การประเมินและการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ [Risk Assessment and Risk Treatment (Threat & Vulner.) of Cybersecurity Act.]

ผู้พิจารณาประเมิน : นายพรชัย คำจันทร์ลา
ผู้บันทึก : นางพรรณี วรธรรม (Lead Implementer)
วันที่ทำการประชุมความเสี่ยงพร้อมบันทึก : 17 มี.ค. 69
สถานที่ : ห้องประชุมตึกส่งเสริม
ที่อยู่ : 57 หมู่ 12 ต.โนนค้อ อ.โนนคูณ จ.ศรีสะเกษ
ระบบบริการที่สำคัญ : All critical application

มาตรการควบคุมไซเบอร์ขั้นต่ำ	
ผลการประเมินความเสี่ยง (เฉลี่ย) โดยรวมขององค์กร (16 Clusters, 160 Risk Id.)	9.4

	Risk Score
แดง (สูง) = 17 เอกสาร เป็นอย่างน้อย	7.0 - 25
เหลือง (ปานกลาง) = 13 เอกสาร เป็นอย่างน้อย	5.1- 6.9
เขียว (ต่ำ) = 10 เอกสาร เป็นอย่างน้อย	1 - 5.0

PART 1 : RISK ASSESSMENT — Risk Analysis | PART 2 : RISK TREATMENT | PART 3 : PROGRESS

No.	หมวดหมู่ความเสี่ยง (Risk Cluster)	ระบุความเสี่ยงด้านไซเบอร์และช่องโหว่ ต่างๆ (Risk Identification): ภัยคุกคาม (Threat)	ช่องโหว่ (Vulner.)	มาตรการควบคุมในปัจจุบัน	มีผลกระทบต่อ: C	I	A	มีผลต่อความรุนแรงแต่ละด้าน: B/F	S	R	I	L	O	A: โอกาสเกิด (Likelihood)	B: ความรุนแรง (Impact)	C = A*B: ระดับความเสี่ยง (Risk Level)	เจ้าของความเสี่ยง (Risk Owner)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk Level) -ของแต่ละ Cluster	ตัวเลือกการตอบสนอง (Risk Treatment)	No.	แผนจัดการความเสี่ยง (Risk Treatment Plan)		คาดว่าดำเนินการแล้วเสร็จ (Expected finish date)	สถานะความคืบหน้า (Progress Status)	หมายเหตุ
	กรอบมาตรฐาน																								
1	การโจมตีด้วยมัลแวร์ (Malware Attacks)	1. มีการดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ ซึ่งอาจแฝงด้วยมัลแวร์	1. ไม่มีระบบหรือมาตรการควบคุมการดาวน์โหลดและติดตั้งซอฟต์แวร์ในองค์กร	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	3	4	12	CSMR	13.6	Mitigate Risk	1	1.1 > ติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์	ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) และ Antimalware ในทุกอุปกรณ์ที่เชื่อมต่อระบบองค์กร	ภายใน 10 ก.ย. 70	70%	
		2. มีการติดมัลแวร์ที่มาจากการใช้อุปกรณ์ USB Storage หรือสื่อเก็บข้อมูลภายนอก	2. ไม่มีการติดตั้งหรืออัปเดตโปรแกรมป้องกันไวรัสเมื่อใช้อุปกรณ์ USB Storage	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	2	2.1 > ควบคุมการใช้งาน USB และอุปกรณ์พกพา	ออกนโยบาย BYOD (Bring Your Own Device) พร้อมกำหนดข้อบังคับในการใช้งานอุปกรณ์ส่วนตัว	ภายใน 10 ก.ย. 70	80%	
		3. ไฟล์แนบในอีเมลมีฟิชชิงและแฝงด้วยมัลแวร์	3. ขาดระบบหรือมาตรการหรือนโยบายการควบคุมการใช้งาน อีเมลที่มีไฟล์แนบ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	3	3.1 > การให้ความรู้และฝึกอบรมพนักงาน	จัดอบรมเกี่ยวกับการหลีกเลี่ยงการดาวน์โหลดไฟล์หรือเข้าเว็บไซต์ที่ไม่น่าเชื่อถือ	ภายใน 10 ก.ย. 70	70%	
		4. การติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ที่ฝังด้วยมัลแวร์	4. พนักงานขาดความรู้ในการติดตั้งไฟล์หรือเว็บไซต์ที่มีความเสี่ยงไซเบอร์	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	x	-	4	5	20	CSMR		Mitigate Risk	4	4.1 > สร้างระบบสำรองข้อมูล (Backup)	กำหนดการสำรองข้อมูลอัตโนมัติเป็นระยะ ๆ	ภายใน 10 ก.ย. 70	80%	
		5. พนักงานเข้าถึงโฆษณาออนไลน์ (Malvertising) ตามเว็บต่างๆ ที่พาไปยังเว็บไซต์ที่มีมัลแวร์	5. ไม่มีระบบกรองเว็บไซต์ ที่ป้องกันมัลแวร์ และอัพเดทเป็นประจำ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	4	4	16	CSMR		Mitigate Risk	5	5.1 > ใช้เครื่องมือความปลอดภัยแบบครบวงจร (Security Suites)	ติดตั้งแพลตฟอร์ม SIEM (Security Information and Event Management) เพื่อตรวจสอบกิจกรรมที่น่าสงสัย	ภายใน 10 ก.ย. 70	80%	
2	การโจมตีด้วยฟิชชิง (Phishing Attacks)	1. การรับอีเมลที่มีฟิชชิงหลอกให้ผู้ใช้กรอกข้อมูลสำคัญ เช่น รหัสผ่าน หรือข้อมูลทางการเงิน	1. ขาดการฝึกอบรมพนักงาน เช่น พนักงานไม่สามารถแยกแยะอีเมลหรือเว็บไซต์ปลอมได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	4	8	CSMR	8.8	Mitigate Risk	1	1.1 > ให้ความรู้และฝึกอบรมพนักงาน	จัดอบรมพนักงานเกี่ยวกับวิธีการระบุอีเมลและลิงก์ฟิชชิง เช่น การตรวจสอบ URL และท้ายอีเมล	ภายใน 10 ก.ย. 70	77%	
		2. Spear Phishing ที่กำหนดเป้าหมายเจาะจงบุคคลหรือหน่วยงาน หลอกเข้ามาในระบบ	2. ไม่มีระบบตรวจจับอีเมลฟิชชิง เช่น ไม่มีการใช้ตัวกรองอีเมลเพื่อบล็อกอีเมลที่เป็นอันตราย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	4	8	CSMR		Mitigate Risk	2	2.1 > ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA)	เปิดใช้งาน MFA สำหรับทุกบัญชี โดยเฉพาะบัญชีที่เกี่ยวข้องกับข้อมูลสำคัญ	ภายใน 10 ก.ย. 70	80%	
		3. มีการรับส่งลิงก์ที่มีฟิชชิงผ่าน SMS หรือโซเชียลมีเดีย	3. การใช้รหัสผ่านซ้ำหรือไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้ซ้ำในหลายระบบ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	3	4	12	CSMR		Mitigate Risk	3	3.1 > ตรวจสอบและควบคุมการเข้าถึงเว็บไซต์	ใช้ระบบ Web Filtering เพื่อบล็อกการเข้าถึงเว็บไซต์ฟิชชิง	ภายใน 10 ก.ย. 70	88%	
		4. เข้าเว็บไซต์ปลอมที่เลียนแบบหน้าล็อกอินขององค์กรหรือบริการออนไลน์	4. ขาดการใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น ระบบไม่มีการยืนยันตัวตนเพิ่มเติมสำหรับการเข้าถึงข้อมูลสำคัญ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	4	8	CSMR		Mitigate Risk	4	4.1 > ใช้เครื่องมือ SIEM (Security Information and Event Management)	ติดตั้งระบบตรวจจับและตอบสนองต่อภัยคุกคามแบบเรียลไทม์	ภายใน 10 ก.ย. 70	33%	
		5. ดูระบบโทรศัพท์ปลอม (Call center) หลอกขอข้อมูลส่วนตัว	5. ไม่มีกระบวนการยืนยันการสื่อสารที่ปลอดภัย เช่น ขาดนโยบายการยืนยันตัวตนของผู้ส่งอีเมลหรือข้อความ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	4	8	CSMR		Mitigate Risk	5	5.1 > นโยบายการรายงานเหตุการณ์ (Incident Reporting)	จัดทำนโยบายสำหรับพนักงานในการรายงานอีเมลหรือกิจกรรมที่น่าสงสัย	ภายใน 10 ก.ย. 70	40%	
3	ภัยคุกคามจากบุคคลภายใน (Insider Threats)	1. การใช้งานข้อมูลโดยใช้อำนาจมิชอบ เช่น พนักงานที่มีสิทธิ์เข้าถึงข้อมูลสำคัญอาจนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต	1. การควบคุมสิทธิ์การเข้าถึงที่ไม่เหมาะสม เช่น พนักงานบางคนได้รับสิทธิ์เข้าถึงข้อมูลมากเกินความจำเป็น	มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	5	5	CSMR	8.8	Continue Monitoring	1					
		2. การรั่วไหลของข้อมูลโดยเจตนา เช่น พนักงานที่ไม่พอใจองค์กรส่งข้อมูลสำคัญให้คู่แข่งหรือบุคคลภายนอก	2. ขาดระบบตรวจสอบพฤติกรรม เช่น ไม่มีการติดตามกิจกรรมที่ผิดปกติในระบบของพนักงาน	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	4	5	20	CSMR		Mitigate Risk	2	2.1 > การฝึกอบรมพนักงาน	ให้ความรู้เกี่ยวกับการป้องกันการรั่วไหลของข้อมูลและผลกระทบของการกระทำโดยมิชอบ	ภายใน 10 ก.ย. 70	33%	
		3. กระทำผิดพลาดโดยไม่ได้ตั้งใจ เช่น การลบข้อมูลสำคัญหรือแชร์ข้อมูลให้บุคคลที่ไม่เกี่ยวข้อง	3. ขาดการฝึกอบรมเกี่ยวกับการปกป้องข้อมูล เช่น พนักงานไม่เข้าใจถึงความสำคัญของการปกป้องข้อมูล	มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	5	5	CSMR		Continue Monitoring	3					
		4. การใช้บัญชีที่ถูกยึดหรือถูกแฮ็ก (inactive users) เช่น บัญชีของพนักงานที่ถูกยึดหรือแฮ็กมีการนำไปใช้ในการกระทำที่ไม่เหมาะสม	4. ไม่มีการจัดการบัญชีผู้ใช้งานที่ออกจากองค์กร เช่น บัญชีของพนักงานที่ลาออกยังคงสามารถเข้าถึงระบบได้	มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	4	4	CSMR		Continue Monitoring	4					
		5. มีการปลอมตัวเป็นบุคคลภายใน เช่น บุคคลภายนอกแฝงตัวเข้ามาในองค์กรผ่านการร่วมมือของพนักงานภายใน	5. ไม่มีการเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลที่สำคัญไม่ได้รับการป้องกัน ทำให้ง่ายต่อการคัดลอกหรือส่งออก	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	2	5	10	CSMR		Mitigate Risk	5	5.1 > สร้างโปรแกรม Insider Threat Program (ITP)	ตั้งทีมเฉพาะกิจเพื่อตรวจสอบและจัดการภัยคุกคามจากบุคคลภายใน	ภายใน 10 ก.ย. 70	66%	
4	การละเมิดข้อมูล (Data Breaches)	1. มีการแฮ็กระบบเพื่อเข้าถึงข้อมูลสำคัญ เช่น ข้อมูลลูกค้า หรือข้อมูลทางการเงิน	1. การขาดการเข้ารหัสข้อมูล (Encryption) เช่น ข้อมูลสำคัญไม่ได้รับการเข้ารหัสทั้งในขณะส่งและจัดเก็บข้อมูล	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	2	4	8	CSMR	11.8	Mitigate Risk	1	1.1 > การเข้ารหัสข้อมูล (Encryption)	ใช้การเข้ารหัสข้อมูลทั้งในระหว่างการส่ง (In Transit) และขณะจัดเก็บ (At Rest)	ภายใน 10 ก.ย. 70	23%	
		2. มีการละเมิดข้อมูลจากการตั้งรหัสผ่านที่อ่อนแอ	2. ระบบที่ไม่ได้อัปเดต (Outdated Systems) เช่น ระบบปฏิบัติการและซอฟต์แวร์ที่ไม่ได้อัปเดตเป็นผลเปิดช่องโหว่ให้ถูกโจมตี	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	3	5	15	CSMR		Mitigate Risk	2	2.1 > กำหนดนโยบายรหัสผ่านที่เข้มงวด	กำหนดให้ใช้รหัสผ่านที่ซับซ้อนและเปลี่ยนรหัสผ่านเป็นระยะ	ภายใน 10 ก.ย. 70	90%	
		3. มีการรั่วไหลของข้อมูลผ่านพนักงาน (โดยเจตนาหรือไม่เจตนา)	3. การตั้งรหัสผ่านที่ไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้รหัสผ่านซ้ำกันในหลายระบบ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	3	5	15	CSMR		Mitigate Risk	3	3.1 > ระบบตรวจสอบและแจ้งเตือนภัยคุกคาม	ติดตั้งระบบ SIEM (Security Information and Event Management) เพื่อตรวจสอบและแจ้งเตือนกิจกรรมที่ผิดปกติ	ภายใน 10 ก.ย. 70	80%	
		4. มีการส่งข้อมูลสำคัญผ่านช่องทางที่ไม่ปลอดภัย เช่น อีเมลที่ไม่มีการเข้ารหัส	4. ขาดระบบตรวจสอบการเข้าถึง (Access Control): ไม่มีการควบคุมสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	3	5	15	CSMR		Mitigate Risk	4	4.1 > ใช้ระบบสำรองข้อมูล (Backup)	กำหนดให้มีการสำรองข้อมูลอัตโนมัติ และเก็บข้อมูลสำรองไว้ในระบบที่แยกออกจากระบบหลัก	ภายใน 10 ก.ย. 70	80%	
		5. มีการโจมตีผ่าน API หรือระบบที่ไม่ได้รับการตรวจสอบความปลอดภัย	5. ขาดการตรวจสอบกิจกรรมในระบบ เช่น ไม่มีการตรวจสอบกิจกรรมที่น่าสงสัยในระบบหรือการแจ้งเตือน	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	2	3	6	CSMR		Mitigate Risk	5	5.1 > การจัดทำแผนรับมือเหตุการณ์ (Incident Response Plan)	สร้างกระบวนการตอบสนองเมื่อเกิดเหตุการณ์ Data Breach	ภายใน 10 ก.ย. 70	80%	