่ยนรหัสผ่าน
21.	นางรัตน์ดา พัฒน์สิงหเสนีย์ นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กพร.	สอบถามความเป็นไปได้ในการการเข้ารหัส 2 ระดับ (2 Factor Authentication)
22.	นายธนวัฒน์ เค้าภูไทย นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศทส.	กล่าวว่า 2 Factor Authentication อาจเป็นการ Authentication และ OTP ทั้งนี้ ต่อไป 2 Factor อาจไม่เพียงพอ อาจต้องเป็น Multi-Factor แต่การจะทำต่างๆ อาจไม่ใช่เพียง User ที่ต้องปฏิบัติ ผู้ดูแลระบบควรปฏิบัติตามด้วย เพื่อความมั่นคงปลอดภัยของระบบ
23.	นางสาวขมพูนุช ดลสุขเลิศ ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร	กล่าวว่า หากเผลอไปกดลิงก์แล้ว หากมัลแวร์เข้ามาในคอมพิวเตอร์แล้ว จะดำเนินการอย่างไร
24.	นางสาวจิรายุ ศักดาศิริสถาพร นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ ศทส.	กล่าวว่า หากกดลิงก์แล้ว หากมัลแวร์เข้ามาในคอมพิวเตอร์ หากเป็นเครื่องคอมของกรมฯ จะมีซอฟต์แวร์ EDR ซึ่งเปรียบเสมือนกล้อง cctv ที่ตรวจมัลแวร์ ถ้าพบจะเตือนที่ระบบของ ศทส. และเจ้าหน้าที่เฝ้าระวังจะไปตรวจความผิดปกติที่คอมพิวเตอร์ โดยเครื่องคอมพิวเตอร์ของกรมฯ มีแอนตี้ไวรัส และต่ออายุ License ทุกปี ทั้งนี้ ความตระหนักรู้อยู่ที่ตัวเรา ไม่ควรคลิกหรือดาวน์โหลดข้อมูลที่ไม่เกี่ยวข้อง

ที่	ผู้แทนหน่วยงาน	ประเด็นการแบ่งปันความรู้
25.	นางสาวชมพูนุช ดลสุขเลิศ ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร	กล่าวว่า ถ้าใช้เครื่องจากภายนอก โดยล็อกอินผ่านระบบกรมฯ จะตรวจจับมัลแวร์ หรือแรมซัมแวร์ ได้หรือไม่
26.	นางสาวจิรายุ ศักดาศิริสถาพร นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ ศทส.	กล่าวว่า การใช้เครื่องคอมพิวเตอร์ภายนอกล็อกอิน ผ่าน Authentication หากมีสิ่งผิดแปลก Fire wall จะช่วยป้องกันได้ส่วนหนึ่ง
27.	นางรัตน์ดา พัฒน์สิงหเสนีย์ นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กพร.	กล่าวว่า การใช้อีเมลราชการมีความปลอดภัย แต่ทราบว่าอีเมลราชการมีจำนวนไม่มาก ขอทราบแนวทางการให้อีเมลราชการ
28.	นางสาวจิรายุ ศักดาศิริสถาพร นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ ศทส.	กล่าวว่า จำนวนอีเมลราชการไม่พอสำหรับทุกคน ขณะนี้กรมฯ มีประมาณ 300 อีเมล จากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ดังนั้น หน่วยงานที่ติดต่อกับหน่วยงานภายนอกและประสงค์ใช้อีเมลราชการ ขอให้ติดต่อ ศทส. และต้องใช้สม่ำเสมอมิเช่นนั้นจะถูกระงับการใช้งาน ทั้งนี้ แต่ละอีเมลมีพื้นที่ประมาณ 1 gigabyte มีหน่วยความจำสำหรับ Drive ประมาณ 5 gigabyte ขณะนี้ ศทส. มีนโยบายทำ mail server โดยขอรับจัดสรรงบประมาณใน ปี พ.ศ. 2569
29.	นางสาวชมพูนุช ดลสุขเลิศ ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร	กล่าวว่า ศทส. มีแนวทางป้องกันแก้ไขปัญหาที่พบอย่างไร เช่น กรณี สทน.7 เผยแพร่ข้อมูลแล้วกลายเป็นเว็บไซต์การพนันออนไลน์
30	นางสาวจิรายุ ศักดาศิริสถาพร นักวิชาการคอมพิวเดอร์ชำนาญการพิเศษ ศทส.	กล่าวว่า เว็บไซต์ สทน. และหน่วยงาน ที่ ศทส. ได้เคยดำเนินการจัดทำให้ ในอดีตหากซอฟต์แวร์ยังไม่มีการอัพเดตหรือหมดอายุอาจถูกโจมตี แต่ปัจจุบัน ศทส. ได้อัพเดตซอฟต์แวร์และใส่ Monitor ที่ Google แล้ว อย่างไรก็ตาม หากสืบค้นชื่อกรมทรัพยากรน้ำ หรือ สทน. ใน Google แล้วพบว่าเป็นเว็บไซต์การพนันออนไลน์ขอให้แจ้ง ศทส. เพื่อดำเนินการแก้ไขต่อไป

การดำเนินงานด้านการบริหาร ความมั่นคงปลอดภัยไซเบอร์



ผู้ช่วยปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
(นายกานตพันธุ์ พิศาลสุขสกุล)

การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

มาตรา 44 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 45 มีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน

มาตรา46 แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยัง สกมช. รวมถึงแจ้งปรับปรุงข้อมูลกรณีมีการเปลี่ยนแปลง

มาตรา58
- ต้องตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อมของหน่วยงาน ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ
- มีการแจ้งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว
- เมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น

การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

01 การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

แต่งตั้งผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security)

02 การบริหารความเสี่ยง (Risk Management)

จัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

เก็บรักษารายการความเสี่ยง ระบุไว้ในทะเบียนความเสี่ยง (Risk register) บริการที่สำคัญ มีการติดตามความเสี่ยง

03 นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

มีการกำหนด และอนุมัตินโยบายในการจัดการความเสี่ยงด้านไซเบอร์ และการป้องกันบริการสำคัญ

ทบทวนอย่างน้อยปีละ 1 ครั้ง

การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์ของ สป.ทส.

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. แผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

- มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบอิสระภายนอก ปีละ 1 ครั้ง
- จัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ของบริการสำคัญ

2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- จัดทำระเบียบวิธีปฏิบัติในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง
- การจัดการความเสี่ยง (Risk treatment) ควบคุม และป้องกันความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- ติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk monitoring and review)
- การรายงานความเสี่ยง (Risk reporting) รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงต่อผู้บริหาร และทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

3. แผนการรับมือภัยคุกคามทางไซเบอร์

- จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
- สื่อสารแผนการรับมือภัยให้ผู้เกี่ยวข้อง
- ทบทวนแผนการรับมือภัย อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง



การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์ของ สป.ทส.

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การจัดการทรัพย์สิน (Asset Management)

- ทำทะเบียนทรัพย์สินของบริการที่สำคัญ และตรวจสอบทะเบียนทรัพย์สิน อย่างน้อยปีละ 1 ครั้ง
- ประเมินความเสี่ยงด้านการยไซเบอร์ของบริการที่สำคัญ อย่างน้อยปีละ 1 ครั้ง

การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

- ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง
- ปรับปรุงทะเบียนความเสี่ยง

การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

- ประเมินช่องโหว่ของบริการที่สำคัญ
- ทดสอบเจาะระบบ (Penetration Testing) ของระบบบริการสำคัญ
- ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 (หนึ่ง)

การจัดการผู้ให้บริการภายนอก (Third-Party Management)

- กำหนดให้ผู้ให้บริการภายนอกต้องรับผิดชอบต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญที่เกี่ยวข้อง และมีข้อตกลงระดับการให้บริการ (Service Level Agreement)

การเชื่อมต่อระยะไกล (Remote Connection) กับบริการสำคัญ

- กำหนดมาตรการการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ

การควบคุมการเข้าถึง (Access Control)

- กำหนดให้มีการจำกัดการเข้าถึงบริการที่สำคัญเฉพาะบุคลากร กิจกรรม อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

- จัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญ



การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์ของ สป.ทส.

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) กับบริการสำคัญ

- กำหนดให้มีการควบคุมในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา กับบริการที่สำคัญ
- กำหนดให้มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

- ทำแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) มีการทบทวนแผนงานอย่างน้อยปีละ 1 ครั้ง

การแบ่งปันข้อมูล (Information Sharing)

- กำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และการบรรเทาผลกระทบ โดยติดตั้งระบบ MISP ของ สกมช.

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

- จัดทำกระบวนเพื่อตรวจจับ จัดประเภท วิเคราะห์ และระบุว่ามีภัยคุกคามทางไซเบอร์และทบทวน อย่างน้อยปีละ 1 ครั้ง

การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

- เข้าร่วมฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ในระดับชาติ

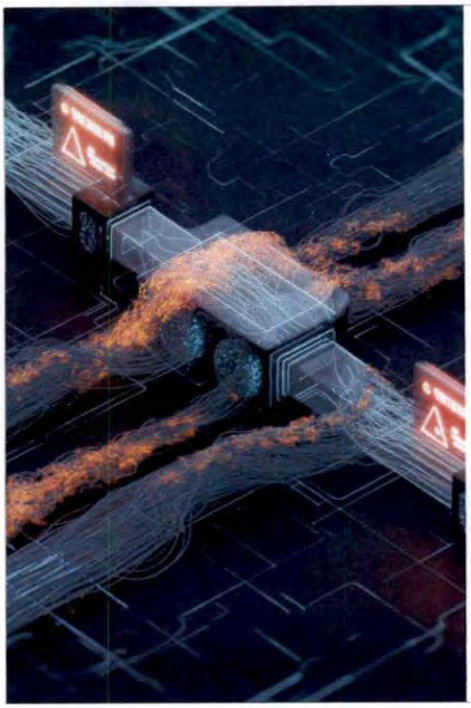
แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

- มีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง

แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

- จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ มีการฝึกซ้อมแผน อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง





ภัยคุกคามทางไซเบอร์ในหน่วยงานภาครัฐของไทย

- ปี 2568 ได้รับการประกาศเป็น "ปีแห่งความปลอดภัยทางไซเบอร์" ของประเทศไทย โดยหน่วยงานด้านความปลอดภัยไซเบอร์แห่งชาติและศูนย์ประสานความปลอดภัยคอมพิวเตอร์
- คาดว่าเศรษฐกิจดิจิทัลไทยจะเติบโตถึง 100 ล้านเหรียญสหรัฐภายในปี 2573 ตามแผนยุทธศาสตร์ความปลอดภัยไซเบอร์แห่งชาติ ซึ่งดำเนินการโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- การโจมตีทางไซเบอร์มีจำนวนเพิ่มขึ้นและซับซ้อนมากขึ้น โดยเฉพาะการโจมตีต่อเนื่องขั้นสูงและการโจมตีที่ทำให้ระบบล่ม ซึ่งส่งผลต่อระบบโครงสร้างพื้นฐานสำคัญของประเทศไทย นับเป็นความท้าทายหลักของหน่วยงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ภัยคุกคามที่มักพบในหน่วยงานภาครัฐ

หน่วยงานภาครัฐไทยกำลังเผชิญกับภัยคุกคามทางไซเบอร์ที่หลากหลายและซับซ้อนมากขึ้น ทั้งการโจมตีผ่านฟิชชิ่ง แรนซัมแวร์แบบหลายชั้น การโจมตีจากรัฐต่างประเทศ และภัยคุกคามที่ขับเคลื่อนด้วยเทคโนโลยี AI (Artificial Intelligence - ปัญญาประดิษฐ์) และ IoT (Internet of Things - อินเทอร์เน็ตของสรรพสิ่ง)



ฟิชชิ่งและมัลแวร์

แคมเปญ อีเมลหลอกลวง ที่มีความซับซ้อนสูงเลียน แบบหน่วยงานรัฐเพื่อโมยข้อมูลสำคัญ สถิติการโจมตีระบบธนาคารออนไลน์ของรัฐเพิ่มขึ้นถึง 40% ในปีงบประมาณที่ผ่านมา



แรนซัมแวร์แบบหลายชั้น

กลยุทธ์การเรียกค่าไถ่ข้อมูลแบบซ้อนทับซับซ้อน ผสมผสานทั้งการเข้ารหัสข้อมูลสำคัญ การขู่เปิดเผยข้อมูลลับ และการโจมตีแบบ DDoS (Distributed Denial of Service - การปฏิเสธการให้บริการแบบกระจาย) ไปพร้อมกันเพื่อเพิ่มโอกาสความสำเร็จ



การโจมตีจากรัฐและ APTs

กลุ่มผู้โจมตีที่ได้รับการสนับสนุนจากรัฐต่างประเทศที่มีทรัพยากรสูง มุ่งเป้าไปที่ข้อมูลความมั่นคงแห่งชาติ นโยบายเศรษฐกิจ และยุทธศาสตร์ด้านการต่างประเทศของไทย APTs (Advanced Persistent Threats - ภัยคุกคามต่อเนื่องขั้นสูง) คือการโจมตีที่มีความซับซ้อนและต่อเนื่องในระยะยาว



การโจมตีด้วย AI และ IoT

ภัยคุกคามอัจฉริยะที่มีความสามารถในการเรียนรู้และปรับตัว ใช้ระบบปัญญาประดิษฐ์ (AI - Artificial Intelligence) วิเคราะห์และค้นหาช่องโหว่โดยอัตโนมัติ พร้อมใช้ประโยชน์จากอุปกรณ์ IoT (Internet of Things - อินเทอร์เน็ตของสรรพสิ่ง) ที่ขาดการรักษาความปลอดภัยในหน่วยงานรัฐ

ภัยคุกคามส่งผลกระทบอย่างไรบ้าง

ภัยคุกคามไซเบอร์ส่งผลกระทบรุนแรงต่อภาครัฐทั้งด้านข้อมูล การบริการ ความมั่นคง และการเงิน ก่อให้เกิดความเสียหายที่ครอบคลุมทุกมิติของการทำงานภาครัฐ

1 การรั่วไหลของข้อมูล (Data Breach - DB)

ข้อมูลสำคัญของประชาชนและข้อมูลความมั่นคงรั่วไหล ส่งผลต่อความเชื่อมั่นและความปลอดภัยของประเทศ การรั่วไหลของข้อมูลส่วนบุคคล (Personally Identifiable Information - PII) และข้อมูลที่มีชั้นความลับ (Classified Information - CI) เป็นภัยคุกคามระดับสูงต่อหน่วยงานภาครัฐ

2 การหยุดชะงักของบริการ (Service Disruption - SD)

ระบบบริการประชาชนถูกตัดขาด ประชาชนไม่สามารถเข้าถึงบริการสำคัญได้ สร้างความเสียหายทางเศรษฐกิจ การโจมตีแบบปฏิเสธการให้บริการ (Distributed Denial of Service - DDoS) และการโจมตีโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure - CI) ทำให้เกิดภาวะหยุดชะงักของบริการสาธารณะ

3 ผลกระทบต่อความมั่นคง (National Security Impact - NSI)

ข้อมูลยุทธศาสตร์อาจถูกโจรกรรม หน่วยงานความมั่นคงสูญเสียความได้เปรียบ เกิดความเสี่ยงต่อความมั่นคงระดับชาติ การโจมตีโดยกลุ่มผู้โจมตีขั้นสูง (Advanced Persistent Threat - APT) และการสอดแนมทางไซเบอร์ (Cyber Espionage - CE) คุกคามความมั่นคงและอธิปไตยของประเทศ

4 ความเสียหายทางการเงิน (Financial Damage - FD)

งบประมาณสูญเสียจากการถูกโจมตี ค่าใช้จ่ายในการกู้คืนระบบสูญภาษีประชาชนถูกนำไปแก้ไขความเสียหาย ต้นทุนทางการเงินทั้งทางตรงและทางอ้อม (Direct and Indirect Cost - DIC) รวมถึงค่าใช้จ่ายในการฟื้นฟูและการดำเนินการตามมาตรการรักษาความปลอดภัย (Security Incident Response Cost - SIRC) สร้างภาระทางงบประมาณอย่างมีนัยสำคัญ

กฎหมายและข้อกำหนดด้านความปลอดภัยไซเบอร์ของไทย

ประเทศไทยได้พัฒนากรอบกฎหมายและข้อกำหนดด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง เพื่อรับมือกับภัยคุกคามที่เพิ่มขึ้น กฎหมายเหล่านี้ครอบคลุมทั้งการคุ้มครองข้อมูล การจัดการเหตุการณ์ และการกำกับดูแลโครงสร้างพื้นฐานสำคัญ หน่วยงานภาครัฐจำเป็นต้องปฏิบัติตามข้อกำหนดเหล่านี้อย่างเคร่งครัด

กฎหมาย	หน่วยงานรับผิดชอบ	ขอบเขต
พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ 2562	สกมช. (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ) / NCSA (National Cyber Security Agency)	ดูแล**โครงสร้างสำคัญทางสารสนเทศ** และจัดการเหตุภัยไซเบอร์
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)	PDPC (คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) / ETDA (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์)	ปกป้อง**ข้อมูลส่วนบุคคล** คล้าย GDPR (กฎหมายคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป)
แนวทางประเมินความปลอดภัยไซเบอร์	ธนาคารแห่งประเทศไทย (Bank of Thailand)	สำหรับ**สถาบันการเงิน** ประเมินความเสี่ยง
พ.ร.บ. คอมพิวเตอร์ (แก้ไข 2560)	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	ควบคุมอาชญากรรมไซเบอร์ เช่น การแฮ็ก
ยุทธศาสตร์ความปลอดภัยไซเบอร์แห่งชาติ	กระทรวงกลาโหม / สมช. (สำนักงานสภาความมั่นคงแห่งชาติ)	แนวทางปกป้องโครงสร้างพื้นฐานสำคัญ
แนวปฏิบัติ ThaiCERT	ThaiCERT (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย) / สกมช.	วิธีรับมือเหตุการณ์ไซเบอร์

ประเภทของภัยคุกคามและวิธีการป้องกัน

ตารางนี้แสดงประเภทของภัยคุกคามทางไซเบอร์ที่หน่วยงานรัฐบาลไทยเผชิญอยู่ พร้อมตัวอย่างของการโจมตีและมาตรการป้องกันที่เหมาะสมสำหรับแต่ละภัยคุกคาม การทำความเข้าใจภัยคุกคามเหล่านี้จะช่วยให้หน่วยงานรัฐสามารถวางแผนกลยุทธ์การป้องกันได้อย่างมีประสิทธิภาพ

Threat Type	Example	How to Protect
Phishing (การหลอกลวงทางอีเมล)	Email fraud, SMS scam	Email security, awareness training, web filters
Ransomware (มัลแวร์เรียกค่าไถ่)	Babuk, LYNX	Regular backups, EDR/XDR (Endpoint Detection and Response/Extended Detection and Response) solutions, timely patching, threat intelligence
APT (Advanced Persistent Threat - การโจมตีแบบต่อเนื่องขั้นสูง)	Nation-state intrusions	Next-Gen Firewalls, IPS (Intrusion Prevention Systems), Cyber Threat Intelligence, network segmentation
Scam Networks (เครือข่ายฉ้อโกง)	Call center frauds, traffic hijacking	DNS (Domain Name System) security, threat intelligence, takedown services
Legacy Infrastructure (โครงสร้างพื้นฐานเก่า)	Outdated VPN (Virtual Private Network), operating systems	Patch management, vulnerability scanning
Insider Threat (ภัยคุกคามจากบุคคลภายใน)	Misuse of privileges, data leaks	DLP (Data Loss Prevention), access control, monitoring
AI/IoT Threats (ภัยคุกคามจาก AI และ IoT)	Deepfakes, IoT (Internet of Things) attacks	IoT security monitoring, AI-based threat modeling

โซลูชั่นด้านความปลอดภัยไซเบอร์

โซลูชั่นด้านความปลอดภัยไซเบอร์มีความหลากหลายและครอบคลุมทุกขั้นตอนของการรักษาความปลอดภัย ตั้งแต่การป้องกัน การตรวจจับ การวิเคราะห์ จนถึงการตอบสนองต่อภัยคุกคาม หน่วยงานภาครัฐควรพิจารณาเลือกใช้โซลูชั่นที่เหมาะสมตามความต้องการและความเสี่ยงขององค์กร



ระบบป้องกัน (Protect)

- ไฟร์วอลล์รุ่นใหม่ (Next Generation Firewall - NGFW)
- ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน (Web Application Firewall - WAF)
- ระบบป้องกันการบุกรุก (Intrusion Prevention System - IPS)
- เกตเวย์ความปลอดภัยเว็บ (Security Web Gateway)
- ระบบป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention - DLP)
- ระบบจัดการสิทธิ์ผู้ใช้พิเศษ (Privileged Access Management - PAM)
- การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication - MFA)
- การเข้าถึงเครือข่ายแบบไม่เชื่อใจ (Zero Trust Network Access)



ระบบตรวจจับ (Detect)

- ระบบตรวจจับและตอบสนองระดับเอนด์พอยต์ (Endpoint Detection and Response - EDR)
- ระบบตรวจจับและตอบสนองแบบขยาย (Extended Detection and Response - XDR)
- ระบบตรวจจับและตอบสนองระดับเครือข่าย (Network Detection and Response - NDR)
- การวิเคราะห์พฤติกรรมผู้ใช้ (User Behavior Analytics)
- แพลตฟอร์มข่าวกรองภัยคุกคาม (Threat Intelligence Platforms)
- เครื่องมือสแกนช่องโหว่ (Vulnerability Scanners)



ระบบวิเคราะห์ (Analyze)

- ศูนย์ปฏิบัติการความมั่นคงปลอดภัย (Security Operations Center - SOC)
- ระบบจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัย (Security Information and Event Management - SIEM)
- ระบบประสานงาน ทำงานอัตโนมัติ และตอบสนองด้านความปลอดภัย (Security Orchestration, Automation and Response - SOAR)
- เครื่องมือล่าภัยคุกคาม (Threat Hunting Tools)
- ระบบตรวจจับความผิดปกติด้วย AI (AI-Based Anomaly Detection)
- แพลตฟอร์มวิเคราะห์นิติวิทยาศาสตร์ดิจิทัล (Forensic Analysis Platforms)



ระบบตอบสนอง (Respond)

- แพลตฟอร์มตอบสนองต่อเหตุการณ์ (Incident Response Platforms)
- เครื่องมือนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics Tools)
- โซลูชั่นสำรองและกู้คืนข้อมูล (Backup & Recovery Solutions)
- ระบบจัดการวิกฤต (Crisis Management Systems)
- เครื่องมือแจ้งเตือนการละเมิดข้อมูล (Breach Notification Tools)
- การฝึกอบรมความตระหนักด้านความปลอดภัย (Security Awareness Training)

การป้องกันตามกรอบ NIST

กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ NIST (National Institute of Standards and Technology) เป็นแนวทางที่ได้รับการยอมรับในระดับสากล ช่วยให้องค์กรภาครัฐและเอกชนสามารถประเมิน จัดการ และลดความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพ กรอบนี้แบ่งเป็น 5 ฟังก์ชันหลักที่สามารถดำเนินการพร้อมกันและต่อเนื่อง

Identify (ระบุ)

การระบุทรัพย์สินดิจิทัลและความเสี่ยง ประกอบด้วยการจัดทำ Asset Management (AM), Business Environment (BE), Governance (GV), Risk Assessment (RA) และ Risk Management Strategy (RM) เพื่อเข้าใจบริบทธุรกิจและทรัพยากรที่ต้องปกป้อง

Recover (ฟื้นฟู)

การกู้คืนและดำเนินการต่อเนื่อง ประกอบด้วย Recovery Planning (RP), Improvements (IM) และ Communications (CO) เพื่อฟื้นฟูระบบและบริการให้กลับมาทำงานได้ตามปกติ พร้อมทั้งปรับปรุงแผนจากบทเรียนที่ได้รับ



Protect (ป้องกัน)

การใช้มาตรการป้องกันที่เหมาะสม รวมถึง Access Control (AC), Awareness and Training (AT), Data Security (DS), Information Protection Processes and Procedures (IP), Maintenance (MA) และ Protective Technology (PT) เพื่อสร้างระบบป้องกันหลายชั้น

Detect (ตรวจจับ)

ระบบตรวจจับการโจมตีทางไซเบอร์ ประกอบด้วย Anomalies and Events (AE), Security Continuous Monitoring (CM) และ Detection Processes (DP) เพื่อติดตามและวิเคราะห์เหตุการณ์ด้านความปลอดภัยอย่างต่อเนื่อง

Respond (ตอบสนอง)

แผนตอบสนองต่อเหตุการณ์ไซเบอร์ ประกอบด้วย Response Planning (RP), Communications (CO), Analysis (AN), Mitigation (MI) และ Improvements (IM) เพื่อรับมือกับภัยคุกคามอย่างเป็นระบบและลดผลกระทบ

โซลูชั่นที่สอดคล้องกับกรอบ NIST

การประยุกต์ใช้กรอบความมั่นคงปลอดภัยไซเบอร์ NIST อย่างมีประสิทธิภาพจำเป็นต้องเลือกโซลูชั่นที่เหมาะสมสำหรับแต่ละฟังก์ชัน ตารางต่อไปนี้แสดงโซลูชั่นด้านความปลอดภัยไซเบอร์ที่ควรพิจารณาสำหรับแต่ละฟังก์ชันของกรอบ NIST เพื่อยกระดับการป้องกันภัยคุกคามทางไซเบอร์แบบครบวงจรสำหรับหน่วยงานภาครัฐไทย

NIST ฟังก์ชัน	โซลูชั่นที่แนะนำ	ประโยชน์ที่ได้รับ
Identify	SIEM (Security Information and Event Management - ระบบจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัย), CTI (Cyber Threat Intelligence - ข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์)	ระบุทรัพย์สินดิจิทัลและวิเคราะห์ภัยคุกคามอย่างครอบคลุม
Protect	NGFW (Next-Generation Firewall - ไฟร์วอลล์รุ่นใหม่), WAF (Web Application Firewall - ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน), DLP (Data Loss Prevention - การป้องกันการรั่วไหลของข้อมูล), Security Web Gateway (ประตูเว็บนิรภัย)	สร้างชั้นป้องกันหลายระดับเพื่อรักษาความปลอดภัยข้อมูลและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต
Detect	IPS (Intrusion Prevention System - ระบบป้องกันการบุกรุก), EDR (Endpoint Detection and Response - การตรวจจับและตอบสนองที่ปลายทาง), XDR (Extended Detection and Response - การตรวจจับและตอบสนองแบบขยาย)	ตรวจจับและวิเคราะห์การโจมตีทางไซเบอร์ในเวลาจริง พร้อมแจ้งเตือนอัตโนมัติ
Respond	SOAR (Security Orchestration, Automation and Response - การประสานงาน ระบบอัตโนมัติ และการตอบสนองด้านความปลอดภัย), SOC (Security Operations Center - ศูนย์ปฏิบัติการความปลอดภัย)	ตอบสนองต่อเหตุการณ์ด้านความปลอดภัยอย่างรวดเร็วและเป็นระบบ ลดผลกระทบจากการโจมตี
Recover	SOC (Security Operations Center - ศูนย์ปฏิบัติการความปลอดภัย), SIEM (Security Information and Event Management - ระบบจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัย), ระบบสำรองและกู้คืนข้อมูล	ฟื้นฟูระบบที่ได้รับผลกระทบ วิเคราะห์สาเหตุรากฐาน และป้องกันการเกิดซ้ำในอนาคต

การเลือกและนำโซลูชั่นต่างๆมาปรับใช้ในหน่วยงาน

การเลือกและประยุกต์ใช้มาตรการป้องกันต้องมีขั้นตอนที่ชัดเจน เพื่อให้เกิดประสิทธิภาพสูงสุด

> กระบวนการปรับใช้โซลูชั่นด้านความปลอดภัยไซเบอร์ที่มีประสิทธิภาพประกอบด้วย 4 ขั้นตอนหลัก: การประเมินความเสี่ยง การพัฒนาแผนงาน การนำไปใช้และบูรณาการ และการติดตามผลเพื่อปรับปรุงอย่างต่อเนื่อง

1 ประเมินความเสี่ยงและความต้องการ

วิเคราะห์ภัยคุกคามเฉพาะของหน่วยงาน รวมถึงทรัพยากรที่มีและข้อจำกัดด้านงบประมาณ

- ทำการประเมินช่องโหว่อย่างสม่ำเสมอ
- จัดลำดับความสำคัญของทรัพย์สินที่ต้องปกป้อง

2 พัฒนาแผนงานความปลอดภัย

จัดทำแผนที่สอดคล้องกับกรอบ NIST (National Institute of Standards and Technology - สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ) และนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- กำหนดมาตรฐานและแนวทางปฏิบัติ
- จัดสรรงบประมาณและทรัพยากรที่จำเป็น

3 ดำเนินการและบูรณาการ

นำโซลูชั่นมาใช้ตามลำดับความสำคัญ ควบคู่กับการฝึกอบรมบุคลากร

- เริ่มจากระบบสำคัญและขยายไปทั่วองค์กร
- สร้างวัฒนธรรมความปลอดภัยทั่วทั้งองค์กร

4 ติดตามและปรับปรุง

ประเมินประสิทธิภาพของมาตรการอย่างต่อเนื่อง และปรับเปลี่ยนตามภัยคุกคามใหม่

- จัดทำการทดสอบเจาะระบบเป็นประจำ
- รายงานและวิเคราะห์เหตุการณ์ด้านความปลอดภัย

การเตรียมพร้อมสำหรับอนาคต

การเตรียมความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับอนาคตของประเทศไทย มุ่งเน้นการพัฒนาในสี่ด้านหลัก: เศรษฐกิจดิจิทัล การรับมือภัยคุกคาม การพัฒนาบุคลากร และโซลูชั่นระดับประเทศ



เศรษฐกิจดิจิทัลที่เติบโตอย่างก้าวกระโดด (DGE - Digital Growth Economy)

คาดการณ์มูลค่าจะเพิ่มขึ้นถึงสองเท่าภายในปี 2573 สร้างโอกาสและความท้าทายใหม่ การพัฒนาเศรษฐกิจดิจิทัลประเทศไทยจะเพิ่มความสามารถในการแข่งขันระดับโลกและขับเคลื่อนนวัตกรรมในทุกภาคส่วน



รับมือภัยคุกคามที่ซับซ้อนยิ่งขึ้น (CTM - Complex Threat Management)

พัฒนาระบบป้องกันแบบปรับตัวได้เพื่อตอบสนองต่อภูมิทัศน์ภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว ประเทศไทยกำลังลงทุนในโครงสร้างพื้นฐานที่มั่นคงเพื่อป้องกันการโจมตีทางไซเบอร์รูปแบบใหม่และการโจมตีขั้นสูง



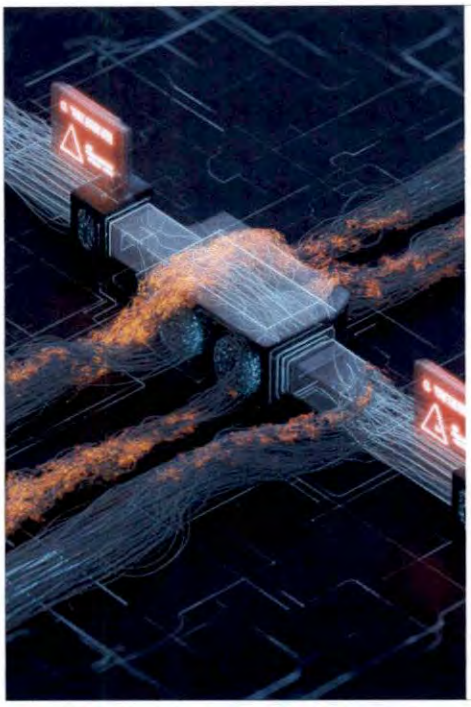
ยกระดับศักยภาพบุคลากรด้านไซเบอร์ (CWD - Cyber Workforce Development)

สร้างกำลังคนที่มีความเชี่ยวชาญสูงและพร้อมรับมือกับความท้าทายด้านความปลอดภัยไซเบอร์ยุคใหม่ แผนพัฒนากำลังคนด้านไซเบอร์แห่งชาติมุ่งเน้นการเพิ่มจำนวนผู้เชี่ยวชาญที่ได้รับการรับรองมาตรฐานสากล



โซลูชั่นระดับประเทศที่ล้ำสมัย (NCS - National Cybersecurity Solutions)

บูรณาการเทคโนโลยีขั้นสูงเพื่อเสริมสร้างความยืดหยุ่นและความแข็งแกร่งทางไซเบอร์ให้ประเทศไทยในระยะยาว โครงการศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCOC) เป็นหนึ่งในความพยายามสำคัญเพื่อยกระดับความพร้อมของประเทศ



ขอบคุณครับ

08-1842-8411

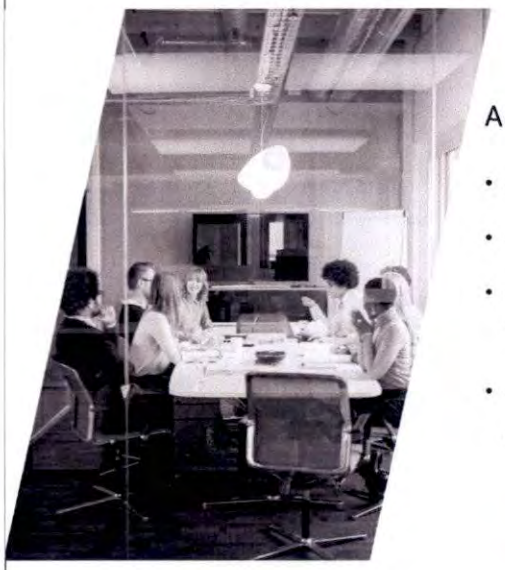
www.mnre.go.th

kantaphan@mnre.go.th

92 ซอยพหลโยธิน 7 ถนนพหลโยธิน
เขต/แขวง พญาไท กทม. 10400

CYBER SECURITY AWARENESS

By
Mr. Suchaya Sanghan
EVP of SCP SYSTEMS CO.,LTD.
Cyber Security and Telecom Department



AGENDA

- ประวัติวิทยากร
- ความเสี่ยงในการถูกโจมตีไซเบอร์
- การป้องกันตนเองและหน่วยงานจากภัยคุกคามไซเบอร์
- ความเสี่ยงในการถูกโจมตีไซเบอร์ การป้องกันและแก้ไขปัญหาจากภัยคุกคามไซเบอร์

<u>คุณวุฒิการศึกษา</u>

- **Primary School and Secondary school : Saint Gabriel College**
- **ปริญญาตรี วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมศาสตร์ไฟฟ้า (ไฟฟ้าสื่อสาร , TELECOMM)**
  จุฬาลงกรณ์มหาวิทยาลัย / เกียรตินิยมอันดับ 1 (Top 5)
- **ปริญญาโท วิทยาศาสตร์มหาบัณฑิต สาขา เทคโนโลยีสารสนเทศ**
  SIU International University / Full Scholarship / 1st in Class

****ปริญญาเอก ได้รับทุนศึกษาต่อที่ USA จาก ศ.ดร. ปรีดา วิบูลย์สวัสดิ์*

<u>International Publication</u>

- **Intelligent P2P VoIP through Extension of Existing Protocols : IEEE in 2007**

<u>ประกาศนียบัตรและใบรับรอง</u>

๑) Certified Cybersecurity Expert (CCE) by Institute of Information Security
๒) CISCO Certified Network Associate (CCNA)
๓) Computer Language Programming: Pascal, Java, Visual Basic, PHP, HTML, MathLab, Maple
๔) Database: MySQL, Oracle, MS Access
๕) Computer Operating System: MS Windows XP, MS Window2003 Server, Linux, Unix
๖) VoIP System Design and Implementation on both Software and Hardware base
๗) Telecommunication and IP & Computer network Test & Measurement
๘) Network Synchronization Design and Implementation
๙) Fiber Optic Network Design and Implementation
๑๐) IT & Telecom Project Management



๑๑) Certificate of Microwave Design and Implementation from Nera Telecommunication (Thailand)
๑๒) Certificate of Fiber Optic Test Solution (MTS-8000) from JDSU/ACTERNA (Singapore)
๑๓) Certificate of Data Monitoring Solution (DA-3400) from JDSU/ACTERNA (Singapore)
๑๔) Certificate of SDH Monitoring Solution (MTS-8000) from JDSU/ACTERNA (Singapore)
๑๕) Certificate of DWDM Monitoring Solution (MTS-8000) from JDSU/ACTERNA (Singapore)
๑๖) Certificate of Ethernet Technology and Ethernet Testing including the Hand-On Testing
๑๗) Certificate of Ethernet Testing Solution (HST-3000) from JDSU/ACTERNA (Singapore)
๑๘) Certificate of IPTV Technology and IPTV Testing including the Hand-On Testing
๑๙) Certificate of VoIP Technology and VoIP Testing including the Hand-On Testing
๒๐) Certificate of DWDM Technology and DWDM Testing including the Hand-On Testing
๒๑) Certificate of Fiber Optic Technology and Fiber Optic Testing including the Hand-On Testing
๒๒) Certificate of Copper Link Technology and Copper Link Testing including the Hand-On Testing
๒๓) Certificate of Circuit Switching Technology and Circuit Switching Testing including the Hand-On Testing
๒๔) Certificate of Mobile Wireless Technology and Mobile Wireless Testing including the Hand-On Testing
๒๕) Certificate of Communication Signaling Technology and Communication Signaling Testing including the Hand-On Testing
๒๖) Certified Cybersecurity Expert (CCE) by Institute of Information Security



ประวัติการเป็นอาจารย์ และ วิทยากร

- วิทยากรพิเศษ : **MBA Class at Mahidol International Management School of Mahidol University**
- อาจารย์พิเศษ : **Information Technology Class at SIU International University**
- วิทยากรอบรม **"Data Network Analysis using IP Analyzer"**, การสื่อสารแห่งประเทศไทย, มกราคม ๒๕๕๑
- วิทยากรอบรม **"Data Network Analysis using IP Analyzer"**, องค์การโทรศัพท์แห่งประเทศไทย, มกราคม ๒๕๕๑
- วิทยากรอบรม **"Data Network Analysis using IP Analyzer"**, กระทรวงมหาดไทย, มกราคม ๒๕๕๒
- วิทยากรอบรม **"Traffic Testing and Optimization using IP Traffic Generator"**, การสื่อสารแห่งประเทศไทย, มกราคม ๒๕๕๑
- วิทยากรอบรม **"Data Network Analysis using IP Analyzer"**, การสื่อสารแห่งประเทศไทย, ธันวาคม ๒๕๕๒
- วิทยากรอบรม **"Traffic Testing and Optimization using IP Traffic Generator"**, การสื่อสารแห่งประเทศไทย, ธันวาคม ๒๕๕๒
- วิทยากรอบรม **"Data Network Analysis using IP Analyzer"**, กรมการสื่อสารทหารอากาศ, ธันวาคม ๒๕๕๒
- วิทยากรอบรม **"Data Network Analysis using IP Analyzer"**, การสื่อสารแห่งประเทศไทย, มีนาคม ๒๕๕๓
- วิทยากรอบรม **"Traffic Testing and Optimization using IP Traffic Generator"**, การสื่อสารแห่งประเทศไทย, มีนาคม ๒๕๕๓
- วิทยากรอบรม **"Optical Network Monitoring using Optical Network management system"**, การสื่อสารแห่งประเทศไทย, มิถุนายน ๒๕๕๒

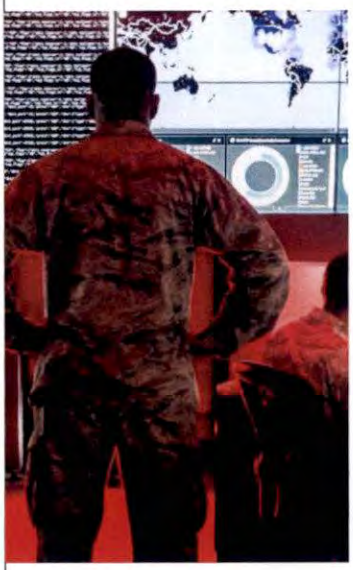


ประวัติการเป็นอาจารย์ และ วิทยากร

- วิทยากรอบรม **"Wi-Fi เทคโนโลยี"**, สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ, มิถุนายน ๒๕๕๖
- วิทยากรอบรม **"Mobile Technology Evolution 2G 3G & 4G"**, สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ, พฤศจิกายน ๒๕๕๖
- วิทยากรอบรม **"Cyber Security Awareness"** ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย, เมษายน ๒๕๖๒
- วิทยากรอบรม **"Cyber Security Awareness"** หลักสูตร มหาบัณฑิต เทคโนโลยีป้องกันประเทศ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, กุมภาพันธ์ ๒๕๖๓
- วิทยากรอบรม **"Cyber Security Awareness"** หลักสูตร ผู้บริหาร การท่าเรือแห่งประเทศไทย, ตุลาคม ๒๕๖๓
- **Project Manager** และวิทยากร โครงการตรวจประเมิน และ พัฒนาความมั่นคงปลอดภัยทางไซเบอร์ รไฟฟ้าส่วนภูมิภาค
- วิทยากรอบรม **"Cyber Security Awareness"** หลักสูตร ผู้บริหาร กรมทรัพยากรน้ำ
- **Project Manager** โครงการตรวจประเมิน และ พัฒนาความมั่นคงปลอดภัยทางไซเบอร์ กรมทรัพยากรน้ำ
- วิทยากรอบรม **"Cyber Security Awareness"** หลักสูตร ผู้บริหาร กรมขนส่งทางราง
- **Team Lead : ISO27001 and ISMS** การรถไฟแห่งประเทศไทย
- **Project Head : National Cyber Exercise (NCX) 2022, 2023, 2024 และ 2025 สกมช.**



ความเสี่ยงในการถูกโจมตีไซเบอร์



ความเสี่ยงในการถูกโจมตีไซเบอร์

- ความตระหนักถึงความเสี่ยงในการถูกโจมตีไซเบอร์ เป็นสิ่งสำคัญมากในโลกยุคดิจิทัล ทั้งในระดับบุคคลและองค์กร เพื่อป้องกันข้อมูลส่วนตัว ทรัพย์สินดิจิทัล และชื่อเสียงจากการถูกละเมิดหรือโจมตีทางไซเบอร์ต่อไปนี้

ความเสี่ยงในการถูกโจมตีไซเบอร์

เข้าใจประเภทของภัยคุกคามไซเบอร์ทั้งตัวบุคคลและองค์กรควรเข้าใจว่าภัยไซเบอร์มีหลายรูปแบบ เช่น

- Phishing (ฟิชชิ่ง): การหลอกให้กรอกข้อมูลสำคัญผ่านอีเมลหรือเว็บปลอม
- Malware (มัลแวร์): โปรแกรมที่มุ่งร้าย เช่น ไวรัส, Ransomware
- Social Engineering: การหลอกล่อหรือใช้จิตวิทยาเพื่อเข้าถึงข้อมูล
- DDoS: การโจมตีให้ระบบล่มด้วยการส่งคำร้องขอจำนวนมาก
- การเจาะระบบ (Hacking): เช่น การใช้ช่องโหว่ของซอฟต์แวร์

หลักการรักษาความมั่นคงปลอดภัยข้อมูล (CIA Triad)

- Confidentiality (การรักษาความลับ): ข้อมูลต้องเข้าถึงได้เฉพาะผู้ที่มีสิทธิ
- Integrity (ความถูกต้องครบถ้วน): ข้อมูลต้องไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต
- Availability (ความพร้อมใช้งาน): ระบบข้อมูลต้องใช้งานได้เมื่อจำเป็น



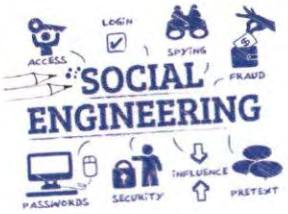
ความเสี่ยงในการถูกโจมตีไซเบอร์

ความรู้พื้นฐานสำหรับบุคคลทั่วไป

- ใช้รหัสผ่านที่รัดกุม และเปิดใช้งาน Two-Factor Authentication (2FA)
- ไม่คลิกลิงก์หรือเปิดไฟล์แนบจากแหล่งที่ไม่น่าเชื่อถือ
- อัปเดตระบบปฏิบัติการและแอปพลิเคชันอย่างสม่ำเสมอ
- ใช้แอนตี้ไวรัส/ไฟร์วอลล์ที่เชื่อถือได้

ความเข้าใจสำหรับระดับองค์กร

- การประเมินความเสี่ยงไซเบอร์: วิเคราะห์ว่ามีช่องโหว่ตรงไหนบ้าง
- นโยบายความปลอดภัย IT (IT Security Policy): จัดทำนโยบายชัดเจน
- การฝึกอบรมพนักงาน: สร้างความตระหนักและสอนแนวทางป้องกัน
- แผนตอบสนองต่อเหตุการณ์ (Incident Response Plan): หากเกิดเหตุแล้วจะทำอย่างไร



ความเสี่ยงในการถูกโจมตีไซเบอร์

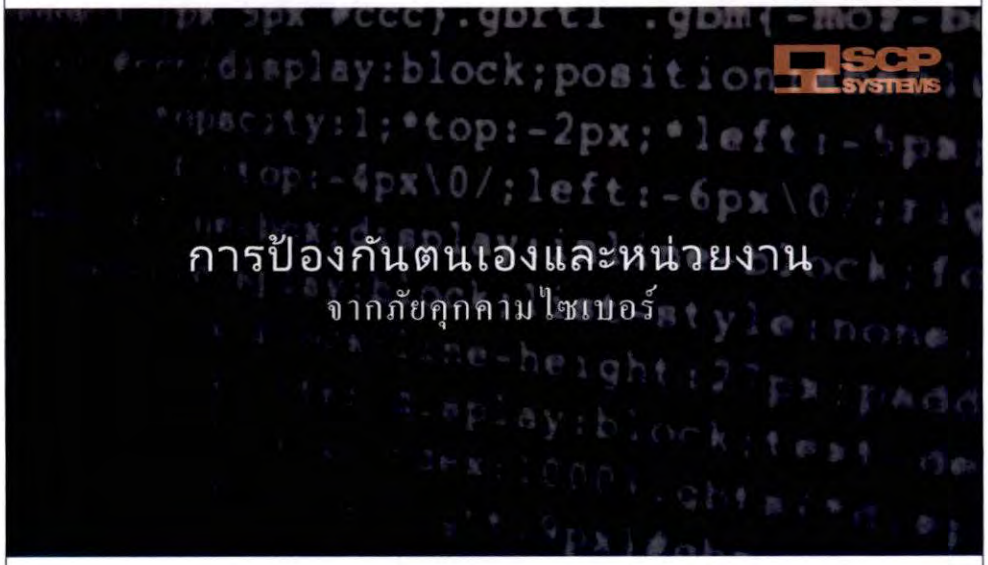
ความตระหนักรู้เชิงจิตวิทยาเข้าใจว่า "ภัยไซเบอร์ไม่ได้เกิดจากเทคโนโลยีอย่างเดียว แต่คนคือจุดอ่อนหลัก" เช่น พนักงานหลงเชื่ออีเมลปลอมความมั่นใจเกินไป หรือการคิดว่า "เราไม่น่าสนใจพอให้ถูกโจมตี" คือกับดักที่อันตราย

"ภัยไซเบอร์ไม่ได้เกิดจากเทคโนโลยีอย่างเดียว แต่คนคือจุดอ่อนหลัก"

เพื่อมี ความตระหนักถึงความเสี่ยงไซเบอร์ อย่างแท้จริง ควรมี

- พื้นฐานความรู้ทางไซเบอร์
- เข้าใจว่าทุกคน ทุกองค์กรคือเป้าหมายได้
- มีพฤติกรรมดิจิทัลที่ปลอดภัย
- วางแผนป้องกันและตอบโต้ภัยอย่างรอบคอบ



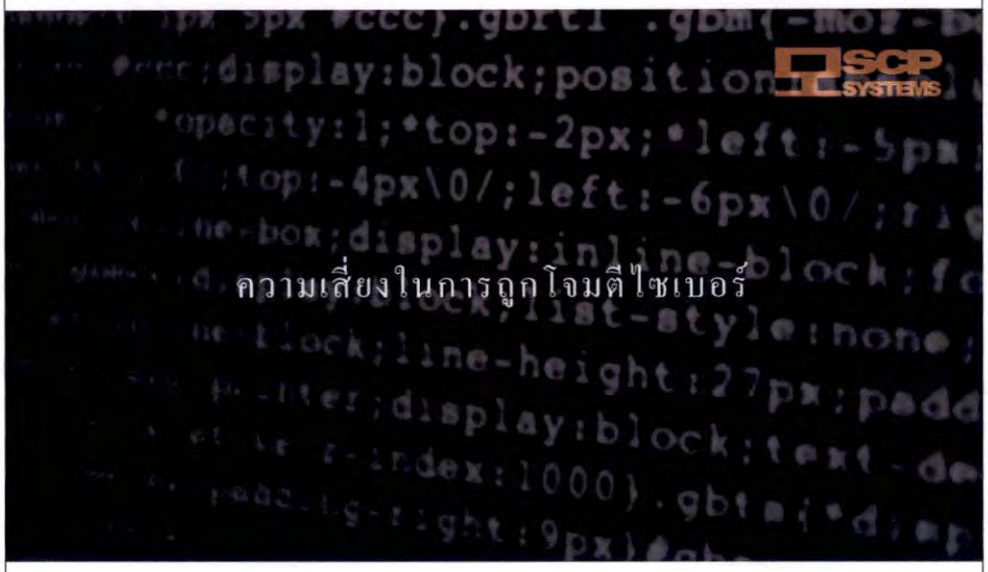


การป้องกันตนเองและหน่วยงานจากภัยคุกคามไซเบอร์

ในฐานะที่คุณเป็น บุคลากรของหน่วยงาน (ไม่ว่าจะเป็นภาครัฐหรือเอกชน) คุณมีบทบาทสำคัญในการ ป้องกันตนเองและหน่วยงานจากภัยคุกคามไซเบอร์ เนื่องจากบุคคลคือจุดอ่อนที่ถูกโจมตีได้ง่ายที่สุดในระบบความมั่นคงปลอดภัยทางไซเบอร์ที่จะมี ความตระหนักถึงความเสี่ยงไซเบอร์ อย่างแท้จริง

- ปฏิบัติตามนโยบายความปลอดภัยขององค์กรเข้าใจว่าทุกคน ทุกองค์กรคือเป้าหมายได้
- ปกป้องบัญชีผู้ใช้ของคุณวางแผนป้องกันและตอบโต้ภัยอย่างรอบคอบ
- ระมัดระวังกับอีเมลและลิงก์
- ใช้เครื่องคอมพิวเตอร์และเครือข่ายอย่างปลอดภัย
- สำรองข้อมูลและปฏิบัติตามแนวทางของ IT
- เพิ่มพูนความรู้และตระหนักรู้ภัยไซเบอร์ อย่างต่อเนื่อง
- เมื่อเกิดเหตุผิดปกติ ควรรู้ว่าจะทำอย่างไร (Incident Response Plan)

"บุคลากรที่มีความตระหนัก + พฤติกรรมที่ปลอดภัย = หน่วยงานที่มั่นคงจากภัยไซเบอร์การป้องกันไม่ใช่หน้าที่ของฝ่าย IT เท่านั้น แต่เป็น ความรับผิดชอบร่วมกันของทุกคนในองค์กร"



ความเสี่ยงในการถูกโจมตีไซเบอร์

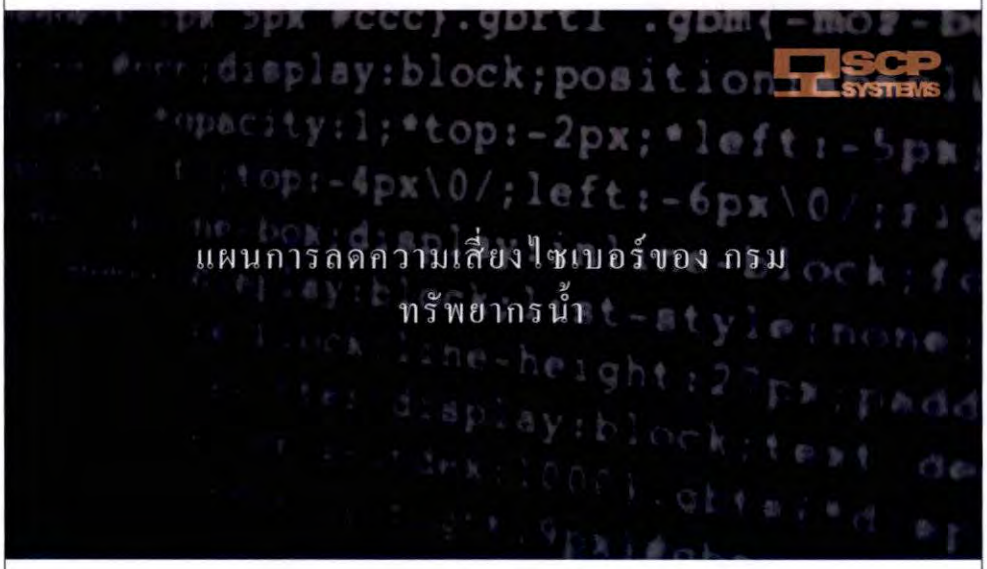
ความเสี่ยงในการถูกโจมตีไซเบอร์มีอยู่หลายด้าน ทั้งในระดับบุคคลและองค์กร ซึ่งหากไม่เข้าใจหรือไม่เตรียมการรับมืออย่างเหมาะสม อาจนำไปสู่การ รั่วไหลของข้อมูล, การสูญเสียทรัพย์สิน, ความเสียหายทางชื่อเสียง, หรือการหยุดชะงักของระบบงานต่อไปนี้คือ ความเสี่ยงหลัก ๆ ในแต่ละด้าน พร้อมแนวทางป้องกันหรือการลดความเสี่ยง

ความเสี่ยงในระดับบุคคล

ความเสี่ยง	ตัวอย่าง	วิธีป้องกัน / ลดความเสี่ยง
1. **การถูกหลอกลวง** (Phishing / Social Engineering)	อีเมลปลอม, โทรหลอก, ลิงก์หลอก	- ตรวจสอบอีเมลและลิงก์ก่อนคลิก- อย่าเปิดเผยข้อมูลส่วนตัวกับบุคคลแปลกหน้า- หมั่นฝึกสังเกตพฤติกรรมต้องสงสัย
2. **รหัสผ่านไม่ปลอดภัย**	ใช้รหัสผ่านง่าย ๆ ซ้ำ ๆ หลายที่	- ใช้รหัสผ่านซับซ้อน- เปิดใช้ 2FA- ใช้ Password Manager
3. **การใช้อุปกรณ์หรือเครือข่ายไม่ปลอดภัย**	ใช้ Wi-Fi สาธารณะ, ไม่อัปเดตเครื่อง	- หลีกเลี่ยง Wi-Fi สาธารณะหรือใช้ VPN- อัปเดตซอฟต์แวร์เสมอ
4. **การดาวน์โหลดไฟล์หรือแอปพลิเคชันอันตราย**	ไฟล์แนบจากอีเมล, แอปเถื่อน	- ดาวน์โหลดเฉพาะจากแหล่งที่เชื่อถือได้- สแกนไวรัสก่อนเปิดไฟล์

ความเสี่ยงในระดับองค์กร

ความเสี่ยง	ตัวอย่าง	วิธีป้องกัน / ลดความเสี่ยง
1. **ช่องโหว่ระบบหรือซอฟต์แวร์** (Vulnerabilities)	ซอฟต์แวร์ไม่ได้อัปเดต	- ติดตาม Patch / Update ระบบ- ใช้เครื่องมือสแกนหาช่องโหว่
2. **พนักงานขาดความรู้ความเข้าใจ**	คลิกลิงก์ฟิชชิง, ส่งข้อมูลให้แฮกเกอร์	- จัดอบรม Security Awareness เป็นประจำ- จำลองเหตุการณ์โจมตีเพื่อฝึกซ้อม
3. **การจัดการสิทธิ์ไม่เหมาะสม**	พนักงานเข้าถึงข้อมูลเกินสิทธิ์	- ใช้หลักการ **Least Privilege**- ตรวจสอบสิทธิ์เป็นประจำ
4. **ขาดการสำรองข้อมูล** (Backup)	โดน Ransomware แล้วข้อมูลหาย	- สำรองข้อมูลอย่างสม่ำเสมอ- ทดสอบการกู้คืนข้อมูล
5. **ไม่มีแผนรับมือเหตุการณ์** (Incident Response Plan)	ไม่รู้ว่าควรทำอะไรเมื่อระบบโดนโจมตี	- จัดทำและทดสอบแผน IR- มีทีมรับมือเหตุฉุกเฉินชัดเจน
6. **ระบบหรือบุคคลภายนอก** (Third-party Risk)	Vendor ที่เชื่อมต่อเข้าระบบถูกแฮก	- ตรวจสอบความปลอดภัยของผู้ให้บริการ- ทำข้อตกลงด้านความปลอดภัย (Security SLA)



วัตถุประสงค์ของแผน

- ลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่อาจส่งผลต่อข้อมูล น้ำ ระบบเครือข่าย และบริการภาครัฐ
- ปกป้องความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ทั้งข้อมูลภายใน และข้อมูลสาธารณะ
- เสริมสร้างความรู้ ความเข้าใจ และวินัยด้านความมั่นคงปลอดภัยทางไซเบอร์ให้แก่เจ้าหน้าที่

การแบ่งหมวดหมู่ความเสี่ยงและแนวทางป้องกัน

ความเสี่ยงด้านข้อมูล (Data Risk)

รายการ	ความเสี่ยง	แนวทางลดความเสี่ยง
A1	ข้อมูลเชิงพื้นที่ (GIS, น้ำท่วม, เขื่อน ฯลฯ) รั่วไหล	- จัดการสิทธิการเข้าถึงข้อมูล (Role-based Access Control)- เข้ารหัสข้อมูลสำคัญทั้งที่เก็บและส่งผ่าน (Encryption)- ตรวจสอบ log การเข้าถึงเป็นประจำ
A2	การจัดเก็บข้อมูลประชาชนเกี่ยวกับผู้ใช้งานระบบร้องเรียน	- ปรับให้เป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)- ลบทำลายข้อมูลเมื่อหมดอายุการใช้งาน- ใช้นโยบายการรักษาความลับภายในหน่วยงาน

การแบ่งหมวดหมู่ความเสี่ยงและแนวทางป้องกัน

ความเสี่ยงด้านระบบและเทคโนโลยี (System/Network Risk)

รายการ	ความเสี่ยง	แนวทางลดความเสี่ยง
B1	ระบบบริการเว็บไซต์กรมถูกโจมตี (เช่น DDoS)	- ติดตั้งระบบ Firewall / Web Application Firewall - จัดทำ Backup ข้อมูลเว็บทุกวัน- ใช้บริการ CDN (เช่น Cloudflare) ป้องกันการโจมตี
B2	ช่องโหว่จากซอฟต์แวร์ หรือแอปพลิเคชันที่ล้าสมัย	- อัปเดตระบบและ Patch ทันทีที่มีเวอร์ชันใหม่ - สแกนหาช่องโหว่เป็นประจำ (Vulnerability Assessment)
B3	การเจาะระบบจากภายนอก (เช่นการแฮกระบบน้ำอัจฉริยะ)	- แยกระบบสำคัญออกจากระบบอินเทอร์เน็ต - ใช้ VPN สำหรับการเข้าระบบภายในจากภายนอก - บังคับใช้การยืนยันตัวตนหลายขั้น (MFA)

การแบ่งหมวดหมู่ความเสี่ยงและแนวทางป้องกัน

ความเสี่ยงจากบุคลากร (Human Risk)

รายการ	ความเสี่ยง	แนวทางลดความเสี่ยง
C1	เจ้าหน้าที่คลิกลิงก์ฟิชชิง / เปิดไฟล์แนบอันตราย	- อบรมภัยคุกคามไซเบอร์อย่างน้อยปีละ 2 ครั้ง - จัดอบรมจำลองสถานการณ์ (Phishing Simulation) - จัดทำคู่มือ/โปสเตอร์เตือนภัยติดตามพื้นที่ทำงาน
C2	พนักงานลาออกแต่ยังเข้าระบบได้	- จัดให้มีขั้นตอน "ถอนสิทธิ์การเข้าระบบ" ภายใน 24 ชั่วโมงหลังลาออก-ตรวจสอบบัญชีผู้ใช้งานประจำเดือน
C3	เจ้าหน้าที่นำแฟลชไดรฟ์หรืออุปกรณ์ส่วนตัวมาเสียบในระบบ	- ติดตั้งระบบป้องกัน USB อัตโนมัติ - ใช้นโยบาย BYOD พร้อมตรวจสอบอุปกรณ์ก่อนเชื่อมต่อ

การแบ่งหมวดหมู่ความเสี่ยงและแนวทางป้องกัน

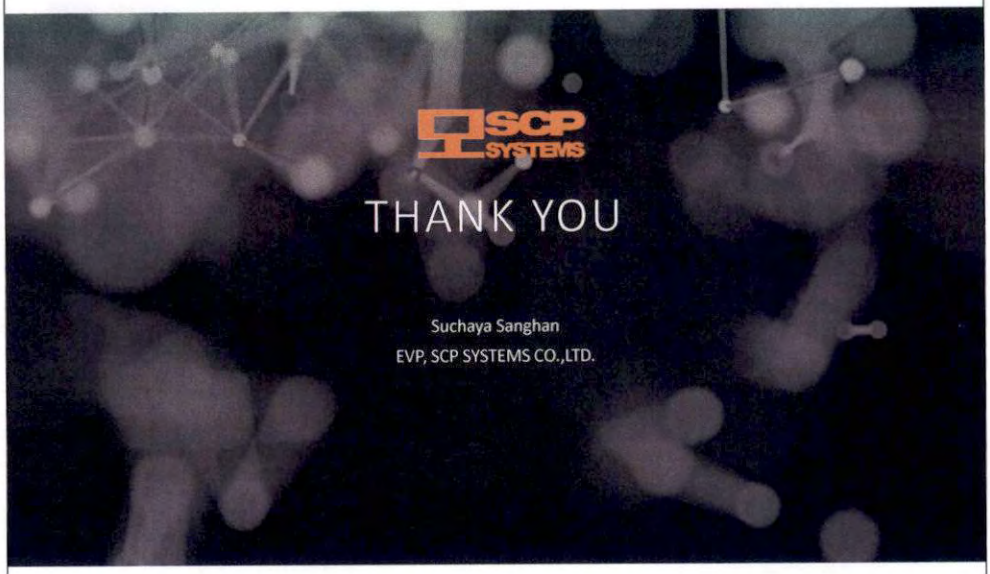
ความเสี่ยงจากการไม่มีแผนรับมือ (Operational Risk)

รายการ	ความเสี่ยง	แนวทางลดความเสี่ยง
D1	ไม่มีแผนรับมือเมื่อเกิดเหตุไซเบอร์	- จัดทำ Incident Response Plan - แต่งตั้งทีม CSIRT (Computer Security Incident Response Team) - ซ้อมแผนทุก 6 เดือน
D2	ข้อมูลสูญหายโดยไม่ได้สำรอง	- สำรองข้อมูลระบบสำคัญทุกวัน และแยกเก็บนอกระบบหลัก- ทดสอบการกู้คืนข้อมูล (Restore) อย่างน้อยเดือนละครั้ง

กำหนดนโยบายและการกำกับติดตาม

- จัดตั้ง คณะทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Committee)
- แต่งตั้ง เจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศ (Information Security Officer) ระดับกรม
- มีการ ประเมินความเสี่ยงไซเบอร์ประจำปี และรายงานผลต่อผู้บริหาร
- ปรับปรุงแผนตามภัยคุกคามที่เปลี่ยนแปลง และตามแนวทางของ พรบ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ระยะเวลา	แผนปฏิบัติ
ระยะสั้น (0-3 เดือน)	- อบรมบุคลากรเรื่องฟิชชิงและพฤติกรรมปลอดภัย - อัปเดตระบบและตรวจสอบบัญชีผู้ใช้งาน
ระยะกลาง (3-6 เดือน)	- จัดทำ Incident Response Plan และทดสอบ - เริ่มใช้ VPN และ MFA สำหรับงานภายใน
ระยะยาว (6-12 เดือน)	- ตรวจสอบช่องโหว่ระบบและรายงานความเสี่ยง- จัดทำรายงานประเมินผลด้านไซเบอร์ต่อผู้บริหาร


SCP
SYSTEMS
THANK YOU
Suchaya Sanghan
EVP, SCP SYSTEMS CO.,LTD.

ความปลอดภัยทางไซเบอร์ (Cybersecurity)



นางสาวสายชล แซ่ลี้
ผู้อำนวยการสำนักประสานงาน (สกมช.)
รักษาการผู้อำนวยการสำนักปฏิบัติการ

ตำแหน่งปัจจุบัน • ผู้อำนวยการสำนักประสานงาน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ประสบการณ์ทำงาน รักษาการผู้อำนวยการสำนักปฏิบัติการ

- ผู้อำนวยการกลุ่มงานส่งเสริมและสนับสนุนความร่วมมือทางวิชาการ ศูนย์พัฒนานโยบายดิจิทัลเพื่อเศรษฐกิจและสังคม สดช.
- ผู้อำนวยการกลุ่ม กองโครงสร้างพื้นฐานด้านมาตรฐานเทคโนโลยีดิจิทัล สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.)
- ผู้อำนวยการกลุ่มงานมาตรฐาน สำนักธุรกรรมทางอิเล็กทรอนิกส์ สป.ทก.
- รองผู้อำนวยการสำนักงานเตรียมการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (สป.ทก.)
- ผู้อำนวยการกลุ่มงานบริหารจัดการโครงสร้างพื้นฐาน สำนักส่งเสริมและพัฒนารัฐบาลอิเล็กทรอนิกส์ สป.ทก.

การศึกษา

- 2544-2547 วท.ม.เทคโนโลยีสารสนเทศและการจัดการ มหาวิทยาลัยเชียงใหม่
- 2541-2543 ศศ.บ.การจัดการทั่วไป (คอมพิวเตอร์ธุรกิจ) สถาบันราชภัฏลำปาง
- 2538-2540 ปวส.คอมพิวเตอร์ธุรกิจ วิทยาลัยอาชีวศึกษาลำปาง

ผลงานสำคัญหรือทักษะหรือความสามารถพิเศษ

2559 โครงการเช่าใช้อินเทอร์เน็ตสาธารณะสู่ชุมชน
2560 โครงการยกระดับโครงสร้างพื้นฐานโทรคมนาคมเพื่อขับเคลื่อนเศรษฐกิจของประเทศ
กิจกรรมที่ ๑ การขยายโครงข่ายอินเทอร์เน็ตความเร็วสูงให้ครอบคลุมทั่วประเทศ เพื่อสนับสนุนการพัฒนาเศรษฐกิจภายในประเทศ (เน็ตประชารัฐ)
กิจกรรมที่ ๒ การเพิ่มประสิทธิภาพโครงข่ายอินเทอร์เน็ตระหว่างประเทศสู่การเป็น ASEAN Digital Hub
2565 โครงการเร่งรัดพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 1
2566 คณะอนุกรรมการกลั่นกรองการกำหนดหลักเกณฑ์ในการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

CERTIFICATES





นางสาวสายชล แซ่ลี้
ผู้อำนวยการสำนักประสานงาน (สกมช.)

เกี่ยวกับ สกมช.

วิสัยทัศน์ VISION

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

พันธกิจ MISSIONS

เสนอแนะนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดแนวทาง มาตรฐาน มาตรการที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต

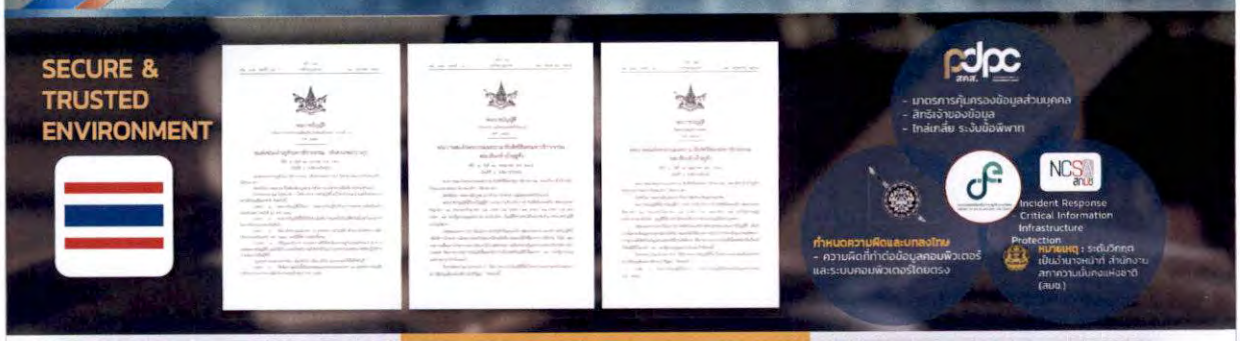
กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้งส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐและเอกชนทั้งในประเทศและต่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

เผยแพร่ความรู้ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



ประเทศไทยได้ออกกฎหมายและกำหนดหน่วยงานสำคัญหลายฉบับเพื่อเน้นการรักษาความมั่นคงทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

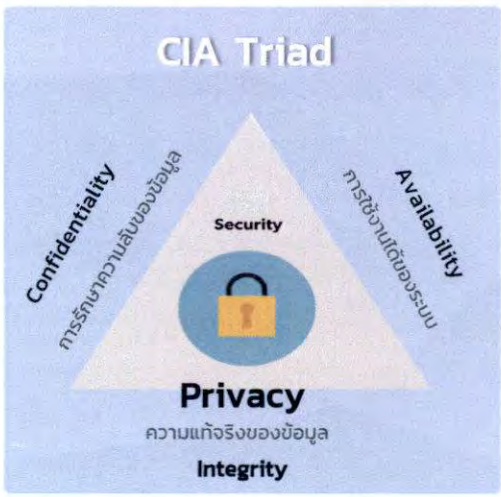


พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ 2560	พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
กฎหมายฉบับนี้ครอบคลุมการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การแฮ็ก และการเผยแพร่ข้อมูลเท็จ เป็นกฎหมายพื้นฐานสำหรับการดำเนินคดีกับผู้กระทำผิดทางไซเบอร์	กฎหมายที่มีเป้าหมายเพื่อความมั่นคงแห่งชาติในโลกไซเบอร์ กฎหมายฉบับนี้บังคับให้องค์กรในภาคส่วนสำคัญ (เช่น การเงิน พลังงาน คมนาคม และสุขภาพ) ต้องดำเนินมาตรการป้องกันโครงสร้างพื้นฐานสารสนเทศที่สำคัญ (Critical Information Infrastructure - CII) และให้สิทธิแก่รัฐบาลในการตรวจสอบและจัดการเหตุการณ์ทางไซเบอร์	มีเป้าหมายในการคุ้มครองข้อมูลส่วนบุคคลของประชาชน โดยกำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ และจัดเก็บข้อมูล พร้อมทั้งให้สิทธิกับเจ้าของข้อมูลในการควบคุมข้อมูลส่วนตัว และกำหนดบทลงโทษกรณีละเมิด



สร้างความตระหนัก และเสริมทักษะจำเป็นด้านความมั่นคงปลออดภัยทางไซเบอร์

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

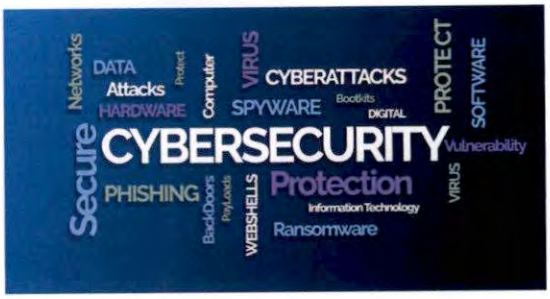
Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มี ความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

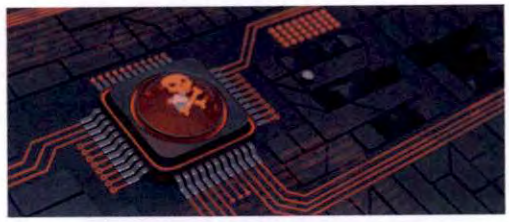
การรักษาความปลอดภัยทางไซเบอร์คืออะไร



Cyber Security คือ ความมั่นคงปลอดภัยทางไซเบอร์ ที่ต้องการป้องกันและการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้อง โดยจุดประสงค์ คือ เพื่อป้องกันการเข้าถึง การแก้ไข การเปลี่ยนแปลง หรือการทำลายข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต หรือบุคคลที่ต้องการเข้าถึงข้อมูลเพื่อวัตถุประสงค์ที่ไม่เหมาะสม

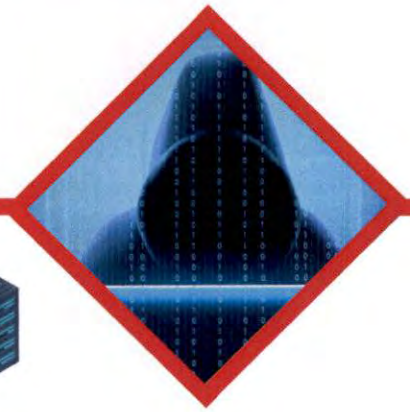
ทั้งนี้หลายองค์กร ต่างให้ความสำคัญเรื่องระบบรักษาความปลอดภัยของข้อมูลไม่แพ้กัน เพราะหากลูกค้าหรือผู้ใช้บริการโดนโจรกรรมข้อมูลทางอิเล็กทรอนิกส์ไป อาจทำให้องค์กรเสียชื่อได้ เพราะฉะนั้น Cyber Security จึงมีความสำคัญ

"ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง



สถานการณ์ภัยคุกคามไซเบอร์ระดับโลก

Ransomware เป็นการโจมตีที่มีสัดส่วนสูงสุด 23% ตามด้วย Data Theft และ Server Access ซึ่งมีสัดส่วน 13% และ 10% ตามลำดับ





1. Ransomware

ไฟล์ถูกเข้ารหัสทำให้ผู้ใช้งานไม่สามารถเปิดไฟล์ได้ โดยผู้ใช้งานจะต้องจ่ายเงินตามข้อความ "เรียกค่าไถ่" เพื่อปลดล็อคกู้ข้อมูลคืนมา



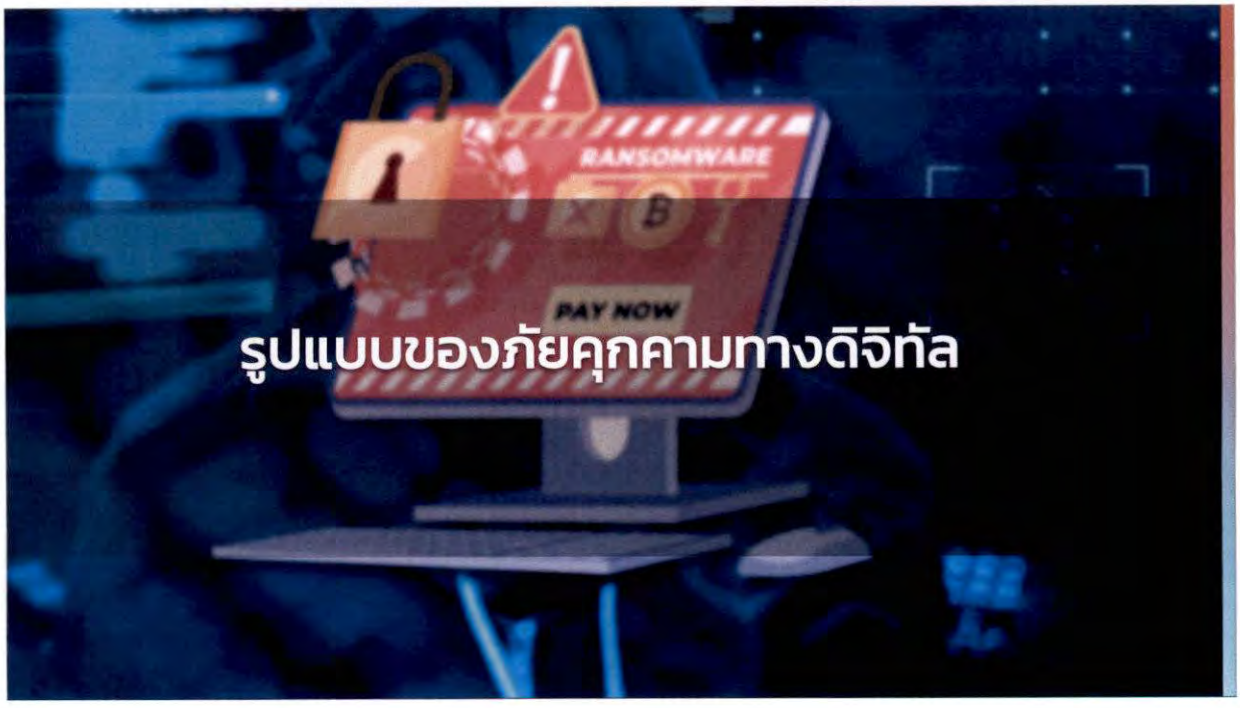
2. Data Theft

ส่วนใหญ่เกิดจากบุคคลภายในองค์กรด้วยมองว่าข้อมูลเป็นสิทธิ์ของตน เนื่องจากเป็นผู้จัดทำขึ้น หรืองงใจละเมิดการเข้าถึงข้อมูลเพื่อเปิดเผยการประพฤติมิชอบของนายจ้างจากมุมมองของสังคม



3. Server Access

การเข้าถึงระบบโดยไม่ได้รับอนุญาต ซึ่งอาจจมีจุดประสงค์ในการขโมยข้อมูล แก้ไขปรับเปลี่ยน หรือทำให้หยุดชะงัก ไม่สามารถให้บริการแก่ผู้ใช้งานได้



รูปแบบของภัยคุกคามทางดิจิทัล

มูลค่าความเสียหายจากอาชญากรรมไซเบอร์ทั่วโลก

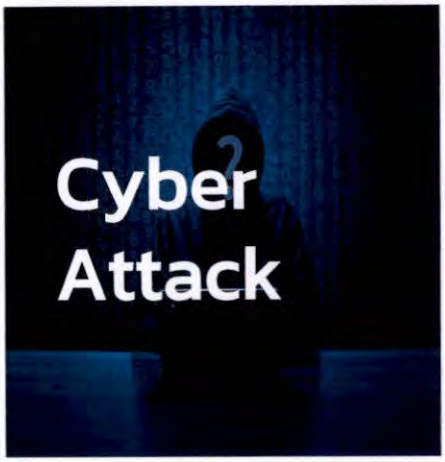
การแยกย่อยของต้นทุนความเสียหายจากอาชญากรรมทางไซเบอร์ทั่วโลกที่ Cybersecurity Ventures คาดการณ์ไว้ในปี 2024:





- 9.5 ล้านล้านเหรียญสหรัฐต่อปี
- 793 พันล้านเหรียญสหรัฐต่อเดือน
- 182.5 พันล้านเหรียญสหรัฐต่อสัปดาห์
- 26 พันล้านเหรียญสหรัฐต่อวัน
- 1 พันล้านเหรียญสหรัฐต่อชั่วโมง
- 18 ล้านเหรียญสหรัฐต่อนาที
- 302,000 เหรียญสหรัฐต่อวินาที

เป้าหมาย ของ Cyberattackers



- **บุคคล** : ผู้โจมตีอาจกำหนดเป้าหมายเป็นรายบุคคลเพื่อผลประโยชน์ส่วนตัว เช่น โดยการขโมยข้อมูลรับรองการเข้าสู่ระบบหรือเรียกค่าไถ่ข้อมูลส่วนบุคคล
- **ข้อมูลส่วนบุคคล** : ผู้โจมตีอาจพยายามขโมยข้อมูลส่วนบุคคลที่ละเอียดอ่อน เช่น ข้อมูลรับรองการเข้าสู่ระบบ ข้อมูลทางการเงิน และหมายเลขประกันสังคม เพื่อขายในตลาดมืดหรือใช้เพื่อขโมยข้อมูลประจำตัว
- **ทรัพย์สินทางปัญญา** : ผู้โจมตีอาจพยายามขโมยข้อมูลที่เป็นกรรมสิทธิ์ เช่น ความลับทางการค้าและเทคโนโลยีที่เป็นกรรมสิทธิ์ เพื่อให้ได้เปรียบในการแข่งขันหรือขายข้อมูลให้กับบุคคลอื่น
- **โครงสร้างพื้นฐานที่สำคัญ** : การโจมตีทางไซเบอร์บนโครงสร้างพื้นฐานที่สำคัญ เช่น โครงข่ายไฟฟ้า โรงบำบัดน้ำ และระบบขนส่ง สามารถส่งผลกระทบร้ายแรงและทำให้การทำงานของการบริการที่จำเป็นหยุดชะงักได้
- **หน่วยงานรัฐบาลและองค์กรทางการเมือง** : ผู้โจมตีอาจกำหนดเป้าหมายหน่วยงานรัฐบาลและองค์กรทางการเมืองเพื่อขโมยข้อมูลที่ละเอียดอ่อนหรือขัดขวางการดำเนินงานของหน่วยงาน
- **ธุรกิจ** : การโจมตีทางไซเบอร์ต่อธุรกิจอาจทำให้สูญเสียข้อมูลที่ละเอียดอ่อน สูญเสียทางการเงิน และทำลายชื่อเสียงของบริษัท

ภาพรวมของ Cybersecurity ในปัจจุบัน

ภัยคุกคามทางไซเบอร์มีความซับซ้อนและหลากหลายมากขึ้น
- รูปแบบการโจมตีพัฒนาอย่างต่อเนื่อง เช่น Ransomware-as-a-Service (RaaS), AI-driven phishing, และ Supply Chain Attacks
- กลุ่มแฮกเกอร์มักทำงานแบบองค์กร มีเป้าหมายชัดเจน และวางแผนระยะยาว

เป้าหมายหลักของการโจมตีเปลี่ยนไป
- จากองค์กรขนาดใหญ่ → สู่ธุรกิจขนาดกลางและเล็ก (SMEs)
- จากข้อมูลส่วนตัว → สู่การเจาะระบบโครงสร้างพื้นฐานสำคัญ เช่น พลังงาน, ระบบสาธารณสุข, การเงิน

การเปลี่ยนแปลงของสภาพแวดล้อมการทำงาน
- การทำงานแบบ Hybrid หรือ Remote Work ทำให้ขอบเขตการรักษาความปลอดภัยยากขึ้น
- อุปกรณ์ส่วนตัวของพนักงานกลายเป็นจุดอ่อนใหม่ (BYOD: Bring Your Own Device)

การใช้ AI และ Automation ในการรักษาความปลอดภัย
- ระบบ AI เริ่มมีบทบาทในการตรวจจับพฤติกรรมผิดปกติ
- แต่ในขณะเดียวกัน แฮกเกอร์ก็ใช้ AI ในการโจมตี เช่น Deepfake, Phishing ด้วยข้อความสมจริง



https://www.getastra.com/blog/security-audit/cyber-crime-statistics/
https://www.thesslstore.com/blog/cyber-crime-statistics/

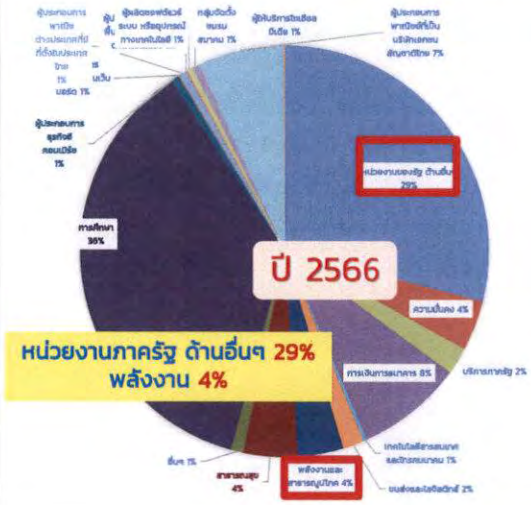
สถิติภัยคุกคามทางไซเบอร์

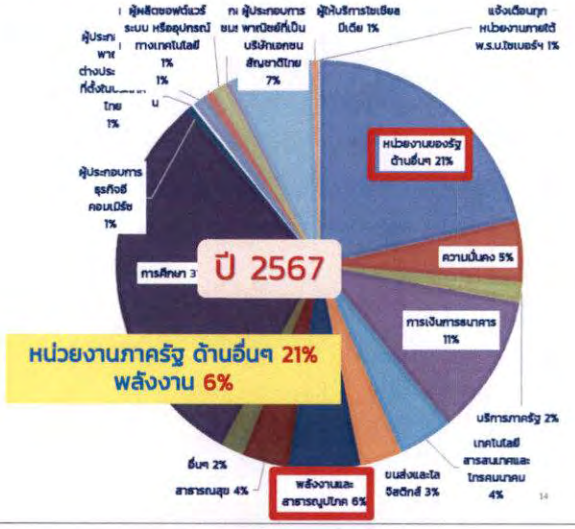
ประเภทภัยคุกคาม	ปีงบประมาณ 2565 (เหตุการณ์)	ปีงบประมาณ 2566 (เหตุการณ์)	ปีงบประมาณ 2567 (เหตุการณ์)	ห้วง ตุลาคม 2567 - พฤษภาคม 2568 (เหตุการณ์)
Intrusion Attempts	414	473	684	579
Fraud	54	221	181	418
Availability	2	5	1	62
Malicious Code	48	35	18	80
Intrusions	4	139	0	21
Information Content Security	0	53	7	272
Other	29	0	0	0
รวมทั้งสิ้น	**551**	**1,808**	**1,827**	**1,432**



ผลการดำเนินงานที่สำคัญภายใต้แผนงานบูรณาการรัฐบาลดิจิทัล

สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์

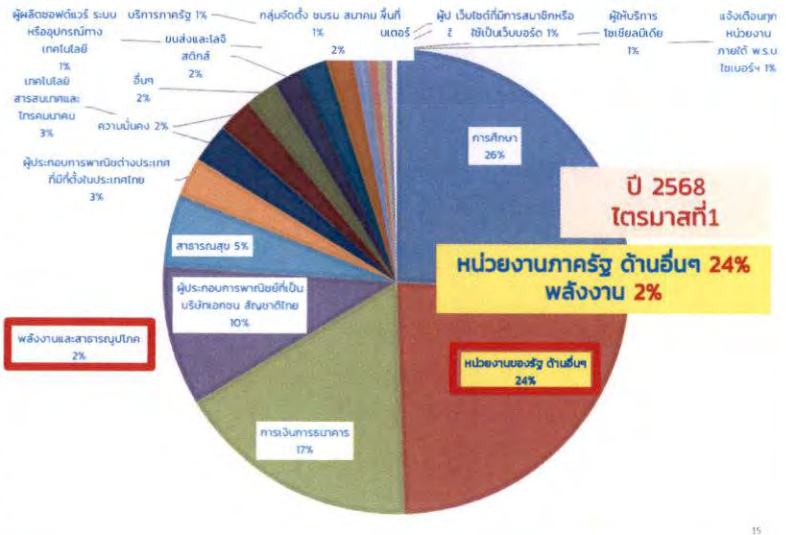




ผลการดำเนินงานที่สำคัญภายใต้แผนงานบูรณาการรัฐบาลดิจิทัล

รวมทั้งสิ้น 1,656 เหตุการณ์

การศึกษา	427
หน่วยงานของรัฐ ด้านอื่นๆ	391
การเงินการธนาคาร	280
ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	161
สาธารณสุข	83
ผู้ประกอบการพาณิชย์ต่างประเทศที่มีที่ตั้งในประเทศไทย	46
เทคโนโลยีสารสนเทศและโทรคมนาคม	46
ความมั่นคง	40
อื่นๆ	37
ขนส่งและโลจิสติกส์	32
พลังงานและสาธารณูปโภค	32
ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	30
ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	17
บริการภาครัฐ	11
กลุ่มจัดตั้ง ชมรม สมาคม	9
ผู้ประกอบการธุรกิจอีคอมเมิร์ซ	8
เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	3
ผู้ให้บริการโซเชียลมีเดีย	2
แจ้งเตือนทุกหน่วยงานภายใต้ พ.ร.บ.ไซเบอร์ฯ	1





NCSA สกมช. ThaiCERT By NCSA Thailand

ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

DATA BREACH







NCSA สกมช. ThaiCERT By NCSA Thailand

ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

DATA LEAK

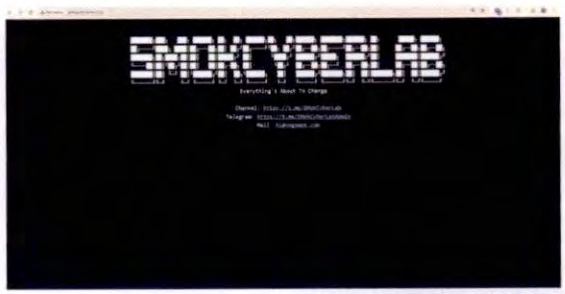
site: .go.th filetype:pdf
หรือ xlsx



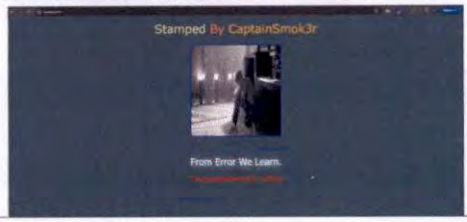


ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

HACKED WEBSITE (DEFACEMENT)







ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

HACKED WEBSITE (GAMBLING)

site: .go.th หรือ .ac.th
"คาสิโน" slot บาคาร่า
sbobet เป็นต้น







ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

SECURITY MISCONFIGURATION

DIRECTORY LISTING

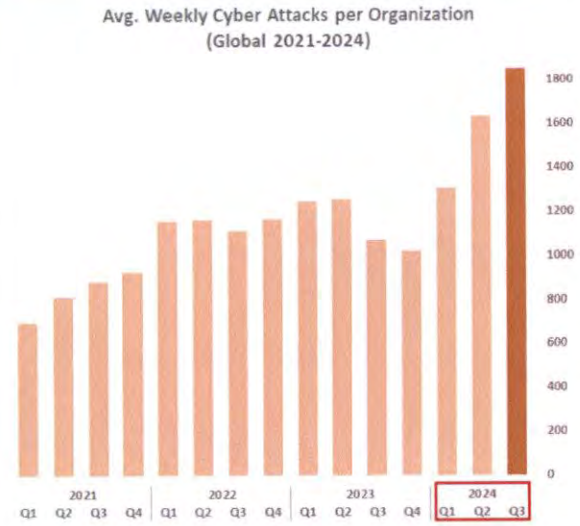
Index of /Web2024

Name	Last modified	Size	Description
Parent Directory		-	
Executive_office/	2023-03-11 10:57	-	
Facebook Messenger C..>	2023-06-28 16:59	1.2K	
Facebook Messenger C..>	2022-07-18 10:29	1.1K	
Logo.png	2020-06-23 09:59	93K	
PM25.php	2024-03-12 09:17	10K	
UpRightSchool/	2022-06-14 13:50	-	
_groups/	2022-06-14 13:50	-	
about.html	2020-06-19 11:07	23K	

Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2016/	2020-11-07 11:08	-	
2017/	2020-11-07 11:08	-	
2018/	2022-10-24 14:00	-	
2019/	2020-12-30 14:39	-	
2020/	2020-12-01 00:05	-	
2021/	2021-12-01 07:00	-	
2022/	2022-12-01 07:01	-	
2023/	2023-12-01 00:07	-	
2024/	2024-12-01 00:04	-	

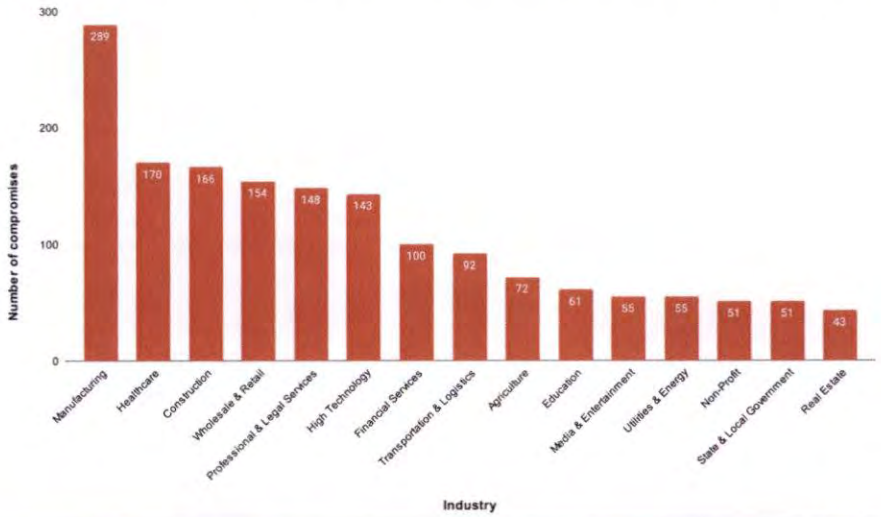
2024: การโจมตีทางไซเบอร์ทั่วโลกพุ่งสูงขึ้น 75%



- **จำนวนการโจมตีที่พุ่งสูงเป็นประวัติการณ์:** ในไตรมาสที่ 3 ปี 2567 มีการบันทึกการโจมตีทางไซเบอร์เฉลี่ย 1,876 ครั้งต่อองค์กร ซึ่งเพิ่มขึ้น 75% เมื่อเทียบกับช่วงเวลาเดียวกันในปี 2566 และเพิ่มขึ้น 15% เมื่อเทียบกับไตรมาสก่อนหน้า
- **การแยกย่อยตามอุตสาหกรรม:** ภาคการศึกษา/การวิจัยเป็นเป้าหมายมากที่สุด โดยมีการโจมตีรายสัปดาห์จำนวน 3,828 ครั้ง รองลงมาคือภาครัฐบาล/ทหาร และภาคการดูแลสุขภาพ โดยมีการโจมตี 2,553 และ 2,434 ครั้ง ตามลำดับ
- **ระดับภูมิภาค:** แอฟริกาเผชิญกับการโจมตีเฉลี่ยสูงสุดที่ 3,370 ครั้งต่อสัปดาห์ (+90% เมื่อเทียบกับปีที่แล้ว) ในขณะที่ยุโรปและละตินอเมริกาก็พบว่าเพิ่มขึ้นอย่างมีนัยสำคัญเช่นกัน
- **Ransomware:** ภัยคุกคามที่คงอยู่: มีรายงานเหตุการณ์ ransomware มากกว่า 1,230 ครั้ง โดยอเมริกาเหนือได้รับผลกระทบมากที่สุด (57% ของเหตุการณ์) รองลงมาคือยุโรป (24%)

https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

Industries Most Impacted by Ransomware



© 2024 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto | UNIT 42

Year-over-Year Ransomware Activity Comparison



© 2024 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto | UNIT 42

ข้อมูล LOCKBIT 2.0 และ 3.0 ที่โจมตีในประเทศไทย







ปีที่พบ	จำนวนหน่วยงาน	มูลค่าความเสียหาย
2022	14	619,000,000
2023	17	690,000,000
2024	5	1,002,000,000
รวม	36	**2,311,000,000**

ความเสียหายที่เกิดจากจาก LOCKBIT 2.0 และ 3.0

รวม 2,3111,000,000 บาท

#ประมาณการจาก ขนาดธุรกิจ ทุนจดทะเบียน จำนวนข้อมูลที่ถูกเผยแพร่ และข้อมูลงบการเงินของบริษัทที่

LockBit ransomware กลับมาอีกครั้ง
จากกู้คืนเซิร์ฟเวอร์ หลังถูกจัดการไป



ได้ย้ายเว็บไซต์ที่มีข้อมูลที่ถูกรั่วไหลไปยังที่อยู่ .onion ใหม่ โดยเว็บไซต์ดังกล่าวมีรายชื่อผู้เสียหาย 5 ราย พร้อมนับถอยหลังสำหรับการเผยแพร่ข้อมูลที่ขโมยมา

24 ก.พ. 2024



ที่มา : i-secure

ไม่ได้อัปเดต PHP ให้เป็นเวอร์ชันล่าสุด"

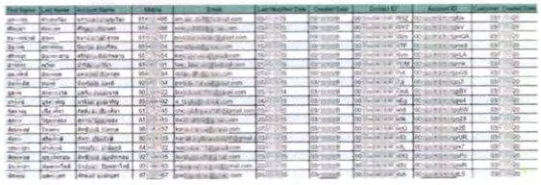
อาจถูกโจมตีโดยใช้ช่องโหว่

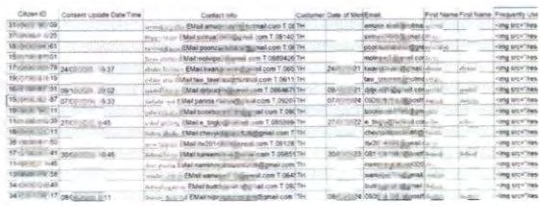


ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

DATA BREACH

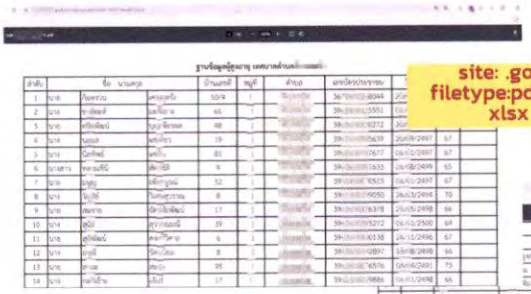


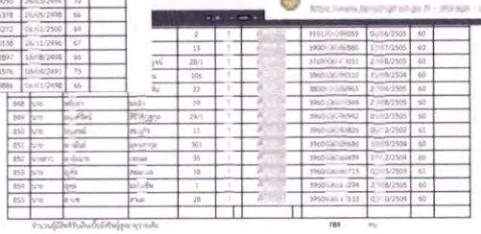




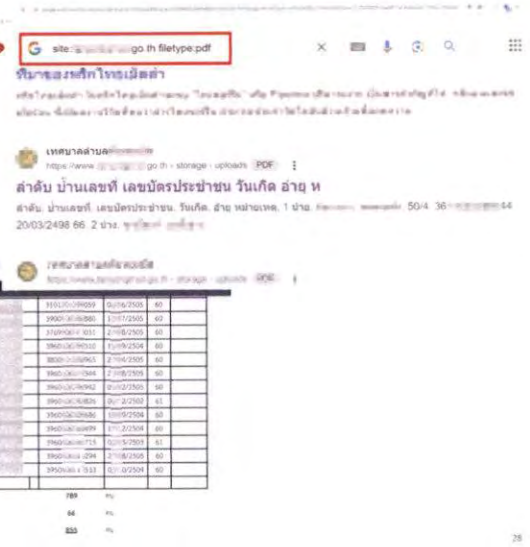
ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

DATA LEAK





site: .go.th filetype:pdf หรือ xlsx



NCSA สกมช. ThaiCERT By NCSA Thailand

ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

HACKED WEBSITE (DEFACEMENT)

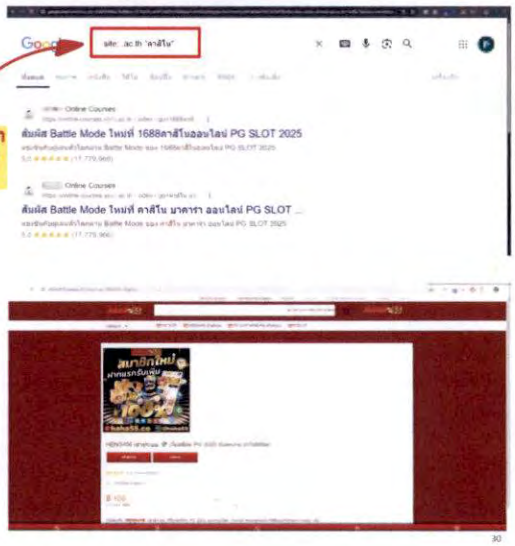


NCSA สกมช. ThaiCERT By NCSA Thailand

ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

HACKED WEBSITE (GAMBLING)

site: .go.th หรือ .ac.th "คาสิโน" slot บาคาร่า sbobet เป็นต้น





ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

SECURITY MISCONFIGURATION

DIRECTORY LISTING

Index of /Web2024

Name	Last modified	Size	Description
Parent Directory		-	
Executive_office/	2023-03-11 10:57	-	
Facebook Messenger C..>	2023-06-28 16:59	1.2K	
Facebook Messenger C..>	2022-07-18 10:29	1.1K	
Logo.png	2020-06-23 09:59	93K	
PM25.php	2024-03-12 09:17	10K	
UpRightSchool/	2022-06-14 13:50	-	
_groups/	2022-06-14 13:50	-	
about.html	2020-06-19 11:07	23K	

Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2016/	2020-11-07 11:08	-	
2017/	2020-11-07 11:08	-	
2018/	2022-10-24 14:00	-	
2019/	2020-12-30 14:39	-	
2020/	2020-12-01 00:05	-	
2021/	2021-12-01 07:00	-	
2022/	2022-12-01 07:01	-	
2023/	2023-12-01 00:07	-	
2024/	2024-12-01 00:04	-	

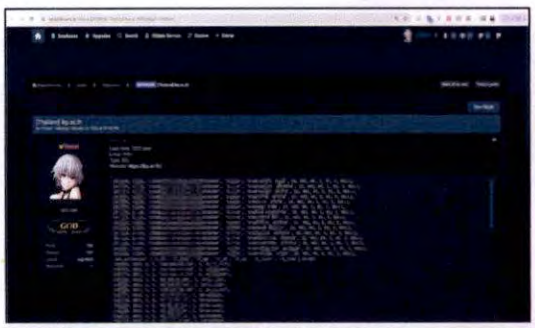
NCSA สกมช. ThaiCERT By NCSA Thailand





NCSA สกมช. ThaiCERT By NCSA Thailand

ประกาศขายข้อมูลหน่วยงานการศึกษาจากเว็บไซต์ BreachForums เป็นข้อมูลของโรงเรียนแห่งหนึ่ง







โรงเรียน ใช้ Username และ Password
ด้วยเบอร์ส่วนตัว ระบบจึงเกิดการโดน แฮก มีข้อมูลนักเรียน/ผู้ปกครอง รั่วไหล

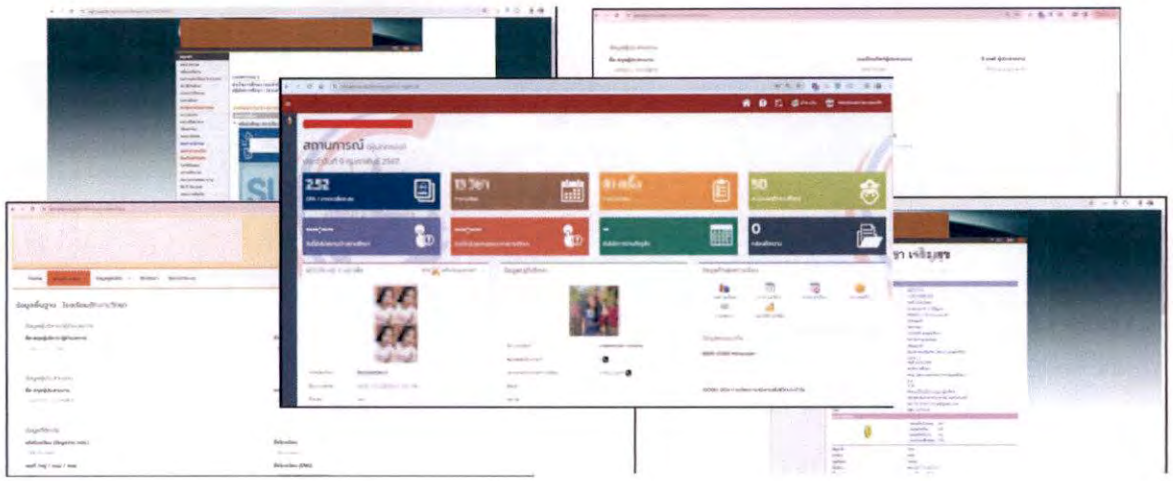






เมื่อวันที่ 10 กุมภาพันธ์ ได้รับแจ้งเหตุภัยคุกคามทางไซเบอร์
พบการเข้าถึงชื่อผู้ใช้งานและรหัสผ่าน ของหน่วยงานการศึกษา
โดย ทางหน่วยงานได้เลือกใช้ชื่อผู้ใช้งานและรหัสผ่านเป็นเบอร์โทรศัพท์ส่วนตัว
ซึ่งเป็นความเสี่ยง ทำให้สามารถโดนเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลสำคัญ
โดยไม่ได้รับอนุญาต

ข้อมูลหน่วยงานการศึกษา รั่วไหล



ประเทศไทยได้เผชิญกับหลายเหตุการณ์ที่เป็นภัยคุกคามทางไซเบอร์ ซึ่งส่งผลกระทบ ต่อความมั่นคงในด้านต่างๆ ต่อไปนี้เป็นตัวอย่างเหตุการณ์สำคัญที่เคยเกิดขึ้น:







1. การโจมตีระบบสาธารณสุข
การโจมตีโรงพยาบาลบางแห่งในประเทศไทย: มีกรณีที่โรงพยาบาลในประเทศไทยถูกโจมตีด้วยแรนซัมแวร์ (Ransomware) ทำให้ระบบข้อมูลผู้ป่วยถูกเข้ารหัสและไม่สามารถเข้าถึงได้ โดยผู้โจมตีเรียกร้องค่าไถ่เพื่อคืนข้อมูล ทำให้การให้บริการทางการแพทย์หยุดชะงัก และสร้างความตื่นตระหนกให้กับผู้ป่วยและบุคลากรทางการแพทย์

2. การโจมตีระบบการเงิน
การโจมตีธนาคารไทย: ในปี 2016 มีกรณีการโจมตีระบบเอทีเอ็มในประเทศไทย โดยการใช้มัลแวร์ทำให้เครื่องเอทีเอ็มหลายร้อยเครื่องสามารถจ่ายเงินสดออกมาโดยไม่ต้องใช้บัตร ทำให้เกิดความเสียหายหลายล้านบาทและส่งผลกระทบต่อความเชื่อมั่นในระบบการเงิน

3. การแฮกข้อมูลส่วนบุคคล
การแฮกข้อมูลจากหน่วยงานรัฐ: มีกรณีที่ข้อมูลส่วนบุคคลของประชาชนถูกแฮกจากฐานข้อมูลของหน่วยงานรัฐ ทำให้ข้อมูลสำคัญ เช่น หมายเลขบัตรประชาชน ที่อยู่ และเบอร์โทรศัพท์ถูกเผยแพร่สู่สาธารณะ ซึ่งสามารถนำไปใช้ในการหลอกลวงหรือการโจมตีทางไซเบอร์ต่อบุคคลเป้าหมาย

ประเทศไทยได้เผชิญกับหลายเหตุการณ์ที่เป็นภัยคุกคามทางไซเบอร์ ซึ่งส่งผลกระทบต่อความมั่นคงในด้านต่างๆ ต่อไปนี้เป็นตัวอย่างเหตุการณ์สำคัญที่เคยเกิดขึ้น:



4. การแพร่ข่าวสารเท็จและการโจมตีทางการเมือง
การแพร่ข่าวสารเท็จ (Fake News): การแพร่ข่าวสารเท็จเกี่ยวกับการเมืองและเหตุการณ์สำคัญของประเทศผ่านสื่อสังคมออนไลน์ ทำให้เกิดความขัดแย้งและความวุ่นวายในสังคม ตัวอย่างเช่น ข้อมูลที่บิดเบือนเกี่ยวกับการเลือกตั้งหรือสถานการณ์ฉุกเฉินต่างๆ ที่ทำให้ประชาชนเข้าใจผิดและตื่นตระหนก

5. การโจมตีโครงสร้างพื้นฐานสำคัญ
การโจมตีระบบโทรคมนาคม: มีกรณีการโจมตีระบบโทรคมนาคมและอินเทอร์เน็ตในประเทศไทย ทำให้การสื่อสารหยุดชะงักเป็นบางช่วงเวลา ส่งผลกระทบต่อการทำงานขององค์กรธุรกิจและการดำเนินชีวิตของประชาชน
กรณีศึกษา
กรณีการโจมตีเว็บไซต์หน่วยงานรัฐ: มีกรณีที่เว็บไซต์ของหน่วยงานรัฐและองค์กรสำคัญถูกโจมตีด้วยวิธีการ DDoS (Distributed Denial of Service) ทำให้เว็บไซต์ไม่สามารถให้บริการได้ชั่วคราว ซึ่งส่งผลกระทบต่อการให้บริการข้อมูลและการติดต่อกับประชาชน

ความเข้าใจที่ผิด ต่อ Cyber Security

1. เข้าใจผิดว่าเป็นเรื่องของฝ่ายไอทีเท่านั้น ไม่เกี่ยวกับฝ่ายอื่น
2. เข้าใจผิดว่าภาครัฐจัดการให้ทั้งหมด
3. เข้าใจผิดว่าเป็นเรื่องของความปลอดภัยของระบบเครือข่าย (Network) อย่างเดียว โดยไม่เกี่ยวข้องกับแอปพลิเคชั่นของผู้ใช้งาน (User Application)
4. เข้าใจผิดว่ามีพาสเวิร์ดสำหรับการล็อกอินก็ปลอดภัยพอแล้ว
5. เข้าใจผิดว่าเป็นเรื่องของการถูกโจมตีจากแฮ็คเกอร์ภายนอกเท่านั้น
6. เข้าใจผิดว่าเป็นเรื่องไกลตัว ยังไม่ต้องรีบ
7. เข้าใจผิดว่าเป็นการทำโครงการครั้งเดียวแล้วเลิก ไม่ต้องหมั่นซ้อม ไม่พัฒนาต่อเนื่อง

จากการวิเคราะห์สาเหตุกรณีหน่วยงานรัฐและเอกชน ในประเทศไทยถูกโจมตีของ ThaiCERT ในปี 2567



ระบบของภาครัฐและเอกชนจำนวนมากทั้งที่จ้างพัฒนาและพัฒนาเองมีความไม่ปลอดภัยและการเขียนโปรแกรมที่ไม่ปลอดภัย



การใช้ซอฟแวร์ที่มีช่องโหว่หรือล้าสมัย



การที่ผู้ดูและระบบใช้ USERNAME และ PASSWORD เดิมที่ติดมากับอุปกรณ์หรือซอฟต์แวร์


ขาดระบบป้องกันและเฝ้าระวังการถูกโจมตี


การป้องกันการรั่วไหลของข้อมูลจากพนักงานภายใน (Insider Threat)


การใช้งานการเข้ารหัสที่ไม่ปลอดภัยหรือไม่มีการเข้ารหัส


หน่วยงานขาดบุคลากรที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์


การขาดบุคลากรด้านการคุ้มครองข้อมูลส่วนบุคคล (DPO)


การจัดการสิทธิ์ของพนักงานที่ออกจากงาน (Offboarding)


ขาดมาตรการกำกับดูแลและการป้องกันการเข้าถึงระบบจากบุคคลภายนอก

คำแนะนำในการป้องกันองค์กรของ สกมช. ในปี 2568

01 อัปเดตซอฟต์แวร์และระบบอยู่เสมอและ หลีกเลี่ยงการดาวน์โหลดและติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ (Software Updates & Patching)

02 สำรองข้อมูลอย่างปลอดภัยและเป็นประจำ (Data Backup and Disaster Recovery)

03 ยกระดับความปลอดภัยด้วยการยืนยันตัวตน 2 ขั้นตอน (2FA)

04 แต่งตั้งและเสริมบทบาทของ DPO และ CISO

05 จัดตั้ง SOC ตลอดจนตรวจสอบและวิเคราะห์กิจกรรมในเครือข่ายอย่างสม่ำเสมอ

06 จัดการความเสี่ยงจากการใช้ AI อย่างมีจริยธรรม (AI Risk Management)

07 ส่งเสริมการใช้รหัสผ่านที่ปลอดภัยและนโยบาย Zero-Trust

08 มีการกำกับดูและคัดเลือกบริษัทที่มีประสบการณ์และมาตรฐานความปลอดภัยและหลีกเลี่ยงการใช้ข้อมูลจริงในขั้นตอนการพัฒนา

09 ป้องกัน Insider Threat และจัดการ Offboarding อย่างปลอดภัย

10 ให้ความรู้แก่พนักงานและปรับปรุงความรู้ด้านความปลอดภัยไซเบอร์

40

การใช้ 2FA เพิ่มชั้นความปลอดภัย

2FA คืออะไร? ทำไมช่วยชีวิตออนไลน์คุณได้

2FA หรือ Two-Factor Authentication เป็นการ ยืนยันตัวตน แบบ 2 ชั้น เพื่อป้องกันรหัสผ่านหลุด ไม่ให้สูญเสียข้อมูลส่วนบุคคล และป้องกันการโดนสวมรอย

ทำงานยังไง? : หลังจากใส่รหัสผ่าน ระบบจะขอ "หลักฐานยืนยันตัวตนอีกขั้น" เช่น

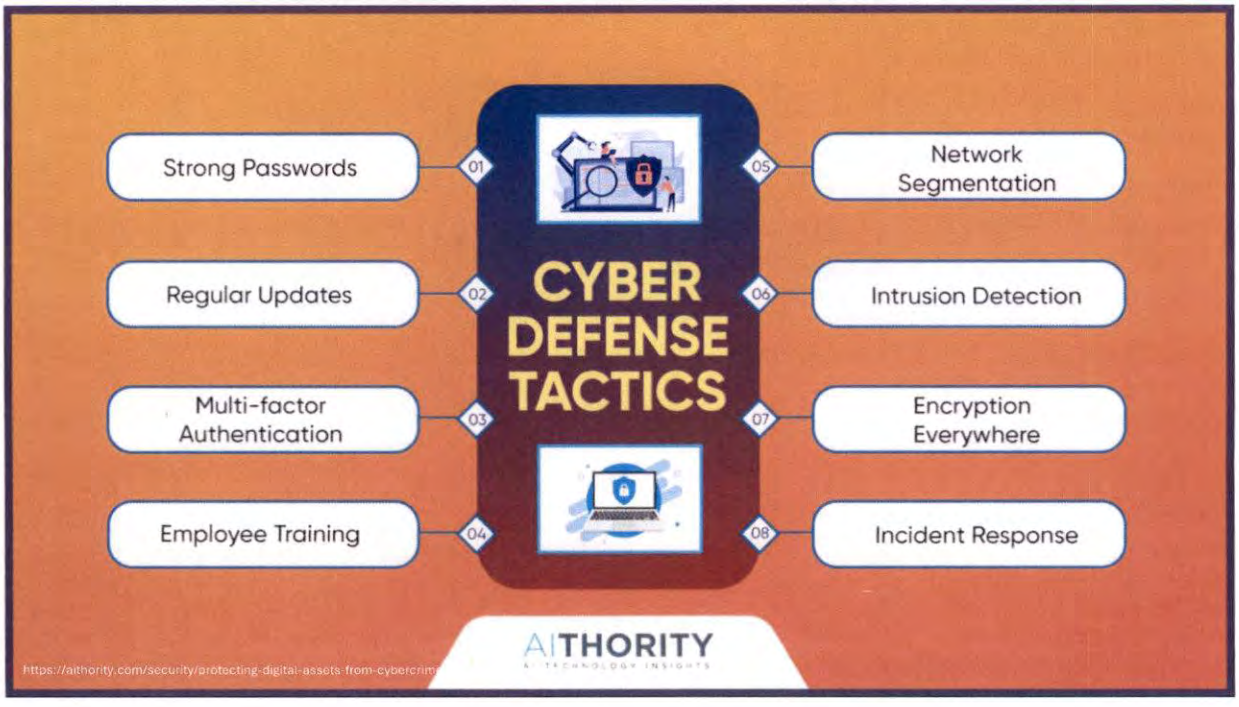
- รหัสผ่านแบบใช้ครั้งเดียว (OTP จากแอป)
- แจ้งเตือนผ่านแอป เช่น Google Authenticator, Microsoft Authenticator
- รหัส OTP ที่ส่งมาทาง SMS/Email
- ลายนิ้วมือ / สแกนใบหน้า

ตั้งไว้ปลอดภัยกว่านะทุกคน

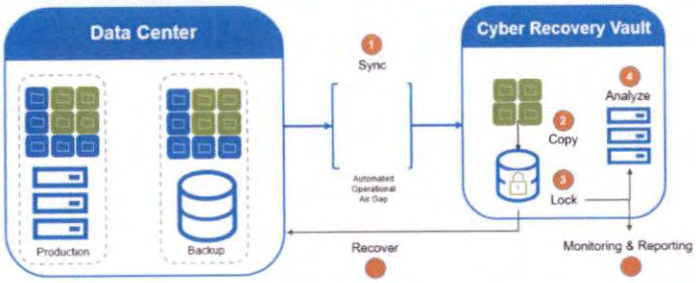
ปัจจัยที่นิยมใช้มี 3 ประเภท:
1.สิ่งที่คุณรู้ (Something you know): เช่น รหัสผ่าน, PIN
2.สิ่งที่คุณมี (Something you have): เช่น โทรศัพท์มือถือ, Token, แอปพลิเคชันสำหรับยืนยันตัวตน (เช่น Google Authenticator)
3.สิ่งที่คุณเป็น (Something you are): เช่น ลายนิ้วมือ, สแกนใบหน้า, ลายนัยน์ตา

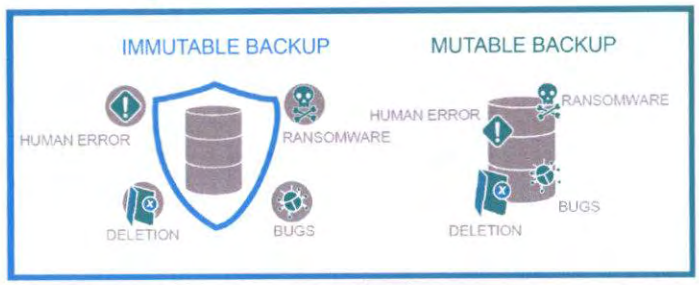
ประโยชน์ของ 2FA: ป้องกันการเข้าถึงบัญชีโดยไม่ได้รับอนุญาต แม้รหัสผ่านจะรั่วไหลลดความเสี่ยงจากการถูกโจมตีแบบ phishing หรือ brute-force

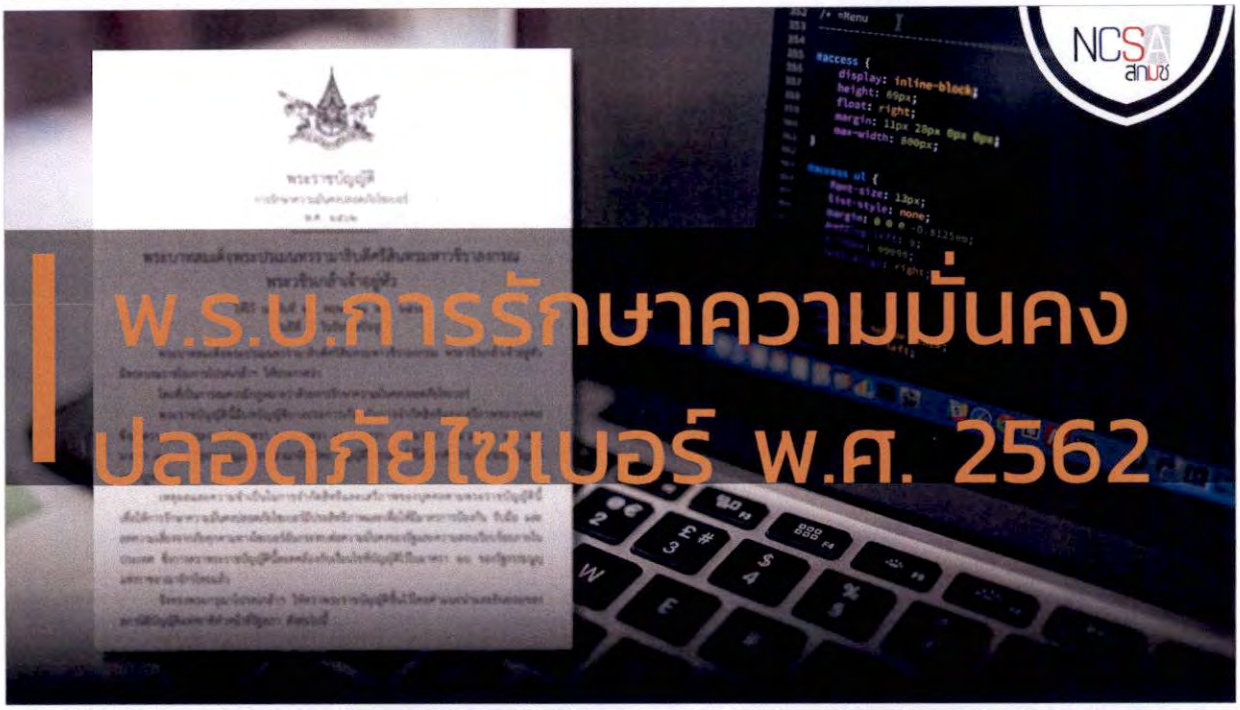
41



Air gap backup/immutable backup







พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

- ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562
- มีผลบังคับใช้ ตั้งแต่วันที่ 28 พฤษภาคม 2562 เป็นต้นไป



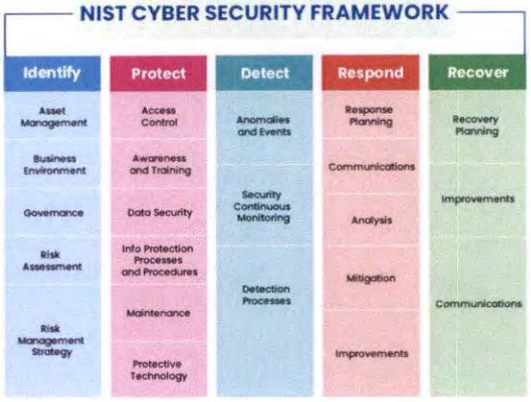
อ้างอิงจาก มาตรา 13 (6) ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หน่วยงาน CII vs หน่วยงานของรัฐ ตาม พ.ร.บ.ไซเบอร์ 62

มาตรา	หน่วยงาน CII	หน่วยงานของรัฐ*
43 ดำเนินการตามนโยบายและแผนฯ	/	/
44 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ	/	/
45 มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน	/	/
46 แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการไปยังสำนักงาน	/	/
52 แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์	/	
53 รับการตรวจสอบมาตรฐานขั้นต่ำจากหน่วยงานควบคุมหรือกำกับดูแล	/	
54 จัดให้มีการประเมินความเสี่ยงฯ รวมทั้งต้องจัดให้มีการตรวจสอบฯ	/	
56 มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์	/	
57 รายงานเหตุภัยคุกคามทางไซเบอร์ และปฏิบัติตามส่วนที่ 4	/	
58 ตรวจสอบ ประเมิน ป้องกัน รับมือ ลดความเสี่ยง และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว	/	/

*หมายถึง หน่วยงานของรัฐที่มิได้เป็นหน่วยงาน CII

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	**CSF 2.0 Category**	**CSF 2.0 Category Identifier**
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	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)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
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



เริ่มต้นยังไง?

Checklist สำหรับหน่วยงานในการรักษาความมั่นคงปลอดภัยไซเบอร์ ตาม พ.ร.บ.ไซเบอร์ 2562

หัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
ประมวลแนวทางปฏิบัติ			
องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)		•	•
องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)	•	•	•
องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	•	•	•
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์			
๑. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)			
๑.๑ การจัดการทรัพย์สิน (Asset Management)	•	•	•
๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	•	•	•
๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)			•
๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)			•
๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)			
๒.๑ การควบคุมการเข้าถึง (Access Control)	•	•	•
๒.๒ การทำให้ระบบมีความเข้มแข็ง (System Hardening)	•	•	•
๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)		•	•
๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)		•	•
๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	•	•	•
๒.๖ การแบ่งปันข้อมูล (Information Sharing)			•
๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)			
๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	•	•	•
๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)			
๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	•	•	•
๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	•	•	•
๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	•	•	•
๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)			
๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)			•

แหล่งที่มา : ประกาศ กกม. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ.2566



ร่วมสร้างการตระหนักรู้ เสริมเกราะป้องกัน
สร้างภูมิคุ้มกันภัยไซเบอร์ไปกับ สกมช.

NCSA สกมช











Download Infographic
เพื่อเผยแพร่ประชาสัมพันธ์

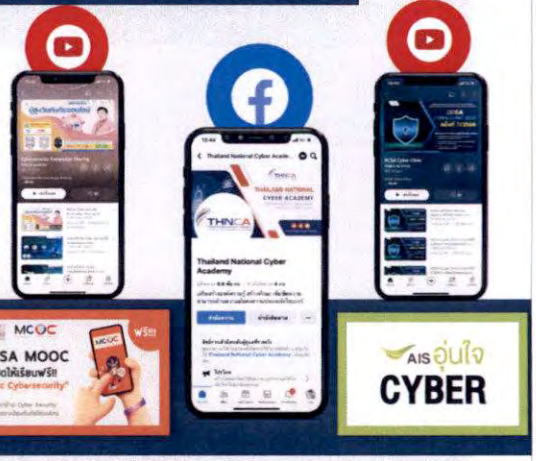
National Cyber Security Agency

NCSA สกมช

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ขอเสนอ คลังความรู้ด้านไซเบอร์

แหล่งเรียนรู้ไซเบอร์สำหรับประชาชนทุกช่วงวัยที่คุณห้ามพลาด สำหรับการ Upskill และ Reskillเพื่อสร้างการตระหนักรู้และมีภูมิคุ้มกันภัยไซเบอร์ สามารถเข้าไปศึกษาได้ฟรี พร้อมรับใบ Certification ไม่เสียค่าใช้จ่าย



โดยมีชั่วโมงการเรียนรู้กว่า 1,000 ชั่วโมง


FREE
เรียนฟรี! ได้ใบ CERTIFICATE!
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
CYBER KNOWLEDGE CENTER
NCSA สกมช
THNCA
"คลังความรู้ด้านไซเบอร์"
SCAN ME
LINK : HTTPS://LINKTR.EE/THNCA
สแกนได้แล้ววันนี้
เรียนรู้ได้อย่างไร้ขีดจำกัด
สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ส่งเสริมสังคมการเรียนรู้และเผยแพร่คลังความรู้ด้านไซเบอร์
เพื่อพัฒนาทักษะและการเรียนรู้ได้อย่างไร้ขีดจำกัด เข้าใจถึงความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์
CYBERSECURITY AWARENESS
CYBERSECURITY KNOWLEDGE SHARING
NCSA MOOC CYBER-LEARNING
ลุ่นใจไซเบอร์ AIS
สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โทรศัพท์ 0-2502-7831 I อีเมล : academic@ncsa.or.th


รับฟังข่าวสารภัยคุกคามทางไซเบอร์
ได้ก่อนใครผ่านทางไลน์โอเพ่นแชท
SCAN NOW
เข้ารหัสเลย 4loTus


Q&A


Contact us
National Cyber Security Agency - NCSA
NCSA Thailand
Line ID : NCSA Thailand
E-Mail: saraban@ncsa.or.th
02-142-6885
shorturl.at/hkAC2
สำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
NCSA
สกมช
NCSA Thailand
facebook

การประชุมสัมมนาแลกเปลี่ยนเรียนรู้ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)



นายโอภาส ถาวร
รองอธิบดีกรมทรัพยากรน้ำ
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO)

Department of Water Resources

www.dwr.go.th 27 พฤษภาคม 2568

CONTENTS

1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพยากรน้ำ (Current status)

- 1.1 ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. 2568
- 1.2 ผลการติดตั้ง Endpoint Detection and Response (EDR)
- 1.3 ผลการประเมินระดับการเตรียมพร้อมและการปรับตัว (Cyber Resilience Assessment)
- 1.4 การเชื่อมต่อแพลตฟอร์ม Malware Information Sharing Platform หรือ MISP
- 1.5 การตรวจสอบและประเมินช่องโหว่ (Vulnerability Assessment) และทำการทดสอบเจาะระบบ (Penetration Testing)

2 ปัญหาและอุปสรรค (Pain Points)

- 2.1 ขาดบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์
- 2.2 งบประมาณโครงการด้านความมั่นคงปลอดภัยไซเบอร์ไม่ได้รับการจัดสรรอย่างต่อเนื่อง
- 2.3 ความตระหนักรู้ของบุคลากรภายในองค์กร เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์
- 2.4 ระบบ IT ที่เก่าและมีความล้าสมัย
- 2.5 พัฒนาการและความหลากหลายของภัยคุกคาม

1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพยากรน้ำ (CURRENT STATUS)

1.1 ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. 2568

ส่วนที่ 1 ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
2) การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
3) แผนการรับมือภัยคุกคามทางไซเบอร์





ส่วนที่ 2 กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิต ร่างกายของบุคคล (Identify)
2) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)
3) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
4) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
5) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

หมายเหตุ:

คณะกรรมการบริหารเทคโนโลยีสารสนเทศระดับสูงของกรมทรัพยากรน้ำ ได้มีมติเห็นชอบ (ร่าง) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. 2568 ในวันจันทร์ที่ 21 เมษายน 2568 และอธิบดีกรมทรัพยากรน้ำได้ลงนามในประกาศดังกล่าวแล้ว ในวันที่ 14 พฤษภาคม 2568

1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพยากรน้ำ (CURRENT STATUS)

1.2 ผลการดำเนินงานของ ENDPOINT DETECTION AND RESPONSE (EDR)

IBM ReaQta (ดำเนินการโดยกรมทรัพยากรน้ำ)

มีการติดตั้ง EDR ยี่ห้อ IBM ReaQta จำนวน 450 Endpoints

โดยแบ่งเป็น กลุ่ม Server จำนวน 22 Endpoints และกลุ่ม Client จำนวน 428 Endpoints

ผลการดำเนินการของระบบ EDR ตั้งแต่เดือนเมษายน 2567 – เมษายน 2568 มีการตรวจจับสิ่งที่อาจจะก่อให้เกิดภัยคุกคามต่อระบบ จำนวน 49,511 รายการ โดยแบ่งเป็น

- ระดับภัยคุกคามเริ่มต้น จำนวน 45,362 รายการ ซึ่งไม่เป็นภัยต่อองค์กร
- และภัยคุกคามระดับที่เป็นอันตรายต่อระบบภายในองค์กร (Malicious) จำนวน 4,149 รายการ โดยระบบฯ ได้ดำเนินการ Kill Process กระบวนการที่คาดว่าเป็นภัยคุกคาม และลบไฟล์ที่ต้องสงสัยตาม Path ที่ระบบฯ ตรวจจับได้



REAQTA
an IBM Company

SentinelOne (ได้รับความร่วมมือจาก สกมช.)

มีการติดตั้ง EDR ยี่ห้อ SentinelOne จำนวน 200 Endpoints โดยประกอบไปด้วยเครื่อง PC ทั้งส่วนกลางและส่วนภูมิภาค

โดยกรมทรัพยากรน้ำมีแผนติดตั้งให้ได้จำนวน 300 Endpoints ภายในสิ้นเดือนพฤษภาคมนี้

ปัจจุบันตรวจพบสิ่งที่คาดว่าเป็นภัยคุกคาม จำนวนกว่า 200 รายการ

กรมทรัพยากรน้ำ ได้มีการประสานงานและตรวจสอบเคสที่เกิดขึ้นกับทีมงาน SOC อย่างสม่ำเสมอ ว่าเป็นภัยคุกคามจริง หรือเป็นการใช้งานปกติของหน่วยงาน (False Positive)

หากเป็นภัยคุกคามจริง กรมทรัพยากรน้ำได้ดำเนินการป้องกันและแก้ไขตามคำแนะนำของ สกมช.



SentinelOne

1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพยากรน้ำ (CURRENT STATUS)

1.3 ผลการประเมินระดับการเตรียมพร้อมและการปรับตัว (CYBER RESILIENCE ASSESSMENT)

ส่วนที่ 1 การประเมินความเสี่ยงตั้งต้นด้านไซเบอร์ (Inherent Risk Assessment – IRA)

ปัจจัยเสี่ยง	ระดับความเสี่ยง			ผลรวมการประเมินแต่ละปัจจัยเสี่ยง
	ต่ำ	ปานกลาง	สูง	
IR 1: เทคโนโลยีและการเชื่อมต่อ	7	3	9	สูง
IR 2: ช่องทางการให้บริการ	0	3	3	ปานกลาง
IR 3: ลักษณะผลิตภัณฑ์และการให้บริการ	0	0	2	สูง
IR 4: ลักษณะเฉพาะขององค์กร	0	3	1	ปานกลาง
IR 5: ประวัติการถูกคุกคามทางไซเบอร์	0	2	0	ปานกลาง

ผลรวมระดับความเสี่ยงตั้งต้น

ปานกลาง

มาตรการควบคุมที่พึงมี

หน่วยงานควรปฏิบัติได้ตามมาตรการที่กำหนดไว้สำหรับ Maturity Level ระดับ Baseline และระดับ Intermediate ที่กำหนดทุกข้อ

1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพยากรน้ำ (CURRENT STATUS)

1.3 ผลการประเมินระดับการเตรียมพร้อมและการปรับตัว (CYBER RESILIENCE ASSESSMENT)

ส่วนที่ 2 การประเมินระดับการจัดการภัยคุกคามทางไซเบอร์ (Maturity Assessment – MA)

การบริหารจัดการความเสี่ยง	รวม	ผลการประเมินการบริหารจัดการความเสี่ยง				
		Pass	Not Pass	Partially Pass	Alternative Control	Not Applicable
D1: การกำกับดูแล (Governance)	39	10	4	12	0	13
Baseline	13	8	1	4	0	0
Intermediate	13	2	3	8	0	0
Advanced	13	0	0	0	0	13
D2: การระบุความเสี่ยง (Identification)	17	5	6	3	0	3
Baseline	12	5	5	2	0	0
Intermediate	2	0	1	1	0	0
Advanced	3	0	0	0	0	3

การบริหารจัดการความเสี่ยง	รวม	ผลการประเมินการบริหารจัดการความเสี่ยง				
		Pass	Not Pass	Partially Pass	Alternative Control	Not Applicable
D3: การป้องกันความเสี่ยง (Protection)	78	30	23	12	1	12
Baseline	55	27	18	9	1	0
Intermediate	11	3	5	3	0	0
Advanced	12	0	0	0	0	12
D4: การตรวจจับ (Detection)	38	14	6	6	0	12
Baseline	16	11	1	4	0	0
Intermediate	10	3	5	2	0	0
Advanced	12	0	0	0	0	12

การบริหารจัดการความเสี่ยง	รวม	ผลการประเมินการบริหารจัดการความเสี่ยง				
		Pass	Not Pass	Partially Pass	Alternative Control	Not Applicable
D5: การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ (Response and Recovery)	15	3	5	5	0	2
Baseline	10	2	4	4	0	0
Intermediate	3	1	1	1	0	0
Advanced	2	0	0	0	0	2
D6: การบริหารความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management)	19	7	7	2	0	3
Baseline	13	7	4	2	0	0
Intermediate	3	0	3	0	0	0
Advanced	3	0	0	0	0	3

Pass = ผ่าน/ดำเนินการแล้ว
Not Pass = ไม่ผ่าน/ไม่ได้ดำเนินการ
Partially Pass = ผ่านบางส่วน/ดำเนินการบางส่วน
Alternative Control = ไม่มีการดำเนินการตามที่มาตรการกำหนด แต่มีอย่างอื่นที่สามารถทดแทนได้
Not Applicable = ไม่เกี่ยวข้อง หรือ ไม่จำเป็นต้องประเมินในส่วนนี้

ผลสรุป
(จากทั้งหมด 206 ข้อ)

Pass : 69
Not Pass : 51
Partially Pass : 40
Alternative Control : 1
Not Applicable : 45

1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพยากรน้ำ

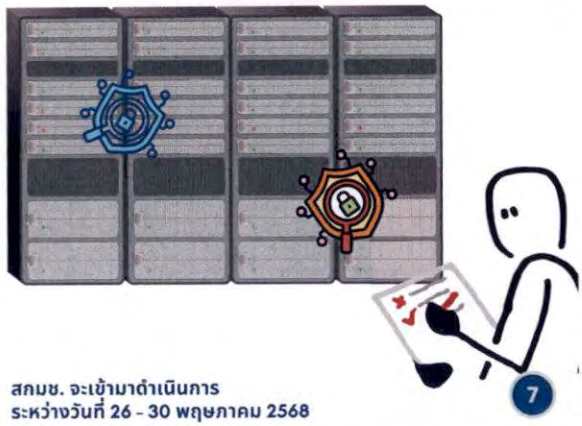
การดำเนินงานภายใต้ความร่วมมือระหว่างกรมทรัพยากรน้ำ และ สกมช.

1.4 การเชื่อมต่อแพลตฟอร์มการแบ่งปันข้อมูลมัลแวร์ (MALWARE INFORMATION SHARING PLATFORM) หรือ MISP

MISP
Threat Sharing



1.5 การสแกนหาช่องโหว่ (VULNERABILITY ASSESSMENT) และทดสอบเจาะระบบ (PENETRATION TESTING)



สกมช. จะเข้ามาดำเนินการ
ระหว่างวันที่ 26 - 30 พฤษภาคม 2568

2 ปัญหา อุปสรรคและผลตอบรับที่หน่วยงานพบเจอ เมื่อดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (PAIN POINTS)

- **2.1** ขาดบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์
- **2.2** งบประมาณโครงการด้านความมั่นคงปลอดภัยไซเบอร์ ไม่ได้รับการจัดสรรอย่างต่อเนื่อง
- **2.3** ความตระหนักรู้ของบุคลากรภายในองค์กร เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์
- **2.4** ระบบ IT ที่เก่าและมีความล้าสมัย
- **2.5** พัฒนาการและความหลากหลายของภัยคุกคาม