

# GPSC

## Information Security Management Program 2024



# Content

No.	Content	Page
1.	Introduction	3
2.	Information security-related business continuity plans	5-6
3.	Information security vulnerability analysis	8-9
4.	Internal audits of the IT infrastructure and/or information security management systems	11-15
5.	Independent external audit of the IT infrastructure and/or information security management systems	17
6.	Escalation process for employees to report incidents, vulnerabilities or suspicious activities	19-21
7.	Information security awareness training	23-26



# Introduction

In today's fast-evolving digital landscape, the protection of information assets is essential to maintaining business continuity, operational efficiency, and stakeholder trust. Recognizing the increasing complexity of cyber threats and the critical importance of safeguarding data, the company has established a comprehensive Information Security Management Program to guide its approach to information protection, risk mitigation, and regulatory compliance. The Information security management program provides a structured framework for identifying, assessing, and managing information security risks across all business units and functions. It aligns with international standards and best practices, promoting a consistent and proactive security culture throughout the organization. The program emphasizes not only technical controls but also governance, policies, awareness, and the continuous improvement of systems and processes. Through this program, the company aims to ensure the confidentiality, integrity, and availability of its information assets while supporting secure business operations, protecting stakeholder interests, and enabling sustainable digital growth.

# Information security-related business continuity plans

# Information security-related business continuity plans

GPSC has the business continuity plan (BCP) as practical approach in recovery the main operation of GPSC. The plan has included the incident response related to business continuity plan (BCP) of GPSC that covers IT System/Network Failure and cyber attack, the structure of management team associated with the incident, role and relevant department, the process of implementation, and the recovery plan from the incidents.

## Objective

- Define the framework for the organization's business continuity management during a crisis situation.
- Establish the structure of crisis management teams and related working groups, including clearly defined roles and responsibilities for each group.
- Outline the procedures to be followed in response to a crisis event. Specify the actions to be taken when the Business Continuity Plan (BCP) is activated.
- Provide definitions and terminology to ensure a shared and accurate understanding

## Scope

This plan has been established for GPSC to serve as a guideline for action in the event that the BCP is triggered to activate. All personnel within the business unit are expected to adhere to the procedures outlined in this plan, as well as those detailed in the unit-specific BCP. Employees who have been assigned designated roles, whether in the Primary Response Team or the Backup Response Team, are responsible for performing the tasks associated with their roles, as specified in both this plan and the relevant unit's continuity plan. The scenarios that are the key disaster for plan activation constitute production interruption, delivery interruption, office deny, and IT System/ Network failure.

## Business continuity plan (BCP)

GPSC Group	หน้า 1 of 13
Work Instruction	ครั้งที่แก้ไข 02
ชื่อเอกสาร: แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	วันที่ประกาศ 15 ตุลาคม 2567
2567	
หมายเลขเอกสาร: PDV-WI-0030	

 Global Power Synergy Public Company Limited	วิธีปฏิบัติงาน Work Instruction
--	------------------------------------

ข้อมูลเอกสารฉบับล่าสุด					
หมายเลขเอกสาร	PDV-WI-0030	Business Unit (Function)	PSE	Dep/Div.	PDV
ชื่อเอกสาร	แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)			สถานะ	ประกาศใช้
Revision	02	วันที่ประกาศใช้	15 ตุลาคม 2567	จำนวนหน้า	13

# Information security-related business continuity plans

As part of GPSC's Business Continuity Plan, the information security component includes scenario-based planning to address critical threats such as IT system or network failures and cyberattacks. These events are identified as key triggers for activating the continuity plan. In response, the plan outlines detailed, step-by-step procedures to guide the recovery process, ensuring that business operations can be restored efficiently and effectively in the event of a disruption. This approach enhances organizational resilience and preparedness against information security incidents.

สถานการณ์หลัก (Key Scenarios)	สถานการณ์ย่อย (Sub Scenarios)
1. การหยุดชะงักของกระบวนการผลิต (Production interruption)	Confidential
2. การหยุดชะงักของการส่งมอบผลิตภัณฑ์ (Delivery interruption)	
3. ไม่สามารถเข้าปฏิบัติงานในสถานที่ (Office Deny)	
4. ระบบเทคโนโลยีสารสนเทศไม่สามารถใช้งาน (IT System/Network Failure)	4.1 โจมตีทางไซเบอร์ (Cyber Attack)

ลำดับ	แผนปฏิบัติงาน	ผู้รับผิดชอบ
1.	เตรียมความพร้อมคอมพิวเตอร์ - จัดหาเครื่องคอมพิวเตอร์สำหรับพนักงาน และ ติดตั้งระบบ Remote Support และ ระบบ Conference ในคอมพิวเตอร์พนักงาน	Confidential
2.	เตรียมความพร้อมสำหรับการทำงานระยะไกล - ติดตั้งระบบ VPN ในคอมพิวเตอร์พนักงาน	
3.	เฝ้าระวังการโจมตีทางไซเบอร์ผ่านระบบ CSOC โดยผู้ให้บริการ PTT Digital	
4.	เตรียมความพร้อมแก้ไขระบบ Network ด้วยกระบวนการ Incident Management	
5.	เตรียมความพร้อมของ DR-Site และมี DR-Drill ของระบบต่าง ๆ ประจำปี	
6.	เตรียมความพร้อมแผนรับมือการโจมตีทางไซเบอร์ของระบบ IT โดยการทำให้ Cyber Drill ประจำปี	
7.	เตรียมความพร้อมแผนรับมือการโจมตีทางไซเบอร์ของระบบ OT โดยการทำให้ Cyber Drill ประจำปี ร่วมกับตัวแทนของโรงงาน	

# Information security vulnerability analysis



# Information security vulnerability analysis (1/2)

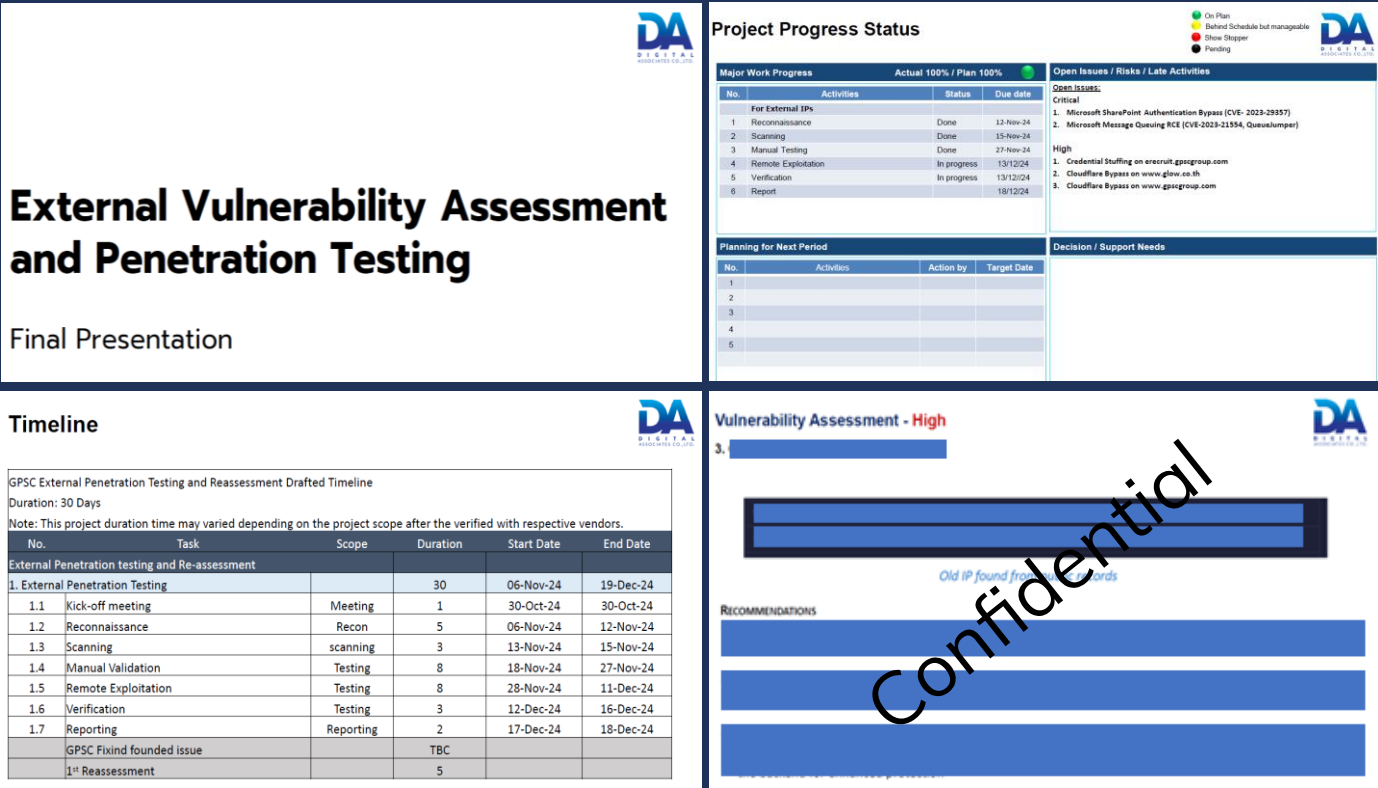
In 2024, GPSC carried out an external audit, including a comprehensive vulnerability assessment and penetration testing, to identify and address potential weaknesses in its digital systems. The evaluation was conducted by specialized cybersecurity firm (DA Digital Associates Co., Ltd.) to ensure the integrity, resilience, and security of GPSC’s IT infrastructure.

**Assessor:** DA Digital Associate Co., Ltd

**Date:** 06 Nov 24 to 18 Dec 24

**Result:**

The assessment resulted in two different level of status, including critical and high levels of vulnerability through testing.





# Information security vulnerability analysis (2/2)

GPSC carried out an external audit for vulnerability assessment to identify and address potential weaknesses in its digital systems. The evaluation was conducted by specialized cybersecurity firm (Tenable, Inc.) to ensure the integrity, resilience, and security of GPSC's IT infrastructure.

**Assessor:** Tenable, Inc.

**Date:** 06 Nov 24 to 18 Dec 24

## **Result:**

The assessment resulted in five different level of status, including critical, high, medium, low, and info levels of vulnerability through testing.



---

# Internal audits of the IT infrastructure and/or information security management systems

# Internal audits of the IT infrastructure and/or information security management systems (1/4)

In 2024, GPSC conducted comprehensive internal audits to evaluate and enhance the integrity, resilience, and security of its IT infrastructure and information security management systems. These audits aimed to ensure preparedness against potential disruptions and cyber threats across the organization. Key activities included a:

- Disaster Recovery (DR) and emergency drill for the SAP S/4 HANA system to test business continuity capabilities,
- Tabletop cyber drills focused on both operational technology (OT) and information technology (IT) systems to simulate and respond to cybersecurity incidents.
- Additionally, GPSC tested its DR plan for Cloud Infrastructure as a Service (IaaS) to validate cloud recovery protocols, and
- Carried out a phishing email simulation to assess employee awareness and response to social engineering threats.

These proactive measures reflect GPSC's commitment to maintaining a secure and resilient digital environment.

# Internal audits of the IT infrastructure and/or information security management systems (2/5)

In 2024, GPSC carried out its annual Disaster Recovery (DR) and Emergency Drill for the SAP system, aiming to ensure organizational readiness in the event of an unexpected incident. The drill was designed to test the effectiveness of incident management procedures, confirm the clarity of roles and responsibilities among employees, and assess their ability to respond promptly and accurately during disruptions. In addition to evaluating the SAP S/4 HANA system, the exercise also involved critical components of GPSC's broader IT infrastructure, including servers, network configurations, storage systems, and backup environments, to ensure system interoperability and infrastructure resilience. The drill assessed the organization's Recovery Point Objective (RPO) and Recovery Time Objective (RTO) in accordance with the defined Service Level Agreement (SLA). This proactive initiative not only strengthens GPSC's operational resilience but also supports continuous improvement in business continuity and IT system recovery capabilities.

**Date of internal audit:** 21 Sep 2024

### Annual disaster recovery and emergency drill (DR drill) for SAP S/4 HANA

Sep 21, 2024

DR process prepared by Sivapong T. & Ratcharin U.



#### Test State

วันเสาร์ที่ 21 กันยายน 2024 เวลา 08.00-22.45 **ระยะเวลาในการซ้อม 12 ชั่วโมง**

DR Drill Step	Activities	Responsible	Duration	
State 1		GPSC DR Team	8.00 – 9.00 น. 1 ชั่วโมง	
State 2		GPSC IT / SAP ECS	9.00 – 16.15 น. 7 ชั่วโมง 15 นาที	
		GPSC End Users / GPSC IT Functional (Partial support by AMS)	16.15 – 18.15 น. 2 ชั่วโมง	
State 3		GPSC IT / SAP ECS	18.15 – 20.10 น. 1 ชั่วโมง 55 นาที	
		GPSC End Users / GPSC IT Functional (Partial support by AMS)	20.10 – 22.10 น. 2 ชั่วโมง	
		GPSC IT	22.10 – 22.45 น. 35 นาที	

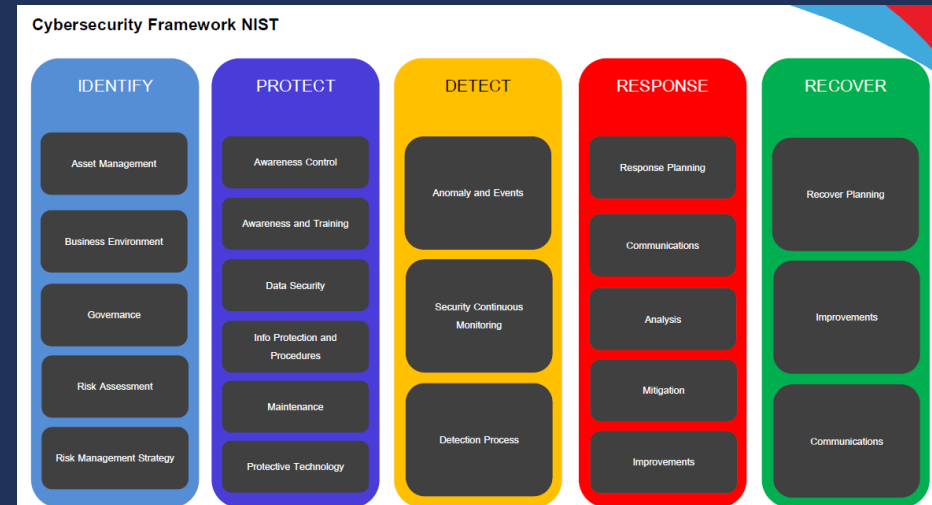


# Internal audits of the IT infrastructure and/or information security management systems (3/5)

GPSC conducted cyber drill tabletop activities for operation technology and information technology in 2024 to prepare the readiness for quick incident response to recover the business operation, establish the comprehensive understanding the process for incident management for employees, and ensure role and responsibility of all employees for cyber security.

The scope of test involved a tabletop exercise combined with the activation of a command center to oversee the response. The simulation focused on handling a cybersecurity threat scenario, specifically a Zero-Day Malware Attack. Key participants in the drill included the Cyber Warfare Team (CWT), Information Security Management System (ISMS) team, Enterprise Technology Management (ETM), Plant Operation (C&I), and external service providers. The simulated attack was designed to impact critical systems such as the PI Server, PI Interface, and OPC, which in turn affected operations at CUP1, CUP4, GIPP, and Phase 5 plants. Notably, the production systems were not shut down, as the exercise was purely procedural. The entire drill was conducted online with the command center operating virtually via Microsoft Teams.

**Date of internal audit:** 21 Oct 2024 to 11 Dec 2024



# Internal audits of the IT infrastructure and/or information security management systems (4/5)


The test focused on evaluating the organization’s response to a critical incident affecting core IT infrastructure. It aimed to assess the effectiveness of emergency communication, decision-making, and coordination between internal teams and service providers. An internal audit tested the continuity of key systems and services, such as user authentication and file access, and involved declaring an emergency to ensure appropriate escalation and recovery actions were taken within the defined timeframe.

**Date of internal audit:** 22 Nov 2024



Test State

จัดซ้อมในวันที่ 22 พฤศจิกายน 2567 รายละเอียดดังนี้

DR Drill Step	Activities	Responsible	Duration
State 1		GPSC DR Team	13.00 – 13.15 น. 15 นาที
		GPSC DR Team	13.15 – 14.45 น. 1 ชั่วโมง 30 นาที
State 2		GPSC IT / Dailitech / PTT Digital	14.45 – 17.35 น. 2 ชั่วโมง 50 นาที
State 3		GPSC IT / Dailitech / PTT Digital	17.35 – 23.55 น. 6 ชั่วโมง 20 นาที

== Internal Use Only ==

3 GPSC

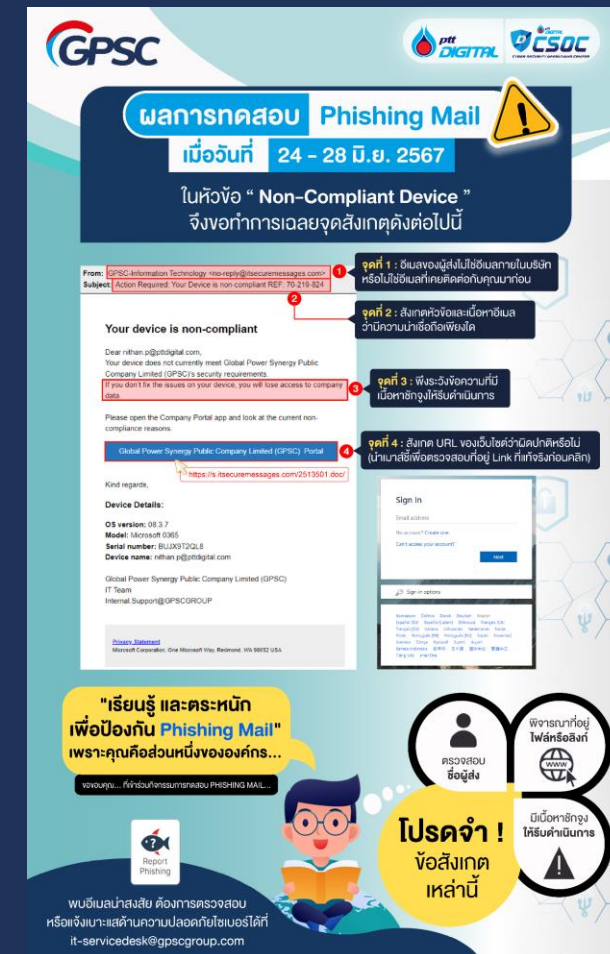


# Internal audits of the IT infrastructure and/or information security management systems (5/5)

Phishing email simulation is one of the key internal audit programs implemented by GPSC across the organization. Conducted annually, this program serves as a practical assessment of employees' ability to recognize and respond to phishing attempts, following their participation in cybersecurity awareness training. The simulation helps evaluate the effectiveness of the training program by measuring real-time responses to potential threats, identifying areas where additional support or education may be needed, and reinforcing a culture of vigilance. This proactive approach plays a crucial role in strengthening the organization's overall cybersecurity posture and minimizing the risk of social engineering attacks.

## Date of internal audit:

- 24 Jun 2024 to 28 Jun 2024
- 26 Aug 2024 to 30 Aug 2024





---

# Independent external audit of the IT infrastructure and/or information security management systems

# External audit of the IT infrastructure and/or information security management systems

In 2024, GPSC underwent an external audit of its IT infrastructure and information security management systems, conducted by BSI Group. As part of this process, GPSC upgraded its certification from ISO/IEC 27001:2013 to **ISO/IEC 27001:2022**. The transition reflects the organization's commitment to maintaining a robust and up-to-date information security framework. The updated 2022 version of the standard introduces a more structured approach to risk management, enhanced alignment with modern cybersecurity practices, and greater emphasis on continual improvement and stakeholder expectations. This upgrade ensures that GPSC's information security management system remains resilient, relevant, and aligned with evolving global security challenges and regulatory requirements.

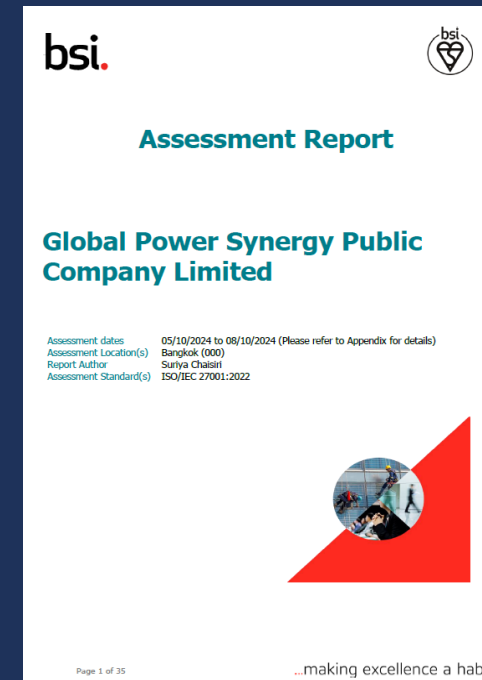
**Assessor:** BSI Group

**Assessment date:** 05 Oct 2024 to 08 Oct 2024

**Certificate date:** 15 Nov 2024 to 14 Nov 2027

## Result:

The organization has demonstrated a strong commitment to enhancing the effectiveness of its management system. Evidence shows that the system has been properly implemented and operated to achieve its intended outcomes. The management team has actively ensured compliance with internal policies, customer expectations, legal obligations, and other relevant requirements, while also fostering a culture of continual improvement. Furthermore, the organization has successfully completed the transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022, reflecting its proactive approach to aligning with updated international standards.



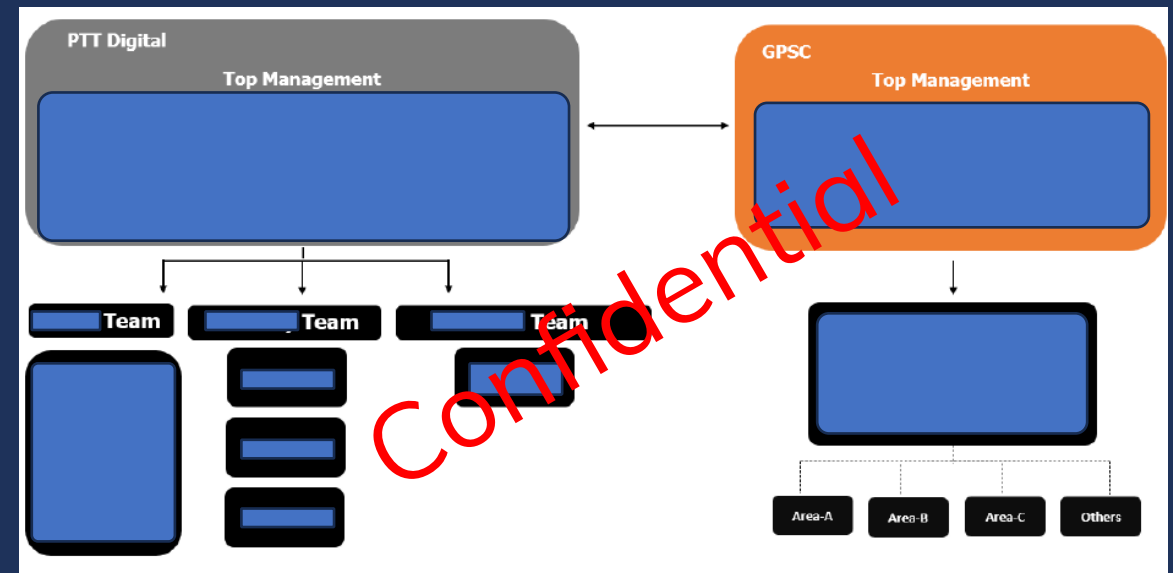
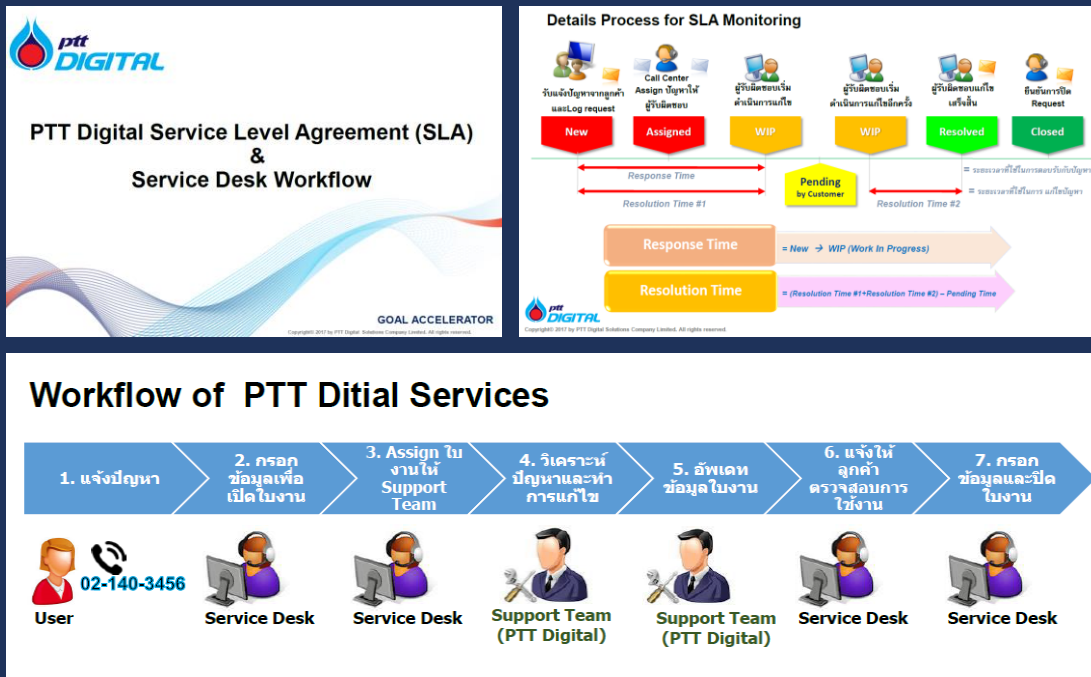
---

# Escalation process for employees to report incidents, vulnerabilities or suspicious activities

# Escalation process for employees to report incidents, vulnerabilities or suspicious activities (1/3)

GPSC, as a PTT flagship company, uses the process of service level agreement (SLA) monitoring and workflow as a clear escalation process of manage information and cybersecurity event/ incident of PTT digital services as well as PTT Digital Service Request Channel for resolving the customers' IT Problems. The workflow is managed by PTT Digital who is the operator of GPSC major IT infrastructure. The process enables GPSC Group's employees can follow on suspicious activities through hotline or service desk.

In addition to escalation process from PTT digital, GPSC has the work instruction of both Operation Technology (OT) and Information Technology (IT) in place for all employees in the organization. The instructions encompass role, responsibility, and workflow between GPSC and PTT Digital team.



# Escalation process for employees to report incidents, vulnerabilities or suspicious activities (2/3)

Specifically, regarding the employee escalation process, GPSC has implemented an internal Incident Management Procedure applicable organization-wide. This procedure is designed to establish a documented structure that defines the rules and standards for managing incidents effectively. It clarifies the roles and responsibilities of employees involved in incident response, promoting transparency and accountability throughout the process. The procedure outlines the methods and best practices to ensure incidents are addressed efficiently and in line with organizational policies. It also incorporates robust internal controls and approval mechanisms throughout the incident management cycle.

Incident management procedure as part of escalation process for employees

  
Global Power Synergy Public Company Limited

ระเบียบปฏิบัติ  
Procedure

ข้อมูลเอกสารฉบับล่าสุด

หมายเลขเอกสาร	PDV-P-0020	สายงาน	PSE	ฝ่าย/ส่วน	PDV
ชื่อเอกสาร	ขั้นตอนการบริหารจัดการเหตุการณ์ระบบสารสนเทศ (Incident management procedure)			สถานะ	
การแก้ไข	02	วันที่ประกาศใช้	15 ต.ค. 2567	จำนวนหน้า	16

# Escalation process for employees to report incidents, vulnerabilities or suspicious activities (3/3)

Additionally, the escalation process use the priority level table to identifies the relative importance of an Incident. Incident priority is based on the combined Impact and Urgency assignments, and is used to identify the required action times. Leading to action to be activated that complies with the stepwise instruction to guide employees in executing the process correctly. Overall, this procedure ensures that incident management efforts align with business objectives and serve the best interests of the organization.

Example of priority level table

Incident Priority		4 - Urgent	3- High	2 - Medium	1 - Low
Incident Priority		Impact			
		Low (1)	Medium (2)	High (3)	
Urgency	High (3)	Medium	High	Urgent	
	Medium (2)	Low	Medium	High	
	Low (1)	Low	Low	High	

Example of Escalation process for employees to report incidents, vulnerabilities or suspicious activities

## 6.3 [P1] Incident Management Process

Procedure Description. In this section, the above process workflow is detailed in a more explanatory procedure description table format.

Reporter	Inform/Notify Event/System Alarm/Complaint	<ul style="list-style-type: none"><li>Inform or notify events, system alarms, or complaints to IT Service Desk through various means, i.e., phone, email, Microsoft Teams, or Service Desk Platform. Some events or system alarms are early detected by Digital Platform Analyst themselves.</li></ul>
----------	--	--

# Information security awareness training



# Information security awareness training (1/4)

GPSC has organized training courses on information security and cybersecurity awareness, including compliance with the company's Information and Communication Technology Policy Standard Practice, covering areas such as computer and software usage, internet access, email communication, and computer virus protection. These trainings are provided to employees at all levels, including new hires, through online platforms such as e-Learning and orientation sessions. The objective is to raise awareness of cyber threats and ensure understanding of the policies and regulations governing the use of information technology systems, which all employees must strictly follow as part of their performance evaluation. In addition to the existing curriculum, the training has been enhanced with new modules covering emerging cybersecurity topics such as ransomware attacks, the rise of cybersecurity AI, potential cybersecurity incidents projected for 2030, AI-based predictive social engineering, zero trust architecture, the role and function of Computer Emergency Response Teams (CERT), and cybersecurity incident preparedness. These additions aim to equip employees with up-to-date knowledge and readiness to respond to evolving cyber threats.

# Information security awareness training (2/4)

# Ransomware Attacks

# Rise of Cybersecurity AI

## Cybersecurity Threat

# AI-Based Predictive Social Engineering




# ภัยคุกคามที่เพิ่มขึ้น

## จาก Ransomware Attacks

Ransomware Attacks ที่ก่อตัว (Malware) ประเภทหนึ่งที่ใช้เข้ารหัสหรือล็อกไฟล์ของเหยื่อ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ให้ไม่สามารถเข้าถึงไฟล์หรือข้อมูลนั้น ๆ ได้ จากผู้โจมตีและผู้โจมตีได้วางเงื่อนไขเพื่อแลกกับการได้ข้อมูลคืน ซึ่งโดยปกติแล้วผู้โจมตีจะดูถูกเหยื่อไม่เท่ากัน ในรูปของเงินสกุลเงินดิจิทัล (Cryptocurrency) เช่น Bitcoin หรือ Ethereum

### สถานการณ์ปัจจุบันของการเผชิญ Ransomware Attacks



**ปี 2022 ปีแห่งการต่อสู้กับ Ransomware** จากบทวิเคราะห์ของ Chainalysis กล่าวว่าการเพิ่มขึ้นของภัยคุกคามได้รับยกย่องว่ามี 456.8 ล้าน USD จากเหยื่อในปี 2022 ซึ่งถือว่าลดลงจากกว่าปี 2021 ที่เคยมีเหยื่อในปี USD 756.6 ล้าน ปี 2022 (ลดลง 40.3%) เป็นสถิติฐานยังถือว่าเป็นเพราะเหยื่อไม่ได้เฝ้าระวังภัยจนทำให้ถูกแฮกเกอร์แอบโจมตีเร็ววันมากขึ้น



### วิธีการป้องกัน Ransomware Attacks สำหรับผู้ใช้งานทั่วไป

1. ปิดตัวเฉพาะทางเพื่อหลีกเลี่ยงจากเหยื่อที่ส่งอีเมลให้ เช่น จากเว็บไซต์ที่ได้รับ
2. เมื่อพบ Website, Link, File ที่ไม่น่าไว้ใจ ให้ลบและทิ้ง ไม่ควรคลิกลิงก์เพื่อลดความเสียหายในโปรแกรม
3. ติดตั้ง Antivirus มั่นใจ Update และ Scan ฉุกเฉิน
4. ทำการ Backup File สำคัญให้หลายๆ ที่โดยเฉพาะการสำรองข้อมูลแบบออฟไลน์ด้วย เช่น Copy ไฟล์เก็บไว้ใน Harddisk เป็นต้น




### Top 3 การโจมตีของ Ransomware

ชื่อ	ประเภท	ความเสียหาย
WannaCry (2017)	Crypto-ransomware	\$4 พันล้านเหรียญ
NotPetya (2017)	Locker-ransomware	\$10 พันล้านเหรียญ
Sodinokibi (2019)	Crypto-ransomware	\$0.2 พันล้านเหรียญ

### เหตุการณ์สำคัญทางธุรกิจโดนตี

ในปี 2021 องค์กร Colonial Pipeline ได้รับรายงานเสียหายจากการโดนโจมตีแรนซัมแวร์ Ransomware ซึ่งส่งผลกระทบต่อบรรยากาศของตลาดการเงินโลก ทำให้บริษัทต้องหยุดการดำเนินงานบางส่วนลงเป็นอย่างมากเพื่อแก้ไขปัญหาและป้องกัน การโดนฉกฉวยประโยชน์จากการลงผลงานของปี ทำให้บริษัทต้องจ่ายค่าไถ่จำนวน 4.4 ล้านดอลลาร์คืนให้กับผู้โจมตีในปีที่ผ่านมา (75 ตั๋วเงินหรือ 4.4 ล้านดอลลาร์สหรัฐฯ) ภายหลังเวลาผ่านไปหลายปี เมื่อจำค่าที่เสียแล้วจะบรรเทาจากการโดนโจมตีซ้ำหรือไม่ขึ้นอยู่กับ




ที่มา Chainalysis cyberline - Trend Micro - astra, World Pipelines, Bendoris, nt cyberline



# Rise Of Cybersecurity AI

## บทบาทของ AI ในการป้องกันความปลอดภัยทางไซเบอร์ในอนาคต



**จากรายงาน World Economic Forum's Global Risks Report 2024** ระบุว่าความไม่มั่นคงปลอดภัยทางไซเบอร์ถือเป็นความท้าทายระดับโลกในช่วงเวลาข้างหน้า โดยในแง่ความเสียหายรุนแรงต่าง ๆ เช่น **Malware, Deepfakes** และภัยคุกคามจาก **บอทก๊อต (bots)** **Reuters** ยังระบุการค้นพบอย่างรวดเร็วจนถึง **AI** ในรูปแบบใหม่เพื่อเพิ่มศักยภาพในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์

การโจมตีที่เพิ่มขึ้นนี้สะท้อนให้เห็นถึงผลกระทบจากการใช้ AI ที่อาจใช้ประโยชน์เพื่อเพิ่มประสิทธิภาพของภัยคุกคาม (GCHQ) ได้ถึงขีดจำกัดของ AI ของสหราชอาณาจักร

คาดการณ์ว่าภัยคุกคามจะเพิ่มขึ้น 2 เท่าภายในปี (2024 – 2026) อย่างหลีกเลี่ยงไม่ได้

**อย่างไรก็ตาม AI ก็เป็นบทบาทสำคัญในการป้องกันความปลอดภัยทางไซเบอร์มากขึ้นเรื่อย ๆ** ในปัจจุบัน แม้ว่าภัยคุกคามจะเพิ่มขึ้น โดย AI นั้นเข้ามามีในการสร้างความปลอดภัยทางไซเบอร์นั้น สามารถตรวจจับความผิดปกติและป้องกันภัยคุกคามได้อย่างรวดเร็วและแม่นยำมากขึ้น

ภัยคุกคามในรูปแบบใหม่ ผ่านการวิเคราะห์ข้อมูลเชิงลึก

**ภัยลวงที่อาจเกิดขึ้นจากการใช้ AI**



**AI Hallucination** เกิดจากการที่ AI ถูกสร้างข้อมูลเนื้อหาที่ไม่ถูกต้องหรือที่ผิด AI ก็มีความเสี่ยงและเผลอข้อมูลที่ไม่ถูกต้องและนำไปสู่การผิดพลาดจากการนำข้อมูลดังกล่าวไปใช้งาน โดยไม่ตรวจสอบ

**Misinformation/Disinformation** เป็นการสร้างข้อมูลเท็จหรือข้อมูลที่บิดเบือนจากการใช้ AI เพื่อสร้างความสับสน และเพิ่มความเสี่ยงต่อความเสียหายจากการนำข้อมูลดังกล่าวไปใช้งานโดยไม่ตรวจสอบ



**Deepfakes** เป็นการสร้างข้อมูลเท็จที่ดูเหมือนจริง โดยใช้ AI เพื่อสร้างเนื้อหาที่เหมือนจริง แต่เป็นข้อมูลที่บิดเบือน ซึ่งสามารถนำไปสู่การตัดสินใจที่ผิดพลาดได้



**ข้อควรระวังการใช้งาน AI**

- สร้างข้อมูลและตีความที่ผิด:** หน่วยงานรัฐอาจมีความเสี่ยงในการใช้ข้อมูลที่ไม่ถูกต้องในการตัดสินใจว่า AI ในการเพิ่มศักยภาพในการป้องกันและตรวจจับภัยคุกคาม
- การเปิดเผยข้อมูลด้วย Algorithms ของ AI:** ที่ทำให้หน่วยงานความปลอดภัยไม่ชัดเจนว่า AI ถูกใช้เพื่อวัตถุประสงค์ใด ๆ ซึ่งอาจนำไปสู่การละเมิดความเป็นส่วนตัวและการเลือกปฏิบัติ
- ความไม่มั่นคงและความปลอดภัย:** ระบบ AI ที่ถูกใช้เพื่อวัตถุประสงค์ในการป้องกันภัยคุกคามสามารถนำไปสู่การละเมิดข้อมูลส่วนบุคคลและข้อมูลที่สำคัญ
- การเลือกใช้งานที่ผิด:** องค์กรที่นำเทคโนโลยี AI มาใช้เพื่อวัตถุประสงค์ในการป้องกันภัยคุกคามอาจมีความเสี่ยงในการเลือกใช้งานที่ไม่เหมาะสม



ที่มา: IBM, Deepmind, reuters, dashlane, threatax, davis



ENISA



KASPERSKY



McKINSEY & COMPANY

## 10 อันดับแรกของการคุกคามทางไซเบอร์ ที่คาดว่าจะเกิดขึ้นในปี 2030



มีการคาดการณ์ 10 อันดับแรกของการคุกคามทางไซเบอร์  
ที่คาดว่าจะเกิดขึ้นในปี 2030 ดังต่อไปนี้

1. การโจมตีหรือบุกรุกซอฟต์แวร์ ที่เกี่ยวข้องกับการควบคุมการผลิตห่วงโซ่อุปทาน
2. การเผยแพร่ข้อมูลเท็จ ที่ใช้เทคนิคขั้นสูง
3. การกำกับดูแลที่เข้มงวดในไลต์วอร์กัสเพิ่มขึ้น ความเป็นส่วนตัวของบุคคลลดลง
4. ความผิดพลาดที่เกิดจากมนุษย์และการใช้งานระบบที่ผิด ภายในระบบนิเวศดิจิทัลและการขยายตัว
5. การปล่อยตัวเป็นเป้าหมายเพิ่มขึ้น โดยใช้อุปกรณ์การป้องกันที่มีอยู่
6. การขยายการโจมตีและควบคุมโครงสร้างพื้นฐานของวัตถุทางปัญญาในอวกาศ
7. การคุกคามแบบผสมผสาน ที่ก่อตัวในโลกออนไลน์ที่ล้ำมากขึ้น
8. การขาดแคลนบุคลากรที่มีทักษะด้าน cybersecurity
9. ผู้ให้บริการในไลต์สารสนเทศและการสื่อสารระหว่างประเทศตกเป็นจุดที่เสี่ยง
10. การใช้อินเทอร์เน็ตระบุตัวในทางที่ผิด คือใช้เปิดปฐมาภพจากอาชญากรรม



ในประเทศไทย Kaspersky ผู้ให้บริการด้านความปลอดภัยทางไซเบอร์ระดับโลก  
ล่าสุดได้เผยแพร่ ในปี 2023 พบว่าเหตุการณ์ด้านภัยคุกคามทางไซเบอร์กว่า 17 ล้านรายการ  
ที่ผ่านหน้าเข้ามาในศูนย์ปฏิบัติการด้านความปลอดภัยทางไซเบอร์ของ Kaspersky  
กับรายงานการรุกรานทางไซเบอร์จากการโจมตีที่เพิ่มขึ้น พหุภาคีของรัสเซีย  
และเจ้าอาชญากรรมทางไซเบอร์จากรัฐบาลในจีนเป็นภัยคุกคามอันดับต้นๆ  
ด้วยแรงเหวี่ยงสูงสุดถึง 163,091 รายการสร้างความเสียหายโดยประมาณ  
ถึง 27,300 ล้านบาท



**McKinsey คาดการณ์ตลาด Cybersecurity**

McKinsey บริษัทที่ปรึกษาชั้นนำระดับโลกได้คาดการณ์ตลาด Cybersecurity โลกในปี 2025 ว่าจะมีการใช้จ่ายถึง 1015 พันล้านดอลลาร์ ในภูมิภาค Asia Cybersecurity  
คาดว่าจะมีค่าใช้จ่ายที่ขยายตัวการรวมการโจมตีของภัยคุกคามทางไซเบอร์ประมาณ 15% ต่อปี  
และคาดว่าจะมีค่าใช้จ่ายถึง 10.5 พันล้านดอลลาร์ต่อปี จากตัวชี้วัดของตลาดดังกล่าว  
แสดงให้เห็นถึงความกังวลเกี่ยวกับการโจมตีทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง



**Global Risk Report จัดอันดับประเทศที่มีความเสี่ยงต่าง ๆ**

Global Risk Report 2023 ของ World Economic Forum ได้จัดอันดับประเทศที่มีความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับโลกตามระดับความรุนแรง ซึ่ง 1 ใน 10 เรื่อง  
ที่มีความเสี่ยงสูงสุดในปี 2025 และ ปี 2030 คือความมั่นคงทางไซเบอร์และ  
ความปลอดภัยทางไซเบอร์ (Widespread Cybercrime and Cyber Insecurity)  
ดังนั้นจึงแตกต่าง ๆ ถึงระดับเตรียมพร้อมรับมือกับเรื่องนี้ในระดับชาติ

รูป : World Economic Forum, Kaspersky, McKinsey, ENISA

[illegible]



# Information security awareness training (3/4)

## Zero Trust to reduce incident



**Zero Trust** ทฤษฎีการยกระดับนโยบายความปลอดภัยทางไอทีสำหรับบริษัทหรือองค์กรขนาดใหญ่

Zero Trust (ZT) ที่แตกต่างจากแบบจำลองความไว้วางใจคือการไม่ไว้วางใจทั้งในเครือข่ายภายในและภายนอกองค์กร และบริการด้านสารสนเทศแบบตามกำหนดที่แน่นอน ในรูปแบบของเครือข่ายที่เชื่อมต่อกันเป็นเครือข่ายเป็นความปลอดภัแบบ Never trust, Always Verify อย่างต่อเนื่องโดยไม่มีจุดตรวจสอบที่เชื่อถือได้ ทุกสิ่งทุกอย่าง ไม่ว่าจะเป็นบุคคล ระบบ หรืออุปกรณ์ต่าง ๆ ที่ทั้งภายในหรือภายนอกองค์กรก็ควรได้รับการตรวจสอบอยู่เสมอ

ความท้าทาย 5 ประการที่อาจเกิดขึ้นเมื่อต้องการนำแนวคิด Zero Trust มาใช้ในองค์กร

Demonstrate Full IT Value	Operation Cost	Focus on Priority Domains
องค์กรต้องสามารถสื่อสารคุณค่าของ Zero Trust ที่มีต่อความสามารถในการดำเนินงานขององค์กรได้อย่างมีประสิทธิภาพ	การนำนโยบาย Zero Trust มาใช้ในองค์กรอาจมีต้นทุนสูงในการดำเนินการและดำเนินการอย่างต่อเนื่อง	องค์กรอาจเน้นดำเนินการในบางพื้นที่สำคัญ เช่น Identity and Access Management (IAM) ซึ่งเป็นส่วนสำคัญของ Zero Trust Architecture และดำเนินการในส่วนอื่น ๆ ตามลำดับความสำคัญ
Build Maturity Over Time	Follow the Right Sequence	
องค์กรต้องนำ Zero Trust Strategy ไปสู่การปฏิบัติอย่างค่อยเป็นค่อยไป	การดำเนินการตาม Zero Trust Strategy ควรดำเนินการตามลำดับความสำคัญ	

**กลยุทธ์ 5 ประการในการปรับตัวเข้าสู่ Zero Trust**

- Identity**  
การตรวจสอบตัวตนของผู้ใช้ก่อนการเข้าถึงทรัพยากร
- Device**  
สามารถตรวจสอบได้ว่าอุปกรณ์ที่เชื่อมต่อมีความปลอดภัยหรือไม่
- Network**  
ตรวจสอบว่าเครือข่ายการสื่อสารมีความปลอดภัยหรือไม่
- Application Workload**  
สามารถตรวจสอบได้ว่าแอปพลิเคชันมีความปลอดภัยหรือไม่
- Data**  
ตรวจสอบว่าข้อมูลมีความปลอดภัยหรือไม่

ที่มา: CISW, CSA, CISO

## AI for Power Industry



**10 อันดับการใช้แอปพลิเคชัน AI ในอุตสาหกรรมพลังงาน**

ในปัจจุบัน AI มีส่วนในการเปลี่ยนโฉมการดำเนินงานของอุตสาหกรรมพลังงาน โดยมีการนำ AI มาใช้ในการวิเคราะห์ข้อมูล การพยากรณ์ การควบคุมระบบ และการเพิ่มประสิทธิภาพ การนำ AI มาใช้ในอุตสาหกรรมพลังงานมีดังนี้

**กรณีศึกษาในอุตสาหกรรมพลังงาน 10 อันดับแรก**

- Smart Grids:** เป็นเครือข่ายการจ่ายไฟฟ้าที่ใช้ AI ในการจัดการระบบการบริโภคโดยวิเคราะห์ข้อมูลแบบเรียลไทม์
- Demand Response Management (DRM):** การจัดการการตอบสนองความต้องการการพลังงานซึ่งเป็นการจัดการการบริโภคไฟฟ้าโดยใช้ AI เชื่อมโยงเชิงโต้ตอบระหว่างผู้ให้บริการและลูกค้า
- Predictive Maintenance:** การบำรุงรักษาโดยใช้ AI ในการตรวจสอบสภาพของโรงไฟฟ้าและอุปกรณ์ต่าง ๆ
- Renewable Energy Forecasting:** การพยากรณ์พลังงานทดแทนโดยใช้ AI ในการวิเคราะห์ข้อมูลสภาพอากาศและข้อมูลอื่น ๆ
- Energy Storage:** ใช้ AI เพื่อเพิ่มประสิทธิภาพการเก็บพลังงานจากแหล่งพลังงานต่าง ๆ เช่น ลม แสงอาทิตย์
- Carbon Capture, Utilisation, and Storage (CCUS):** การดักจับและการใช้ประโยชน์จากคาร์บอนไดออกไซด์
- Energy Trading:** การซื้อขายพลังงานโดยใช้ AI ในการวิเคราะห์ข้อมูลตลาดพลังงานและข้อมูลอื่น ๆ
- Oil and Gas Exploration:** การสำรวจและผลิตปิโตรเลียมโดยใช้ AI ในการวิเคราะห์ข้อมูลการสำรวจและข้อมูลอื่น ๆ
- Nuclear Power Plant Monitoring:** การตรวจสอบโรงไฟฟ้าพลังงานนิวเคลียร์โดยใช้ AI ในการตรวจสอบความปลอดภัยและประสิทธิภาพ
- Nuclear Power Plant Monitoring:** การตรวจสอบโรงไฟฟ้าพลังงานนิวเคลียร์โดยใช้ AI ในการตรวจสอบความปลอดภัยและประสิทธิภาพ

ที่มา: Secureframe

## AI Energy Storage



**AI Energy Storage** คือ การนำปัญญาประดิษฐ์ (AI) เพื่อเพิ่มประสิทธิภาพของระบบเก็บพลังงาน โดยปัญญาประดิษฐ์หรือ AI สามารถเข้ามาช่วยเพิ่มประสิทธิภาพในการเก็บพลังงาน ที่อาจช่วยลดต้นทุนการดำเนินงานได้

**การทำงานของระบบการเก็บพลังงาน (Energy Storage System :ESS)**

การทำงานของระบบการเก็บพลังงาน (Energy Storage System :ESS) คือ การนำพลังงานที่ผลิตได้มาเก็บไว้ในแบตเตอรี่หรือระบบเก็บพลังงานอื่น ๆ เพื่อใช้ในเวลาที่ต้องการ

**บทบาทของ AI ในการเพิ่มประสิทธิภาพของ Energy Storage โดยย่อ**

- การจัดการความต้องการใช้พลังงาน**  
AI สามารถช่วยในการจัดการความต้องการใช้พลังงานที่ผันผวนได้
- การประยุกต์ใช้กับพยากรณ์อากาศ**  
การพยากรณ์อากาศที่แม่นยำสามารถช่วยในการตัดสินใจเกี่ยวกับการเก็บพลังงานได้
- การคาดการณ์การบำรุงรักษาสถาปัตยกรรม**  
AI สามารถช่วยในการคาดการณ์การบำรุงรักษาสถาปัตยกรรมได้
- การคาดการณ์การเกิดอุบัติเหตุ**  
AI สามารถช่วยในการคาดการณ์การเกิดอุบัติเหตุได้

**กรณีตัวอย่างการดำเนินการ AI Ethic ในองค์กร**

กรณีตัวอย่างการดำเนินการ AI Ethic ในองค์กร คือ การนำ AI มาใช้ในการตัดสินใจเกี่ยวกับการเก็บพลังงาน

ที่มา: PEA, FTI, mappeng, Breaking Energy, Smart City Thailand, BBL

## Computer Emergency Response Team (CERT)



**Computer Emergency Response Team (CERT)**

Computer Emergency Response Team หรือ CERT เป็นหน่วยงานที่รับผิดชอบในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางคอมพิวเตอร์

**โดยในประเทศไทยหน่วยงาน CERT ที่ได้รับการยืนยันแล้ว มีทั้งหมด 10 หน่วยงาน เช่น**

- ศูนย์ประสานการรับมือภัยคุกคามทางคอมพิวเตอร์ (MODCSIRT)
- ศูนย์ประสานการรับมือภัยคุกคามทางคอมพิวเตอร์ (TB-CERT)
- ศูนย์ประสานการรับมือภัยคุกคามทางคอมพิวเตอร์ (Energy CERT)

**CERT หรือ Computer Emergency Response Team**

เป็นหน่วยงานที่รับผิดชอบในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางคอมพิวเตอร์

**และเนื่องจาก CERT เป็นเครื่องมือการแจ้งเตือนภัย**

ดังนั้น ศูนย์ที่ทำการประสานและรับมือเหตุการณ์ด้านความปลอดภัยทางคอมพิวเตอร์จะต้องมี CERT เป็นเครื่องมือการแจ้งเตือนภัย

**Computer Emergency Response Team (CERT) ในอุตสาหกรรมพลังงานประเทศไทย**

สำหรับประเทศไทย Energy CERT เป็นศูนย์กลางการประสานงาน เพื่อรับมือและแก้ไขปัญหาภัยคุกคามทางคอมพิวเตอร์ในภาคพลังงาน

**หน่วยงาน CERT ในต่างประเทศ และตัวอย่างเหตุการณ์สำคัญ**

ในปี 2564 Colonial Pipeline ถูกโจมตีด้วย ransomware ส่งผลให้เกิดการหยุดชะงักของการจ่ายน้ำมันในสหรัฐอเมริกา

ที่มา: ThaiCERT, MOD, TechTarget, CISA, BBC



# Industrial Transformation through Digital Twin

# Cloud Computing in Energy Industry

# Cybersecurity Prevention

## Ransomware Attacks Prevention

# การป้องกัน

## Ransomware Attacks

**ในอุตสาหกรรมภาคพลังงาน**

การโจมตีด้วย Ransomware ในธุรกิจพลังงานเป็นประเด็นที่สำคัญและเพิ่มละแวกภัยมากขึ้น เนื่องจากธุรกิจนี้มีความเสี่ยงต่อโครงสร้างพื้นฐานสำคัญที่มีผลกระทบต่อความมั่นคงและสังคมทั่วโลก การการกีดกันข้อมูลและหยุดยั้งที่ทันเวลาสามารถหลีกเลี่ยงการเป็น แสงส่องผลกระทบต่อความมั่นคงของชาติ



**ผลกระทบด้านความเสียหายที่เกิดขึ้นกับธุรกิจพลังงานจาก Ransomware Attack**

			
<p>การหยุดชะงักของการทำงานเนื่องจากการโจมตีที่ส่งผลกระทบต่อกระบวนการผลิตพลังงาน เช่น การขาดแคลนน้ำมันเชื้อเพลิงในบางพื้นที่ เป็นต้น</p>	<p>ความสูญเสียจากการโจมตีบริษัทอาจต้องจ่ายค่าไถ่เป็นจำนวนเงินมหาศาล และต้องต้องเสียค่าใช้จ่ายในการกู้คืนระบบและข้อมูล รวมถึงค่าปรับที่ล่าช้าต่อลูกค้าและผู้สนับสนุนลูกค้าทั่วโลก</p>	<p>ความเสียหายต่อชื่อเสียงของบริษัทพลังงานที่ถูกโจมตีอาจสูญเสียความเชื่อมั่นจากลูกค้าและผู้ถือหุ้นที่ไม่ได้รู้สึกปลอดภัยจากการรับประกัน</p>	<p>ความเสียหายต่อความมั่นคงของชาติ การโจมตีที่กระทบพลังงานของระบบภาคพลังงาน อาจส่งผลให้เกิดความไม่มั่นคงทางความมั่นคงของชาติและสังคมของประเทศ</p>

### แนวทางการรับมือหรือหนีกับ Ransomware Attack

#### การป้องกันเชิงรุก

อัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้สอดคล้องกับมาตรฐานความปลอดภัยและป้องกันภัยคุกคามที่ทันสมัย เช่น AI และ Machine Learning เพื่อระบุและตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้น

#### การตอบสนองเชิงเหตุการณ์

สร้างแผนการตอบสนองเหตุการณ์ที่ทันเวลาและสอดคล้องกับแผนการฟื้นฟูระบบการโจมตี ransomware การทดสอบแผนการเป็นระยะเพื่อฝึกฝนว่าสามารถทำงานได้อย่างมีประสิทธิภาพ

#### การฝึกอบรมพนักงาน

ฝึกอบรมพนักงานเกี่ยวกับวิธีการที่ถูกต้องในการใช้คอมพิวเตอร์ และป้องกันการโจมตีทางเทคนิค เช่น การไม่คลิกลิงก์ที่น่าสงสัย การไม่เปิดไฟล์แนบจากแหล่งที่ไม่รู้จัก

#### การสร้างความร่วมมือระหว่างหน่วยงาน

ร่วมสร้างกับหน่วยงานรัฐบาลและองค์กรที่เกี่ยวข้องเพื่อแลกเปลี่ยนข้อมูลและสร้างความร่วมมือกับภาคอุตสาหกรรม และสร้างความปลอดภัย

**ตัวอย่างการโจมตีจาก Ransomware!!!**



**Norsk Hydro** บริษัทพลังงานสัญชาตินอร์เวย์ เผชิญภัยคุกคาม ransomware ในปี 2019 โดยมีการใช้เงินในการกู้คืนและค่าเสียหายจากการโจมตีโดยคร่าวๆ 40 ล้านดอลลาร์สหรัฐ



**Enel Group** บริษัทไฟฟ้าสัญชาติอิตาลี ได้รับผลกระทบโดยตรงจากเหตุการณ์ Ransomware ในปี 2020 ทำให้สูญเสียรายได้หลายล้านดอลลาร์สหรัฐ และส่งผลต่อความเชื่อมั่นของลูกค้าเป็นอย่างมาก

PDF-Cybersecurity ฉบับ 02/67

หุ้น : CRN, BBC

หน่วยงานผู้จัดทำโครงการและเผยแพร่



# Thank You

