isentia
AUTHOR: No author available SECTION: STARBIZ PAGE: 4,5 PRINTED SIZE: 1585.00cm² REGION: KL
MARKET: Malaysia PHOTO: Full Color ASR: MYR 80,074.00 ITEM ID: MY0061521037

25 NOV, 2024

How secure is M`sia`s energy value chain?

The Star, Malaysia

How secure is M'sia's energy value chain?

Cyberthreat actors can range from nation-state adversaries, who seek to disrupt the critical infrastructure of their foes (and allies), to hacktivists who seek to make political statements.

THERE used to be a division between the energy company's information technology (IT) and operational technology (OT) networks. However, the digitalisation of generation-transmission-distribution-retail systems has seen the convergence of these ecosystems.

While making the organisation more efficient and responsive to stakeholder expectations, it has a downside. The integration of the ecosystems presents a significantly enlarged playground for cyberthreat actors to play hit-and-run games that are nefarious in intent and outcomes.

What is alarming is the rise in the frequency and intensity of such cyberthreats and attacks in recent years.

This has required the energy sector to scrutinise its readiness in the face of potential cyberattacks, or in some unfortunate cases, in the wake of one. While every part of the value chain is vulnerable, what is of concern is the OT space, which is not as secure as IT. This has now become the focus of energy companies.

Energy Malaysia spoke to Rahayu Ramli, Head of Cyber Strategy & Architecture, Petroliam Nasional Bhd (PETRONAS), who provided insights on how PETRONAS and the energy sector as a whole are securing themselves against existing and oncoming cyberthreats.

"The energy industry has been a geo- and socio-political tool for decades, highlighting the influence of the industry on the economy, society and way of life.

"The rise of cyberwarfare as a component of national and private arsenals has only amplified the issue, moving from field wars such as in the Gulf States in the nineties to guerrilla tactics in cyberspace today due to pervasive industry digitalisation," said Rahayu.

In the complex energy sector, technology can be divided primarily into IT (for example, laptops, mobile devices, servers, cloud and similar) and OT (for example, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Supervisory Control and Data Acquisition System (SCADA), Industrial Control Systems (ICS), Distributed Control Systems (DCS), Human Machine Interfaces (HMIs) and similar.

Historically, these environments were kept mostly separate. However, the industry is seeing the lines blurring between IT and OT with the increased reliance on digital tools, the cloud, and the growing use of remote operations.

There is a definitive increase in the use of Internet of Things (IoT) and robotics, the sharing of OT data, the implementation of ruggedised mobile devices and personal wearables – all extending beyond what used to be a relatively static OT security perimeter.

Unfortunately, the convergence of IT and OT ecosystems is also potentially a wonderland of attack vectors and entry points into systems of varying criticality and importance.

Cyberthreat actors can range from nation-state adversaries, who seek to disrupt the critical infrastructure of their foes (and allies), to hacktivists who seek to make political statements about the environment, economics or society in general.

OT space vulnerability

In many energy companies, there is a re-examination of the segregated approach by which OT landscapes have been previously designed and protected. "IT security has been an aspect of technology operations for decades. On the other hand, OT cybersecurity as a specific practice is a relatively new focus," said Rahayu.

"As such, there is renewed interest to ramp up security in the OT space, with new startups, products and investment channelled towards mitigating existing and oncoming cyberthreats. It is an exciting but also an unpredictable space to be in at the moment."

Besides external factors, internal ways of working may also contribute to the vulnerabilities within the connected IT and OT ecosystem, where system availability is critical and downtime avoidance is paramount. While digital transformations have spurred innovation and accelerated technological advances, the speed of application and pressure of delivery has often caused system security to take a back seat.

"Eventually, it is addressed but often after a system is live and operational, and in some unfortunate cases, only after a breach or incident has occurred," pointed out Rahayu.

Additionally, increased digitalisation across a supply chain of vendors and partners is creating flexibility and options in products and services. The flip side is that it expands the exposure to unfortunate breaches or incidents, starting at one supplier and cascading down the network of companies and users.

Polycrisis scenario

The "Global Risks Report 2023" published by the World Economic Forum introduced the term "polycrisis", which translates to "a cluster of related global risks with compounding effects, with an overall impact that exceeds the sum of each part".

The energy industry is no stranger to this scenario, given its volatility and uncertainty in recent years resulting from the energy transition and rapid digitalisation.

The global risk scenario also includes cyber risks that are borderless. The industry as a whole expects cyberthreats to continue to increase against IT and OT assets and operations, as energy companies become more reliant on connected digital technologies to operate.

Individual companies have embarked on their own journey to reevaluate and improve their security posture, acknowledging that the support required to do so is not purely driven by technology, but more importantly, must also be supported by education of the entire organisation, and a continuous review and revamp of its security capability and requirements.

The work cannot be done in silo either. It requires support and collaboration across the industry to minimise blind spots that may affect everyone in the industry and the communities that interact with them.

Rahayu said, "At PETRONAS, we have various cybersecurity memoranda of understanding (MoUs) with vendors to help us better focus our efforts in designing a more secure OT technology.

"We also engage with other industry players for knowledge exchange and upskilling. In addition, we work closely with non-profits and academia to raise awareness on the importance of cybersecurity, of how it applies to our daily lives and to also scout for potential talent.

"The general aim of these types of collaboration is that the integration of the IT and OT ecosystem across people, processes and technology will eventually lead to an equilibrium of a hybrid-skilled cybersecurity workforce (within and beyond PETRONAS), creating a more sustainable loop to manage and respond to any cyberthreat that may appear on the immediate horizon," she added.

Securing the cyberspace environment

From the onset of its digital transformation journey in 2017, PETRONAS recognised the importance of establishing a cyber secure environment across the entire organisation. "It was the prerequisite for PETRONAS going digital," said Rahayu.

"As the organisation became more data-driven in decision making and needed to incorporate new and different technologies more rapidly into various portfolios, it made sure that every move was made securely. This approach became one of the cornerstones of the PETRONAS digital transformation strategy.

"It saw the establishment of the PETRONAS cybersecurity function as a single point of accountability to oversee IT and OT – to govern, steer and shape the minimum requirements to sustain the targeted level of cybersecurity maturity," she added.

PETRONAS embraces OT security through the secure-by-design approach, with cybersecurity-related requirements as part of the PETRONAS Technical Standards (PTS). It began with a focused project known as the real-time OT (RTOT) programme, to design and implement a new standard, architecture and roadmap to manage its IT and OT patch management and OT asset management in near real-time.

"Our OT footprint is large, thus we focused on assets considered to be the crown jewels of the organisation and continue to deploy this programme across our local and international sites," said Rahayu. When PETRONAS completes the initial RTOT programme, it will continue to expand secure capability into other aspects of OT.

"Identity is a complex area within OT," added Rahayu. "It is an area of particular concern given the distributed nature of our OT systems.

"While IT has always had the advantage in establishing more robust identity and access management, we are exploring ways to do the same for our OT environment and are working towards eliminating the use of shared accounts, establishing proper identity governance and ensuring secure remote access."

There is also emphasis on having a robust all-encompassing cybersecurity-governance structure.

The launch of the organisation-wide Enterprise Cyber Security Governance Framework (ECSGF) was followed by a customised OT programme in early 2023, underscoring its importance as well as its vulnerability.

As a result, cybersecurity risk assessments are now part of the Management of Change (MOC) process for both greenfield and brownfield projects to guide design in the OT environment.

These initial steps have laid the foundation for the real-time visibility of PETRONAS's assets and cyber vulnerabilities in order to remediate based on the business criticality. Meanwhile, employees and other stakeholders are continuously kept up to date on secure behaviours through the Human Firewall programme, which emphasises the need for staying alert at work, home and play.

This programme is run through a combination of training, communication and community engagements, and supported by an extensive network of cybersecurity change agents who champion the message and awareness across our business and sites.

There is also continuous staff training to ensure they have the appropriate cybersecurity knowledge to support their day-to-day work.

For example, business system owners are required to attend training on cyber risk management for the systems they oversee; lead OT focals at site are assigned training on OT cybersecurity upon joining and refreshed every two years to ensure they have the latest cybersecurity knowledge with respect to the systems that they work with.

Protecting hotspots

PETRONAS uses a risk-based approach to cybersecurity that allows it to identify critical systems effectively, thus enabling "hotspots" to be more rigorously protected, while ensuring that there are safeguards in place at every level of the company's technological (defence-in-depth) and organisational landscape.

This involves organisation-wide governance and policies as well as continuous education and awareness across the employee population.

A primary concern is the OT environment, where complex systems have a much longer lifespan and maintenance/updates require meticulously scheduled downtimes in very specific parts of the year.

This is one of the main reasons why PETRONAS has deployed the RTOT programme as a priority to enhance security practices, address potential vulnerabilities and minimise the impact of cyberthreats.

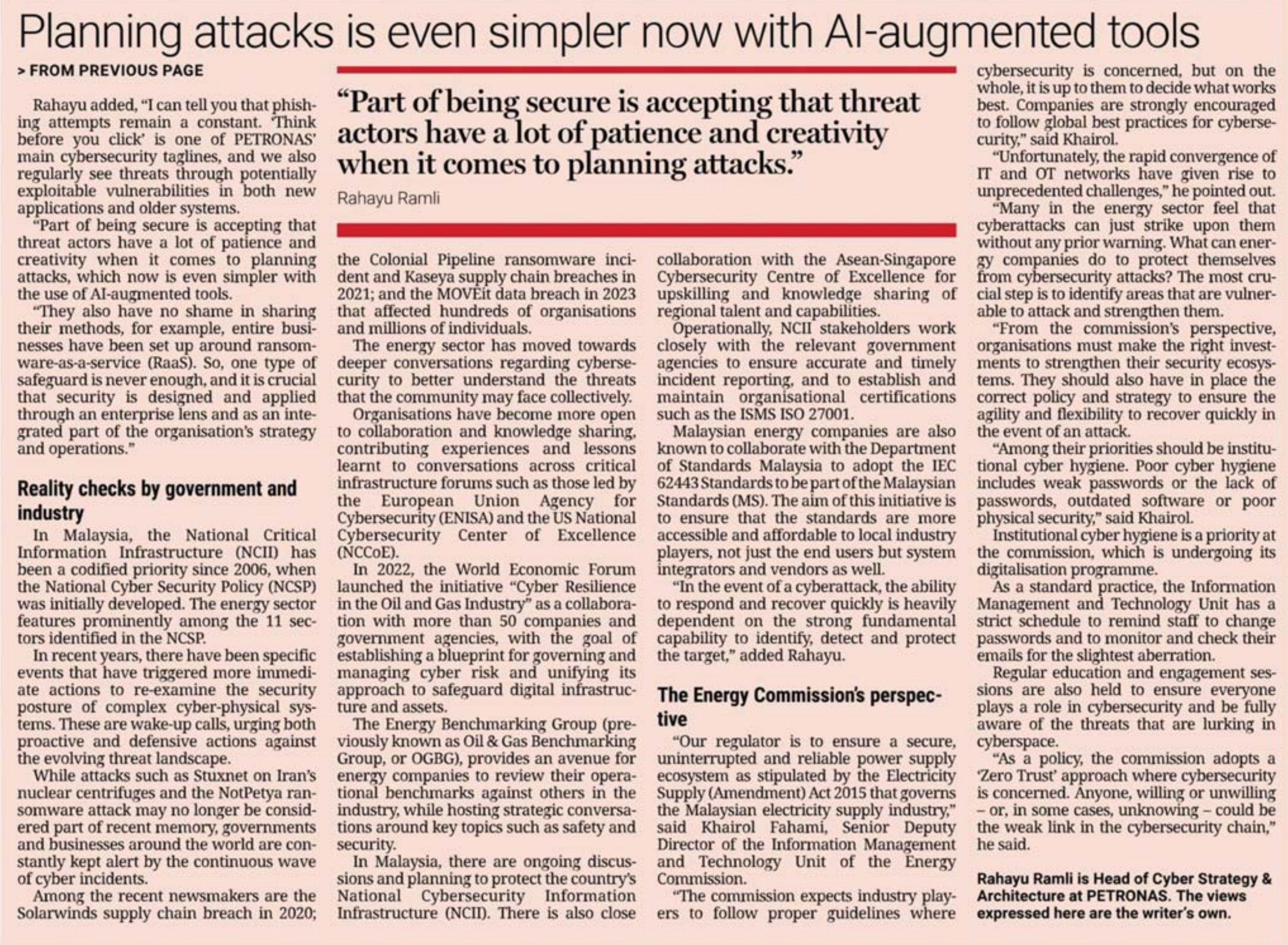
At the other end of the spectrum, it has been consistently shown that people remain one of the biggest weak points in any organisation.

Social engineering through methods such as phishing remains a primary way into a company's systems. According to the Cofense Phishing Report 2022, 67% of all phishing attempts are meant to steal login and password details from their victims.

This is so prevalent that it is estimated that more than 90% of company networks around the world can be penetrated by cybercriminals.

Breaches can occur in IT or OT in this manner, and while threat actors may not gain immediate access to a given critical system, gaining a foot in the door through an employee's login credentials may be sufficient to drop malware, trigger a ransomware attack, or stage a long-term reconnaissance programme by lurking in their victim's environment, an example of what's known as Advanced Persistent Threats (APTs), which can lead to even more malicious activity like data theft.

> SEE NEXT PAGE



Planning attacks is even simpler now with AI-augmented tools

> FROM PREVIOUS PAGE

Rahayu added, “I can tell you that phishing attempts remain a constant. ‘Think before you click’ is one of PETRONAS’ main cybersecurity taglines, and we also regularly see threats through potentially exploitable vulnerabilities in both new applications and older systems.

“Part of being secure is accepting that threat actors have a lot of patience and creativity when it comes to planning attacks, which now is even simpler with the use of AI-augmented tools.

“They also have no shame in sharing their methods, for example, entire businesses have been set up around ransomware-as-a-service (RaaS). So, one type of safeguard is never enough, and it is crucial that security is designed and applied through an enterprise lens and as an integrated part of the organisation’s strategy and operations.”

> “Part of being secure is accepting that threat actors have a lot of patience and creativity when it comes to planning attacks.”
>
> Rahayu Ramli

Reality checks by government and industry

In Malaysia, the National Critical Information Infrastructure (NCII) has been a codified priority since 2006, when the National Cyber Security Policy (NCSP) was initially developed. The energy sector features prominently among the 11 sectors identified in the NCSP.

In recent years, there have been specific events that have triggered more immediate actions to re-examine the security posture of complex cyber-physical systems. These are wake-up calls, urging both proactive and defensive actions against the evolving threat landscape.

While attacks such as Stuxnet on Iran’s nuclear centrifuges and the NotPetya ransomware attack may no longer be considered part of recent memory, governments and businesses around the world are constantly kept alert by the continuous wave of cyber incidents.

Among the recent newsmakers are the Solarwinds supply chain breach in 2020; the Colonial Pipeline ransomware incident and Kaseya supply chain breaches in 2021; and the MOVEit data breach in 2023 that affected hundreds of organisations and millions of individuals.

The energy sector has moved towards deeper conversations regarding cybersecurity to better understand the threats that the community may face collectively.

Organisations have become more open to collaboration and knowledge sharing, contributing experiences and lessons learnt to conversations across critical infrastructure forums such as those led by the European Union Agency for Cybersecurity (ENISA) and the US National Cybersecurity Center of Excellence (NCCoE).

In 2022, the World Economic Forum launched the initiative “Cyber Resilience in the Oil and Gas Industry” as a collaboration with more than 50 companies and government agencies, with the goal of establishing a blueprint for governing and managing cyber risk and unifying its approach to safeguard digital infrastructure and assets.

The Energy Benchmarking Group (previously known as Oil & Gas Benchmarking Group, or OGBG), provides an avenue for energy companies to review their operational benchmarks against others in the industry, while hosting strategic conversations around key topics such as safety and security.

In Malaysia, there are ongoing discussions and planning to protect the country’s National Cybersecurity Information Infrastructure (NCII). There is also close collaboration with the Asean-Singapore Cybersecurity Centre of Excellence for upskilling and knowledge sharing of regional talent and capabilities.

Operationally, NCII stakeholders work closely with the relevant government agencies to ensure accurate and timely incident reporting, and to establish and maintain organisational certifications such as the ISMS ISO 27001.

Malaysian energy companies are also known to collaborate with the Department of Standards Malaysia to adopt the IEC 62443 Standards to be part of the Malaysian Standards (MS). The aim of this initiative is to ensure that the standards are more accessible and affordable to local industry players, not just the end users but system integrators and vendors as well.

“In the event of a cyberattack, the ability to respond and recover quickly is heavily dependent on the strong fundamental capability to identify, detect and protect the target,” added Rahayu.

The Energy Commission’s perspective

“Our regulator is to ensure a secure, uninterrupted and reliable power supply ecosystem as stipulated by the Electricity Supply (Amendment) Act 2015 that governs the Malaysian electricity supply industry,” said Khairol Fahami, Senior Deputy Director of the Information Management and Technology Unit of the Energy Commission.

“The commission expects industry players to follow proper guidelines where cybersecurity is concerned, but on the whole, it is up to them to decide what works best. Companies are strongly encouraged to follow global best practices for cybersecurity,” said Khairol.

“Unfortunately, the rapid convergence of IT and OT networks have given rise to unprecedented challenges,” he pointed out.

“Many in the energy sector feel that cyberattacks can just strike upon them without any prior warning. What can energy companies do to protect themselves from cybersecurity attacks? The most crucial step is to identify areas that are vulnerable to attack and strengthen them.

“From the commission’s perspective, organisations must make the right investments to strengthen their security ecosystems. They should also have in place the correct policy and strategy to ensure the agility and flexibility to recover quickly in the event of an attack.

“Among their priorities should be institutional cyber hygiene. Poor cyber hygiene includes weak passwords or the lack of passwords, outdated software or poor physical security,” said Khairol.

Institutional cyber hygiene is a priority at the commission, which is undergoing its digitalisation programme.

As a standard practice, the Information Management and Technology Unit has a strict schedule to remind staff to change passwords and to monitor and check their emails for the slightest aberration.

Regular education and engagement sessions are also held to ensure everyone plays a role in cybersecurity and be fully aware of the threats that are lurking in cyberspace.

“As a policy, the commission adopts a ‘Zero Trust’ approach where cybersecurity is concerned. Anyone, willing or unwilling – or, in some cases, unknowing – could be the weak link in the cybersecurity chain,” he said.

Rahayu Ramli is Head of Cyber Strategy & Architecture at PETRONAS. The views expressed here are the writer’s own.