

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)

หน้า 1 of 13	ครั้งที่แก้ไข 02	วันที่ประกาศ 15 ตุลาคม			
GPSC Group	Work Instruction	ชื่อเอกสาร: แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)			
2567	หมายเลขอากาศ: PDV-WI-0030				
 Global Power Synergy Public Company Limited		วิธีปฏิบัติงาน Work Instruction			
ข้อมูลเอกสารฉบับล่าสุด					
หมายเลขอากาศ	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)	
2. การหยุดชะงักของการส่งมอบผลิตภัณฑ์ (Delivery interruption)	
3. ไม่สามารถเข้าถึงปฏิบัติงานในสถานที่ (Office Deny)	
4. ระบบเทคโนโลยีสารสนเทศไม่สามารถใช้งาน (IT System/Network Failure)	4.1 โจมตีทางไซเบอร์ (Cyber Attack)

Confidential

ลำดับ	แผนปฏิบัติงาน	ผู้รับผิดชอบ
1.	เตรียมความพร้อมคอมพิวเตอร์ – จัดหาเครื่องคอมพิวเตอร์สำรอง พนักงาน และ ติดตั้งระบบ Remote Support และ ระบบ Conference ในคอมพิวเตอร์พนักงาน	
2.	เตรียมความพร้อมสำหรับการทำงานระยะไกล - ติดตั้งระบบ VPN ใน คอมพิวเตอร์พนักงาน	
3.	เน้นร่วงการโฉมตีทางไซเบอร์ผ่านระบบ CSOC โดยผู้ให้บริการ PTT Digital	
4.	เตรียมความพร้อมแก้ไขระบบ Network ด้วยกระบวนการ Incident Management	
5.	เตรียมความพร้อมของ DR-Site และมี DR-Drill ของระบบต่าง ๆ ประจำปี	
6.	เตรียมความพร้อมแผนรับมือการโฉมตีทางไซเบอร์ของระบบ IT โดยการ ทำ Cyber Drill ประจำปี	
7.	เตรียมความพร้อมแผนรับมือการโฉมตีทางไซเบอร์ของระบบ OT โดย การ ทำ Cyber Drill ประจำปี ร่วมกับด้วยหน่วยงานของโรงงาน	

Confidential

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.

External Vulnerability Assessment and Penetration Testing

Final Presentation

Timeline

GPSC External Penetration Testing and Reassessment Drafted Timeline
Duration: 30 Days
Note: This project duration time may varied depending on the project scope after the verified with respective vendors.

No.	Task	Scope	Duration	Start Date	End Date
1.	External Penetration Testing		30	06-Nov-24	19-Dec-24
1.1	Kick-off meeting	Meeting	1	30-Oct-24	30-Oct-24
1.2	Reconnaissance	Recon	5	06-Nov-24	12-Nov-24
1.3	Scanning	scanning	3	13-Nov-24	15-Nov-24
1.4	Manual Validation	Testing	8	18-Nov-24	27-Nov-24
1.5	Remote Exploitation	Testing	8	28-Nov-24	11-Dec-24
1.6	Verification	Testing	3	12-Dec-24	16-Dec-24
1.7	Reporting	Reporting	2	17-Dec-24	18-Dec-24
	GPSC Fixind founded issue		TBC		
	1 st Reassessment		5		

Project Progress Status

Actual 100% / Plan 100% Green

No.	Activities	Status	Due date
1	Reconnaissance	Done	12-Nov-24
2	Scanning	Done	15-Nov-24
3	Manual Testing	Done	27-Nov-24
4	Remote Exploitation	In progress	13/12/24
5	Verification	In progress	13/12/24
6	Report	Completed	18/12/24

Open Issues / Risks / Late Activities

Open Issues: Green Critical
1. Microsoft SharePoint Authentication Bypass (CVE-2023-29357)
2. Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper)

Open Issues: Red High
1. Credential Stuffing on eresruit.gpscgroup.com
2. Cloudflare Bypass on www.glow.ee.th
3. Cloudflare Bypass on www.gpscgroup.com

Planning for Next Period

No.	Activities	Action by	Target Date
1			
2			
3			
4			
5			

Vulnerability Assessment - High

3. [Progress Bar] Old IP found from our records

RECOMMENDATIONS

DA DIGITAL ASSOCIATES CO., LTD. DA DIGITAL ASSOCIATES CO., LTD.

8

GPSC

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

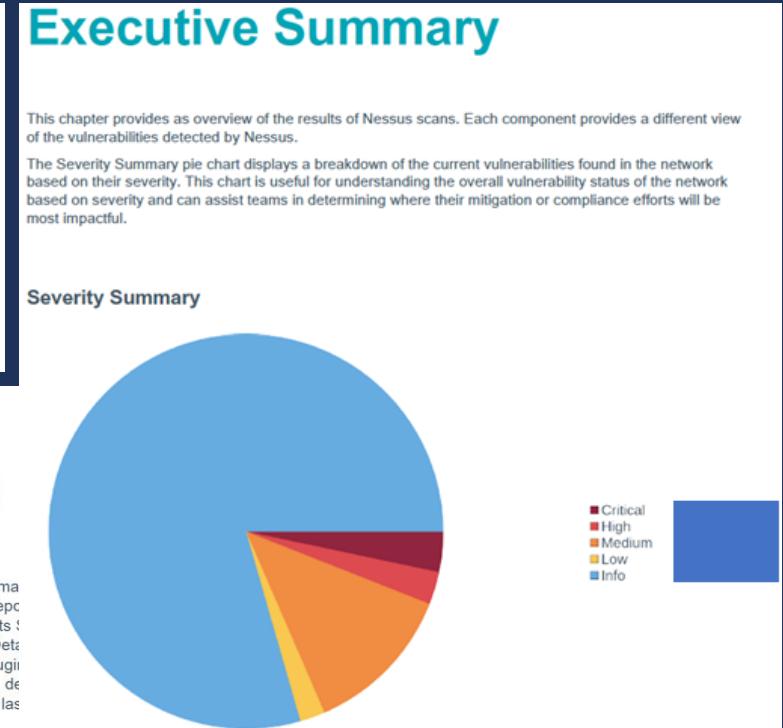
Result:

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

 **GPSC 2_2024 VA**
Generated on May 30, 2025 at 6:16 PM +07
Suphanni Rattana [zsuphanni.r]
PTT GROUP

Vulnerabilities by Host

This chapter contains an iterator that lists scanned IP addresses and detailed information about vulnerabilities detected on each. The DNS name, NetBIOS name, MAC address, repc vulnerability count, and last scan date are included for each IP address. The Results table displays the number of vulnerabilities found on that host by severity. The Results Details information for each vulnerability detected, including the plugin ID, plugin name, plugin protocol, port used, exploitability, and CPE. The plugin text, including the synopsis, description, and plugin output, is also included in the table. Lastly, the first detected and last noted for each vulnerability.



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



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
		GPSC IT / SAP ECS	9.00 – 16.15 น. 7 ชั่วโมง 15 นาที
State 2		GPSC End Users / GPSC IT Functional (Partial support by AMS)	16.15 – 18.15 น. 2 ชั่วโมง
		GPSC IT / SAP ECS	18.15 – 20.10 น. 1 ชั่วโมง 55 นาที
State 3		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

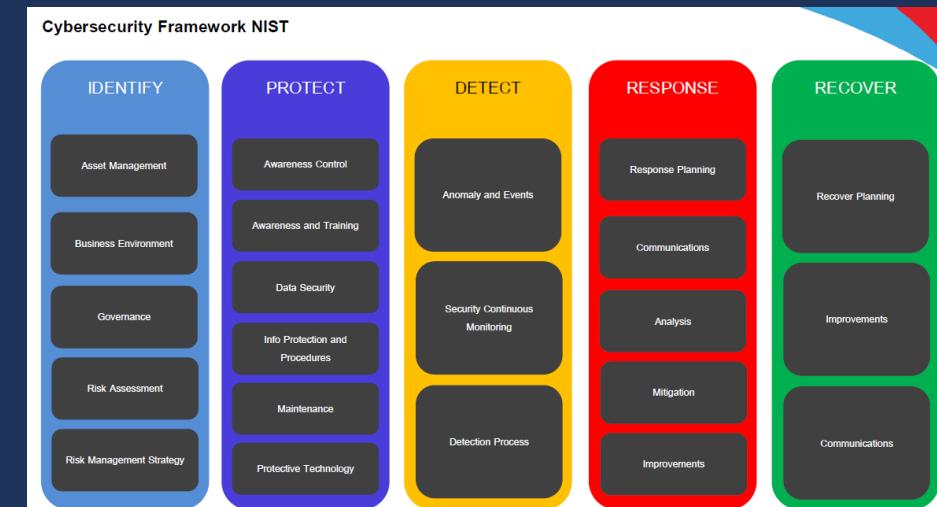
Example

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 LRR 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 ==

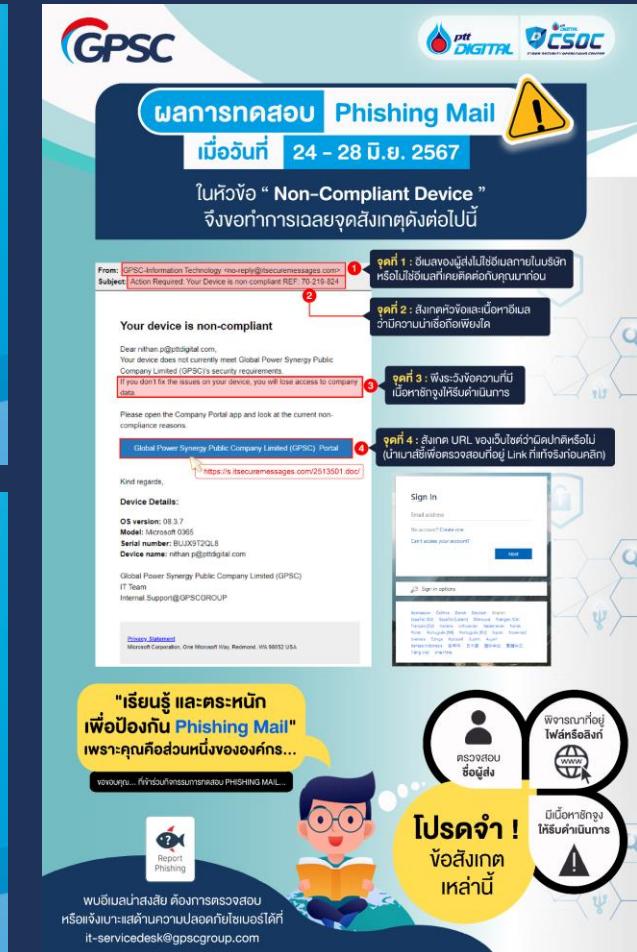
3 GPSC

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.

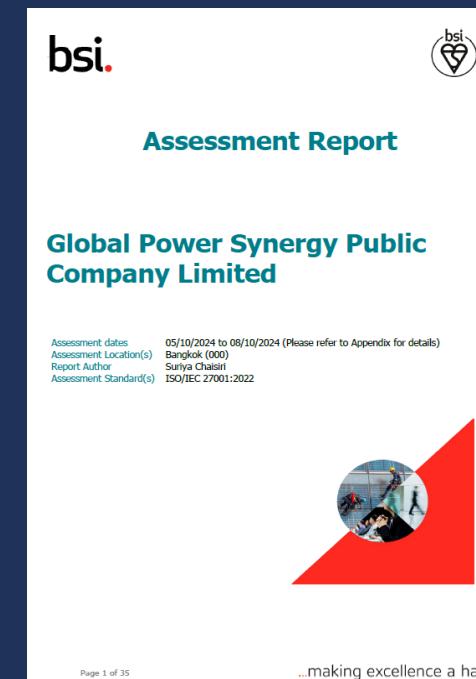
Assessor: BSI Group

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.

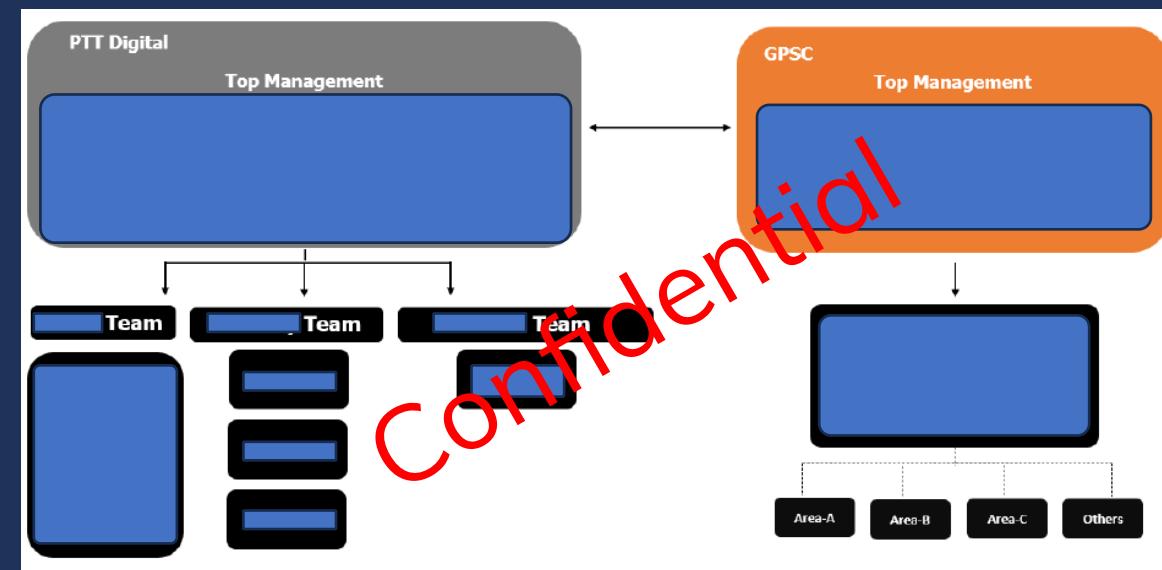
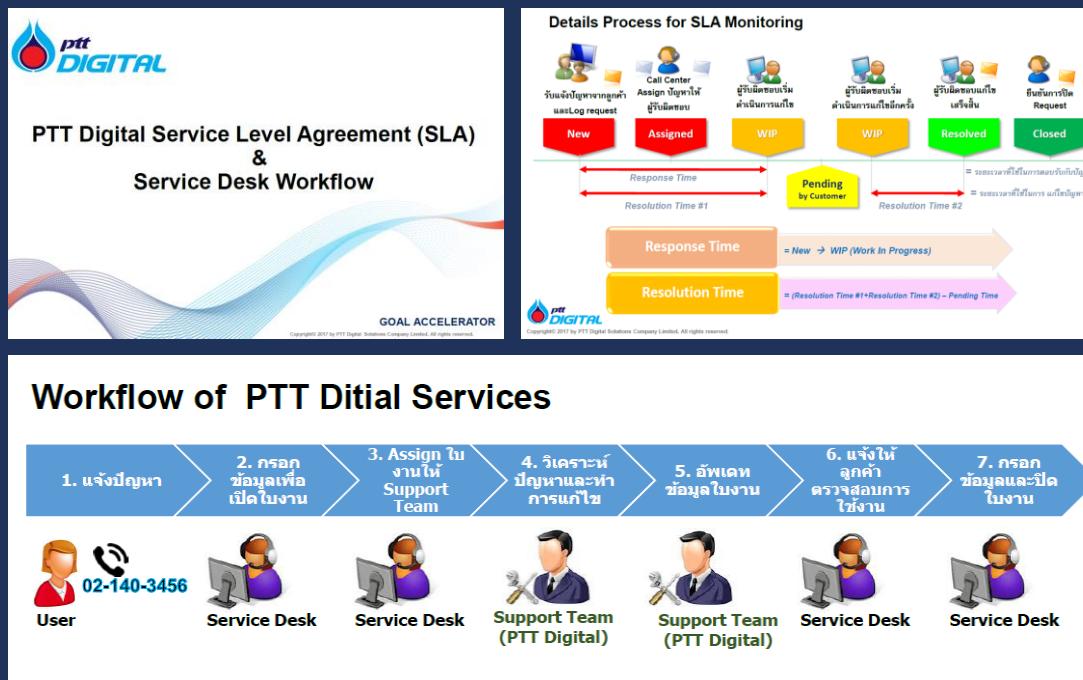


Escalation process for employees to report incidents, vulnerabilities or suspicious activities

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					
หมายเหตุเอกสาร	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			
Urgency	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">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.
----------	--	--

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 Thread

GPSC

ACT SPIRIT
The strong one inside the eagle!

10 อันดับแรกของภัยคุกคามทางไซเบอร์ที่คาดว่าจะเกิดขึ้นในปี 2030

นักคาดการณ์ 10 อันดับแรกของภัยคุกคามทางไซเบอร์ที่คาดว่าจะเกิดขึ้นในปี 2030 ได้ดังนี้

- การโจมตีหรือบุกจ�ของฟิล์วิค ที่ก่อให้ข้อมูลทางเศรษฐกิจหัวหอดิจิทัลหายไป
- การเผยแพร่เชื้อไวรัสที่ก่อให้เกิดภัยคุกคามรุนแรง
- การก่อภัยดุลและผู้คนหันมาสนใจใช้ชีวิตรักษาสุขภาพเพิ่มขึ้น ควบคู่ไปกับความต้องการที่จะรักษาสุขภาพของบุคคลทดลอง
- ความไม่สงบภายในที่ก่อให้เกิดความบุกเบิกและการใช้ชีวิตรบแบบที่ ก้าวไปในระดับภัยคุกคามและภัยพิบัติ
- การบุกรุกเพื่อหักเหล็กกล้าและควบคุมธุรกิจสร้างอาชญากรรมชั้นนำ
- การยกเว้นการค้าและคุ้มครองสิ่งที่พื้นที่อยู่ในอวกาศ
- การคุกคามแบบแฮมม์มอน ที่จะจ่อให้เกิดอุบัติเหตุร้ายแรงที่สุด
- การหักเหล็กกล้าในไซเบอร์และภัยคุกคามทางไซเบอร์
- ผู้ให้บริการเทคโนโลยีหักเหล็กกล้าและภัยคุกคามที่มีความรุนแรงที่สุด
- การใช้ปุ๋ยทางเคมีซึ่งเป็นภัยคุกคามที่ดี ทั่วไปเกิดปัญหาของอาชญากรรม

Kaspersky เผยว่า

kaspersky

ในประดิษฐ์ Kaspersky ผู้ให้บริการด้านความปลอดภัยก้าวข้ามไปยังระดับโลก ล้ำหน้าเดียวใน 2 ปี นับตั้งแต่ก่อตั้งมาจนถึงปัจจุบัน ทั่วโลกกว่า 17 ล้านเครื่องที่ก้าวเดินบนแพลตฟอร์มที่ได้รับการยอมรับ ที่ก่อให้เกิดภัยคุกคามที่มีความซับซ้อน กับอาชญากรรมทางไซเบอร์ที่เพิ่มขึ้น พบการร้องขอเรื่อง และเสียดายของผู้เชี่ยวชาญด้านอาชญากรรมของมนุษย์ผ่านเว็บไซต์ของบ้านต่างๆ รวมทั้งอาชญากรรมสูงสุด 163,091 รายการสร้างความห่วงโซ่ยืดยาวนานถึง 27,300 ล้านนาที

McKinsey คาดการณ์ว่า

McKinsey & Company

McKinsey บริษัทที่ปรึกษาด้านภัยคุกคามและอาชญากรรมทางไซเบอร์ในอุตสาหกรรม Cybersecurity ในอุตสาหกรรม 2025 คาดว่ามีการใช้จ่ายเพิ่ม 1015 พันล้านดอลลาร์ ในบริการด้าน Cybersecurity ค่าใช้จ่ายที่เพิ่มขึ้นก้าวตามจักษุการประเมินว่าจะมีการเติบโตเพิ่มขึ้นประมาณ 15% ต่อปี และคาดการณ์ว่าตัวเลขจะเพิ่มขึ้นอีก 100 พันล้านดอลลาร์ภายในปี 2030 ภาคอุตสาหกรรมที่คาดว่าจะเติบโตเร็วที่สุด คือสินค้าและบริการที่เกี่ยวกับการเงินและการค้าปลีก ตามที่คาดการณ์ว่าจะมีการเติบโตเพิ่มขึ้น 10%

Global Risk Report วิเคราะห์เป็นความเสี่ยงต่อ ๆ

Global Risk Report 2023 ของ World Economic Forum ได้วิเคราะห์เป็นประเด็นความเสี่ยงต่อๆ กันที่มีความรุนแรงและรุนแรงที่สุด ซึ่ง 1 ใน 10 เรื่องที่มีความเสี่ยงสูงสุดในปี 2025 และปี 2030 คืออาชญากรรมทางไซเบอร์และอาชญากรรมที่เกี่ยวข้องกับการเงินที่มีความเสี่ยงต่อความมั่นคงทางโลก ดังนั้นองค์กรต่างๆ จึงต้องตระหนักรู้และเตรียมพร้อมรับมือกับภัยคุกคามที่คาดว่าจะเกิดขึ้นในระยะยาว

from: World Economic Forum, Kaspersky, McKinsey, ENISA

AI-Based Predictive Social Engineering

Information security awareness training (3/4)

Zero Trust to reduce incident

AI for Power Industry

10 อันดับการใช้แอปพลิเคชัน AI ในอุตสาหกรรมพลังงาน	
ในปัจจุบัน AI มีส่วนในการเปลี่ยนแปลงนิเวศการดำเนินธุรกิจพลังงาน โดยมีส่วนต่างๆ ที่ปรับเปลี่ยนไป เช่น การรักษาความปลอดภัยภายในไฟฟ้าห้ามดับ เพื่อการเข้าถึงเครื่องขับตัวการปฏิบัติภารกิจที่มีประสิทธิภาพ อิ่งยั่งและเพิ่มความปลอดภัยแก่ผู้ใช้งาน	
การใช้ AI ในอุตสาหกรรมพลังงาน 10 อันดับเดียวกัน	
1	Smart Grids: เป็นเครือข่ายการจ่ายไฟฟ้าที่ใช้ AI ในการคุมการผลิตแบบ การใช้ไฟฟ้าอัตโนมัติที่มีข้อมูลในอิฐดู: Real Time
2	Demand Response Management (DRM): การจัดการการตอบสนอง ความต้องการของลูกค้าเชิงบันทึกยุคใหม่ที่มีประสิทธิภาพการใช้ไฟฟ้า โดยใช้ AI เมื่อใดก็อย่างเชิงได้ลดระดับภาระผู้ให้บริการและผู้รับบริการ
3	Predictive Maintenance: การบำรุงรักษาโดยใช้ AI ในการติดตามผู้รับบริการน้ำยาใน โรงงานที่มีแนวโน้มเสื่อมเสื่อมได้รับการบำรุงรักษาอย่างต่อเนื่อง
4	Renewable Energy Forecasting: การพยากรณ์พลังงานทดแทนเช่นพลังงานแสงอาทิตย์ AI คาดการณ์การเพิ่มพลังงานของบ้านเรือนหรือที่พักอาศัย ฯ เช่น ถนนและแสงอาทิตย์
5	Energy Storage: ใช้ AI เพื่อประยุกต์ใช้การจัดเก็บพลังงานบ้านเรือนเพื่อจ่าย ไฟฟ้าช่วงเวลาจากปีวันต่อต่อ ฯ เช่น อุปกรณ์ อุปกรณ์ และเครื่องจักรในอิฐไฟฟ้า
6	Carbon Capture, Utilisation, and Storage (CCUS): กรณีการห้ามการปลด การปลดปล่อย CO ₂ และการรักษาอิฐในห้องน้ำห้องน้ำ AI ในการรับรู้ที่เหมาะสม กับอุตสาหกรรมการจัดการอิฐที่ดีที่สุด
7	Energy Trading: การประยุกต์ใช้ AI วิเคราะห์การเปลี่ยนแปลงของตลาด การจ่ายไฟฟ้าทั่วโลก บริการความต้องการและผลิตภัณฑ์ที่เปลี่ยน ของตลาดในอิฐอุตสาหกรรมพลังงาน ให้อยู่ในสถานะการค้าปัจจุบัน Portfolio การลงทุนในห้องน้ำห้องน้ำ
8	Smart Homes and Buildings: การต่อตัวอิฐกับบ้านและอาคาร ผ่านระบบ AI วิเคราะห์การใช้จ่ายไฟฟ้า ฯ เช่น ถนนบริการอิฐของอุตสาหกรรม จะช่วยลดการใช้ไฟฟ้าและลดต้นทุน
9	Oil and Gas Exploration: บนอิฐของ AI ในการค้นหาร่องรอยน้ำมันและแก๊ส ด้วยการวิเคราะห์ข้อมูลธรณีวิทยาที่มีอยู่ สามารถระบุร่องรอยน้ำมันและแก๊ส ที่มีอยู่ในอิฐที่ดีที่สุด
10	Nuclear Power Plant Monitoring: ดูแลและรักษาอิฐไฟฟ้าอย่างต่อเนื่องและมีประสิทธิภาพ โดยใช้ AI ในการตรวจสอบระบบความปลอดภัยให้ได้มาตรฐานสูง ผู้ดูแล: วิเคราะห์ปัญหาอิฐ ในโรงงาน 24 ชั่วโมง ระบบแจ้งเตือนเมื่อสิ่งที่ไม่ดี

AI Energy Storage

Computer Emergency Response Team (CERT)




ความสำคัญของ

Computer Emergency Response Team (CERT)

ต่อการรักษาความปลอดภัยทางไซเบอร์

Computer Emergency Response Team หรือ CERT เป็นหน่วยงานที่รับผิดชอบในการดูแลและดูแล รักษาความปลอดภัยของระบบเครือข่ายด้านความปลอดภัยที่มีความสำคัญ เช่น ธนาคาร รัฐบาล วิสาหกิจ และอุตสาหกรรมต่างๆ ที่มีภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง ทั้งนี้ เพื่อ การป้องกันและลดความเสี่ยง ภัยคุกคาม และการแก้ไขปัญหาที่อาจเกิดขึ้น ให้กับผู้ใช้บริการ ที่สำคัญที่สุด คือ การเฝ้าระวัง ติดตาม และจัดการภัยคุกคาม ที่อาจส่งผลกระทบต่อระบบและข้อมูลทางไซเบอร์ ของประเทศ ให้สามารถรับมือและจัดการภัยคุกคาม อย่างมีประสิทธิภาพ ทั้งนี้ ยังช่วยให้ผู้ใช้บริการ สามารถมั่นใจได้ว่า ข้อมูลและระบบของตน ปลอดภัย ไม่ถูกขโมย หรือถูกโจมตี

ไทยในประเทศไทยของไทยของ CERT ที่ได้รับการเชื่อมต่อ นี้ ทั้งหมด 10 หน่วยงาน เช่น



ศูนย์ประสานการรักษาความปลอดภัยของประเทศไทย (MOPDCSIRT)
 ศูนย์ประสานงานการรักษาความปลอดภัยของประเทศไทย (TBCERT)
 ศูนย์ประสานการรักษาความปลอดภัยของประเทศไทย (Energy CERT)

CERT หรือ Computer Emergency Response Team

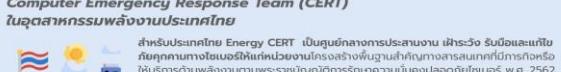
เป็นเครือข่ายของสถาบันที่มีภารกิจในการจัดการความปลอดภัยของซอฟต์แวร์และระบบการประมวลผล (Software Engineering Institute – SEI) หลังจากที่สถาบัน Carnegie Mellon



และเป็นผู้เชี่ยวชาญในการจัดการความปลอดภัยของระบบและเครือข่าย ที่มีภารกิจในการเฝ้าระวัง ติดตาม และจัดการภัยคุกคาม ที่อาจส่งผลกระทบต่อระบบและข้อมูลทางไซเบอร์ ของประเทศไทย ให้สามารถรับมือและจัดการภัยคุกคาม อย่างมีประสิทธิภาพ ทั้งนี้ ยังช่วยให้ผู้ใช้บริการ สามารถมั่นใจได้ว่า ข้อมูลและระบบของตน ปลอดภัย ไม่ถูกขโมย หรือถูกโจมตี

Computer Emergency Response Team (CERT)

ในประเทศไทย



สำหรับประเทศไทยของไทยของ CERT เป็นกลุ่มของสถาบันที่มีภารกิจในการจัดการความปลอดภัยของระบบและเครือข่าย ที่มีภารกิจในการเฝ้าระวัง ติดตาม และจัดการภัยคุกคาม ที่อาจส่งผลกระทบต่อระบบและข้อมูลทางไซเบอร์ ของประเทศไทย ให้สามารถรับมือและจัดการภัยคุกคาม อย่างมีประสิทธิภาพ ทั้งนี้ ยังช่วยให้ผู้ใช้บริการ สามารถมั่นใจได้ว่า ข้อมูลและระบบของตน ปลอดภัย ไม่ถูกขโมย หรือถูกโจมตี

หน่วยงาน CERT ในต่างประเทศ และตัวอย่างหน่วยงานที่สำคัญ

ใน 2014 ของไทยของไทยของ CERT เป็นกลุ่มของสถาบันที่มีภารกิจในการจัดการความปลอดภัยของระบบและเครือข่าย ที่มีภารกิจในการเฝ้าระวัง ติดตาม และจัดการภัยคุกคาม ที่อาจส่งผลกระทบต่อระบบและข้อมูลทางไซเบอร์ ของประเทศไทย ให้สามารถรับมือและจัดการภัยคุกคาม อย่างมีประสิทธิภาพ ทั้งนี้ ยังช่วยให้ผู้ใช้บริการ สามารถมั่นใจได้ว่า ข้อมูลและระบบของตน ปลอดภัย ไม่ถูกขโมย หรือถูกโจมตี



กูรู : thaiscert, MDE, techtarget, cisa, BBC

Information security awareness training (4/4)

Industrial Transformation through Digital Twin




การปฏิรูปอุตสาหกรรมพลังงาน ด้วยเทคโนโลยี *Digital Twin*

การใช้งาน Digital Twins ในอุตสาหกรรมพลังงาน

Distribution and Storage of Energy

วิธีการนำดิจิทัลและเทคโนโลยีเข้ามายังอุตสาหกรรมพลังงาน ที่มีประสิทธิภาพมากขึ้น

Analysis of Energy Consumption

ตรวจสอบและแก้ไขปัญหาเบื้องต้นที่เกิดขึ้น ช่วยให้สามารถใช้พลังงานได้ดีขึ้น

Distribution and Management of the Grid

โครงสร้างไฟฟ้าแบบเรียกน้ำ回去ได้ตรวจสอบข้อมูลของเครื่องจักรที่อยู่ในระบบ และการจัดการพลังงานที่มีประสิทธิภาพ

Optimization of Renewable Energy

วิธีการนำดิจิทัลมาใช้ในการติดตั้งเครื่องจักรที่ต้องการ เพื่อเพิ่มประสิทธิภาพ ในการจัดการพลังงาน ไม่ว่าจะเป็นพลังงานแสงอาทิตย์ ลม น้ำ หรือไอน้ำ

Improving Safety Procedures

วิธีการนำดิจิทัลมาใช้ในการติดตั้งเครื่องจักรที่ต้องการ เพื่อเพิ่มประสิทธิภาพ ในการจัดการพลังงาน ไม่ว่าจะเป็นพลังงานแสงอาทิตย์ ลม น้ำ หรือไอน้ำ

ตัวอย่างการดำเนินงานที่สำคัญในอุตสาหกรรมพลังงาน

บริษัทก่อสร้างพลังงาน

เพิ่มประสิทธิภาพการจัดการ
ด้านพลังงาน

ลดมลพิษการปล่อยก๊าซเรือนกระจก
ได้ด้วยเทคโนโลยี

บริษัทก่อสร้างพลังงาน

ใช้เทคโนโลยี Digital Twins
เพื่อเพิ่มประสิทธิภาพ Echo

ควบคุมมลพิษการปล่อยก๊าซเรือน
กระจกได้ด้วยเทคโนโลยี

ที่มา: Forbes, toobler, eonenergy

PDV - Cybersecurity Audit 009/67

ห้องปฏิบัติการด้านความปลอดภัยไซเบอร์

Cloud Computing in Energy Industry

Cybersecurity Prevention

Ransomware Attacks Prevention

การป้องกัน

Ransomware Attacks

ในอุตสาหกรรมภาคพลังงาน

การโจมตีด้วย Ransomware ในธุรกิจพลังงานเป็นภัยเรื้อรังเดินที่สุดคุณและผู้ผลิตของอุตสาหกรรมที่มีส่วนร่วมในห่วงโซ่อุปทานซึ่งต้องการข้อมูลลับซึ่งสำคัญมากที่สุด เช่น แผนผังและลักษณะของสถานที่ สามารถถูกใช้เพื่อโจมตีอุปกรณ์และข้อมูลที่สำคัญมาก เช่น ท่อส่งน้ำและไฟฟ้า ทำให้เกิดการล้มเหลวของอุตสาหกรรมและส่งผลกระทบต่อชีวิตประจำวันของผู้คน

ผลกระทบหรือความเสี่ยงหากที่เกิดขึ้นกับธุรกิจพลังงานจาก Ransomware Attack

การหยุดงาน: ข้อห้อง
การดำเนินการของอุตสาหกรรมที่สำคัญที่สุดที่ต้องดำเนินการอย่างต่อเนื่อง
และควบคุมการผลิต
หยุดการทำงาน เช่น
การผลิตเชื้อเพลิงน้ำมันและก๊าซ ที่มีผลต่อ
ไฟฟ้าในบ้านเรือน ที่มีผลต่อ

ความเสี่ยงที่มีภัยการเข้า
บุกรุกของผู้โจมตีที่ต้องการ
เข้าถึงข้อมูลเชิงลึก เช่น
โครงสร้างของระบบ และข้อมูล
ในการดำเนินการ เช่น บัญชี
และการตั้งค่าของอุปกรณ์

ความเสี่ยงหากต้องรีบเชื่อมต่อ
เครือข่ายที่ไม่ปลอดภัย
อาจส่งผลให้เกิดภัย
ทางไซเบอร์และสูญเสีย
การรักษาความเรียบร้อย

ความเสี่ยงต่อความเป็นส่วน
ของอุตสาหกรรม ที่ต้องดำเนินการ
ที่ต้องให้ผู้รับเหมาต้องลง
ของจดหมายคุณภาพที่ต้องดำเนิน
การและต้องรักษาความเรียบร้อย
และสิ่งแวดล้อมของประเทศ

แนวทางการรับมือหรือแก้ไข Ransomware Attack

การป้องกันเมือง
ป้องกันระบบปฏิบัติการและซอฟต์แวร์เพื่อ
ลดความเสี่ยงให้ต่ำที่สุดโดยไม่ได้รับผลกระทบ
และเข้มแข็งของข้อมูลเช่น AI และ
Machine Learning เพื่อระบุและตัดสินใจ
ต่อสิ่งที่ภัยคุกคามที่อาจเกิดขึ้น

การฝึกอบรมบุคลากร
การอบรมบุคลากรที่เกี่ยวกับการรับมือกับภัยคุกคาม
ที่มีอยู่ เช่น AI และ
Machine Learning เพื่อให้สามารถตัดสินใจ
ต่อสิ่งที่ภัยคุกคามที่อาจเกิดขึ้น

แผนการตอบสนองเหตุการณ์
สร้างแผนการตอบสนองเหตุการณ์ที่มีประสิทธิภาพและยืดหยุ่นในการรับมือ
ภัยคุกคามในทุกๆ สถานที่การดำเนินการ
เป็นไปอย่างต่อเนื่องเพื่อรับมือกับภัยคุกคามที่อาจเกิดขึ้น

การรับรู้ความเสี่ยงของภัยคุกคาม
รับรู้เกี่ยวกับแนวโน้มของภัยคุกคามและองค์กร
ความปลอดภัยที่ต้องการเพื่อป้องกันภัยคุกคาม
เช่น AI และเครื่องมือของบุคคล

ตัวอย่างการโจมตีจาก Ransomware!!!

Norsk Hydro ปรับปรุงสิ่งงานด้านไซเบอร์ด้วยวิธีการและเครื่องมือที่มีประสิทธิภาพมากขึ้น หลังจากที่มีภัยคุกคาม ransomware ในปี 2019 ได้รับผลกระทบอย่างรุนแรง ทำให้ต้องจ่ายเงินค่าฟื้นฟูและต้องจ่ายเงินเพื่อจัดการกับภัยคุกคามในคราวนี้

Enel Group บริษัทไฟฟ้าอิตาลีได้รับผลกระทบโดยตรงจากการโจมตี ransomware ในปี 2020 ที่ทำให้สิ่งงานเชิงโครงสร้างและอุปกรณ์ของอุตสาหกรรมพลังงานเสื่อมและสูญเสียไปอย่างมาก ทำให้ต้องจ่ายเงินค่าฟื้นฟูและต้องจ่ายเงินเพื่อจัดการกับภัยคุกคามในคราวนี้

ที่มา : CNN, BBC

PDV-Cybersecurity ฉบับที่ 012/67

นับแต่เดือนตุลาคม 2567 ถึงเดือนกุมภาพันธ์ 2568

Thank You

