Towards a World-Class Energy Sector

Suruhanjaya Tenaga
Energy Commission

ENERGY

MALAYSIA

www.st.gov.my

Volume 25 | 2024

COVER STORY

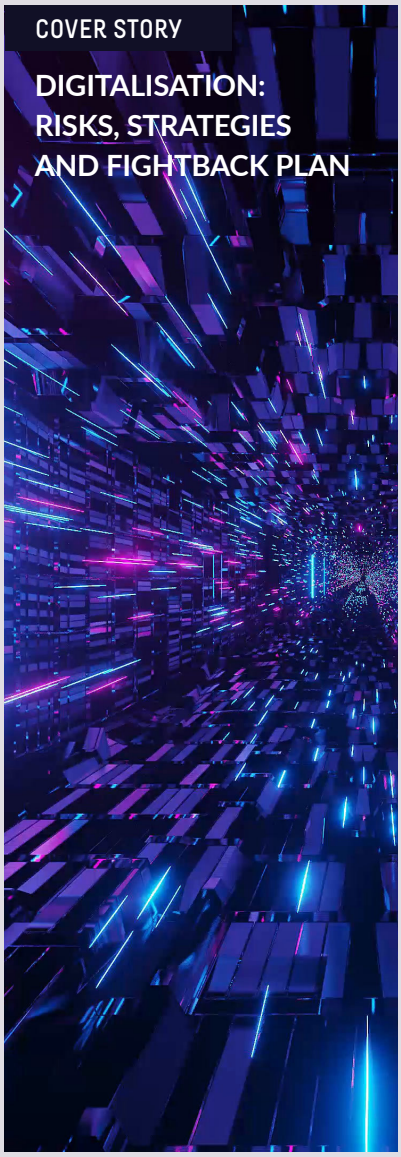
DIGITALISATION: RISKS, STRATEGIES AND FIGHTBACK PLAN

ISSN 2948-3603

Be Energy smart

VOL.25 / 2024

CONTENTS

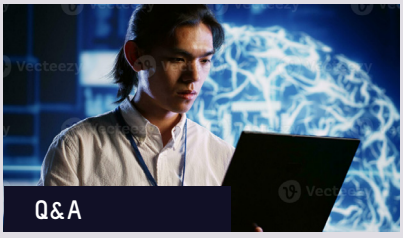


COVER STORY

DIGITALISATION: RISKS, STRATEGIES AND FIGHTBACK PLAN

REALITY CHECK

CYBERATTACKS SPIKING IN THE ENERGY SECTOR



Q&A

URGENTLY NEEDED: TALENT TO BEAT CYBERCRIMES

BEYOND BORDERS

CRITICAL INFRASTRUCTURE: A CALL TO ACTION

REGULARS

FEATURES

PUBLISHED BY
Suruhanjaya Tenaga *(Energy Commission)*
No. 12, Jalan Tun Hussein, Precinct 2,
62100 Putrajaya, Malaysia
T : (603) 8870 8500 **F** : (603) 8888 8637
www.st.gov.my

PRINTER
Dolphin Press International Sdn. Bhd. (0803493W)
No. 1, Jalan 13/118B, Desa Tun Razak,
56000 Kuala Lumpur

PUBLISHING CONSULTANT
pVm communications sdn. bhd.
www.pvmpublish.com.my

Writers
Premilla Mohanlall
Dyll Rohan Selveraj
Magella Gomes
Azizah Mohamad

ISSN : 2948-3603
ST Publication No. : ST(P)08/06/2024

THE DOWNSIDE OF DIGITALISATION

DATO' IR. TS. ABDUL RAZIB DAWOOD
Chief Executive Officer

This edition of Energy Malaysia calls for everyone and anyone using the internet to be in a state of readiness to deal with cyberthreats and attacks. Cybercrime has been on the rise since the COVID-19 pandemic, and attacks are no longer a question of "If" but "When", say the experts featured here.

This is the price to be paid for digitalisation, which has spawned an underworld of actors, comprising nation states wanting to undermine the functioning of unfriendly countries, organised syndicates seeking financial gains, even social activists wanting to make their stand.

This trend is alarming for the energy sector as it is for all other critical infrastructure sectors. Our cover story, "Digitalisation: Risks, Strategies and Fightback Plan" highlights the efforts of the Malaysian Government to protect National Critical Information Infrastructure (NCII), which includes energy, with the Cyber Security Strategy 2020-2024. This is a comprehensive plan to enhance national cybersecurity preparedness and resilience, a responsibility entrusted to the National Cyber Security Agency (NACSA).

With Malaysia priming itself to become a digital economy by 2030, it is potentially a lucrative field of easy pickings for cybercriminals. Already, some critical infrastructure companies have experienced a spate of incidents. Cybercriminals will be facing sterner action with the Cyber Security Bill that was tabled in Parliament in April this year. The Act, which some quarters consider as being long overdue, gives NACSA the legal authority to take action against cybercrimes.

To give us an insight of how grave the situation is becoming, the segment called Reality Check lists major attacks on energy infrastructure in recent years. This story entitled "Cyberattacks Spiking in the Energy Sector" is worrying. It cites a report that says that in the industrial environment, threat actors were most intensely focused on the energy sector.

The report also found that 60% of attacks were led by state-affiliated actors. Additionally, 33% were enabled by internal personnel. It is an alert for energy industry players to take a deep and hard look at plugging internal leaks and fortifying their digital defences against external assaults.

We also take a look at how other countries are protecting their critical infrastructure in the Beyond Borders segment, with the article entitled "Critical Infrastructure: A Call to Action" that takes a look at the challenges experienced in the United States of America (USA) and the European Union (EU), with suggestions of solutions that are being applied. Policymakers, regulators and equipment providers also play a central role in enhancing the cybersecurity of power systems.

In our Consumer and Special Focus segments, two lead players in the Malaysian energy industry speak up. In "How Secure is Consumer Data?", Malaysia's largest public utility Tenaga Nasional Berhad (TNB) shares how it is protecting consumer information, while at the same time, urging consumers to play their part in personal data protection, by offering a selection of tips. In the Special Focus story "How Secure is Your Value Chain?", Malaysia's national oil company PETRONAS shares how the convergence of information technology (IT) and operational technology (OT) systems, while enhancing corporate and operational efficiency, has also enlarged the cyberattack surface. While securing it is considered as an organisational responsibility, it works even better with an all-of-nation approach, involving collaborations with the Government, academic institutions, vendors and other industry players.

One of the reasons for collaboration is to address the shortage of cybersecurity professional talent, which is a global problem. The Q&A segment with the story "Urgently Needed: Talent to Beat Cybercrimes" presents the views of Dato' Ts. Dr. Amirudin Abdul Wahab, Chief Executive Officer of CyberSecurity Malaysia, who points out that cybersecurity professionals must be creative and have a deep understanding of both technology and human behaviour for their action plans to be effective.

In the Parting Shot segment's story, "Cybersecurity in the Supply Chain: Challenges & Solutions", our columnist, Rushdi Abdul Rahim, President and Chief Executive Officer of the Malaysian Industry-Government Group for High Technology (MIGHT), notes that many mid-to-small vendors and contractors believe in the notion of "security through obscurity" — that nobody would want to attack them because they are small.

What they do not seem to realise is that by attacking small businesses or "supply chain attacks", cybercriminals can gain access to large corporate organisations. In the article, Rushdi suggests various solutions to reduce supply chain vulnerabilities, which I am happy to note also includes public-private sector collaborations to address cybersecurity challenges collectively as well as the role of big energy companies in this regard.

More than anything, this issue of Energy Malaysia highlights that organisations and individuals need to allocate serious money to keep their digital world secure from cyberthreats that are growing in complexity and frequency.

Happy reading!

"Cybercrime has been on the rise since the COVID-19 pandemic, and attacks are no longer a question of "If" but "When", say the experts featured here."

NEWS FROM MALAYSIA AND AROUND THE WORLD

MALAYSIA

Energy Needs to Double in Asia, Says Prime Minister While Announcing Road Maps to Guide Malaysia

By 2030, Asia will see a 100% increase in demand for energy and meeting this challenge will be a daunting task. Dato' Seri Anwar Ibrahim, Prime Minister of Malaysia issued this caution in his keynote address at the Energy Asia Conference 2023 held in Kuala Lumpur. The conference themed "Charting Pathways for a Sustainable Asia" was attended by 3,000 delegates from 27 nations.

"Striking a balance between the energy trilemma, which are energy security, affordability, and sustainability, will be key to ensure a smoother energy transition in Asia," the Prime Minister highlighted. He also announced two roadmaps that will guide Malaysia's energy transition goals during his speech. They are the National Energy Transition Roadmap (NETR) and the Hydrogen Economy and Technology Roadmap (HETR), targeted for rollout later this year.

He said that the NETR will lay the overarching strategy and initiatives to ramp up energy transition efforts, whereas the HETR will complement NETR, by paving the way towards achieving an environmentally sustainable, long-term energy security that will be driven by technological innovation. The Prime Minister also said Malaysia would continue to see natural gas playing a pivotal role in the energy transition as it is one of the cleanest burning fossil fuels.

Source: The Petri Dish, 05 July 2023

"Striking a balance between the energy trilemma will be key to ensure a smoother energy transition in Asia."

More Malaysians Transitioning to Solar Power

Industry players believe there is an increasing demand for solar panel installations in Malaysia driven by consumer concerns over higher electricity bills, leading to a shift towards renewable energy (RE) and a reduction in installation costs. Ng Yew Weng, co-founder and Chief Operating Officer of Progressture Solar said his company has seen an increase in domestic sales, with over 60 inquiries for home solar panel installations in a week.

The Government is promoting solar energy usage through the Net Energy Metering (NEM) programme. Under this scheme, NEM users become 'prosumers' – producing and consuming energy at the same time. NEM, which allows excess PV-generated energy to be exported back to the grid on a "one-on-one" offset basis, has three categories, namely NEM Rakyat for domestic users, NEM GoMEn for Government buildings and NEM Net Offset Virtual Aggregation (NOVA) for industrial and agricultural usage.

Shamsul Bahar Mohd Nor, Chief Executive Officer of Malaysia Green Technology and Climate Change Corporation (MGTC) said due to the high demand for solar energy products, which are also categorised as green products, companies dealing in such products are encouraged to obtain MGTC's MyHIJAU certification. Registered green products and services will be listed in the MyHIJAU Directory, which is a reference for green procurement.

Source: Asia News Today, 06 July 2023

Energy Exchange to Support Renewable Energy Exports

Malaysia will launch an Energy Exchange to support the export of renewable energy (RE) to neighbouring countries, said Nik Nazmi Nik Ahmad, Minister of Natural Resources, Environment and Climate Change. "The Energy Commission is preparing a working paper on this Energy Exchange for us to approve at the Government level," he added.

"We will look at some of the available models and among the goals is to first secure enough RE to supply in the country, and then ensure we get the best value for sales abroad and allow that value to be reinvested to boost the RE sector in Malaysia," he said at the Malaysian Industrial Development Finance Berhad (MIDF) roundtable today.

To support the energy transition in the country, Malaysia should look at other sources of energy generation such as mini-scale hydropower. "We should not look at large-scale hydropower, which is quite problematic for us to carry out because of its many trade-offs," Nik Nazmi said. The Minister also emphasised Malaysia's need to look at battery storage systems that will play an increasingly pivotal role to support cheaper RE prices.

Source: Bernama, 20 July 2023

Better Returns Await CGPP Winners

Winners of the Corporate Green Power Programme (CGPP) could potentially enjoy better returns compared to the fourth cycle of the large-scale solar (LSS4) projects. MIDF Research said going by its initial ballpark estimates, CGPP could reap internal rate of returns (IRRs) in the high-single-digit levels.

This is because the initiative, which will be utilising virtual power purchase agreements, is based on a willing buyer-willing seller approach. "Under the CGPP, players are free to secure their own off-taker, hence giving better pricing power as opposed to stiff competition to supply to a single off-taker under the LSS auction mechanism," said the research firm in a report.

It added that CGPP tariffs are also likely to reflect a premium for environmental attributes like renewable energy (RE) certificates. As a benchmark, the research firm noted that the Green Electricity Tariff sold by Tenaga Nasional Berhad (TNB) was raised to 21.8 sen per kilowatt hour (kwh), effective August this year.

Meanwhile, the system's marginal price under the New Enhanced Dispatch Arrangement (NEDA) wholesale market is averaging about 25 sen per kwh as of June 2023, which is "a decently large premium to LSS4 winning bids of 18 to 20 sen per kwh for 30-50 MW packages," it said.

Earlier, the Energy Commission had announced that a total 563.42 MW under the CGPP were awarded to 22 solar power producers. There is still a balance of 236.58 MW quota of the 800 MW offered under CGPP, which received a total of 71 applications, according to the Commission. A number of listed companies were among the winners.

Source: The Star, 09 August 2023

Energy Commission Allocates 1,899 GW of Green Energy under GET Programme

A total of 1,899 GW of green energy is available for subscription when the Green Electricity Tariff (GET) programme reopens on 11 August, said the Energy Commission. The new quota is applicable for a 5-month contract period from 1 August to 31 December 2023, said a statement on Thursday.

The GET programme enables companies or industries to immediately achieve their 100% renewable power goal with the internationally-acclaimed Malaysia Renewable Energy Certificate (mREC). "The mRECs certify that every kWh of green energy purchased by a GET subscriber is uniquely identified to the particular renewable energy (RE) generation source, which in turn is connected to the national grid infrastructure and thus dispatchable to the GET subscriber," said the Commission's statement.

In addition, the GET programme provides successful GET subscribers with full exemption from the Imbalance Cost Pass-Through (ICPT) charges on their green energy utilised in their electricity bill.

First implemented in 2022, the GET programme is a strategic initiative by the Government to supply green electricity generated from renewable sources to customers of TNB who intend to reduce their carbon footprint. Last month, Nik Nazmi Nik Ahmad, Minister of Natural Resources, Environment and Climate Change announced that the tariff for the GET programme has been raised to 21.8 sen / kWh effective 1 August 2023, in line with regional green electricity retail price benchmarks.

Source: The Edge, 10 August 2023

"GET subscribers will be exempted from the ICPT charges on their green energy utilised in their electricity bill."

National Energy Awards Recognises 29 Players

The Ministry of Natural Resources, Environment and Climate Change together with the Malaysian Green Technology and Climate Change Corporation (MGTC) announced 29 winners of the National Energy Awards (NEA) 2023, selected from a total of 114 submissions. Of the 29 winners, 23 will represent Malaysia at the ASEAN Energy Awards (AEA) to be held on 24-25 August 2023.

The NEA, held annually since 2018, was set up to recognise Malaysian corporations and institutions for adopting game-changing sustainability initiatives in line with the nation's Just Energy Transition, Net Zero, and sustainable development agenda. The initiative is aligned with Malaysia's aspiration to be a net-zero greenhouse gas (GHG) emissions nation by 2050.

In his address, the Minister, Nik Nazmi Nik Ahmad, pointed out that that the Ministry organises the annual NEA as a way to raise awareness, acceptance and adoption of sustainable energy practices across industries. Malaysia, he said, requires everyone to play a part in the race to net zero.

Source: The Star, 18 August 2023

NETR Phase 2 To Focus on Biomass, Waste-To-Energy, Carbon Capture Among Others

The Government will announce on Tuesday (29 August 2023) the extension of the first phase of the National Energy Transition Roadmap (NETR), known as Phase 2, which will focus on biomass, waste-to-energy usage, Carbon Capture and Storage (CCS), and hydrogen integration, among others.

Dato' Ir. Ts. Abdul Razib Dawood, Chief Executive Officer of the Energy Commission said the roadmap will be "more than policy" covering across sectors, with discussions on "more actionable items" after the first phase was announced in July 27. "In the second phase of the NETR, we will discuss more actionable items on how to reach the 2050 targets," he said at the dialogue session on "Forward-thinking Policies and Regulations that Shape the Energy Transition" at the Energy Transition Conference 2023 organised by Tenaga Nasional Berhad (TNB).

He highlighted that the primary challenge in the energy transition is to increase the renewable energy (RE) capacity, pointing out that solar projects are currently the only viable option in Malaysia, while other forms of RE are still in their early stages of development.

"We need at least 2.5 GW RE installation per year to achieve 70% of RE in the power mix by 2050. But first the grid has to be ready to take on these RE projects," said Dato' Razib. On CCS and hydrogen, he said that while it is still at a nascent stage, it is essential to get the infrastructure ready.

"We have to start somewhere, maybe we need a Government funding system to begin with. We aspire to be a hydrogen hub for this region. For CCS, PETRONAS has already embarked on it, but it is still at an early stage and also expensive. But we need to be ready," he said.

Phase 1 of the NETR that was announced on 27 July 2023 identified six key energy transition levers, namely, energy efficiency, RE, hydrogen, bioenergy, green mobility, and carbon capture, utilisation and storage. It also saw 10 flagship projects and 50 initiatives being announced.

Source: The Star, 18 August 2023

Prime Minister Launches Energy Transition Roadmap, Including RM2 Billion Facility

Dato' Seri Anwar Ibrahim, Prime Minister of Malaysia launched the National Energy Transition Roadmap (NETR) on 29 August 2023, with Putrajaya allocating a RM2 billion "seed fund" as an energy transition facility.

Speaking at the Tenaga Nasional Berhad's Energy Transition Conference, Dato' Seri Anwar said while Malaysia's move to embrace sustainability has been gaining momentum, there is a need to ensure energy is affordable and secure.

"The NETR will drive the creation of high-paying job opportunities and boost domestic and foreign investment participation while ensuring the continuity of Malaysia's foreign energy supply. Ultimately, this will make Malaysia a regional leader in the clean energy industry."

Dato' Seri Anwar, who is also Finance Minister, said an investment of at least RM1.2 trillion is needed between 2023 and 2050 to enable a responsible energy transition. He also said the National Energy Council will be activated to ensure holistic energy planning and policy development, while monitoring the progress of the roadmap.

Dato' Seri Anwar said the champions of the projects and initiatives under the NETR are from the public sector, Government-Linked Companies (GLCs) and industry players, signifying a whole-of-Malaysia approach.

Putrajaya will also launch a major retrofit programme to enhance energy efficiency in Government buildings. A platform for Energy Service Companies (ESCO) will be established to serve as an intermediary that pools Government building retrofitting projects and encourages public-private coordination in the ESCO market, he said.

Source: FMT News, 29 August 2023

Sarawak Energy's Battery Energy Storage Plan

Sarawak Energy Berhad has embarked on a pilot 60 MW battery energy storage system (BESS) at its Sejingkat coal-fired power plant here. According to Tan Sri Abang Johari Tun Openg, the Premier of Sarawak, BESS will provide critical grid services, such as peak shaving as well as spinning reserve and optimise generation assets to minimise carbon emissions associated with traditional power generation.

"It will also help mitigate intermittency issues associated with variable renewable energy (RE), such as solar, making them more viable," he said when opening the Sustainable and Renewable Communities Forum 3.0 in Kuching. Abang Johari said Sarawak Energy has the potential to plant up to 1,500 MW of solar capacity based on its generation and network capacity until 2031.

Source: The Star, 11 September 2023

Malaysia's Largest Renewable Energy Power Plant Commences Operation

Malaysia's largest renewable energy (RE) power plant at Bukit Tagar Enviro Park (BTEP), Hulu Selangor, Selangor with a capacity of 12 MW has commenced operations. The Waste to Energy (WtE) plant is one of the methods for treating solid waste while generating new RE.

BTEP is the largest power generation plant from landfill gas in Malaysia. It can convert methane gas from solid waste into RE, channelling approximately 339 million kilowatt-hours (kWh) of electricity to the national grid.

The initiative is in line with the country's goal of achieving 40% RE contribution to national power generation by 2035, of which solid waste is one of the contributors to the goal through WtE technology. The 12 MW plant is also in line with the Government's policy to develop at least one WtE-concept solid waste management facility in each State in Malaysia.

Source: The Star, 20 September 2023

Parliament Passes Energy Efficiency and Conservation Bill 2023

The Parliament today passed the Energy Efficiency and Conservation Bill 2023 to regulate the efficient consumption and conservation of energy in the country. Nik Nazmi Nik Ahmad, Minister of Natural Resources, Environment and Climate Change said the Bill, among others, would strengthen the legal framework related to energy efficiency and conservation practices to ensure full involvement at various levels.

"The Bill closely aligns itself with the energy transition initiative towards achieving net-zero greenhouse gas (GHG) emissions by energy-related sectors by 2050 and it is also one of the key initiatives under the National Energy Transition Roadmap (NETR). I believe that the Bill will enable the Government to make more effective long-term energy development plans in all identified sectors and optimise investment costs in the construction of electric power generation facilities," he said at the tabling of the Bill.

"The Energy Efficiency and Conservation Bill would strengthen the legal framework for energy efficiency and conservation practices to ensure full involvement at various levels."

The Bill also detailed the appointment of the Energy Commission to advise the Minister in all matters relating to energy efficiency and conservation. The Commission also has the authority to recommend to the Government any policy, laws, actions and measures relating to energy efficiency and conservation; and to promote, develop or implement policies and initiatives.

Meanwhile, the Bill also emphasises comprehensive oversight under the provisions of Energy User Obligations, specifically targeting large energy consumers in the industrial and commercial sectors. Energy users exceeding the threshold value of 21,600 GJ per year are also required to implement energy saving measures, which include the mandatory appointment of Registered Energy Managers to develop energy management systems and conduct energy audits, according to the Bill.

Source: NST, 11 October 2023

Energy Commission Reports 32 Electrical Accident Cases, 16 Deaths as of 30 September 2023

A total of 32 electrical accident cases was recorded in Peninsular Malaysia and Sabah as of 30 September 2023, with 16 cases resulting in death. Puan Fairus Abd Manaf, Senior Deputy Director of the Consumer Affairs Unit of the Energy Commission said the incidents occurred in homes and factories and a fatal case in Melaka was due to electric shock when current flowed from the zinc roof.

"As such the Commission is committed to increasing awareness on the importance of electrical safety by ensuring that electrical installations at residential premises are safe and comply with the required technical standards. We also advise the public to always be aware and to avoid any unnecessary risks as well as to immediately replace electrical wiring that are old, especially over 30 years-old," she told Bernama when met after a Corporate Social Responsibility (CSR) programme to upgrade the wiring system at Kampung Bukit Senggeh, Selandar here today.

The Commission has allocated about RM270,000.00 to implement Touchpoint CSR programmes nationwide to raise public awareness on electrical safety. This involves its officers inspecting and upgrading electrical wiring systems at selected residential homes, especially low-income households.

Source: NST, 12 October 2023

Government Extends Net Energy Metering and Urges Companies to Spur NEM Adoption

The Government is developing a rooftop solar buyback programme and will extend the current Net Energy Metering (NEM) programme to 31 December 2024 in a bid to incentivise rooftop solar installations, said Dato' Seri Anwar Ibrahim, Prime Minister of Malaysia.

At the same time, the Government is calling for companies to offer a model for residential rooftop solar installation that requires zero capital expenditure (CAPEX), such as those currently offered by PETRONAS' green energy unit Gentari Sdn. Bhd. Earlier in August, Rafizi Ramli, the Minister of Economy said that the Government intends to implement market reforms enabling residential rooftop owners to earn income from their rooftops through solar installations.

Under this plan, companies would invest in these installations and pay monthly rent to the rooftop owners. Although the mechanism is still being refined, Gentari and SOLS Energy have introduced a subscription-based service to make rooftop solar installations accessible to interested consumers without upfront costs. Other models available include full purchase that requires consumers to pay the full system costs to own the rooftop solar assets.

Malaysia's residential NEM programme — where electricity generated from a house's rooftop solar power system offsets consumption on a one-to-one basis — has a 26.03 MW quota balance, out of 150 MW made available. For non-domestic consumers, the quota balance stands at 151.11 MW, out of 800 MW made available, according to data from the Sustainable Energy Development Authority (SEDA).

Source: The Edge Properties, 13 October 2023

INTERNATIONAL

Indonesia Optimistic of Reaching Net Zero Emissions by 2060 or Earlier

Indonesia is optimistic of reaching a net zero emissions target by 2060 or sooner, a Senior Minister said, after the Government submitted its updated nationally determined climate goals to the United Nations (UN). The new net zero emissions target was at least a decade earlier than the previous 2070 target.

While Indonesia maintained its headline target to lower greenhouse gas emissions by 41% by 2030 with international assistance, the country has updated its adaptation measures and included a new long-term strategy for low carbon development in the document filed to the UN last week.

Luhut Pandjaitan, Coordinating Minister for Maritime and Investment Affairs, told a virtual seminar on Tuesday that he was optimistic Indonesia, the world's eighth biggest greenhouse gas emitter, could reach net zero emissions within 50 years. In the energy sector, the Government plans to stop using coal, oil and gas by 2060 and aims to have 85% of its energy needs from renewable sources and the rest from nuclear energy, according to a document presented by Luhut at the seminar.

Indonesia, the world's top thermal coal exporter, currently sources 60% of its energy from coal. Luhut said that Indonesia was also looking into utilising energy storage and hydrogen fuel cell technology. He also added that a mega hydropower plant in North Kalimantan is expected to start construction in October 2023 to support renewable energy (RE) contribution.

Source: Reuters, 27 July 2023

"The Energy Commission is committed to increasing awareness on the importance of electrical safety by ensuring that electrical installations are safe and comply with the required technical standards."

Brunei Adopts Mandatory Carbon Emission Reporting

Brunei Darussalam now requires facilities emitting greenhouse gases (GHG) to submit quarterly and annual emission reports as part of the country's commitment to decarbonise.

The Brunei Darussalam National Council on Climate Change (BNCCC) issued a directive making reporting mandatory back in April 2023. "The directive serves as a clear demonstration of the Government's dedication to transparency and accountability, in addition to enabling Brunei Darussalam to achieve its national and international obligations," said a press statement from the Prime Minister's Office. This is an important first step on the path to track progress towards our national pledges and commitments on reducing GHG emissions, through accurate and reliable data, it added.

The Council will be requiring companies to submit emissions reports for the keeping of a transparent and reliable carbon inventory, which requires a measuring, reporting, and verification system. A centralised online reporting platform is being developed to standardise data reporting and provide a user-friendly overview of GHG data.

Source: BIMP-EAGA Online Post, 16 August 2023

Largest White Hydrogen Deposit Found in France by Accident

Researchers at the University of Lorraine in France were looking to assess levels of methane gas in defunct coal mines in the northeastern part of the country when they chanced upon what might be the world's largest deposit of white hydrogen so far, the researchers wrote in "The Conversation", one of the world's leading publishers of research-based news and analysis.

As the world looks to shift away from fossil fuels, hydrogen has been touted as a potential replacement. The cleanest source of hydrogen production is the usage of renewable sources of energy to split water molecules, known as green hydrogen. White hydrogen, on the other hand, is the term used to describe naturally occurring hydrogen. It is even greener than the greenest hydrogen humanity can make today.

Jacques Pironon and Phillipe de Donato, both Directors of Research at the National Centre of Scientific Research (CNRS) in France, wrote that their team was looking at the sub-soil of the Lorraine mining basin, once known for its coal, for the presence of methane. It was then that they came across hydrogen concentrations that reached 20% at 4,100 feet (1,250 m). Extrapolating from the data they have seen, the researchers estimate that at a depth greater than 9,800 feet (3,000 metres), hydrogen concentration could cross 90%.

This would mean that the now-defunct coal mine could be the site of 46 million tonnes of white hydrogen, which is not only the world's largest but could single-handedly replace more than half of the world's current production of grey hydrogen that is generated from natural gas or methane.

To confirm their calculations, the research team must demonstrate that the hydrogen is evenly distributed in the area, reach depths of 9,800 feet (3,000 metres) and confirm that hydrogen is present in such high concentrations. For this, the researchers are teaming up with commercial and institutional partners and hope to get started with further exploration early next year.

Source: https://interestingengineering.com/ 26 September 2023

"Singapore and Malaysia are both moving towards a low-carbon and sustainable future. We are pursuing cross-border electricity trading, which will be a win-win for both countries."

Singapore, Malaysia to Strengthen Cooperation on Renewable Energy

Singapore and Malaysia have agreed to strengthen cooperation on renewable energy (RE), says Lee Hsien Loong, the Prime Minister of Singapore. "Singapore and Malaysia are both moving towards a low-carbon and sustainable future. We are pursuing cross-border electricity trading, which will be a win-win for both countries," said Lee at a joint press conference with his Malaysian counterpart Dato' Seri Anwar Ibrahim today. Both Prime Ministers met in Singapore today for the 10th Singapore-Malaysia Leaders' Retreat.

According to a joint statement issued at the end of the retreat, the leaders affirmed the commitment to collaborate on RE co-development and cross-border electricity trading. It added that both leaders also looked forward to energy collaboration on other fronts, such as the sharing of low-carbon and RE technologies, carbon capture and storage, and carbon credits. In this regard, the leaders noted the ongoing discussions for Singapore to import RE from Sarawak, and the Malaysian Government will give its assistance in accelerating the process.

Dato' Seri Anwar said that Malaysia has given its commitment to supply RE as Singapore has increased investments in Malaysia, including through the setting up of data centres. "And our commitment (is) to accelerate the proposal by Sarawak to export energy to Indonesia and Singapore," he said. In addition, the leaders acknowledged the recently signed Memorandum of Understanding between Singapore Power and Tenaga Nasional Berhad to explore the technical feasibility of a second interconnector. "These efforts will further enhance energy security and enable greater RE integration," said the statement.

Source: BeritaKini, 30 October 2023

DIGITALISATION: RISKS, STRATEGIES AND FIGHTBACK PLAN

With Industry 4.0 charging ahead as a global phenomenon, everyone is becoming increasingly connected at some level or other, pushing human endeavour higher up the ladder of productivity, efficiency and ingenuity. This is fertile ground for innovation, disruptive technologies and the democratisation of society.

However, like all industrial revolutions, the fourth has a dark side too. Lurking below the amazing connectivity is an underworld of crime that is borderless and usually faceless. New technologies celebrating the ingenuity of men is being countered by malicious alter egos who are equally ingenious. They can take the form of state actors staging assaults to cripple the socio-economy of enemy territory to profit-making syndicates or individuals infiltrating online systems for money.

There has been a proliferation of attack types and scenarios in recent years. High risk attack surfaces include power systems, and this has sent the energy sector into high alert to plug weak spots and adopt proactive postures. Cybersecurity is becoming the newest C-suite leadership function in vulnerable organisations.

Malaysia, which is priming itself to become a digital economy by 2030, is potentially a lucrative field of easy pickings for cybercriminals. Already, critical infrastructure Agencies have experienced a spate of incidents. According to global cybersecurity solutions provider Fortinet, Malaysia ranks among the most vulnerable locations in the region.

Energy Malaysia speaks to Ir. Dr. Megat Zuhairy Megat Tajuddin, Chief Executive of the National Cyber Security Agency (NACSA), who says NACSA is here to lead and coordinate initiatives to secure Malaysia's resilience in facing the threats of cyberattacks. He highlights the Government's efforts such as the Malaysia Cyber Security Strategy 2020-2024 to strengthen cybersecurity governance and management in Malaysia.

Another effort is the Cyber Security Bill, which grants NACSA the legislative authority to further strengthen its handling of national cybersecurity risks, threats and incidents, coordinate and manage National Critical Information Infrastructure (NCII) as well as regulate cybersecurity providers.

Ir. Dr. Megat Zuhairy Megat Tajuddin
Chief Executive, National Cyber Security Agency (NASCA)

"The COVID-19 pandemic of 2020-2022 accelerated the digital transformation of many organisations in Malaysia," says Ir. Dr. Megat Zuhairy Megat Tajuddin, Chief Executive of NACSA. "Organisations, both public and private, were forced to use digital tools to keep in touch with stakeholders and survive the trying time. However, in the rush to digitalise operations, cybersecurity was often overlooked, leading to an expanded and unchecked attack surface," he adds.

Although cybersecurity has been a priority of the Government for some years, it is being ramped up following the outbreak of numerous cyberattacks on key economic sectors. The launch of the Digital Economy Blueprint in 2021 is another compounding factor. Aimed at taking nation to the next stage of growth as a digital economy by 2030, the Government has rolled out wide-ranging incentives to attract technology-based investments.

The country's digital transformation involves integrating more technology into business operations. This includes the use of cloud services, Artificial Intelligence (AI), big data analytics and the Internet of Things (IoT) devices. While these technologies drive innovation and efficiency, they are potential cyber risks because attackers can exploit the connectivity of systems to access networks and find vulnerabilities.

IoT devices are set to grow exponentially. According to statista.com data, the number of IoT devices in the world is forecast to double almost from 15.1 billion in 2020 to more than 29 billion in 2030. Ensuring the security of these devices and cloud environments needs to be a top priority, otherwise attackers can penetrate weak entry points on interconnected networks.

Already, cybercriminals are leveraging on Ransomware-as-a-Service (RaaS) platforms, AI and automation to successfully launch sophisticated and targeted attacks. While these technologies have the capability to be used to protect data, they can also compromise it. AI and machine learning have significant benefits for research and analytics but is also being favoured by hackers for advanced attacks in the form of deep fakes and malicious bots.

"Government Agencies and companies, regardless of size, are potential targets for cyberattacks," points out Ir. Dr. Megat. Safeguarding operations, brand reputation and revenue pipelines are crucial. What we are finding is that organisations are focusing on assessing the cyberattack surface and vectors towards enhancing resilience and recovery.

"In Malaysia, ransomware represents a major threat to our National Critical Information Infrastructure (NCII) organisations in the financial services, healthcare, energy & utilities, Government and manufacturing sectors," says Ir. Dr. Megat.

It is noted that banks and fintech companies are most prone to cyberattacks because of the vast amounts of money and sensitive customer data they manage. Healthcare systems are also lucrative targets because of the wealth of personal information they store. Government Agencies, meanwhile, are attractive to criminals involved in espionage and data theft while critical infrastructure such as utilities are susceptible to attacks aimed at disrupting the essential services.

Ir. Dr. Megat says that small and medium enterprises (SMEs) can potentially be weak links because they often lack robust cybersecurity measures.

Technology companies and information technology (IT) service providers are also targeted because they often manage data from a wide range of clients that includes sensitive information. "Companies are not the only ones at risk. So is every individual internet user," he says.

"The more prevalent threat is social engineering targeting low hanging fruits. This takes the form of online scams and fraud to convince unsuspecting victims to share personal information and hand over their money to tech-savvy criminals," he adds.

The majority of cybercriminals exploit the vulnerability of weak passwords. Passwords are often the first line of defence against unauthorised access, and attackers use various methods, such as brute force attacks or dictionary attacks to crack weak passwords. Misconfiguration is another common issue. This can occur when security settings are not properly set up or when default settings are not changed. Misconfigurations can leave systems open to attacks, allowing unauthorised users to access sensitive data or even take control of systems.

"It is important to note that cyberthreats are continuously evolving in the ever-changing cybersecurity landscape. Staying vigilant, adopting robust cybersecurity protection mechanisms such as Multi-Factor Authentification (MFA) and zero trust, as well as adapting to emerging threats to organisations and individuals alike must be treated as priorities," adds Ir. Dr. Megat.

"While technologies drive innovation and efficiency, they are potential cyber risks because attackers can exploit the connectivity of systems to access networks and find vulnerabilities."

Malaysia's Digital Economy and Cyber Security Bill

Malaysia embarked on its digitalisation journey in 1996, with the roll-out of the Multimedia Super Corridor (MSC), a superhighway of internet connectivity between Kuala Lumpur, Cyberjaya and KLIA. MSC was to be populated by high technology companies and knowledge workers leveraging on high internet speeds.

Today, the entire nation is being powered by 4G and 5G digital infrastructure as Malaysia future forwards itself as a digital economy to fuel growth. It aims to attract USD16.1 billion in digital investment by 2025; and the sector is set to contribute more than 22.5% of GDP. According to a Reuter's report (02 June 2023), the digital economy is one of the fastest growing sectors in Malaysia, the recipient of an impressive USD15.7 billion of investment in the third quarter of 2022 alone.

The foundation of this new direction was laid in 2021 with the unveiling of Malaysia Digital Economy Blueprint (MyDIGITAL) to transform the country into a digitally driven high income nation and a regional leader in digital economy by 2030. It saw the establishment of the Digital Investment Office, charged with smoothing the way for investments encompassing everything from robotics to Artificial Intelligence (AI), Internet of Things (IoT), cloud technology and blockchain technology. Already, the country is sought out by investors keen to establish hyperscale data centres.

The question now is how secure is the Malaysian cyberspace? The New Straits Times reported that Malaysia experienced an average of 84 million cyberattacks every day during the fourth quarter of 2022, according to global cybersecurity solutions provider Fortinet, which ranked Malaysia among the most vulnerable locations in the region.

The Prime Minister of Malaysia has stressed that "there will be no compromise on national security, including in the digital domain and cyber ecosystem." To address this, the Cyber Security Bill was tabled and approved in Parliament on 3 April 2024. The Cyber Security Bill aims to establish a more comprehensive, all-encompassing cybersecurity law to complement existing legislation. The Prime Minister also stated that "the Government is concerned about cybersecurity threats, and we are working on it to enhance and expedite the readiness, capability, and efficiency of cybersecurity in Malaysia."

NACSA will be strengthened to become the leading national cybersecurity Agency and the enforcer of the Bill. The Bill will provide NACSA the clear legal authority to regulate and enforce laws related to cybersecurity and improve the effectiveness of its functions.

Sources: MIDA website; TechwireAsia, 14 July 2023; New Straits Times, 24 and 28 November 2023

MALAYSIA CYBER SECURITY STRATEGY 2020-2024

MCSS is structured around five key pillars, each with specific strategies and action plans. They are:

PILLAR 1 **Effective Governance and Management:** Enhancing the country's critical ICT infrastructure and improving the ability to manage more effectively cybersecurity issues.

PILLAR 2 **Strengthening Legislative Framework and Enforcement:** Reviewing of existing legislation and formulation of new laws related to cybersecurity to ensure a robust legal framework.

PILLAR 3 **Catalysing World Class Innovation, Technology, R&D and Industry:** Fostering innovation and adopting world standard cybersecurity technology.

PILLAR 4 **Enhancing Capacity and Capability Building, Awareness and Education:** Improving capacity development and enhancing the skills of the cybersecurity workforce.

PILLAR 5 **Strengthening Global Collaboration:** Fostering regional and international cooperation to protect Malaysia's cyberspace.

MCSS, the Fightback Plan

In response to increasing cyberthreats, the Government launched the Malaysia Cyber Security Strategy (MCSS) 2020-2024. Funded by a RM1.8 billion budget allocation, this is a comprehensive plan designed to enhance national cybersecurity preparedness and resilience against all forms of cyberattacks.

It consists of five pillars that cover 11 sectors, which includes energy. And they comprise 12 strategies, 35 action plans and 113 programmes, demonstrating the comprehensive nature of the MCSS. The goal is to step up national cybersecurity preparedness to counter effectively all forms of cyberattack.

Ir. Dr. Megat says, "For MCSS to work well at ground level, there is a lot of coordination with stakeholders. This will ensure we have robust defence mechanisms to safeguard critical infrastructure.

"As I see it, MCSS plays a pivotal role in bolstering national security and in supporting the Government's digital economy agenda. However, it is important to acknowledge that there is still much work to be done, particularly in terms of collaboration and coordination with stakeholders. This has to be a dynamic effort because only then can Malaysia's NCII sectors be recognised for their robust cybersecurity defences and resilience to recover quickly," he adds.

MALAYSIA'S NATIONAL CRITICAL INFORMATION INFRASTRUCTURE

Source: https://www.nacsa.gov.my/cnii.php

Energy Industry Challenges and Solutions

The Energy Commission's Senior Deputy Director of Information Management and Technology Unit, Khairol Fahami Ismail, says that the Commission keeps a careful watch on developments on the cybersecurity horizon, to ensure the security of the country's power supply.

Khairol Fahami Ismail
Senior Deputy Director, Information Management and Technology Unit

"By law, companies in the electricity supply chain are responsible for playing their part in ensuring the security of power supply. This is clearly stipulated by Sections 52A and 52B of the Electricity Supply (Amendment) Act 2015," says Khairol.

"While we do not regulate companies as far as their cybersecurity is concerned, we expect them to take all actions necessary to make sure their complex operations, including IT and operational technology networks, are secure in every sense.

"Companies in the energy industry generally have access to more resources than others," points out Khairol, "and are thus able to invest in people, infrastructure, applications and the latest technology. We encourage them to adopt ISO/ISMS 27001, which is internationally recognised as the best practice framework for information security management standards worldwide."

Companies are free to adapt ISO/ISMS 27001 features as required to suit their respective situations. "The purpose of working around specifics is to enable the industry to have the freedom to access the latest technology in the dynamic cybersecurity environment. Otherwise, they may get pinned down by following one set of rules," explains Khairol.

The Commission also recognises that the cybersecurity priorities of companies within the energy industry are likely to vary from each other. All entities, of course, will try to prevent breaches that lead to the denial of service (DoS), for instance. But DoS may affect some businesses more than others."

Khairol predicts that the energy industry will need to steel itself to a surge in cybersecurity incidents because of the convergence of the digital and physical worlds. This is a trend that is predicted globally, with the growing popularity of the Internet of Things (IoT), where everyday devices are embedded with electronics that collect information and connect to a network. Consumer devices and domestic appliances like refrigerators, microwaves, televisions are becoming increasingly connected. Wearable technology allows people's health to be monitored remotely from a wristwatch and homes and cars have beacons, cameras and alarms that can be triggered in the event of an intrusion or emergency.

To further complicate matters, a great deal of this information is now being stored in the cloud. Companies used to have control over their own systems, networks and servers. Today, devices, software and data are accessed through virtual or cloud computing.

The convergence of IT and OT networks is another big challenge because it enlarges the attack surface further. Many in the energy sector opine that cyberattacks can happen at anytime and catches everyone off guard.

"By law, electricity supply chain companies are responsible for ensuring the security of supply and we strongly encourage them to adopt ISO/ISMS 27001."

SECTIONS 52A AND 52B OF THE ELECTRICITY SUPPLY (AMENDMENT) ACT 2015

Section 52A: Supply Infrastructure Information Security

1. "Any licensee as directed by the Commission providing supply of electricity to consumers shall be responsible for the preservation of confidentiality, integrity and availability of its information, information systems and supporting network infrastructure pertaining to its duties and other matters as provided under this Act.

2. The licensee shall:

A	B	C
take the necessary measures, establish and implement standards and employ the relevant information security controls to prevent, avoid, remedy, recover or restore its information, document, instrument or records stored in its computers and for its operational system by its computers from any risk of (i) threat or unauthorised access; and (ii) intrusion or removal;	take necessary measures to ensure the resiliency of its supporting network infrastructure to minimise business impact against various threats to its activities under the licence; and	ensure that the reliability, continuity and quality of electricity supply, its performance of duties and conformity to the provisions of this Act and any regulations made thereunder shall not be jeopardised thereby, and shall report to the Commission within the time specified by the Commission, and in the event of any incident which interferes or affects the performance of the activities under the licence, report such incident immediately to the Commission and other relevant authorities.

3. Any licensee who fails, neglects to comply with or contravenes any provision of this section commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

Section 52B: Obligation to Give Information

1. The Commission may authorise any of its officer to obtain any information pertaining to the licensee or any other person under this Act and shall be given access to such information whether stored in a computer or otherwise.

2. Any officer authorised by the Commission under this subsection shall have the power to require the production of records, accounts, data, computerised data and documents kept by a licensee or any other person and to inspect, examine and to download from them, make copies of them or take extracts from them.

3. For the purposes of this section, "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerised data.

4. Any person who refuses to give any information which may reasonably be required of him under subsection (1) and which he has in his knowledge or power to give commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

"For NACSA, the energy sector is one of the NCII sectors that must be well-protected because any compromise will affect the national security, economy, image, Government, public health and safety capabilities of the country.

"The energy industry stands in a challenging position in the current dynamic cyber-threatening environment. Private energy companies face several challenges, and as we see it, mitigating cyber risks will require collaborative efforts between energy companies and the Government," says Ir. Dr. Megat.

CYBERSECURITY CHALLENGES FOR THE ENERGY INDUSTRY

1

LACK OF INVESTMENT

This is partly because cybersecurity is a relatively new field, and the energy industry is heavily capital-intensive. However, it is crucial for energy companies to understand that investing in cybersecurity can prevent costly breaches and downtime.

2

LEGACY SYSTEMS

Malaysia has a long history of electrification dating back to the 1900s. Despite regular upgrades, legacy systems continue to exist, and they were not designed with cybersecurity in mind.

3

SUPPLY CHAIN RISKS

Energy companies rely on a complex network of vendors and suppliers who can introduce cyber risks. When these third parties don't have robust cybersecurity measures, they expose their principals. Therefore, it is important for energy companies to vet their suppliers carefully and establish strong security requirements for them.

4

HUMAN ERROR

Employees can accidentally click on phishing emails or lose track of their passwords, leading to security breaches. To mitigate such risks, companies need to invest in cybersecurity training for employees to raise awareness of potential threats and to promote best practices.

Currently, Malaysia's national public utility Tenaga Nasional Berhad (TNB) has embarked on the multi-billion-ringgit smart grid project, which carries numerous benefits. Reliant on digital technologies, the transformative smart grid also presents a multilayered and wide-spanning attack surface to state actors, hacktivists and other cybercriminals. "This grid must be equipped with the right and robust safeguarding measures because the consequences of a successful cyberattack are severe. They can range from localised power outages throwing local communities into disarray, to a national economic and security collapse. Ensuring the resiliency of grid assets and systems at all costs and all the time cannot be understated," says Ir. Dr. Megat.

This will involve prioritising the protection of critical assets such as Supervisory Control and Data Acquisition (SCADA) systems, Industrial Control Systems (ICS) and communication networks. "A multi-layered defence strategy is required," says Ir. Dr. Megat. "It will require the implementation of the right cybersecurity controls that includes access control and firewalls, intrusion detection and protection systems, regular patching and updates, network segmentation among others, as well as tried and tested incident response plans."

He adds, "For proactive defence, threat intelligence is crucial. This involves gathering information on emerging cyberthreats, vulnerabilities and the attacker's tactics, techniques and procedures (TTPs). Grid operators can use threat intelligence for threat hunting, anomaly detection, vulnerability management and incident prediction."

"Power companies should embed a culture of ethical data handling, to ensure employees understand the ethical implications of mishandling consumption data."

Consumer information stored by power suppliers is becoming a popular attack target for cybercriminals. To prevent such data theft, companies should embed a culture of ethical data handling, to ensure employees understand the ethical implications of mishandling consumption data. They should also educate consumers of their rights with regard to their power consumption data, how it is used and how they can protect themselves.

This is critical to ensure that the privacy of every Malaysian power consumer is not infringed. Besides, it will foster trust and confidence in the country's electricity supply system.

"There have been instances of consumer data being compromised, not particularly in the energy sector," admits Ir. Dr. Megat. NACSA had stepped in to assist in accordance with the National Cyber Crisis Management Plan. NACSA can respond effectively as a result of its cooperation and coordination at national, regional, and international levels on threat intelligence and incident management.

Self-consumers (SELCOs), prosumers and consumers can also unwittingly compromise energy systems. Their defences may be down due to the shortage and cost of cybersecurity expertise; resource constraints; inability to keep pace with technological advancements; exposure to third party risks; failure to comply with regulatory requirements, among others.

HOW TO PREVENT DATA BREACHES

- Conduct regular risk assessment and vulnerability analyses to identify potential weaknesses in their systems.
- Establish robust security policies and procedures.
- Implement strong access control and authentication.
- Deploy continuous monitoring and intrusion detection systems.
- Utilise encryption tools for data in transit and at rest to protect sensitive information.
- Update software, firmware and hardware with latest security patches and updates.
- Develop and test the incident response plan.
- Educate employees on cybersecurity best practices.
- Collaborate with industry peers, regulatory bodies and Government Agencies for threat intelligence and best practices.

New Legislation and Regulatory Environment

Previously, Malaysia had no specific cybersecurity legislation to govern the cybersecurity environment.

Scams, frauds and other criminalities in relation to cybercrimes were being dealt with under the Penal Code (Act 574), Computer Crime Act 1997 (Act 563), Communications and Multimedia Act 1998 (Act 588) and other relevant domestic legislation. Given Malaysia's digital economy agenda and pervasive cyberattacks experienced recently, it became contingent upon the Government to be more stringent in securing the country's cyberspace.

"The Cybersecurity Bill is expected to boost Malaysia's cybersecurity capacity and capabilities, focusing on the development of more local talent, more comprehensive processes and the compulsory reporting of incidents by Agencies in the NCII sectors."

"The recently passed Cyber Security Bill empowers NACSA with the legal authority to strengthen national cybersecurity," says Ir. Dr. Megat. With this, NACSA can become more effective in implementing existing strategies as well as act against the non-compliance of Agencies not taking the necessary preventive measures in cybersecurity," he adds.

Envisaged to address gaps in the existing legal landscape, the Bill was drawn up to streamline existing legal mechanisms, procedures, monitoring and enforcement. Additionally, it strengthens coordination in the management and governance of the country's cybersecurity and aligns them with national, regional and international requirements. The priority is to ensure that the cybersecurity sector's development is carried out responsibly and complies with internationally agreed treaties.

For the Government, the Cybersecurity Bill provides specific powers to the Minister responsible for cybersecurity, which among others includes instruction to take the necessary steps to detect and prevent any cyberthreat. This is critical, particularly when the Government receives threat intelligence or is privy to incidents that can be harmful to NCII assets and the country in general.

The Bill also empowers the Government to improve the efficiency of cybersecurity governance, management and monitoring, with the involvement of NCII stakeholders from both the public and private sectors. The goal is to improve coordination and response mechanisms to cybersecurity incidents, especially when they contain sensitive information.

Under the Bill, the NCII and supply chain will be subject to higher standards of cybersecurity and required to comply with the law and regulations introduced by NACSA. They will be required to ensure that their cybersecurity ecosystems are at a level that is consistent with the normative frameworks of the international community.

Failure to comply is punishable by law under the new Bill, which is drawing up a list of new offences and penalties. "We want cybersecurity to be a shared responsibility between the Government and the private sector," says Ir. Dr. Megat.

"The intention is to ensure that all parties understand and internalise the importance of national cybersecurity. Enforcement and punishment are the last steps, after all other efforts have been exhausted."

The Focus of 2024

With technologies moving at a fast pace and cybercriminals matching this pace, the Government is currently in the midst of implementing various initiatives, says Ir. Dr. Megat. "The National Cyber Coordination and Command Centre (NC4) is currently undergoing enhancements to receive better threat intelligence not only at national level but also with our international counterparts.

2024 is a milestone year for NACSA following the passing of the Cyber Security Bill, which has boosted its standing as the enabler for the betterment of national cybersecurity coordination, management and governance in Malaysia.

CYBERATTACKS SPIKING IN THE ENERGY SECTOR

Cyberattacks in the energy sector have spiked. And the future may be ominous.

In the first half of 2022 alone, Germany-based independent researcher KonBriefing Research listed 34 successful cyberattacks on the energy sector, stating that this figure was based on known incidents. They ranged from email, website and database leakages to attacks on power grids, nuclear, oil & gas installations and storage facilities, liquefied natural gas (LNG) operations, wind turbines and district heating operations. There was even a distributed denial-of-service (DDoS) assault on the website of a regulatory authority in Milan, Italy and hacking of electric vehicle charging stations in Russia.

The majority of attacks occurred in Europe, which is not surprising given the fall-out from the Russia-Ukraine crisis. A surprising entry, however, was the Caribbean Island of Sint Maarten, where utility company NV Gebe was the victim of a BlackByte ransomware cyberattack that crippled its computer systems. Closer home to Malaysia, Indonesia's State-backed oil and gas utility, Perusahaan Gas Negara is said to have been struck by the ransomware gang Hive in April 2022.

"The crooks are becoming better by the day, so we need to become better by the day," said Leonhard Birnbaum, the Chief Executive of E.ON, one of Europe's largest utilities, in an interview with US digital newspaper "Politico" (23 November 2023). "I'm worried now, and I will be even more worried in the future."

Preparation for the future includes lessons from past incidents. Energy Malaysia handpicks a few high-profile cases in the past 10 years that offer invaluable insights.

2015 - Power Grid Attack, Ukraine

Power Outages for 230,000 Customers for Between One and 65 Hours

This grid attack resulted in power outages for around 230,000 customers across Ukraine for between one and 65 hours. The hit was attributed to an advanced persistent threat group known as "Sandworm" and became the first publicly-acknowledged attack on a power grid.

It is considered one of the most significant threats implemented by cybercriminals on an entire community or country. At the time of this attack, consumers of two other energy distribution companies were also being affected by cyber issues on a smaller scale.

In an article published in "Wired" (3 March 2016), Robert M. Lee, who assisted in the investigation, describes the attack as meticulously planned. A former cyber warfare operations officer for the United States (US) Air Force and co-founder of Dragos Security, a critical infrastructure security company, he says, "In terms of implementation, most people always focus on the malware that's used in an attack. To me, the logistics, planning and operations and what's going on during the length of it had been well strategised."

Lee says everything about the Ukraine power grid attack suggests it was primarily designed to send a message. "'We want to be seen, and we want to send you a message,'" is how he interprets it.

Whatever the intent of the blackout, it was a first-of-its-kind attack that set a sinister precedent for the safety and security of power grids everywhere. The people in charge of the world's power supplies have been warned. This attack was relatively short-lived and benign. The next one might not be.

2017 – Triton Malware Attack on a Petrochemical Plant, Middle East

70 Days to Recover with a Cost of Tens of Millions of Dollars

A World Economic Forum (WEF) White Paper published in May 2021 cites the case study of a malware attack on a petrochemical plant. According to the paper, from 2014-2017, a malicious adversary had breached the cyber defences of an oil and gas refinery using an operational technology (OT) specific malware called Trisis / Triton to target the safety systems used for oil and gas production. After going undetected for three years, attackers activated their malware to disrupt the refinery's safety instrumented systems in 2017.

However, an error in the malware caused the plant to shut down instead of causing significant physical damage and severely injuring or killing company workers as intended. Immediately following the attack, plant security personnel – and their third parties – did not consider the sudden shutdown to be a direct result of a cyberattack and, thus, did not investigate this possibility as a root cause in their analysis.

Having failed to correctly recognise and block the ongoing cyberbreach threat, the plant went back into operation with the malicious actor still present. A month later, attackers made a second attempt to disrupt the refinery's safety system. Again, they failed due to a different error. This time the plant's security team requested support from OT specialists to investigate the shutdowns in greater depth. Only then did they find that the plant's OT systems were being manipulated and took steps to secure the breach.

Recovering from the incident and then restoring the refinery to full operation took over 70 days and cost tens of millions of dollars.

The WEF White Paper Key Takeaways

1. Adversary errors prevented casualties in this incident, but board governance can and should make organisations more resilient against OT cyberthreats to critical safety infrastructure by taking an OT-specific approach to cybersecurity where appropriate.

2. Attacks will happen as not all can be prevented, but organisations can also detect and respond, making themselves more resilient.

3. After incidents, sharing information and lessons learned from past threats helps other organisations in the oil and gas value chain to be more prepared.

Utilities Not Fully Prepared, Says IEA

An International Energy Agency (IEA) report (1 August 2023) found that the average number of cyberattacks against utilities each week have more than doubled between 2020 and 2022 worldwide — with 1,101 weekly attacks registered last year. In the European Union (EU), companies scrambled to hire cybersecurity experts in the month following Moscow's assault on Kyiv, the report noted, indicating "utilities were not fully prepared."

2017 - NotPetya Virus Spread, Worldwide

No Access to Files in Hard Drives

This virus was first discovered in June 2017 and quickly spread around the world causing a wave of cyberattacks to occur and costing billions of dollars in damage. The NotPetya virus encrypted victims' hard drives and prevented them from accessing their files. Initially targeting Ukrainian energy companies, it spread to many other businesses worldwide, forcing them to shut down because of the virus.

The NotPetya virus was particularly dangerous because it masqueraded as a ransomware. This allowed it to spread quickly, as people were tricked into thinking that it was a software upgrade, hence they readily downloaded and installed it. However, unlike typical ransomware, the NotPetya virus did not provide a way for victims to recover their data. This made it much more destructive.

The NotPetya virus affected businesses of all sizes, but it hit Ukrainian organisations particularly hard. This is because the virus was said to have initially spread through a piece of accounting software that was popular in Ukraine. From there, it quickly spread to other countries.

While the NotPetya virus caused billions of dollars in damage, its true purpose is still unknown. Some experts believe that it was created as a form of information warfare, while others believe that it was simply a prank gone wrong. Either way, it is clear that the NotPetya virus was one of the most destructive cyberattacks in history.

2020 – SolarWinds Supply Chain Attack, United States of America

Undetected Spying on Companies and Organisations

SolarWinds, a major information technology (IT) firm in the United States of America (USA), was the subject of a cyberattack that spread to its clients and went undetected for months. It began in early 2020, when hackers secretly broke into Texas-based SolarWinds' systems and added a malicious code into the company's software system. The system, called "Orion," is widely used by companies to manage their IT resources.

As a routine practice, SolarWinds sent out software updates to its customers that included the hacked code. The code created a backdoor to customers' IT systems, which hackers then used to install even more malware that helped them spy on companies and organisations.

The hackers, allegedly foreigners, were then able to spy on private companies like the elite cybersecurity firm FireEye and the upper echelons of the US Government.

SolarWinds later announced that up to 18,000 of its customers were infected through its compromised software update across a wide spectrum of verticals, including the Government, consulting, telecommunications, and technology companies. The malicious SolarWinds software also infected more than a dozen critical infrastructure companies in the electricity, oil and manufacturing industries. Other victims included Original Equipment Manufacturers (OEMs) who have remote access to critical parts for the installation of new software or even control critical operations. This means that hackers who breached the OEMs could potentially use their credentials to control critical customer processes.

Key Lessons According To Experts

1. Supply chain exposures shouldn't be ignored.
2. Third parties must prioritise cybersecurity.
3. Practise defence-in-depth, a cybersecurity strategy that uses a number of layered, redundant defences to protect itself from a variety of threats.
4. Harden on-premises systems because the ability of actors to conduct this attack hinges on the initial compromise of customer's on-premises systems.
5. Adopt a long term, programmatic approach to supply chain security.
6. Make it mandatory to use cyberthreat intelligence platform(s).
7. Use Static Application Security Testing (SAST) tools that are designed to detect backdoor codes.
8. Use secure Security, Information, and Event Management (SIEM) solutions that facilitate accelerated vulnerability monitoring, which in turn helps reduce security breaches across the entire IT infrastructure of an organisation.
9. Use behavioural analytics-based threat detection – it is important to note that preliminary detection of the SolarWinds compromise by cybersecurity firm FireEye did not notice complicated lateral movements or even data exfiltration.
10. Note that Multi-Factor Authentication (MFA) is not as secure as you think. SolarWinds hackers ran laps around the MFA security, effectively creating their own authentication tokens that allowed them to access and continue their intrusion.

2021 – Colonial Gas Pipeline Ransomware Attack, United States of America

Operations Shutdown for More Than Five Days

On 7 May 2021, Colonial Gas Pipeline fell victim to a ransomware attack, described as the largest cyberattack on an oil infrastructure in American history. The company paid the ransom of about 75 bitcoins or USD 4.4 million within hours. However, it needed time to restore the system to a working state. Colonial Pipeline systems and operations began to return to normal from 12 May onwards.

The 8,850 km long pipeline carries three million barrels of fuel per day between Houston, Texas and New York. It supplies gasoline, home heating oil, aviation fuel and other refined petroleum products to communities and businesses throughout the Southern and Eastern regions of the United States of America (USA). The cyberattack caused a shutdown of their operations for more than five days, resulting in a fuel shortage along the East Coast. The attackers also stole nearly 100 gigabytes of data and threatened to release it on the internet if the ransom was not paid.

Joe Biden, the President of the USA, declared a state of emergency on 9 May 2021, and called for "a whole-of-Government response to get fuel more quickly to where it is needed and to limit the pain being felt by American customers."

He signed an Executive Order on 12 May, to increase software security standards for sales to the Government, tighten detection and security on existing systems, improve information sharing and training, establish a Cyber Safety Review Board, and improve incident response. The US Department of Justice (DoJ) also convened a cybersecurity task force to increase prosecutions. Meanwhile, the State Department issued a statement that a USD10 million reward would be given for information leading to the arrest of the perpetrators.

The Federal Bureau of Investigation (FBI) and various media sources identified the criminal hacking group, DarkSide, as the responsible party.

On 7 June, DoJ announced that it had recovered 63.7 of the bitcoins, about 84% of the original ransom payment but due to the bitcoin crash in late May, the recovered bitcoins were worth around USD2.3 million, roughly half of their original value.

This was one of the first high profile corporate cyberattacks, which started from a breached employee personal password rather than a direct attack on the company's systems.

DarkSide's Bitcoin Wallet

Cryptocurrency security firm Elliptic stated that a bitcoin wallet opened by DarkSide in March 2021 showed it had received an average of USD1.9 million from 47 different bitcoin wallets, including the Colonial Pipeline ransom. In total, DarkSide had received USD90 million in ransom payments.

2021 – Kaseya Supply Chain Cyberattack, United States of America

Ransomware Compromise for SMEs

Kaseya, an information technology (IT) solutions developer for Managed Service Providers (MSPs) and enterprise clients, announced there was a cyberattack on 2 July 2021, over the American Independence Day weekend. According to reports, Revil, one of the world's most active ransomware gangs claimed responsibility. Their payment portal went live, and they were said to be actively negotiating with victims.

Kaseya is a Dublin-based IT solutions provider company that has an American headquarters in Miami, Florida. The vendor maintains a presence in 10 countries.

According to Chief Executive Officer Fred Voccola, less than 0.1% of the company's customers were embroiled in the breach – but as their clientele includes MSPs, this means that smaller businesses have also been caught up in the incidents. At that point in time, estimates suggested that 800 to 1,500 small to medium-size businesses may have experienced a ransomware compromise.

The attack is reminiscent of the SolarWinds security fiasco, in which attackers managed to compromise the vendor's software to push a malicious update to thousands of customers.

Kaseya instructed its clients to shut down their VIA Site Management (VSM) servers. And it took down its cloud-based services as a precaution. After more than a week of analysis and software hardening, Kaseya restored its services on 11 July. On 26 July, the company disclosed that it did not pay a ransom – either directly or indirectly through a third party – to obtain the decrypted key for the Revil ransomware attack.

In March 2022, the alleged hacker Yaroslav Vasinskyi was extradited and arraigned in a Dallas court in Texas. An indictment, unsealed on 8 November 2021, charged Vasinskyi, 22, a Ukrainian national, with conducting ransomware attacks against multiple victims, including the July 2021 attack against Kaseya, the US Department of Justice said.

2021 – Power Supply Attack at a Nuclear Facility in Natanz, Iran

Blackout in Nuclear Facility

Within hours of Iran proudly announcing the launch of its latest centrifuges, a power blackout damaged some of the precious machines at its site in Natanz, reports BBC (12 April 2021).

Some reports have suggested a cyberattack might have been responsible, but Iran has talked of "infiltrators" amid reports of an explosion linked to the power generator. One thing the reports seem to agree on is that an "incident" affected the power distribution network at Natanz, leading to a blackout until emergency power systems kicked in.

A blackout is a serious matter at a nuclear facility. Centrifuges are slender machines linked up in what are called cascades that enrich uranium gas by spinning it at incredibly high speeds using rotors. The stress on the advanced materials involved is intense and the process is technically immensely challenging.

A small problem can send a centrifuge spinning out of control, with parts smashing into each other and damaging a whole cascade. Ensuring the power supply reaching a centrifuge is perfectly balanced is vital, which means sabotage of that supply can be catastrophic.

Natanz is where the world's first real cyberattack took place more than a decade ago in 2010, an incident referred to as Stuxnet, a sophisticated malware targeting "high value" infrastructure in Iran. Stuxnet is believed to be the first known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.

It caused physical damage by altering the speed of centrifuges at the uranium enrichment plant at Natanz then, disrupting Iran's nuclear programme.

Ripple Effect on Interconnected Systems

On 23 November 2023, "Politico" reported that Damian Cortinas, who chairs the board of the European Union (EU)'s electricity network association ENTSO-E, as saying that tackling cyberattacks is especially "high priority" for operators due to how interconnected Europe's power systems are. He added that the EU needs to help countries that are the "weakest links."

Earlier in the year, the EU had imposed new cybersecurity requirements on critical sector companies including the energy sector under its NIS2 Directive, which is to become applicable in October 2024. The bloc also set up networks of private and public cybersecurity services in key sectors that are meant to improve sharing between countries on large-scale digital assaults.

The European Commission, the EU's Executive Body, also presented new plans in September asking EU countries to better liaise on cross-border threats and strengthen cooperation with the North Atlantic Treaty Organisation (NATO) after the apparent acts of sabotage that destroyed the Russia-to-Germany Nord Stream gas pipelines in 2022.

2023 – Coordinated Cyberattacks On 22 Energy Organisations, Denmark

Obtaining Device Configurations and Usernames from Vulnerable Firewalls

In May 2023, threat actors targeted 22 energy organisations over a few days, making this the largest attack against Danish critical infrastructure to date.

"Denmark is constantly under attack. But it is unusual that we see so many concurrent, successful attacks against critical infrastructure. The attackers knew in advance who they were going to target and got it right every time," notes a report by SektorCERT, a non-profit cybersecurity centre for critical sectors.

It began on 11 May 2023, with attacks on 16 energy organisations, executing commands on the vulnerable firewalls to obtain device configurations and usernames. The systems in 11 companies were compromised. All networks were secured by the end of the day.

A second wave of attacks, observed on 22 May, involved new tools and exploitation of two zero-day[1] vulnerabilities. The bugs were patched on 24 May. On the same day, the attackers started targeting multiple Danish energy firms with different payloads and exploits and continued their assault on 25 May as well. SektorCERT says it worked together with victim organisations, to apply the available patches and secure the compromised networks immediately after identifying the attacks.

Throughout the assault campaign, some of the vulnerable firewalls were infected with a Mirai bot, subsequently used in Distributed Denial-of Service (DDoS) attacks against entities in the United States of America (USA) and Hong Kong.

1. A zero-day vulnerability is a software vulnerability discovered by attackers before the vendor has become aware of it. Because the vendors are unaware, no patch exists for zero-day vulnerabilities, making attacks likely to succeed.

   Source: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

Threat Actors Are Most Intensely Focused on the Energy Sector, Says Report

The global study conducted by Cyentia Institute and Rockwell Automation analysed 122 cybersecurity events that included a direct compromise of operational technology (OT) and / or industrial control system (ICS) operations. The in-depth research study collected and reviewed nearly 100 data points for each incident in industrial environments. The findings were published in a report called "Anatomy of 100+ Cybersecurity Incidents in Industrial Operations" released in September 2023.

Its key findings were that almost 60% of attacks were led by State-affiliated actors. Additionally, 33% were enabled by internal personnel. Threat actors were most intensely focused on the energy sector (39% of attacks) at over three times more than the next most frequently attacked verticals, critical manufacturing (11%) and transportation (10%).

Phishing remained the most popular attack technique (34%), underscoring the importance of cybersecurity tactics such as segmentation, air gapping (isolation of a network system from external connections), zero trust and security awareness training to mitigate risks. More than 80% of threat actors came from outside organisations, yet insiders played an unintentional role in opening the door for threat actors in approximately one third of incidents.

In the Operational Technology / Industrial Control System (OT / ICS) incidents studied, 60% resulted in operational disruptions and 40% resulted in unauthorised access or data exposure.

However, the damage of cyberattacks extended beyond the impacted enterprise, as broader supply chains were also impacted 65% of the time. OT / ICS cybersecurity incidents in the last three years have already exceeded the total number reported between 1991-2000. In more than half of OT / ICS incidents, Supervisory Control and Data Acquisition (SCADA) systems were targeted (53%), with Programmable Logic Controllers (PLCs) as the next-most-common target (22%).

The research indicates that strengthening the security of information technology (IT) systems is crucial to combatting cyberattacks on critical infrastructure and manufacturing facilities. More than 80% of the OT / ICS incidents analysed started with an IT system compromise, attributed to increasing interconnectivity across IT and OT systems and applications.

Source: https://www.rockwellautomation.com/en-us/company/news/press-releases/New-Research-Finds-Cyberattacks-Against-Critical-Infrastructure-on-the-Rise-State-affiliated-Groups-Responsible-for-Nearly-60.html

URGENTLY NEEDED: TALENT TO BEAT CYBERCRIMES

Dato' Ts. Dr. Amirudin Abdul Wahab
Chief Executive Officer, CyberSecurity Malaysia

As advancements in technology and online work-and-life styles become more entrenched, so are cybercrimes that have become more rampant, daring and sophisticated. Cyber defenders are urgently sought to keep our information technology (IT) and operational technology (OT) systems secure from cyberattacks and better still predict future trends and strikes.

Energy Malaysia talks to Dato' Ts. Dr. Amirudin Abdul Wahab, Chief Executive Officer, CyberSecurity Malaysia, who points out that what the country needs is well-trained cybersecurity experts with the appropriate technical competencies as well as creativity and a deep understanding of both technology and human behaviour. He highlights efforts taken by CyberSecurity Malaysia to ensure a secure and resilient cyberspace in Malaysia as well as to nurture world-class cybersecurity workers and professionals.

Q According to media reports in 2023, cybercrimes have been increasing in frequency and severity of attacks. Why is this happening?

A In this digital age, people rely heavily on the internet and digital technology to stay connected, carry out their daily activities and conduct business operations. However, with the world being highly connected, internet users have become more vulnerable and are targeted by cybercriminals for their nefarious activities and illicit gain. Nowadays, cybercriminals are undergoing a rapid evolution. They are opportunists and have become bolder, more knowledgeable, and increasingly sophisticated, making good use of advanced technologies such as Artificial Intelligence (AI) in executing cyber-attacks. They are more proactive and organised in the way they conduct their attack operations.

Cybercriminals might attack individuals, whole organisations or sectors of the economy. Numerous sectors have already reported incidents of ransomware, malware, data breaches, online defacement, and other assaults meant to render them crippled.

The unpredictability of the economy and the rising rate of inflation have also contributed to the abrupt increase in cybercrime in recent years. As a result, organisations now need to increase their budget for proactive, preventative, and reactive cybersecurity measures. However, due to the economic slowdown, it has left organisations with no choice but to downsize their organisation's budgets.

Businesses are struggling to have enough insurance coverage for cybersecurity breaches and cannot afford the high cost of cyber insurance. In addition, existing cybersecurity personnel are overworked, and occasionally IT and OT systems are being compromised by human error. In this regard, an organisation needs to strike a delicate balance between the need to increase skilled IT security teams and the downsizing of budgets.

Generally, the lack of personnel, tools and processes makes it difficult for companies to establish Security Operations Centres (SOCs) and to gather Cybersecurity Threat Intelligence (CTI) in order to have strong defence structures. An SOC consists of an IT security team while CTI is information collected by an organisation to understand possible cyberthreats. They also face the arduous task of detecting, responding to and preventing cyberattacks without such defensive mechanisms.

"The country needs 26,340 cybersecurity professionals by 2025 to achieve and enhance its digital economy ambition. Currently, there are only 15,248 workers identified as cybersecurity experts."

Awareness is also a crucial aspect of cybersecurity. This is important in order to address the human aspect of cybersecurity. People are the weakest link of an organisation. The lack of awareness and understanding among the public, businesses and even Government entities are among the most critical issues that Malaysia needs to continue addressing. Insufficient knowledge regarding best practices, such as using strong passwords, identifying phishing attempts or regularly updating software, can make individuals, businesses and organisations vulnerable to cyberattacks.

Most organisations in Malaysia, especially Small and Medium Enterprises (SMEs) still lack the necessary awareness and defences against cyberthreats. SMEs often assume that being insignificant makes them a less likely target. But in truth, they are easy targets to be exploited. Apart from that, they can be used as a proxy to launch attacks against bigger corporations or within the supply chain. Criminals often target smaller organisations due to their indifference, financial weakness and weaker security.

Organisations are also prone to insider threats, whether intentional or unintentional. The different types of insider threats are oblivious, negligent, malicious and also professional insiders. So, it is important to prevent insider threats by updating and enforcing security policies, educating employees, monitoring employee activities and enforcing the principles of least privilege (access control).

Outdated or traditional machines, legacy technologies and ageing infrastructure also add to the vulnerability of IT and OT systems. It is important to note that addressing these vulnerabilities is an ongoing process. As technology and threats evolve, the organisation must adapt and invest in cybersecurity measures to protect both IT and OT systems effectively. Collaboration between IT and OT teams is critical for success in securing an organisation's infrastructure. Other than that, they must have the basic cybersecurity fundamentals and hygiene, conduct risk assessment, asset management control, regular updating and patching and replacing and upgrading outdated systems, data back up and recovery, employee training and the like.

Q What are common cybersecurity breaches and what talent is needed to deal with them?

A No matter how big and secure an organisation is, one way or another, cybercriminals are able to find loopholes and vulnerabilities in their system. They may find loopholes in an organisation's process, technology and especially people. This is because people are the most gullible and vulnerable target. Some of the most common cybersecurity breaches are from social engineering attempts, fraud, phishing attacks, supply-chain attacks and zero-day attacks.

Due to cybercriminals being more opportunistic, they make use of weekends and public holidays to conduct their activities when most employees tend to be more relaxed and less prepared to fend off a cyberattack.

Furthermore, cyberattacks are rarely apparent to employees and tend to be hidden unless they are properly trained to detect, which becomes a challenge to determine the actual time or period of any attack. The flexibility and agility of cyberattackers is the challenge that cybersecurity teams have to deal with daily. According to America's Security Magazine, there are over 2,200 attacks each day, which breaks down to nearly one cyberattack every 39 seconds!

In Malaysia, CyberSecurity Malaysia received 4,898 reported cyber incidents as of October 2023, with fraud incidences making up the majority (63%) of cyberthreats to date for the entire year. The common attacks were phishing, social engineering, malware, Distributed Denial of Service (DDoS), spam and hacking.

We are living in the digital era with emerging technologies harbouring villainous alter egos such as AI malware, complicated Internet of Things (IoTs) attacks, and crypto jacking. The perpetrators of these attacks are demonstrating their capabilities in targeting bigger organisations and stronger nations with dangerous implications.

Therefore, we expect to see more state-sponsored attacks, information warfare, AI-powered attacks, attacks targeted at remote workers, supply-chain attacks, quantum threats, ransomware-as-a-service, zero-day exploits, 5G network attacks, and threats that are coming from the Internet of Everything (IoE). According to Trend Micro Incorporated, most organisations in Malaysia believe that they will be attacked in the next 12 months. The sectors more prone to cyberattacks are the SMEs and National Critical Information Infrastructure (NCII).

Unfortunately, there are not enough cybersecurity experts around to support the industry needs. There is a gap between the quality of cybersecurity personnel available and the industry's needs and expectations. This is due to many cybersecurity professionals not being sufficiently equipped with the right technical skills and at the same time possessing the creativity and deep understanding of both technology and human behaviour.

It takes time to build a workforce of knowledgeable cybersecurity experts. Strategic public-private partnerships (PPPs) and rewards from diverse sources, such as scholarships, mentorships, and internships with job guarantees are needed to close this human capital gap.

"Due to cybercriminals being more opportunistic, they make use of weekends and public holidays to conduct their activities when most employees tend to be more relaxed and less prepared to fend off a cyberattack."

Q How is CyberSecurity Malaysia building up the local cybersecurity industry?

A At CyberSecurity Malaysia, our goal is for a secure, resilient and trusted cyber environment that can sustain the country's competitiveness and prosperity. We have developed about 40 products and services in cyber domains such as assessment and rectification, information security management, monitoring, control and response, capability, and capacity development.

These products and services are available to industry professionals and companies in the form of:

- Information and Communications Technology (ICT) Systems Guarantee.
- Detection, Eradication and Forensics.
- Cyberthreat Intelligence (CTI).
- Vulnerability Assessments.
- Capacity Building.
- Awareness Building Campaigns.

In addition, we also review policies and plans to determine the best approach to counter cyberspace breaches. For this purpose, we have produced various cybersecurity guidelines that are posted on our corporate website as references for cybersecurity professionals. They include Cyber Security Guidelines for Industrial Control Systems (ICS); Cyber Security Guidelines for the IoTs; and Cyber Security Guidelines for Industry 4.0 (IR4.0) that may also be applied to critical infrastructure.

To ensure robust IT systems, we offer the Information Security Management System (ISMS) Audit and Certification-CyberSecurity Malaysia 27001 Scheme; Business Continuity Management System (BCMS) and Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme.

Cybersecurity does not work in a silo. Everyone should be responsible for the security of IT and OT networks and systems, whether in the workplace, home or public spaces. Through the CyberSecurity Malaysia Collaboration Programme (CCP), collaboration will be utilised as solutions to cyber risks that require a combined approach. CCP has been established to meet growing cyber demands, by promoting research, education, and technological innovation and the transfer of knowledge with strategic alliances between Government Agencies, private industry and academic institutions.

Q Is the cybersecurity profession receiving the attention it deserves?

A Nowadays, big corporates, especially public listed companies, have made cybersecurity a part of their risk management function and a C-suite responsibility. Chief Information Security Officers (CISOs) are being hired for the management, implementation and usability of information and technology.

Among their primary duties are creating business value through technology, ensuring the company technology systems are in line with business goals, and managing IT development and cyber risks as part of their technology budgets. While CISOs monitor changes or advancements in technology to identify ways to ensure their business has a competitive advantage, they are also equally responsible for ensuring that their company's IT and OT systems have the capacity to detect and respond to threats and attacks.

With a spate of personal data breaches, the Ministry of Communications and Digital is reviewing the need for data protection officers to monitor organisations so as to protect user data. The Personal Data Protection Act (PDPA) 2010 is being amended and the draft legislation is expected to be tabled in Parliament soon. It will introduce new obligations for both data users and data processors.

The Ministry is also collaborating with the cybersecurity community to explore quantum-safe cryptographic solutions to strengthen the nation's digital resilience.

"CISOs are also equally responsible for ensuring that their company's IT and OT systems have the capacity to detect and respond to threats and attacks."

Q How well prepared is Malaysia to deal with small and large-scale threats in terms of deployment of cybersecurity experts and enforcement personnel?

A According to a recent study by the Department of Skills' Centre for Instructor and Advanced Skill Training (CIAST) and CyberSecurity Malaysia, there are only 15,248 cybersecurity knowledge workers while our country requires at least 26,340 cybersecurity knowledge workers by the end of 2025. This acute shortage of experts is being addressed by various capacity-building measures.

To build a pool of cybersecurity experts and enforcement personnel, CyberSecurity Malaysia introduced its flagship programme called CyberGuru which focuses on building cybersecurity practitioners. Another flagship programme is Global Accredited Cybersecurity Education (Global ACE), which aims to develop cybersecurity managers, strategists and professionals. There are also other internationally aligned courses available not only for Malaysians but also for participants from ASEAN and Organisation of Islamic Cooperation (OIC) nations.

Q How vulnerable is the energy sector in terms of cyberattacks?

A The Malaysia Cyber Security Strategy 2020-2024 has identified the energy sector as an National Critical Information Infrastructure (NCII) that must be safeguarded and conserved to ensure the nation's security, economy, health and safety.

The energy sector is highly susceptible to cyberattacks. For example, a swift cyberattack on Malaysia's critical infrastructure such as power supply can occur instantaneously, catching authorities off guard. Once an attack is unleashed, it has the potential to disable the entire electrical grid and disrupt all internet-connected systems. This is the worst-case scenario.

About CyberSecurity Malaysia

CyberSecurity Malaysia is a Government Agency that traces its history to the early years of Malaysia's digital journey. Then as now, its priority is to safeguard the nation's cyberspace.

Initially a modest unit of the Malaysian Institute of Microelectronic Systems Berhad (MIMOS), the Government's strategic R&D pillar, it was entrusted with the Malaysia Computer Emergency Response Team (MyCERT). Gradually, it evolved to become the National ICT Security Response Centre (NISER), under the aegis of the then Ministry of Science, Technology and Innovation (MOSTI). When MOSTI embarked on the implementation of the National Cyber Security Policy in 2006, NISER was tasked to provide technical support.

In 2007, NISER was rebranded as CyberSecurity Malaysia to reflect its wider mandate. CyberSecurity Malaysia is now an Agency under the Ministry of Digital, which is responsible for ensuring the security and resilience of the national digital infrastructure. It offers a variety of services that includes capacity development programmes to boost the quantity and quality of cybersecurity professionals in the country.

We note that cyberthreats and attacks have been escalating in recent years, starting with the surge in illegal cryptocurrency mining activities in 2022. Law enforcement Agencies, the Energy Commission and Tenaga National Berhad (TNB) have raided and dismantled multiple mining operations scattered across various regions.

The subtle way in which illicit cryptocurrency mining works in the background while users are occupied with other things makes it more damaging. Tracing the accountable entity behind these operations is made more difficult by the inherent absence of user contact.

Furthermore, the rise in data breaches, ransomware and malware are among the critical threats that require urgent attention.

For an organisation, there is no such thing as being 100% secure since cyberthreats and attacks are always evolving. The interconnectivity among the various technologies means a cyberattack on one sector may collapse another critical sector. Thus, organisations must become cyber resilient and proactive in handling cybersecurity. In the end, each organisation must choose the level of risk it is ready to take on in the light of the industry, the sensitivity of the information at stake, and the expectations of the data owner.

Security is never an endpoint of being safe; rather, it is an ongoing process of lowering risk. Organisations should concentrate on areas where their greatest vulnerabilities are found, manage those risks using a combination of proactive and reactive measures, and periodically asssessing their security programme to find opportunities for improvement.

Q What are the job opportunities in cybersecurity in Malaysia?

A Malaysia has embraced digitalisation, which in turn creates a new environment with various benefits and technologies to explore. Companies that are investing in digitalisation technology recognise they also need to invest in cybersecurity infrastructure and resources as well. This will include hiring skilled professionals who can help detect, prevent and respond to security threats and ensure business continuity.

Recent studies show a surge in global demand for cybersecurity professionals and this trend is expected to continue. The United States of America (USA) Bureau of Labor Statistics reports that employment in the cybersecurity field is projected to grow by 31% from 2019 to 2029, which is much faster than the average for all occupations. We predict a similar trend in Malaysia.

This increased demand for cybersecurity professionals has also led to higher salaries and good career prospects. According to the US News & World Report, the median salary for cybersecurity professionals in the USA is around USD100,000.00 or approximately RM473,000.00 per year, and the demand for these professionals is expected to remain high in the foreseeable future.

As a profession, cybersecurity is a growth industry. Also, it should not be viewed through a single lens because it involves different competencies for different job scopes.

"The US Bureau of Labor Statistics reports that employment in the cybersecurity field is projected to grow by 31% from 2019 to 2029, which is much faster than the average for all occupations. We predict a similar trend in Malaysia."

Q Does the energy sector face a shortage of cybersecurity professionals and specialists? What kind of qualifications and experience must they have?

A The ISC Squared (ISC²) Cybersecurity Workforce Study 2023 reported that the global shortfall of cybersecurity knowledge workers in the energy industry currently stands at 70%.

As for cybersecurity qualifications in the energy sector, it calls for a combination of technical skills, industry knowledge, and soft skills that can be adapted and applied accordingly.

Education, certifications, and experience may play a critical role in hiring. It is the ability to continuously learn and stay updated with the latest trends that are essential for any cybersecurity professional and specialist.

Q Does CyberSecurity Malaysia collaborate with foreign Governments and companies to train cybersecurity professionals?

A We leverage on strategic collaborations with foreign firms and create joint research with the Government, industry, and academia to raise industry standards.

Over the years, we have been developing affordable training and certification programmes that are customised to our local needs and aligned to international standards. Our value proposition for training and certification is to make it affordable so that more people can get a chance to be trained and certified. All this is done without compromising quality.

"Continuous learning and staying updated with the latest trends is the mark of a high-calibre cybersecurity professional and specialist."

CyberSecurity Malaysia's Key Capacity Building Programmes

CyberGuru is a flagship capacity building programme designed in-house by technical experts in the industry. Apart from content development, CyberGuru involves partnerships with other international security platform providers such as SysAdmin, Audit, Network and Security (SANS) Institute and others to provide comprehensive training modules.

Global Accredited Cybersecurity Education (Global ACE) is a certification scheme for security professionals developed in collaboration with Government Agencies, industry partners and Institutions of Higher Learning (IHLs). Global Ace is aligned to the ISO/IEC 9001 while its professional examinations follow the ISO/IEC 17024 standards.

Global ACE has won the World Summit on the Information Society (WSIS) 2020 Winner's project for the Global ACE Certification Centre of Excellence for Building and Lifelong Learning. It offers the following professional certifications:

- Certified Penetration Tester.
- Certified Malaysian Common Criteria Evaluation and Certification (MyCC) Evaluator.
- Certified Secure Application Practitioner.
- Certified Digital Forensic for First Responder.
- Certified Information Security Awareness Manager.
- Certified Information Security Management System Auditor.

Pemulih Siberkasa Upskilling Programme is for newcomers to the industry. It integrates Global ACE Certification training, certification examinations and lifelong learning plans through professional memberships. Participants are eligible for the Global ACE Certification scheme when they pre-qualify for the certification course. After that, they can move up the career ladder by applying to become professional technologists or certified technicians with the Malaysian Board of Technology (MBOT).

Malaysian Technical Cooperation-Programme (MTCP) designs cybersecurity courses for participants from ASEAN member nations.

Organisation of Islamic Cooperation-Computer Emergency Response Team (OIC-CERT) are customised certification courses for participants from OIC nations.

CyberSecurity Malaysia Collaboration Programme (CCP) is where public and private sectors collaborate to forge a dynamic and secure cyber ecosystem by promoting innovation, supporting the economy and enhancing national security. Its goal is to develop solutions that require a holistic, collaborative approach to combat cyber risks.

CCP promotes research, education, technological innovation and transfer of knowledge through strategic alliances between Government Agencies, the private sector and academic institutions.

Among our key initiatives are CyberGuru and Global ACE Scheme, whose objectives are to train, retrain, and certify cybersecurity personnel as a world-class competent workforce in cybersecurity and promote the development of cybersecurity professional programmes within the region.

Q What are some of your international collaborations?

A Malaysia notes that due to the cross-border nature of cybersecurity incidents, international coordination and cooperation remain crucial, particularly in the area of investigation and mitigation. Therefore, tackling security issues relating to ICT even within the country calls for regional and international cooperation.

There is an urgent need for international collaboration for sharing information, skills, best practices, practical legal and technical approaches, capacity building and cybersecurity awareness and education. Some of our international collaborations are with:

- ASEAN Member States.
- Asia-Pacific Computer Emergency Response Team (APCERT).
- Organisation of Islamic Conference-Computer Emergency Response Team (OIC- CERT).
- The Council for Security Cooperation in the Asia Pacific (CSCAP).
- World Trustmark Alliance (WTA).
- Forum of Incident Response and Security Team (FIRST).

The fact is no entity can act alone to counter cyberthreats in this digital age. Inherently, there is the need to instil, build and develop trust between each other in order to overcome these issues in the longer run. The public and private sectors need to work closely together in all areas to deal with cybersecurity issues.

Public-Private-Participation (PPP) is an enabling factor between various parties and involves knowledge sharing in terms of technological advancement, expertise, and processes. There is a need for continuous PPP enhancements in the following areas:

- Sharing of information amongst relevant parties.
- Cyber incidents response and coordination.
- Innovative & collaborative research.
- Capacity building.
- Cybersecurity awareness and education.

All in all, we need to ensure a secure, resilient and trusted cyber environment in order to sustain progress and prosperity. In this regard, a more innovative and proactive adaptive security approach is required to forestall threat situations. Adaptive cybersecurity encompasses predictive, detective, responsive and corrective capabilities. In addition, the approach must be adaptive, dynamic and innovative, and take into account of people, processes and technologies.

Q Is there anything else you would like to add, Dato'?

A With large investments flowing into digital initiatives and projects, Malaysia has become a potential target for various cyberattacks. There have been various cybercrimes ranging from hacktivism to cyber espionage in Malaysia. In view of this, cybersecurity will continue to be one of the national security challenges for Malaysia, the region and the global community.

Malaysia will continue to enhance its readiness to handle any incident, to reduce its impact and duration as well as recover quickly from any attack. Our National Cybersecurity Policy has outlined strategies to help ensure the resilience of our national digital infrastructure and various assets which are vital for national defence and the economy.

On a final note, it is equally important to promote a culture of cybersecurity and cyber safety awareness and education across the Government, private sector and society in general.

This can help build stakeholder confidence in Malaysia's digital environment as a regional leader protecting the interests of our investors and citizens.

"Promoting awareness and safety in a cybersecurity culture can help build stakeholder confidence in Malaysia's digital environment as a regional leader in protecting the interests of investors and citizens."

HOW SECURE IS CONSUMER DATA?

Azlan Ahmad
Chief Information Officer, Tenaga Nasional Berhad (TNB)

With rapid digitalisation, the protection of customer data accumulated over the years has become critical given the sophistication of escalating cyberthreats.

What are common customer data breaches, and what proactive measures are power utilities implementing to prevent such incidents? And how can customers do their part in safeguarding their data and in preventing cybercrimes?

For insights, Energy Malaysia speaks to Azlan Ahmad, Chief Information Officer (CIO), Tenaga Nasional Berhad (TNB), Malaysia's public utility with more than 10 million customers.

As Malaysia's leading provider of sustainable energy solutions, Tenaga Nasional Berhad (TNB) leverages on technologies and digital systems by making various investments to enhance operational efficiency and improve customer service. These investments include initiatives such as the smart grid programme, smart meter roll-out, online billing and payment systems, and an online customer assistance hub. These automated and smart systems have resulted in the convergence of information and operational technologies (IT and OT), enabling TNB to spearhead a responsible Energy Transition (ET), operate more efficiently and provide better service experience to its customers.

The unfortunate reality is the digital world has paved the way for cybercrime, with threat actors launching cyberattacks for monetary gains or other reasons. Recognising that security of electricity supply to the country is an essential service and classified as National Critical Information Infrastructure (NCII) – meaning that it is fundamental to the economy and security of the nation – the industry has implemented several measures and mechanisms to ensure the security of its cyberspace.

Azlan Ahmad, Chief Information Officer (CIO) of TNB says, "At TNB, customer information is always of greatest importance. We adhere to world standards, regulations, compliances, and legislations such as Malaysia's Personal Data Protection Act 2010 (PDPA) and the European Union's (EU's) General Data Protection Regulation (GDPR), when it comes to handling customer information."

The PDPA governs the processing of personal data in commercial transactions while the GDPR is an important component of the EU's privacy and human rights law, particularly Article 8 (1) of the Charter of Fundamental Rights of the European Union. The GDPR also regulates the transfer of personal data outside the EU and the European Economic Area (EEA) countries.

"TNB only retains customer data that is relevant to our business," says Azlan. "We do not collect other personal information such as banking details or any other personal or business information. Additionally, any data collected from a customer must be obtained with appropriate consent of the owner before it can be processed for our business transactions."

Cause for Concern

In today's digital landscape, customer-related cybercrimes have become a significant concern. Customers need to exercise caution due to the widespread occurrence of phishing, identity theft, online fraud and various other online scams.

"Email scams are one of the most common tactics used to target TNB customers," says Azlan. "Fraudsters typically send emails claiming that customers have won promotions or cash giveaways. However, these emails often come with a catch – they require personal information or upfront payments before customers can receive their supposed benefits. To protect themselves, customers must refrain from sharing personal information or making any payments without first verifying the authenticity of both the email and the sender," says Azlan.

"Our customers are also advised to be vigilant about SMS scams," he adds. "These scams entice customers with offers or rewards of compensation for blackout incidents and provide a link to a fake website. The intention is to trick customers into revealing personal information or making payments. Customers are strongly advised to exercise extreme caution when receiving such messages," advises Azlan.

"Each organisation's threat landscape, risk tolerance and cybersecurity approach is unique, and there's no one-size-fits-all solution. Even within the utility sector, cybersecurity strategies vary significantly based on critical infrastructure responsibilities. As a trusted custodian of the nation's critical infrastructure, TNB holds a societal responsibility to safeguard its end users' interests. Our commitment to maintaining the security and integrity of our systems is paramount in fulfilling this obligation," says Azlan.

"There is no such thing as zero risk in cybersecurity," he adds. Instead, I'll say that cybersecurity is a continuous journey, and we continue learning and growing and doing the best that we can with the resources that we have to ensure that we have truly done all that is possible. In an IT and OT converged environment, safety, security and interoperability are vital.

"It is also crucial for companies to have a well-defined cybersecurity strategy that effectively differentiates between data security, data protection and data privacy. This distinction is important to ensure that each aspect can be effectively and efficiently addressed," says Azlan. "The objective of data privacy is to ensure that only authorised individuals, processes or systems can access the data, which is protected by various authentication tools in place.

"What is needed also is "people-centric security", explains Azlan. "This means working out who will likely be attacked in your organisation and protecting and equipping them. They are your VAPs – your "Very Attacked Persons". "If you know who they are, you can work out your business risks, and protect them better," he adds.

"In the end, there's a balance to be struck between educating the workforce and protecting them by understanding your VAPs and why they might be targeted. Once you've done that, you can act, and invest in additional technology to mitigate against future attacks.

"As custodians of our customers' data, we also invest considerably in doing whatever is possible to elevate the cybersecurity of our customers," says Azlan. "TNB is actively pursuing the adoption of various technologies including the use of Artificial Intelligence (AI) in its cybersecurity measures. This AI technology aims to enhance the detection of sophisticated attempts at identity fraud and the exploration of system vulnerabilities. By leveraging on AI, TNB hopes to strengthen its cyber defence and protect end users' data more effectively."

"It is crucial for companies to have a well-defined cybersecurity strategy that effectively differentiates between data security, data protection and data privacy in order for each aspect to be effectively and efficiently addressed."

Data Security vs Data Protection vs Data Privacy

Data security, protection and privacy all play pivotal roles in keeping sensitive data safe, but they each have their own goals and characteristics. Although there is a degree of overlap between them, there are also key differences between the three.

Data Security is designed to thwart a malicious attack against an organisation's data and other information technology (IT) resources. Although data security focuses specifically on keeping data secure, it also incorporates infrastructure security -- it's difficult to adequately secure data if the underlying infrastructure is insecure.

Data Protection centres around backup and recovery and is the process of safeguarding important information from corruption, compromise or loss. It is designed to ensure data can be restored, if there is a cyber incident.

Data Privacy is about ensuring that only authorised personnel, processes and systems have access the data.

Tokenisation Trend

Regulations such as the European Union's (EU's) General Data Protection Regulation (GDPR) and the United States of America's (USA's) Health Insurance Portability and Accountability Act of 1996 (HIPAA) focus heavily on ensuring the privacy of personally identifiable data. One way in which organisations are protecting themselves, while also helping to ensure consumer privacy, is by tokenisation.

Tokenisation involves removing personally identifiable information from data and replacing that information with a data token. This token is usually a number or a random string of characters and serves to separate the data from its subject. That way, if the data was leaked, there wouldn't be an easy way for the recipient of that data to associate a data set with an individual consumer.

Source: https://www.techtarget.com/searchdatabackup/tip/Comparing-data-protection-vs-data-security-vs-data-privacy.

"While we've made significant strides in educating internally on the fundamentals of safety, security, availability, confidentiality and integrity, we cannot be complacent. There's still more effort needed. But we're getting there, and I appreciate that it's now being driven collectively within TNB as a cyber-safety topic."

He explains further, "The sensitivity of data is determined by the domain or data owner, who recommends the appropriate classification category. This is because data sensitivity can vary from domain to domain and owner to owner. Nevertheless, as a standard practice, our cybersecurity policy classifies all customer data as sensitive data by default."

One of the challenges faced by businesses is the constant emergence of new and evolving cyberthreats. Azlan says, "We have a policy of continuously updating and upgrading our cyber defence solutions. I believe that cybersecurity is everyone's responsibility. As I see it, the need to manage cyberthreats extends beyond the organisation itself and rests with everyone who interacts with the organisation through our digital delivery channels, including vendors, contractors, industry partners and customers.

"I will also advise that collectively, we explore ways and means to band together to defend ourselves effectively. We need to start seeing cybersecurity as a cooperative effort, with imminent threat intelligence shared quickly and cybersecurity practitioners coming out to support one another. I see a big improvement in growing communities of cybersecurity leadership within the company and across industries that are very active and evolving into a nationwide ecosystem. We must continue this momentum to develop formal, effective and automated means of active defences at local, national and regional levels," adds Azlan.

"Cybersecurity is everyone's responsibility and the need to manage cyberthreats extends beyond the organisation itself, and rests with everyone who interacts with the organisation."

TNB TIPS!

TIPS TO PREVENT DATA THEFT

TIP 1

Exercise caution with emails and links
Be cautious when dealing with spam emails and suspicious links. Avoid clicking on unknown or unsolicited links, as they might be phishing attempts or malicious websites. Stay vigilant and protect yourself from potential threats.

TIP 2

Strengthen device and account security
Use strong and unique passwords for all your devices and accounts. Regularly update these passwords to enhance their effectiveness.

TIP 3

Install reliable security software
Protect your systems by installing comprehensive antivirus and other security software. Keep these programmes up to date to ensure they can effectively handle emerging and new threats.

TIP 4

Practise diligent log-out habits
Whenever you finish using the email, social media or online banking accounts, remember to log out. This simple habit reduces the risk of unauthorised access to your sensitive information.

TIP 5

Enable login notification alerts
Stay informed about any suspicious activities by enabling login notification alerts. This way, you will receive immediate notifications if someone tries to access your account(s) without permission.

TNB has a Scam Alert page on its corporate website that lists the modus operandi of cybercriminals by the year. They range from spoof emails impersonating TNB staff to fake notifications to customers that they are the lucky winners of competitions, or with offers of cash rewards and promotions from TNB. Another common scam is to call up customers, asking them to settle their bills within two hours or else their power supply will be cut.

When such suspicious phone calls or emails are received, TNB urges customers to disregard them, and to report them to TNB Careline Facebook or X (formerly Twitter) @Tenaga_Nasional.

Some victims have chosen to publicise their cases on the mass media and social media platforms. Such news reports are also posted on the TNB website, to educate customers.

Based on the recent spate of online scams, TNB suggests customers adopt the above practices to ensure the security of their internet activities, and to avoid becoming victims of cybercrime.

HOW YOU CAN PROTECT YOURSELVES AGAINST CYBERATTACKS

The following tips are recommended by various experts, ranging from cybersecurity firms to academic institutions and the Forbes Technology Council, to help consumers protect themselves from cyberattacks.

Keep Software Up to Date

Software companies typically provide software updates for three reasons: to add new features, fix known bugs, and upgrade security. Always update your computer / devices with the latest version of your software to protect them from new or existing vulnerabilities.

Keep Hardware Up to Date

Outdated computer hardware may not support the most recent software security updates. Additionally, the speed of old hardware is slower, which compromises immediate response to cyberattacks.

Use Anti-Virus and Anti-Malware

As long as you are connected to the web, it is impossible to have complete and total protection from malware. However, you can significantly reduce your vulnerability with an anti-virus software or at least one anti-malware installed on your computer.

Stay Sceptical

Maintain a healthy degree of scepticism about everything you receive via the internet, whether it's an email, text message, chat message or even a good old-fashioned telephone call. Do not do online quizzes or use add-on apps for social media unless you are absolutely sure the originating source is safe. When a pop-up or spam email appears on your window, and asks to share your username and password, ignore it.

Use Strong Passwords

A strong password is at least 12 characters long and is hard to guess. A combination of letters, numbers and symbols is recommended. You can use a tool like howsecureismypassword.net to find out how secure your password is.

Never Reuse Passwords

Use unique passwords for every website. Otherwise, if one website is compromised, the same password can be used to access your other web services.

Don't Save Passwords in Your Browser

Resist the habit of storing passwords in your browsers. Browser-stored passwords make login easier for hackers to enter your system.

Enable 2-Factor Authentication

Many platforms now allow you to enable 2-factor authentication, which is an electronic authentication method that requires two or more pieces of evidence before access is granted, keeping your accounts more secure. It works as another layer of protection that helps verify that it is actually you who is accessing your account, and not someone who is not authorised. Enable this feature when you can.

Double Check for HTTPS On Websites

The alphabet S in HTTPS stands for secure. When a website does not have HTTPS, there is no guarantee that the transfer of information between you and the site's server is secure. Double check that the website is using HTTPS, before giving any personal or private information away.

Always Use a Virtual Private Network (VPN)

For a more secure and privatised network, use a Virtual Private Network (VPN). All your personal information, location, and other data will be kept secure and private by an encrypted tunnel while your device is accessing the internet which in turn minimises the risk of other people gaining access to your information.

Avoid Public Networks

When you connect to a public network, you are sharing the network with everyone else who is connected to it. Any information you send or retrieve on the network is vulnerable. Stay away from public networks or use a VPN when you are connected to one.

Secure Mobile Devices

If your mobile device is unsecure, lost or stolen, it could be used to access your personal information, money, steal your identity and / or your irreplaceable data like photos and messages. Secure your devices with anti-virus software; setting a password to unlock as well as before applications are installed; and enable remote locking / swiping functions, if your device supports them.

Disable Bluetooth When Not in Use

Devices can be hacked via Bluetooth, and subsequently personal information can be stolen. Turn off your Bluetooth, when you don't need it.

Back Up Important Data

Important data can be lost as a result of a security breach. To restore data that is lost, back up important information frequently on a cloud or a local storage device.

HOW SECURE IS MALAYSIA'S ENERGY VALUE CHAIN?

Rahayu Ramli
Head of Cyber Strategy & Architecture
Petroliam Nasional Berhad (PETRONAS)

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 their 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 Berhad (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," says Rahayu Ramli, Head of Cyber Strategy & Architecture of PETRONAS.

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," says 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," points 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 says, "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 adds.

"While IT security has been an aspect of technology operations for decades, OT cybersecurity as a specific practice is a relatively new focus."

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," says 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 adds.

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," says 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," adds 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.

Rahayu adds, "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."

"In recent years, specific events triggered a re-examination of the security posture of complex cyber-physical systems. They are wake-up calls urging proactive and defensive actions against the evolving threat landscape."

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," adds Rahayu.

The Energy Commission's Perspective

"Our regulatory role 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," says 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 the them to decide what works best. Companies are strongly encouraged to follow global best practices for cybersecurity," says Khairol.

"Unfortunately, the rapid convergence of information technology (IT) and operational technology (OT) networks have given rise to unprecedented challenges," he points out. "Many in the energy sector feels 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," says Khairol.

Institutional cyber hygiene is a priority at the Commission, which 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 says.

Khairol Fahami Ismail
Senior Deputy Director, Information Management and Technology Unit

"Organisations must invest to strengthen their security ecosystems and also have in place the correct policy and strategy to ensure agility and flexibility to recover quickly from cyberattacks."

CRITICAL INFRASTRUCTURE: A CALL TO ACTION

The steady functioning of any country depends heavily on the seamless operations of its critical infrastructure. From power generation and distribution, oil & gas and minerals extraction to refineries, telecommunications and transportation, heavy industrial companies in these sectors are deemed critical infrastructure for the global economy. Increasingly digitalised and decentralised, they have become attractive targets for cybercriminals.

In the Global Cybersecurity Outlook 2022 report, the World Economic Forum asked 120 senior cyber leaders what worried them the most, and they answered unequivocally that infrastructure breakdown due to a cyberattack is their number one concern.

The United States of America (USA) was one of the earliest countries to engage in critical infrastructure protection. It codified what constitutes as critical infrastructure in 1998 under the Presidential Decision Directive 63, which reads: "Critical infrastructure are those physical and cyber-based systems essential to the minimum operations of the economy and Government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both Governmental and private."

The directive sought to have a clear mission to set up public-private cooperation models that help assure the provision of essential services to the Government, the economy and the public. In the US, Government programmes have led to a huge increase in cybersecurity spending, to over USD105 billion in 2021.

Over the last 20 years, the Organisation for Economic Co-operation and Development (OECD) Governments have experimented with various programmes to involve private companies in fighting cybercrimes. The EU Cybersecurity Act and the US Cyber Incident Reporting for Critical Infrastructure Act of 2022 were pushed through to incentivise the private sector to invest more in cybersecurity.

Heavy industrials face unique challenges due to their vastly distributed, decentralised governance structures and large operational technology (OT) environments. They have invested heavily in the past to becoming "cyber mature", as have other at-risk industries such as financial services and healthcare, leaving these companies at times short-funded to prepare for mounting threats in the present highly digitalised landscape.

As awareness of present and the possibility of new malicious threats grows, many top executives at these companies are focusing even more on cybersecurity. They are asking key questions like: What does it take to transform our cybersecurity capabilities? What investments will address most cyber risks? How much should we be spending? Leading companies are now rethinking their cybersecurity organisational and governance models.

Evolving Threats

There are several factors causing a growing threat environment in the heavy industrial sector. One is the rise of geopolitical tensions, which has led to attacks targeting critical national infrastructure. Heavy industrial operations can become collateral damage in broader attacks even when they are not the target, given that information technology (IT) networks are connected to OT networks through new technologies. These threats have become a major concern for top managers and boards of private companies as well as Government entities since they affect the nation's economy and security.

Recent discoveries in the networks of power distribution companies based in the USA and European Union (EU) indicate that cybercriminals established vantage points within OT networks from which to launch attacks at a future date. An example of this is the Dragonfly syndicate, which has been blamed for the breach of American and EU power companies to gather intelligence and build cyber capabilities to compromise OT systems. Groups like Dragonfly are increasingly procuring private-sector offensive tools, enabling them to deliver highly sophisticated cyberattacks.

Electricity, mining and oil and gas companies have revealed four main security challenges that are less prevalent in industries that are more cyber-mature, such as financial services and technology. One challenge comes from the digital transformations that many of these heavy industrial companies are undertaking. The other three relate to their distributed footprint, their large OT environment, and exposure to third-party risks.

"Among the factors threatening the heavy industrial sector is the rise of geopolitical tensions which led to attacks targeting critical national infrastructure."

CYBERSECURITY CHALLENGES FACED BY INDUSTRIES

DIGITAL TRANSFORMATION

While undergoing digital transformation, decision-makers at heavy industrial companies often overlook the cost of managing associated cybersecurity risks. Cybersecurity is not often a key component of the transformation, and cybersecurity architects are brought in only after a new digital product or system has been developed. In addition, cybersecurity capabilities that are bolted on top of technology products and systems are less effective than those built in by design. Bolt-on cybersecurity can also harm product usability, causing friction between developers and user-experience designers on one side, and cybersecurity architects on the other. This compromises the cybersecurity of a company's operational technology (OT) system.

DISTRIBUTED FOOTPRINT

The wide geographical footprint of heavy industrials can harm their cybersecurity efforts. It limits their ability to identify and protect key assets. They may struggle in managing vulnerabilities across end devices. While they have control over their IT assets managed centrally, they have little to no visibility over assets managed by business units or third parties.

LARGE OPERATIONAL TECHNOLOGY ENVIRONMENT

Most security efforts to protect OT involve network-based controls such as firewalls that allow data to leave the OT network for analysis, but do not allow data or signals to enter it, making these controls ineffective against attacks originating from within the OT network, such as malware on removable devices. Additionally, many traditional cybersecurity tools cannot be applied to the OT environment. In some cases, these tools can harm sensitive devices that control plant equipment leading cybersecurity teams to work around the problem that is less effective at managing risk. Adding more risk and complexity to the mix are newer technologies such as industrial Internet of Things (IoT) devices, cloud services, mobile industrial devices and wireless networking.

EXPOSURE TO THIRD-PARTY RISKS

Compared with information technology (IT), the OT environment is highly customised as it supports processes specific to a given operation. The proprietary nature of OT equipment means that companies rely on the Original Equipment Manufacturer (OEM) to maintain it and make changes. This equipment is often a "black box" to its owner, who has no visibility into security features or levels of vulnerability. Companies are increasingly outsourcing maintenance and operation of OT or adopting build-operate-transfer contracts. These types of relationships require third parties to gain physical access to OT networks. Where remote maintenance is required, the owner needs to establish connections to the OEM networks. These remote connections are mostly unsupervised by owner organisations, leaving a blind spot. Several heavy industrials have reported that third parties frequently connect laptops and removable storage devices directly into their OT network, without any prior cybersecurity checks despite the dangers of infection.

Investing in Solutions

Top management at heavy industrials are now integrating cybersecurity early in their digital transformation initiatives, in both the IT and OT environments. If they are to manage cyber risks effectively, they will need to embed security earlier in the process, with investments in cybersecurity programmes, developer training and oversight – with deep integration of cybersecurity functions in the IT and OT ecosystems.

According to a 2019 report by McKinsey and Company, one way to accomplish this is to create an integrated security operations centre that covers both IT and OT, housing detailed escalation protocols and incident response plans for OT-related attack scenarios.

Petroleum giant, Shell Oil Company, has invested heavily in working with some of its IT networking providers and some OT OEMs to develop a unified security-management solution for plant-control systems across over 50 plants. Solutions like these will enable centralised asset management, security monitoring, and compliance, dynamically and in real-time.

Renewable Energy Risks

In Europe, the sophistication of Russian cyberattacks against Ukraine has been a wake-up call as to how vulnerable digitalised and interconnected power systems could be to hacking. While cyber campaigns that Russia has been running against Ukraine have been very targeted at Ukraine, European energy companies and utilities are following it keenly, to observe and learn from it.

According to a Reuters report (15 June 2023), European power companies as well as half a dozen independent tech security experts stressed that the digitalised and interconnected technology of thousands of renewable assets and energy grids springing up across Europe presented major – and growing – vulnerabilities to infiltration. "The new energy world is decentralised. This means that we have many small units such as wind, solar plants, and smart meters that are connected in a digital way," said Swantje Westpfahl, Director at Germany's Institute for Security and Safety.

"This networking increases the risks because there are significantly more possible entry points for attacks, with much greater potential impact."

While malware packages like Triton might be exotic algorithmic weapons, the most common mode of entry used by hackers looking to deliver them is via phishing emails designed to elicit data from employees like network passwords. Such attacks are "more or less constant", according to Cem Gocgoren, information security chief at Svenska Kraftnaet, a Swedish grid operator that has roughly quadrupled its cybersecurity team to about 60 in the last four years and is raising awareness among staff. "We have to make them understand that we are under attack all the time. It's the new normal."

Traditional power plants like gas and nuclear typically operate on airgapped IT infrastructure that's sealed off from the outside, making them less susceptible to cyberattacks than physical sabotage, a senior researcher at Kasperky's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) that studies and detects cyberthreats on industrial facilities, told Reuters. "By contrast, the ever-growing number of smaller renewable installations around Europe are being run on diverse third-party systems that are digitally hooked up to the power grid and are below the power-generation monitoring threshold set by safety authorities," he added.

This kind of interconnectedness was demonstrated in February 2023 when a Russian cyberattack on a Ukrainian satellite communications network knocked out the remote monitoring of more than 5,800 wind turbines of Germany's Enercon and shut them down, said Mathias Böswetter, head of IT security at German energy industry group BDEW. While the incident did not affect the electricity grid, it showed the escalating cyber vulnerabilities posed by the energy transition.

"The new energy world is decentralised, which increases cybersecurity risks because there are significantly more possible entry points for attacks, with much greater potential impact."

An IEA Report: Is the Power System Lagging Behind in Cybersecurity?

Finding and Retaining Skilled Professionals

2022 was a record year for cybersecurity incidents targeting oil and energy, says S&P's Global Energy Security Sentinel. It reported that there had been 45 cyberattacks on energy since 2017, with the United States of America (USA) most targeted and Europe heavily earmarked. In the third quarter of 2023 alone, there were five cyberattacks targeting the energy market compared to only two in the previous quarter. These incidents were focused more on the power, gas and nuclear sectors than oil.

Acknowledging the alarming rise in cyberattacks on energy, particularly utilities, the International Energy Agency (IEA) says increased attacks may be due to serious difficulties utilities have in finding and retaining skilled professionals needed to defend themselves. The IEA report entitled "Is the Power System Lagging Behind" (01 October 2023) states that while electric power utilities across the globe already dedicate substantial budgets to cybersecurity - averaging 8% of total information technology (IT) budgets in the USA and Canada - job posting data from major power utilities in the USA shows that cyberattack events trigger sudden increases in demand for cybersecurity professionals, suggesting a lack of long-term strategy or planning in the past. Smaller companies in the USA and others in developing economies could show a similar behaviour in the future after suffering preventable attacks.

Utilities in the European Union (EU) have also been in reactive mode, it adds. Past trends suggest that EU utilities were not fully prepared at the time to face critical events such as the COVID-19 pandemic and Russia's invasion of Ukraine.

Despite occasional spurts in cybersecurity job postings by power utilities, long-term data from the USA shows a slight decrease in the share of cybersecurity among total postings in the sector since 2010.

By contrast, the share of cybersecurity job postings in finance and insurance companies in the USA has increased almost threefold during the same period, and that in the public administration almost twofold. The figures indicate that the number of cybersecurity expert job postings in power utilities has not evolved as rapidly as total job posting trends in the sector, despite the increasing digitalisation of power systems and their exposure to cyberattacks. Very similar trends have been observed in Canada and the United Kingdom.

Salaries Lag Behind

The report also noted that salaries offered to cybersecurity hires in power utilities are among the lowest among US industries. In 2021 and 2022, US power utilities offered an average annual salary of USD81,800, higher than in educational services but substantially lower than top sectors such as finance and insurance, which offered more than USD100,000.00. Given the wide range of job vacancies, cybersecurity experts are likely to prefer sectors offering better conditions, further increasing the shortage of professionals in the power utility sector. Finance and banking, in particular, is a sector well known for its high levels of investment in cybersecurity.

What's more, the salary gap for new cybersecurity positions at top paid sectors in comparison with power utilities has been wider than ever since early 2021. While this may be explained in part by differences across sectors in wages (and the degree to which firm-level revenue is shared with workers), the relatively low and stagnant salaries for cybersecurity workers within power utilities is a cause for concern in the face of increasing threats.

Policymakers, Regulators and Equipment Providers Have a Role to Play

The responsibility for securing power systems does not rest exclusively with power utilities, says the IEA report. Policymakers play a central role in enhancing the cybersecurity of power systems, along with regulators and equipment providers.

Without a strategic approach towards ensuring cyber skills, power system stakeholders may not be able to effectively cope with future attacks. IEA suggests that the main action areas besides having skilled professionals to achieve a better secure cybersecurity framework, lies with institutionalising responsibilities and incentives; identifying, managing and mitigating risks; monitoring progress; and responding to and recovering from disruptions. Smaller utilities may require additional support from policymakers and regulators, as their fixed costs for cybersecurity infrastructure and systems are higher in relative terms.

The report says that some power utilities have relied on external support from specialised companies instead of creating large in-house cybersecurity teams. But internal adaptation to current cyberattack trends across teams is necessary as it involves the whole value chain of power utility companies. Cyberthreats will continue to evolve and become both more frequent and more powerful, given the established business models of cybercriminals and the wide range of advanced technologies at their disposal. It is therefore essential that every power utility, big or small, includes cybersecurity as a core element of their business strategy and ensures access to in-house cybersecurity professionals and their skills, continuously updating them and ensuring talent retention.

FROM COMPUTERISATION TO DIGITALISATION, A NATURAL PROGRESSION

As early as the 1960s, the newly independent Government of Malaysia had set its sights on the computerisation of Government departments, to make them more efficient. It was to spell the end of manual operations that were prone to error, speed up the work pace, and enable the Government to have databases of the many public services and segments of the population it serves. The goal was to make governing more structured, systematic and effective.

The first adopter of computerisation was the public utility National Electricity Board or NEB (the precursor to Tenaga Nasional Berhad - TNB), which was then a Government entity. It was the first organisation in the country to install a computer system, an IBM 1440, at its new head office in Jalan Bangsar, Kuala Lumpur, to expedite accounting functions, as electricity demand grew. A larger and more compatible system, the IBM System 360/30, followed by the IBM System 370/4300, were later installed to streamline and expedite other operations, especially engineering.

These computers were large mainframe structures that looked like huge cabinets that had to be installed in specially built temperature-controlled rooms.

Given its head-start with computers, the NEB proceeded to develop an accounting system that became one of its most effective management tools in the 1960s. By 1979, computerisation had progressed to several operational areas, and NEB went on to establish a fully computerised control centre – the National Load Dispatching Centre (NLDC) – that was set up in the head office. With the computerised NLDC, the network system became more integrated and could also be better monitored.

By the 1980s, NEB had built sufficient computerised infrastructure and earned a good service record. By then, many other large private organisations too had woken up to the wonders of the information technology (IT) revolution that was sweeping the world. They began investing in computerisation to manage their businesses with data processing and management information systems.

Between the 1960s and 1980s, there was a wave of computerisation, mainly IBM mainframes that served large enterprises, while minicomputers were preferred by medium-sized enterprises. Personal computers were a rarity until Microsoft founder, Bill Gates declared "to have every home own a computer, using Microsoft software", as part of his company's vision to conquer the world.

Initially, computers were used for financial systems, to monitor costs and revenue. Malaysia Airlines System (MAS), for example, began its computerisation journey at the Finance Department. After that, they were used for other core business functions, from management decision-making to customer services. In time, computer facilities became standard in reputable organisations, but they had not yet penetrated homes and were not as yet owned by the majority of individuals.

Then, came the critical turning point in 1996, when Malaysia rolled into the world of the internet that was revolutionising the West, with the launch of the Multimedia Super Corridor (MSC). Thereon, computerisation was overtaken by digitalisation that relied on the internet, web-based technology and connectivity. They opened up a new world of possibilities, not just for businesses but also for the public at large.

"The internet is a tidal wave. It changes the rules. It is an incredible opportunity as well as an incredible challenge."

Malaysia was not far behind the West in embarking on its digital journey, and the credit for this goes to the foresight and political will of former Prime Minister Tun Dr. Mahathir Mohamad who was instrumental in spearheading the MSC, which had an international advisory panel that included global tech titans. In its wake, the Malaysia Digital Economy Corporation (MDEC) was established to spur local and foreign investments in digitally-driven businesses in the country.

A First in Malaysia

The National Electricity Board's first computer made its debut at the head office building in Jalan Bangsar in 1965. It was officially launched by the Prime Minister of the day, Tunku Abdul Rahman Putra al-Haj, and it marked the beginning of a brand new chapter not just for the public utility but also for Government departments. The IBM 1440 is the first computer in the country, and it was used to automate staff payroll.

In an interview with The Star newspaper in conjunction with Malaysia's 50th anniversary, Mohd Hanafi Abdul Jabbar, senior manager of regional operations, recalled: "The computer looked like those in old James Bond movies. I was told it took two engineers and three other staff to put it together."

The IBM 1440 cost RM700,000.00 and had a 8 KB storage capacity. Today, more than four decades later, a personal desktop computer costs about RM3,000.00 and has a 320 GB capacity – roughly 40 million times that of the old timer!

Source: Lighting Up Lives, TNB's 40th Anniversary publication.

For Malaysia, a trading nation since time immemorial, entering the digital age was a strategic national decision. It was acknowledged by successive Governments that the country will lose out in the increasingly competitive global economy if the country is not connected to its trading partners, both existing and potential. By the late 20th century, digitalisation was recognised as vital to give the country access to export markets as well as to improve overall socio-economic prosperity.

Today, Malaysia has an active internet space, with millions of users and hundreds of technology companies developing applications. The main issue for some years was the internet speed and the digital divide between urban and rural areas. The Government is addressing these issues by upgrading and expanding digital infrastructure across the country, although the industrial Klang Valley, Penang and Johor are given priority.

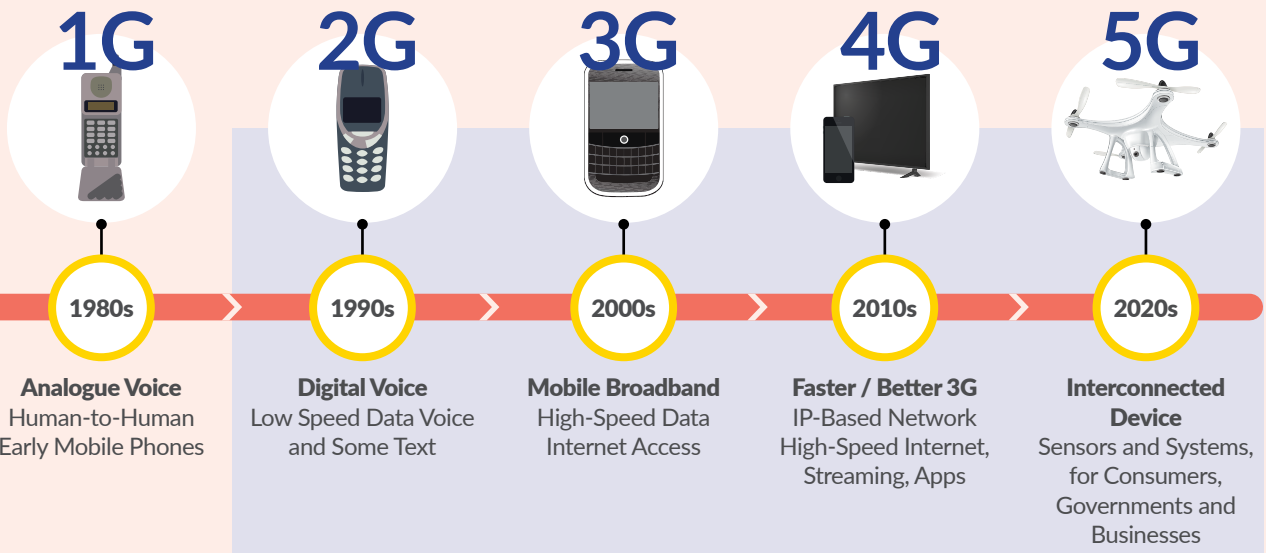
Malaysia's internet connectivity journey began with 1G in the 1980s, followed by 2G and 3G. They are now history, and today, under the Malaysian Communications & Multimedia Commission's (MCMC's) Jalinan Digital Negara (JENDELA) programme, 4G has become standard, with 5G communication now available in selected areas and set to become nationwide in the next few years.

Continuous upgrading of digital infrastructure is crucial for Malaysia to pursue its current digital economy ambitions. Equally crucial is the adoption of digitalisation industry-wide, particularly among Small and Medium Enterprises (SMEs). Besides economic gains, digitalisation is recognised as an enabler of the national decarbonisation goals.

Like elsewhere, the challenges lie in ensuring that organisations have adequate resources to go digital – financially as well as in terms of talent and cybersecurity.

THE JOURNEY TO CONNECTIVITY

Since its establishment more than 25 years ago, the Malaysian Communications and Multimedia Commission (MCMC) has facilitated the regulation of mobile cellular service provisioning including 3G, 4G, and 5G, in line with international standards.[1]



1998 - Convergence Framework via the Enactment of the Communications and Multimedia Act 1998

National Telecommunication Policy
1994-2020

- A national policy to ensure the growth of telecommunications services and its use to support national development.

MyICMS
2006-2010

- A strategy to drive forward the delivery of advanced information, communications and multimedia services which includes focusing on 3G broadband adaption.

National Broadband Initiative
2010-2020

- A national strategy that brings broadband to the whole nations.

Jendela
2020-2025

- Planning for 5G hubs started with the formation of 5G Task Force (2018) and 5G Demonstration Projects & Test Beds / Trials (2019).
- Launch of National Fiberisation & Connectivity Plan (NFCP) 2019-2020 with intention to improve coverage, speed and quality of connectivity.
- The outcome of the National Digital Infrastructure Lab (NIDL) 2020 is the formulation of JENDELA 2020-2025, which is a plan to improve coverage and quality of service and set the foundation for 5G.

1 International Mobile Telecommunications (IMT) standards defined by the International Telecommunication Union (ITU).

Digitalisation - Enabler of Energy Transition

Digitalisation is the cornerstone of the Fourth Industrial Revolution. It is recognised as an important driving force for new technologies that are rewriting the script for global economic growth since the 1990s. In the energy industry, digitalisation has been playing a key role as the enabler of energy efficiency and energy substitution.

It has catalysed "re-industrialisation" strategies to improve the efficiency of resource allocation and optimise the industrial structure. It also sparked an awakening that with the deep integration of digitalisation and real economy, new ideas are likely to surface to solve existing energy problems.

The International Energy Agency (IEA) reported that global energy consumption increased by 50% and 75% between 1985 and 2020 respectively, and that by 2025 it is estimated to increase by 54%, compared with 2020 figures.

In industrialised countries alone, energy consumption will increase at an annual rate of 1.2% while in developing countries in Asia, it is set to more than double from 2020. This implies that global energy consumption will increase dramatically in the future since it is a critical component of modern industrialisation. Industrialisation is on the agenda of developing countries in their quest for economic growth and prosperity.

As for carbon emissions, in 2018, global carbon emissions stood at 600 million tonnes, of which carbon emissions from the energy sector increased by 2.2%. Carbon emissions continued to increase by 0.5% in 2019, while in 2020, due to the COVID-19 pandemic, global carbon emissions fell for the first time by 5.8%. But there was a rebound effect at the end of 2020.

In the aspiration for a win-win scenario between economic growth and environmental conservation, global energy systems are undergoing an energy transition, to slow global warming by reducing energy consumption and intensity and to turn to renewable resources to curb emissions.

Already, digital technologies are changing how, where and when energy is produced, supplied and consumed. One outcome of digitalisation is micro-grids and Artificial Intelligence (AI) optimisation systems that are connecting micro-grids to busbars trunking systems and remote terminal units, to substantially reduce power consumption especially in rural areas. Another is the Internet of Things (IoT) based micro-grid control, a cloud-based server that has the capability to facilitate electrical network regulation, while avoiding fluctuations in the daily supply of power. Recent literature suggests innovative technological applications that can be used to improve distribution networks with on-site energy storage.

Digital technologies are also being used to improve energy efficiency in buildings by equipping them with smart appliances and intelligent energy management systems. In transportation, automated, connected, electric and shared mobility are set to shape the future of energy consumption.

"Technology is shifting the balance of power from the seller to the buyer."

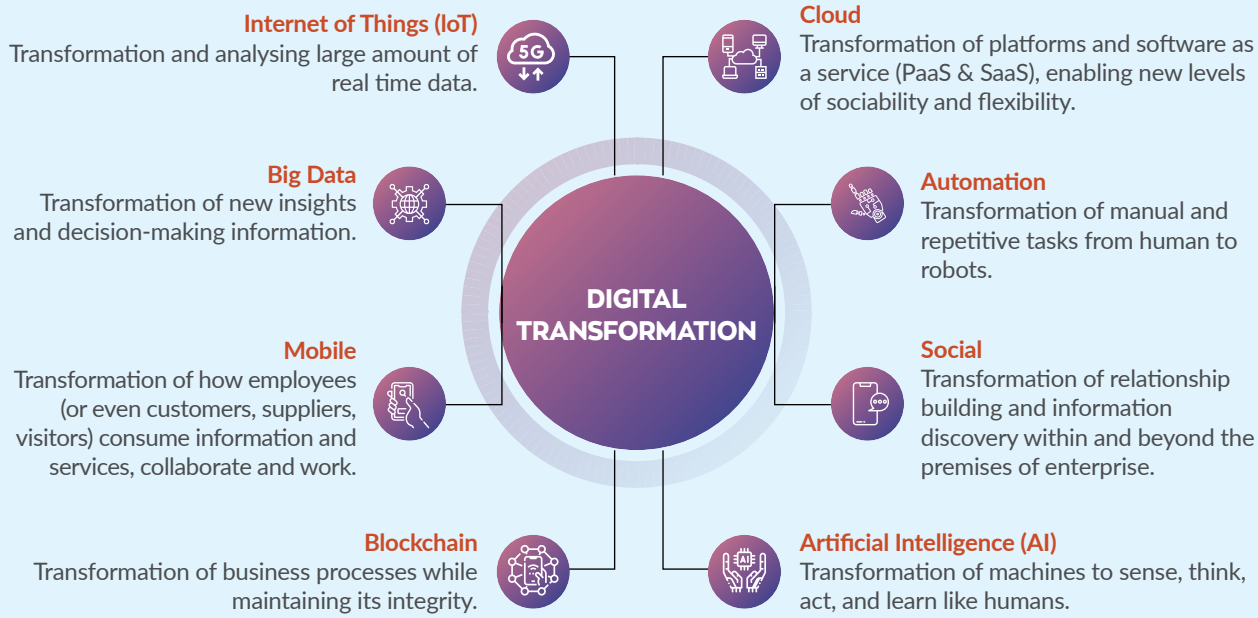
From the utility perspective, digital technologies allow them to monitor their systems, to determine where there's pressure and to procure services and solutions needed to keep their systems running smoothly, efficiently and profitably.

In fact, information and communication technology (ICT) is already being leveraged upon for the integration of Renewable Energy Sources (RES) based distributed generation through an efficient energy management. Also implemented are smart interconnection of microgrids to distribution networks; optimal IoT-based Energy Management (EM) frameworks; and smart grids (that is meeting energy balance with minimum cost) to ensure through intelligent services and the implementation of various IoT technologies which is a list of innovative digital developments that is endless and set to continue.

The Case for Digitalisation in Energy

In his much-cited book "Digital Transformation – Building Intelligent Enterprises", Anup Maheshwari identifies eight key drivers of digitalisation. They are IoT, cloud, big data, automation, mobile, social, blockchain and Artificial Intelligence (AI). Through these technologies, businesses can transform themselves to become more responsible and sustainable entities that are driven by customer and environmental considerations.

DIGITAL TRANSFORMATION KEY DRIVERS



Digitalisation will also enable consumers to participate in energy system operations. It creates opportunities for them to interact directly in balancing demand with supply in real time. Throughout this process, centralised transmission networks will continue to be the backbone supporting the transition, balancing the overall system.

In the digital economy, it is no longer simply about the management empowering workers. It is also the empowerment of consumers / customers / stakeholders. Access to new and powerful technological tools is giving customers the ability to conduct transactions on their own terms. Technology is shifting the balance of power from the seller to the buyer.

In a nutshell, some of the benefits consumers stand to gain from digitalisation are as follows:

- Monthly utility bills can be reduced from better efficiency and lesser costs of supply.
- Power grids become more resilient and reliable so power outages can be reduced and response times can be faster.
- More choice and control over energy consumption and generation due to smart appliances, distributed energy resources, and digital platforms.

DIGITAL TRANSFORMATION BENEFITS FOR THE ENERGY SECTOR

1. Optimise production, operations and maintenance through data analytics, automation and Artificial Intelligence (AI).
2. Enable innovation, collaboration and scalability through cloud computing, blockchain and Internet of Things (IoT), to reduce emissions.
3. Help overcome barriers of legacy systems, cultural resistance and unclear value propositions that often hinder new solutions.
4. Lower monthly utility bills due to improved efficiency and reduce cost of energy supply.
5. Reduce outages and have faster response times due to enhanced reliability and resilience of power grids.
6. Leverage on smart appliances, distributed energy reserves and digital platforms, to create more choices and control over energy consumption and generation.

Source: "Digital Transformation – Building Intelligent Enterprises" by Anup Maheshwari.

Interconnected Electricity Systems

According to the IEA, it is estimated that by 2040, more than 1 billion households and 11 billion smart appliances could participate in interconnected electricity systems, thanks to smart meters and connected devices. This is likely to allow homes to influence when and how much electricity they can draw from the grid.

Also, according to the IEA, with the help of smart thermostats, smart lighting and other digital tools, buildings could reduce their energy use by 10% by using real-time data to improve operational efficiency. Meanwhile, massive amounts of data, ubiquitous connectivity, and rapid progress in AI and machine learning are enabling new applications and business models across the energy system, from autonomous cars and shared mobility to three-dimensional (3D) printing and connected appliances.

Transformation is also taking place in how energy is produced – from smart oil fields to interconnected grids, and increasingly, renewable power. Digital technologies could help integrate the higher share of variable renewables into the grid by better matching energy demand to solar and wind supply. The energy supply sector also stands to gain from greater productivity and efficiency, as well as improved safety for workers.

Risks, Regulations and Mindset

While creating new horizons and opportunities, digitalisation also raises the spectre of cyberthreats that have the potential to disrupt the security of markets, businesses, jobs, even national defence. For example, IoT devices herald significant benefits in terms of energy efficiency for domestic, commercial and industrial consumers. However, they can also be used to launch cyberattacks on owners as well as others connected to their devices. Such attacks are becoming common, cheaper and easier to organise. What is unfolding is that consumers can be the entry points for cyberattacks on big organisations because of poor digital security embedded in their computers and smart phones.

It is thus critical to take the necessary measures to minimise such risks, although many experts believe that cyberattacks are going to be on the rise. And it is the responsibility of every internet user to take the precautions to ensure they are operating safe and secure networks, computers and all other connected devices such as smart phones, smart television sets and the like.

Another concern is the question of who controls the data and information and how it is used. Digitalisation and data collection should enable the establishment of an open, transparent and non-discriminatory market for the utilities and market providers. At the same time, precautions must be taken not to compromise on data privacy and security.

There is also a need to change the mindset of the industry, for them to know that digitalisation will force changes upon them, on both the management and employees. They have to be alert to changes happening quickly and be prepared to unlearn and relearn quickly. That is the face of innovation, where the business-as-usual scenario is fast becoming obsolete.

Policymakers and regulators also have to play their part. They have to ensure a nurturing environment where digital technologies can flourish. New solutions are typically digitally-driven, and it is vital to have policies and regulations to encourage the birth of new technological solutions that can make things better today and prepare nations to face future challenges with more confidence.

Malaysia's Energy Transition

Malaysia was recognised as the best country in Southeast Asia in the Energy Transition Index 2023 by the World Economic Forum. The Government is committed to low-carbon development aimed at restructuring the economic landscape to become a more sustainable one.

The National Energy Policy (NEP) that covers the period 2022-2040 outlines the Government's priorities for the energy sector. It streamlines various existing policies and creates a long-term vision, which is coordinated across various stakeholders, and provides an updated direction for the energy sector. Essentially, it lays down the game plan for the country's energy transition.

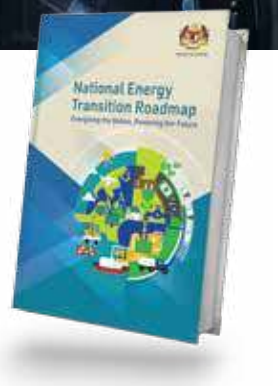
Malaysia's commitments are toward net zero carbon emission by 2050, which involves decarbonising the generation sector by shifting away from thermal generation, while advancing with sustainable low carbon technologies across the energy value chain. The NEP is a live document, which acknowledges the fast pace of technology and that telescoping into the distant future can derail the best laid plans. What it has done is to set a series of targets to guide Malaysia to first become low carbon society by 2040, before taking the final leap into a net zero nation in 2050.

How this is to be done has been detailed in the Malaysia's National Energy Transition Roadmap (NETR) launched in August 2023. The NETR's focus is on developing capabilities and boosting the clean energy capacity through flagship projects centred around energy efficiency, renewable energy (RE), hydrogen, bioenergy, green mobility and Carbon Capture, Utilisation and Storage (CCUS). Technology and infrastructure development are identified as among the enablers to realise the goals of the NETR.

Running parallel to NETR is the Digital Economy Blueprint, also launched by the Government in 2023. On the one hand, Malaysia aspires to become a net zero carbon emissions nation by 2050, while on the other hand, it is revving up to becoming a digital economy by 2030.

By harnessing synergies between these two roadmaps, we can expect the pace of digitalisation of Malaysia's energy sector to quicken and in turn make substantial contributions to help Malaysia achieve its Nationally Determined Contribution (NDC) as per the Paris Agreement. Currently, Malaysia's NDC is to reduce its greenhouse gas (GHG) emissions intensity of Gross Domestic Product (GDP) by 45% by 2030, relative to the emissions intensity of GDP in 2005.

EVENTS AND ACTIVITIES
IN AND AROUND ST



MALAYSIA LAUNCHES ROADMAP FOR NET ZERO 2050

The Malaysian Government has embarked on an ambitious plan to transform the country's energy landscape with the National Energy Transition Roadmap (NETR) that was released in July 2023. The roadmap outlined measures to achieve the country's goal to become a net zero carbon emissions nation by 2050.

In presenting Phase 1 of NETR, the Minister of Economy, Rafizi Ramli, said, "The NETR is this administration's effort to change the economics of renewable energy (RE) so that we can rapidly scale up our installed capacity with the right infrastructure and technology.

The NETR is split into two phases. Phase 1 comprises 10 flagship projects based on six energy transition levers – energy efficiency, RE, hydrogen, bioenergy, green mobility and Carbon Capture, Utilisation and Storage (CCUS) – and is estimated to create about 23,000 jobs. Phase 1 will leverage on projects that are already ongoing and Phase 2 will focus on developing a low carbon pathway for Malaysia.

Rafizi added that the NETR is not just another policy document. Instead, it represents a "different way of thinking" about the economy and livelihoods. "For example, instead of asking every household to pay for an expensive solar panel, the Government wants to offer an income opportunity. In every home, we intend to give households the option to lease out their rooftops in return for a monthly income that could lower their electricity bills and put more cash in their pockets. The Government is taking the lead in this by allocating RM80 million for solar panels to be installed on the rooftops of Government buildings. Soon, we would like to see solar panels installed nationwide, covering offices, factories, multipurpose halls and all types of buildings."

KEY TARGETS OF NETR

- **Installing 70% renewable capacity and phasing out coal-fired power plants by 2050.**
- **Phasing out grey hydrogen production and setting up of a low carbon hydrogen hub by 2030 and another two hubs by 2050.**
- **Increasing bioenergy capacity to 3.5 billion litres by 2050.**
- **Increasing biomass and biogas generation capacity to 1.4 GW by 2050.**
- **Developing three CCUS hubs with a total storage capacity up to 15 million tonnes per annum (Mtpa) by 2030, and another three hubs with total storage capacity between 40 and 80 Mtpa by 2050.**

The NETR also aspires to install 10,000 electric vehicle charging stations along highways and commercial buildings by 2025. This will be done in collaboration with strategic partners such as Tenaga Nasional Berhad (TNB), PLUS Malaysia Berhad, Permodalan Nasional Berhad (PNB), Petroliam Nasional (PETRONAS)'s Gentari and the Sunway Group.

Malaysia is to also build Southeast Asia's largest hybrid solar photovoltaic (PV) power plant under the NETR: a 1 GW power plant at an Integrated RE Zone. "The scale of our ambition has attracted high profile global investments from major economic blocs, totalling RM6 billion," said Rafizi. The Memorandum of Understanding (MoU) for the Integrated RE Zone was inked following the launch of the NETR.

The Minister also said that the roadmap will open up the hydrogen gateway in Sarawak that is implementing projects to emerge as the hydrogen hub in the country. This will put in place the framework for Carbon Capture and Storage (CCS) so that catalyst projects can be implemented.

Other catalytic NETR projects include the setting up of five centralised Large Scale Solar (LSS) parks with 100 MW capacity each, to be co-developed by TNB. The utility giant will also develop 2.5 GW of hybrid hydro-floating solar PV projects at its hydro dams. Rafizi shared that by 2050, NETR could attract investments ranging from RM435 billion to RM1.85 trillion.

Climate change expert, John Yeap of international law firm Pinsent Masons said, "In setting out a roadmap, Malaysia is showing its commitment to its net zero target. As is to be expected, the drivers for setting out a roadmap and the tools available in the toolbox for doing so, are consistent with its neighbours and elsewhere. As an export economy, the implications of legislative developments elsewhere such as the European Union (EU)'s Carbon Border Adjustment Mechanism and the United States of America (USA) Inflation Reduction Act will have to be factored into the need to decarbonise that goes beyond just delivering on its net zero commitment."

TENAGA NASIONAL BERHAD'S
INAUGURAL ENERGY TRANSITION CONFERENCE

On 28-29 August 2023, Tenaga Nasional Berhad (TNB) hosted a two-day inaugural Energy Transition Conference, which sought to generate meaningful conversations between thought leaders involved in shaping the direction of energy and sustainability. As the world moves towards a cleaner and greener energy transition, panel discussions were held, centred around the four key pillars affecting the global energy landscape, namely, the future of energy, green mobility, sustainable cities and digitalisation, to observe and learn from it.

Featuring experts in the various fields related to the power industry and sustainability, the conference shared insights and outlooks based on the complexities facing the world as it moves towards a clearly defined pathway to decarbonisation.

During the conference, the Guest of Honour, Prime Minister Dato' Seri Anwar Ibrahim launched Phase 2 of the NETR and announced the allocation of a RM2 billion seed fund as an energy transition facility. He said, "This facility will enable catalytic blended finance to ensure a seamless flow of financial resources towards energy transition projects that are marginally bankable or yielding below-market returns." He added that the allocation was vital due to the present state of the country's decarbonisation technologies, which he said were still at a nascent stage.

The progress of the country's development, he said, hinged on alternative energy sources as well as robust regional and international collaboration. "As the paramount challenge in energy transition is financing, it is estimated that an investment of at least RM1.2 trillion between 2023 and 2050 is needed to enable a responsible energy transition."

The Prime Minister added, "The energy transition is not an option, and the Government welcomes the private sector as an equal partner by participating and investing in the transition."

He added that the NETR would drive the creation of high-paying job opportunities and boost domestic and foreign investment participation while ensuring the continuity of Malaysia's green energy supply. "Ultimately, this will make Malaysia a regional leader in the clean energy industry," he said.

TNB chairman Dato' Abdul Razak Abdul Majid highlighted that the conference's programme covered three economic sectors: power, transportation and cities, mirroring the approach taken by the utility company in crafting strategies for cleaner power generation, the future grid and supply network; electrification of the transport sector; and sustainable cities.

"With more than 70 years of experience in the energy industry, our dedication to both the nation and the industry's future remains unwavering. TNB acknowledges our role within the electricity value chain, and we are determined to actively participate in the country's quest for a responsible energy transition," he said.

In 2021, TNB officially declared its net zero by 2050 commitment, and since then it has been ramping up efforts to decarbonise the power sector, develop a flexible cross-border grid, fast-track electrification of vehicles and empower prosumers.

TNB President and Group Chief Executive Officer, Dato' Seri Ir. Baharin Din said, "TNB plans to invest up to RM90 billion in the grid over the next six years, out of which 40% will go towards energy transition related capital expenditure to ensure that TNB's grid is flexible enough to accommodate the evolving energy landscape." He also pointed out that TNB and its ASEAN counterparts have agreed that the timing was right to make the ASEAN Power Grid a reality because it is now a matter of survival. The conference attracted over 2,000 attendees and 68 speakers from around the world and was supported by 33 partner organisations.

INTERNATIONAL GREENTECH & ECO-PRODUCTS EXHIBITION & CONFERENCE MALAYSIA

In its 13th year running, the annual International Greentech & Eco Products Exhibition & Conference Malaysia 2023 (IGEM 2023) has established itself as one of Southeast Asia's leading trade events for green technologies and eco-solutions.

Held over three days from 4-6 October, IGEM 2023's theme "Race Towards Net Zero: Leadership for Climate Action" brought together exhibitors who showcased game-changing green technology, experts who provided insightful talks, and facilitated business matching sessions for participants.

In his opening address, the Minister of Natural Resources, Environment and Climate Change, Nik Nazmi Nik Ahmad, said, "With around 3.3 billion people living in highly vulnerable contexts globally, ongoing climate change innovation, mitigation and adaptation continues to be paramount. Preparations for the IGEM 2023 are in full force, as Malaysia looks to host an impactful and insightful event that will offer a plethora of innovative technologies, products and solutions to support climate action."

IGEM 2023 was organised by the Ministry, together with its Agency, Malaysian Green Technology and Climate Change Corporation (MGTC). The Malaysian Investment Development Authority (MIDA) continued to be a strategic partner for IGEM 2023, as in previous editions. The event also offered participants with the latest developments in Government policies, incentives and support services available for investors in the green technology industry and Electric Vehicle (EV) mobility sector.

One of the highlights was the inaugural exclusive seminar on solar energy that drew more than 50 participants, including major solar companies and consultants. The seminar themed "Elevate Your Green Profile: Smart Investments for Sustainable Business Growth", was organised in collaboration with the Malaysian Photovoltaic Industry Association (MPIA), UOB Malaysia and North Consult Engineering. The importance of collaboration in reshaping Malaysia's green energy landscape was emphasised by the President of MPIA, Davis Chong, who envisioned a brighter and cleaner future through collective efforts.

In an exclusive interview with Bernama (posted on MIDA's corporate website), Lim Bee Vian, Deputy Chief Executive Officer (Investment Development) of MIDA, elaborated that green technology investments in Malaysia have continued to grow, recording RM1.3 billion between January and June 2023, representing a 21.9% year-on-year increase. She added that this growth is supported by the approval of 348 green technology projects and services, including renewable energy (RE), all in alignment with the objectives of the National Energy Transition Roadmap (NETR).

LAUNCH OF ROBOST

As part of its electrical and gas safety campaign, the Energy Commission launched a mascot called RoboST, a child superhero with his companions Adam, Mei Lee and Ravi, who have special powers to prevent electrical and piped gas incidents and make homes and workplaces safe.

There are many life lessons to be shared with consumers in the adventures of these comic characters in an illustrated comic book called Adiwira ST which will be distributed by the Energy Commisison during events that involve children to increase safety awareness.

RoboST was launched on 8 May 2023.

ST DATASHARE

01 Jan to 31 December 2023

ELECTRICITY AND PIPED GAS SUPPLY

Total Energy (GWh):
133,613 GWh

Peak Demand (MW):
19,716 MW [11 May 2023]

Installed Capacity (MW):
25,862 MW

Reserve Margin (%):
31.20%

*This data only covers the Peninsular part of the grid system.

Generation Mix (%)

Coal: **57.10%**
Solar: **1.60%**
Gas: **36.50%**
Others: **0.20%**
Hydro: **4.60%**

SAIDI (Minutes / Customer / Year)

Peninsular Malaysia:
46.10
Minutes / Customer / Year

Sabah:
266.35
Minutes / Customer / Year

ENERGY SUSTAINABILITY

PPTEC Compliance (%):

79%
1,566 installations

Electricity Savings under NEEAP (%)*:

5.85%
8,593 GWh
i.e., equivalent to
RM2.15 billion

RE Installed Capacity (%)

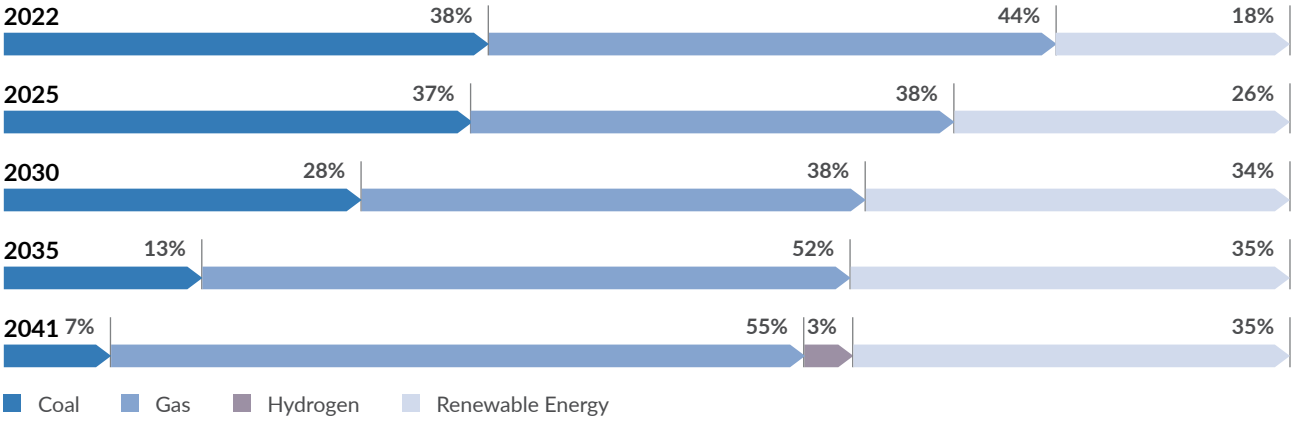
Hydro **46.30%**
Biomass **4.88%**
Solar **46.34%**
Biogas **2.48%**

Covers Peninsular Malaysia and Sabah only.
- Data sources are TNB, IPP, SESB, Single Buyer, SEDA, MGTC, OAS and ECOS.
- Self-gen with "other" fuel is excluded.
- Total hydro includes mini hydro capacity.
- Refers to renewable energy installed capacity in 2022.

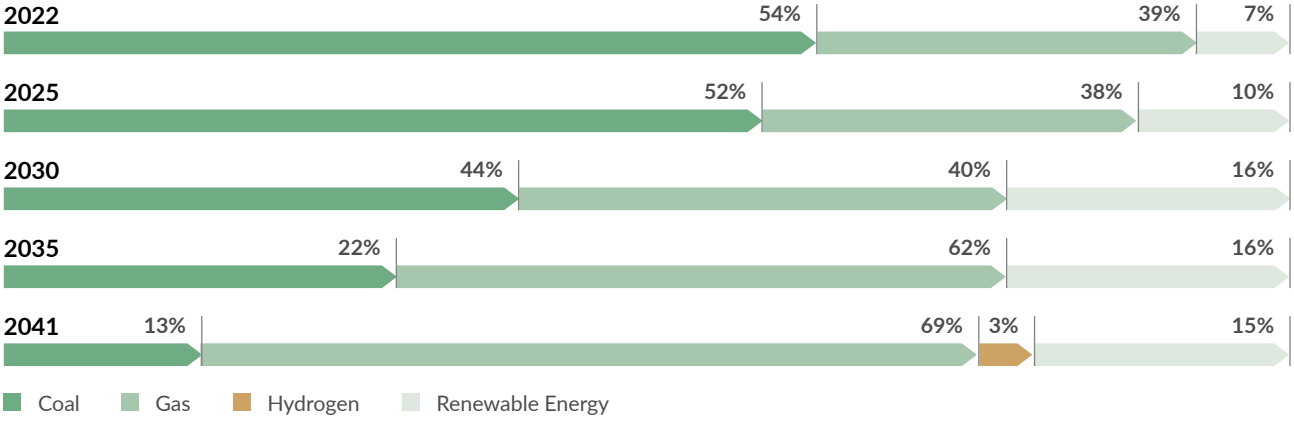
RENEWABLE ENERGY POWER PLANTS FOR COMMISSIONING

Idiwan Solar Sdn. Bhd. *Machang, Kelantan* **30.00 MW**	**Greenviro Solutions Sdn. Bhd.** *Seberang Perai Selatan, Pulau Pinang* **10.00 MW**	**Solar Citra Sdn. Bhd.** *Kerian, Perak* **10.95 MW**	**Coral Power Sdn. Bhd.** *Manjung, Perak* **9.99 MW**	**Suriamas Energy (Maritime) Sdn. Bhd.** *Manjung, Perak* **25.00 MW**
Energy ES Sdn. Bhd. *Kulim, Kedah* **20.76 MW**	**JAKS Solar Nibong Tebal Sdn. Bhd.** *Seberang Perai Selatan, Pulau Pinang* **50.00 MW**	**Selarong Solar Sdn. Bhd.** *Padang Meha, Kedah* **15.00 MW**	**Bikam Energy Sdn. Bhd.** *Batang Padang, Perak* **13.00 MW**	**Teja 1 Sdn. Bhd.** *Kampar, Perak* **15.00 MW**
Sinarmas Energy Sdn. Bhd. *Kuala Selangor, Selangor* **13.00 MW**	**Kellie Energy Sdn. Bhd.** *Kinta, Perak* **15.00 MW**	**Grooveland Sdn. Bhd.** *Perak Tengah, Perak* **17.36 MW**	**Serimas Energy Sdn. Bhd.** *Manjung, Perak* **12.00 MW**	

PROJECTED CAPACITY MIX OF PENINSULAR MALAYSIA, 2022-2041 (%)



PROJECTED ENERGY MIX OF PENINSULAR MALAYSIA, 2022-2041 (%)



Note:
1. The above figures had been rounded up to exclude decimal points.
2. Refers to projections in 2022.

ECONOMIC EFFICIENCY

Regulatory Period:

RP3 (2022-2024)

Average Base Tariff Rate for Peninsular Malaysia:

39.95 Sen / kWh

Targeted Tariff Adjustment under ICPT Mechanism for July to December 2023:

- Domestic Consumers (Usage of 1,500 kWh and below): Rebate of 2 sen / kWh
- Domestic Consumers (Usage of above 1,500 kWh): Surcharge of 10 sen / kWh
- Non-Domestic Consumers under the B, D, H, H1 & H2 and Water & Sewerage Operator Categories: Surcharge of 3.7 sen / kWh
- Other Non-Domestic Consumers: Surcharge of 17.0 sen / kWh

The Government had allocated RM5.2 billion for the implementation of ICPT from the period of July to December 2023.

REGULATORY QUALITY

Number of Complaints Received:

1,581
Complaints

Number of Complaints Resolved:

1,447
Complaints

Number of Complaints Under Investigation / For Further Action:

134
Complaints

SAFETY

PRIMARY CAUSES OF ACCIDENTS

ELECTRICITY

- Improper maintenance.
- Work activities by the public near electrical installations.

PIPED GAS

- None.

PRIMARY ACCIDENT LOCATIONS

ELECTRICITY

- Residential areas.

PIPED GAS

- None.

Number of Electrical Accidents:

44 Cases

Number of Piped Gas Accidents:

0 Cases

COMPETENCY & CONTRACTORS

Total Number of Electrical Certificates of Competency Issued:

5,942 Certificates

Number of Electrical Contractor Registrations (ERC, EC, ESC, ESIC, SBM, PWU):

8,124 Registrations

Total Number of Institutions Accredited to Facilitate Electrical Competency Examinations:

137 Institutions

Total Number of Gas Certificates of Competency Issued:

1,244 Certificates

Number of Gas Contractor Registrations:

114 Registrations

Total Number of Institutions Accredited to Facilitate Gas Competency Examinations:

2 Institutions

ERC: Electrical Repair Contractor
ESIC: Electric Sign Contractor
EC: Electrical Contractor
SBM: Switchboard Manufacturer
ESC: Electrical Service Contractor
PWU: Private Wiring Unit

CERTIFICATES OF APPROVAL

Number of Certificates of Approval for Electrical Equipment

10,374 New Certificates of Approval
6,593 Renewals

Number of Certificates of Approval for Manufacturers, Assemblers and Importers for Electrical Equipment:

293 New Certificates of Approval
771 Renewals

Number of Certificates of Approval for Gas Fittings, Appliances and Equipment:

1,392 Certificates of Approval

Number of Certificates of Approval for Manufacturers, Assemblers and Importers for Gas Equipment

174 Certificates of Approval

Number of ATI and ATO

2,178 ATI and **2,012** ATO

ELECTRICAL AND GAS LICENCES

Number of Electrical Licences:

3,641 Licences

Number of Third Party Access Licences:

39 Licences

Number of Private Gas Licences:

3,944 Licences

Number of Retail Gas Licences:

671 Licences

INVESTIGATION PAPERS

Number of Investigation Papers Opened for Legal Action:

71 Investigation Papers

Number of Prosecution Cases:

4 Cases

Number of Compounds:

133 Compounds

Amount of Compounds Paid:

RM144,500.00

CYBERSECURITY IN THE SUPPLY CHAIN: CHALLENGES & SOLUTIONS

Rushdi Abdul Rahim
President and Chief Executive Officer
Malaysian Industry-Government Group for High Technology (MIGHT)

The digitalised energy industry has a mix of large, midsize and small companies. For all, investing in cybersecurity is a must, and usually involves budget allocations for infrastructure, equipment and expertise that need regular upgrading. This can be particularly challenging for mid-to-small vendors and contractors, but the harsh reality is that they cannot afford to be the weak link in the power supply chain. Already, supply chain digital lapses are being cited as among the top reasons for cybersecurity breaches in the industry.

So, what can be done to ensure the integrity and security of supply chain digital systems? Energy Malaysia's columnist Rushdi Abdul Rahim, President and Chief Executive Officer, Malaysian Industry-Government Group for High Technology (MIGHT) writes on what is happening on the ground, and solutions at hand to reduce supply chain vulnerabilities.

Cyberthreats facing the power supply industry, comprising mainly electricity and gas companies, are fairly typical and for most parts similar to those in other industries. The main threats are data theft, billing fraud and ransomware. However, several characteristics of the energy sector heighten the risk and impact of cyberthreats against utilities.

Some cyberattacks are part of a broader campaign where critical infrastructure such as power production facilities and grids are targeted in retaliation for some geopolitical development. Otherwise, it could be entirely for profit as in the case of the ransomware attack on the computer systems of the American city of Baltimore in May 2019. It disabled the city's computers for weeks, incurring an estimated USD18.2 million in damages — more than the demanded ransom.

One obvious pain point for Malaysia is the frequency of security breaches.

In 2023, Malaysia fell victim to multiple cyberattacks, which included data theft from a national registry and a payment gateway data breach. There were also cases involving a ransomware attack on an airline, compromising the data of five million passengers and employees. Additionally, a telecommunications company reported a data breach, which exposed the personal information of customers, including their names, national identification, passport numbers and contact details.

As for plus points, there exist a very strong high-level awareness coupled with concerted efforts to remedy the situation. The formulation of the National Cyber Security Policy (NCSP) in 2006 is one such effort. The NCSP was specifically developed to address the risks to the National Critical Information Infrastructure (NCII) that is made up of 11 sectors. The NCSP recognises the critical and highly interdependent nature of the NCII and aims to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cybersecurity measures.

This serious intent is reflected in the Global Cyber Security Index 2020 report conducted by the International Telecommunications Union. Among the nations with the highest commitment to cybersecurity, Malaysia scores 98.06 among 194 countries, and ranked a joint fifth along with Russia and the United Arab Emirates. At the Asia Pacific level, Malaysia is ranked second, after South Korea and Singapore tied for the first position with a score of 98.52.

Cyberthreats: Small Companies are also at Risk

Cybersecurity is both a technical and mindset issue. Small businesses are just as much at risk from cybersecurity threats as are large enterprises. Many small business owners may believe in the notion of "security through obscurity" — that nobody would want to attack them because they are small. Many do not realise that attacking small businesses or "supply chain attacks" is an effective way to target larger corporate organisations.

This is of particular concern to grid facilities, which when attacked, will have dire consequences on electricity supply. According to the Malaysian Digital Economy Corporation (MDEC), in 2021, about 84% of small and medium enterprises (SMEs) in Malaysia were compromised in one way or another by cyberthreat incidents, while 76% SMEs suffered more than one attack. The trend is increasing as attackers becomes more technology savvy.

Small businesses often do not have a dedicated cybersecurity team or enterprise-grade defences. They often do not conduct regular cybersecurity training and are less likely to have robust security tools like Multi-Factor Authentication (MFA) or password managers.

Another major obstacle is funding. Investments in the form of capital cost for cybersecurity systems, hardware and infrastructure is costly with intangible returns. In addition, the skills and talent of a cybersecurity workforce need to be developed.

Malaysia still lacks approximately 11,000 cybersecurity experts of various fields against current readiness of about 15,000 people. The typical requirement for cybersecurity personnel is between 20-30 people per outfit depending on the company size.

MIGHT's Multi-Platform, Multi-Stakeholder Approach

MIGHT is a technology think tank that brings together the Government-private sector-academia to manage digitalisation opportunities and challenges.

Its take on digitalisation and smart economy initiatives is for a multi-platform, multiple stakeholder approach at the industry, state, national and international levels. The many levels of interaction with stakeholders allows it to garner input and resources and is the pathway for MIGHT's policymaking, and Government and corporate advisory efforts. It is thus well-positioned to provide holistic solutions on subjects such as cybersecurity.

Government Solutions

The seriousness of the Government intent to resolve cybersecurity shortfalls is evident. In the Budget 2024, the Government allocated RM2.84 billion to enhance digital connectivity initiatives, digital economy, cybersecurity, as well as to support the development of local talent. Additionally, a total of RM60 million is to be channelled to CyberSecurity Malaysia to develop a 5G Cyber Security Testing Framework as well as to enhance local capabilities in 5G technology. To encourage digitalisation among the SMEs, the Government also announced a RM100 million allocation for digitalisation grants of up to RM5,000.00, which will benefit over 20,000 SMEs and micro-entrepreneurs.

Additionally, MDEC has launched several cybersecurity talent development programmes encompassing industry growth, innovation and talent development, including Skill-Up Programme, NxFORCE Programme and CYBER100.

Tax credits can also help incentivise companies to adopt cybersecurity-related initiatives such as investments in training programmes and education, research and development, investment in technologies to protect the operation of Information Communication Technologies (ICT), and the procurement of energy conservation ICT products and solutions. Smaller companies also require technical knowledge assistance and incentives to boost the adoption of cybersecurity. This may be in the form of cybersecurity tax credits to help companies reduce their tax liability, accelerate adoption and enhance industry competitiveness.

New incentive instruments can be both fiscal and non-fiscal, based on recognition of the need for constant upgrading. For instance, the Welsh Government has invested £9.5 million into a Cyber Innovation Hub in South Wales. This hub is expected to bring Government, industry and academic partners together to grow the Welsh cybersecurity sector and become a global leader in cybersecurity. Via this fund's incentives, it is expected to train more than 1,000 cyber-skilled talents and attract more than £20 million in private equity investment by 2030.

Along similar lines, the Malaysian Government launched the Malaysia Cyber Security Strategy (MCSS) 2020-2024, with an allocation equivalent to USD434 million to step up national cybersecurity preparedness and to upgrade the country's cybersecurity measures. The importance of building agile and competent cybersecurity talents and increasing cybersecurity uptake among businesses underscores the Malaysia Digital Economy Blueprint (MyDIGITAL) to advance Malaysia as a tech-driven economy and positioning the nation competitively.

Role of Big Power Players

Big power companies have a role to play too. To ensure their vendors / supply chain do not compromise the integrity of their online systems, they need to implement various measures throughout the life cycle of their energy delivery systems.

One crucial step is to embed cybersecurity in the procurement of energy delivery systems. Embedding robust security measures in their procurement policy is essential to safeguard sensitive data, mitigate cyberthreats, and preserve business relationships across the entire value chain. Studies show that 41% of big organisations that suffered a material impact from a cyberattack have cited a third-party as the origin for the attack. It is thus important for big power players to play a proactive role to ensure that their vendors along the supply chain comply with the integrity of their online systems.

Principal companies should also consider establishing a robust data privacy and protection framework, with strong guidance and active support from top management and the board. Consistent communication, training and awareness should be provided to employees and supply chain companies to enhance awareness on cybersecurity. Additionally, leveraging on appropriate technologies within their information governance frameworks is essential, encompassing

data identification, categorisation, retention or disposal, and data consolidation.

Other leading practices include strict requirements for organisations handling personal data by appointing a data protection officer and continuous monitoring through regular audits to minimise non-compliance with regulations. There must also be penalties to act as deterrents. For instance, over 89,000 data breaches were reported by the European Union (EU), resulting in fines totalling €56 million in 2018. In 2019, the UK's Information Commissioner's Office (ICO) fined British Airways €183 million and Marriott International €110 million for data breaches that affected millions of customers.

In the Malaysian context, the Vulnerability Assessment Centre (MyVAC) under CyberSecurity Malaysia plays the role of enhancing the national information security ecosystem and increasing the nation's ability to defend itself against cyberthreats.

Large companies are also putting in place systems to monitor performance or facilitate data recovery. There are, in addition, systems applied to monitor the integrity of the digital system and to check for system interference. The integrity of the system also must be evaluated from time to time to ensure resilience. These should all fall under the ambit of an effective governance and management of cybersecurity risks as outlined in the MCSS 2020-2024.

Tenaga Nasional Berhad (TNB), for example, has demonstrated a strong effort towards cyber resilience of its information technology (IT) and operational technology (OT) systems, by complementing with the ISO/IEC 27001:2013 Information Security Management System (ISMS) certification across various domains. Malakoff Corporation Berhad, the largest independent power producer in the country, on the other hand, has maintained a 99% availability of critical systems and recorded zero major cybersecurity incidents. It has also maintained compliance to ISO/IEC 27001 to manage and ensure sufficient safeguards of data security. YTL Power also emphasises the maintenance of high standards in cybersecurity through recertifications of ISO/IEC 27001.

Smaller Companies: Gains and Pains

Smaller companies can enjoy certain advantages when it comes to responding to cyberthreats compared to larger enterprises. While large companies may face challenges related to their size, complexity and bureaucracy, small businesses can leverage on their agility, flexibility, and closer-knit organisational structure to respond more effectively to cyberthreats.

Smaller businesses typically have fewer layers of bureaucracy and decision-making hierarchies compared to large enterprises. This streamlined decision-making process enables faster responses to cybersecurity incidents, as there are fewer hurdles to overcome when implementing security measures or allocating resources.

Moreover, communication channels between employees, management, and IT personnel are often more direct and transparent. This facilitates efficient collaboration and coordination during incident response efforts, enabling faster detection and containment of cyberthreats.

However, while small companies may have inherent advantages in responding to cyberthreats, they still face unique challenges such as limited budget and expertise. Therefore, it's essential for small businesses to prioritise cybersecurity, invest in appropriate security measures, and leverage available resources effectively to mitigate the risks posed by cyberthreats. Additionally, seeking guidance from cybersecurity experts and leveraging external resources can further enhance the ability of small companies to respond to and recover from security incidents.

In addition to traditional funding mechanisms such as digitalisation grants for small businesses, there are increasingly novel financing methods such as Mastercard's Strive EU Innovation Fund, which offers up to €500,000.00 to 20 winners who develop digital and data-first solutions that support small businesses.

Reverse infection, or supply chain attacks, is unfortunately more rampant than we think. Here, attackers compromise a trusted vendor or supplier to gain access into the systems of their customers or partners. An example is the Distributed Denial of Service (DDoS) attacks launched against a domain name system provider, which caused several global online services to be disrupted.

Another notable example of a supply chain attack is when attackers compromised the software build process of a major IT management software provider based in the United States of America (USA). Unknown to them, attackers had inserted a backdoor virus into their software updates that were distributed to customers, who included Government Agencies, corporations, energy companies and other organisations in various countries.

Supply chain attacks have become a growing concern since they can bypass traditional security measures, gaining unauthorised access to sensitive information to conduct espionage, and carry out other malicious activities.

These attacks highlight the importance of supply chain security and the need for organisations to vet their suppliers and vendors rigorously, implement robust security controls, and remain vigilant against emerging threats. In addition, layers of system security need to be designed to ensure a high level of protection to the system and mitigate plausible risks and circumstances.

"Big power companies should provide consistent communication, training and awareness for their employees and supply chain companies to enhance awareness on cybersecurity."

User-friendly Solutions for Prosumers

Cybersecurity issues are likely to worsen with the entry of micro-enterprises, community groups and households as clean energy generators. The rise in the number of prosumers, who often utilise various devices and platforms, expands the attack surface for cybercriminals. Each device that is invariably connected to the internet represents a potential entry point for cyberattacks.

With Malaysia's power supply industry evolving with various energy schemes such as Net Energy Metering (NEM) and Renewable Energy Certificates (REC) and the like, bi-directional connections between power users and producers may severely compromise critical customer information and real time data.

In this context, the most possible security incident will be password attacks where hackers will aim to obtain the user's or account's password through various methods such as password-cracking programmes, password sniffers and dictionary attacks.

Additionally, prosumers often share files, software, and content online. One prosumer's infected device can quickly spread malware to others through these shared resources, leading to a broader cybersecurity threat. On the flipside, prosumers themselves may be the target of cybercrime given that they may lack robust cybersecurity measures in place, making them easier targets compared to large corporations or Government entities with more advanced security defences.

In targeting a mass audience, user-friendly cybersecurity solutions are necessary. These should be tailored to the needs and technical capabilities of prosumers and include easy-to-use anti-virus software, password managers, and secure messaging applications that prioritise simplicity without sacrificing security.

Encouraging secure-by-design principles in the development of hardware, software and online platforms will also take the guesswork out of cybersecurity for prosumers. By prioritising security from the outset, developers can minimise vulnerabilities and create products that are more resistant to cyberattacks.

However, it all hinges on high public awareness of security issues. Getting the message out there quickly and in a timely manner requires a strong public-private sector collaboration including Government Agencies, cybersecurity firms, technology companies, and consumer advocacy groups to address cybersecurity challenges collectively. Public-Private Partnerships (PPP) can facilitate information sharing, coordinate responses to cyberthreats, and promote the development of innovative cybersecurity solutions.

Models to Emulate

Malaysia's power supply industry is maturing rapidly as a national growth engine, and it is being populated by wide-ranging players from multinational green energy investors to households renting out their rooftops for solar energy generation. With this maturity comes the complexity of managing cybersecurity risks. Fortunately, there are some international models that we can emulate.

The United Kingdom (UK) is a good example of proactive and comprehensive cybersecurity management. The country is the top target for cyberattacks, accounting for 24% of all of Europe in 2021. This is of concern given that the UK is dependent on gas supplies from continental Europe, with expected increases in electricity interconnections.

Recognising the immense damage arising from breaches in cybersecurity, it has established a code of practice to effectively address the threat of cyberattacks. These include a systematic inventory and audit of tangible and non-tangible assets to understand the linking of assets, and regular performance of vulnerability assessments through troubleshooting protocols.

Meanwhile, the European Commission has adopted a directive on the security of network and information systems aiming to boost the overall level of cybersecurity. One of the key directives is the Directive on Security of Network and Information Systems (NIS Directive). Its key features include risk management and incident reporting, penalties and enforcement and information sharing.

The USA also adopts a highly extensive approach to ensure effective implementation of cybersecurity practices worth emulating. This includes security by design and capitalising on emerging tools, systems, and architecture coming online as energy systems evolve. They also proactively carry out operational collaboration among experts from Government and industry to analyse, mitigate, and defend against cyberthreats to the power industry sector.

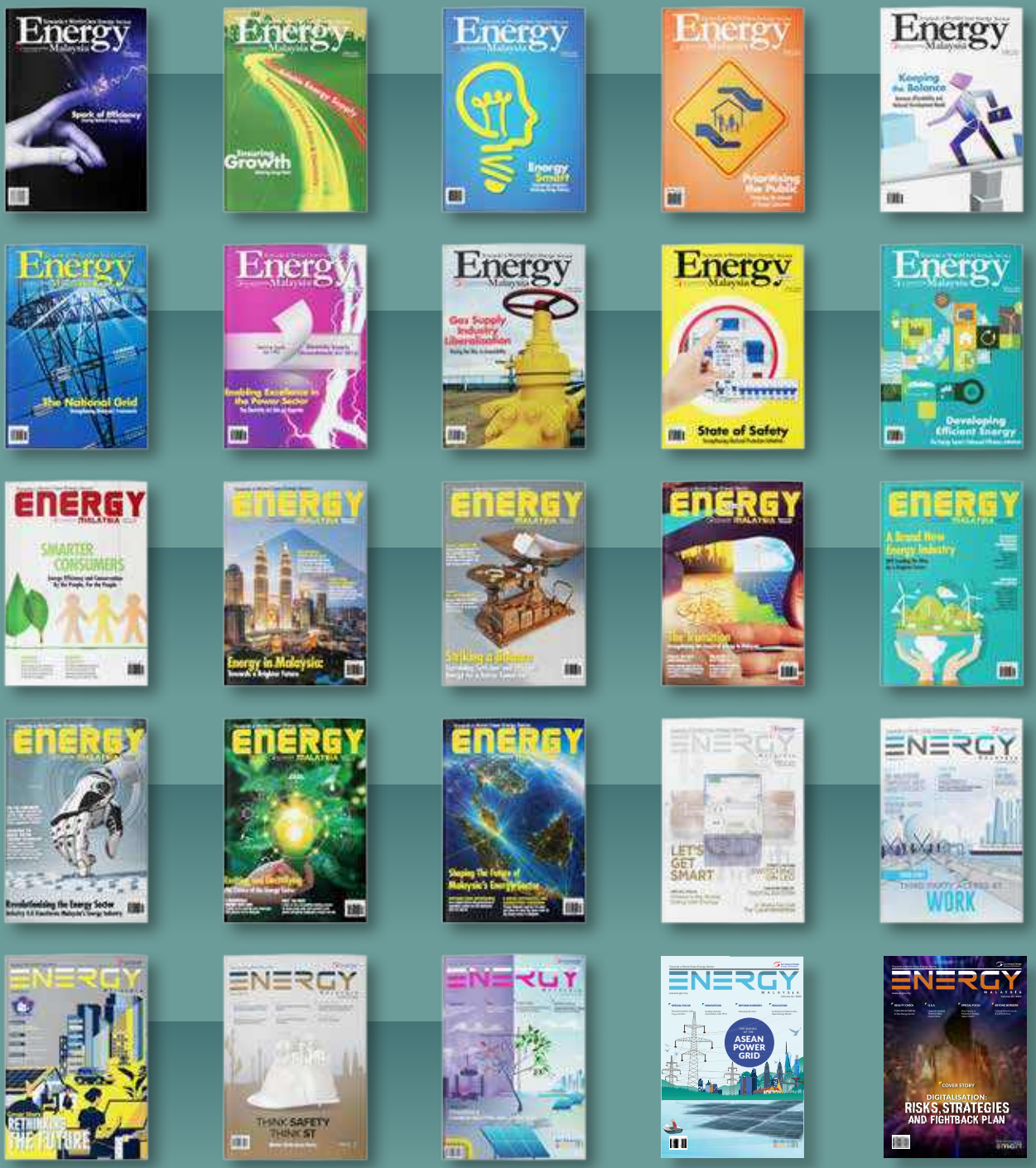
These measures provide a good benchmark on international best practices for ensuring continuity should the unthinkable happen.

Ultimately, with the widespread use of the Internet of Things (IoT), risk mitigation will come centre stage. The most common risks that need to be addressed in cybersecurity are the misuse of user personal data, internet-related fraud, shortage in the cybersecurity workforce, insider threats (social engineering ploys) and a lack of good cyber hygiene habits.

From the technological perspective, infrastructure, equipment manufacturers and system solution providers need to optimise technology use to manage vulnerabilities and cyberthreats. Hence, strategic collaboration across the value chain in the power supply industry is an essential factor to build strong cyber defence and to ensure resilience of the power industry ecosystem.

ENERGY MALAYSIA

For comprehensive insights and information on the energy industry in Malaysia and what's trending in the New Energy World.

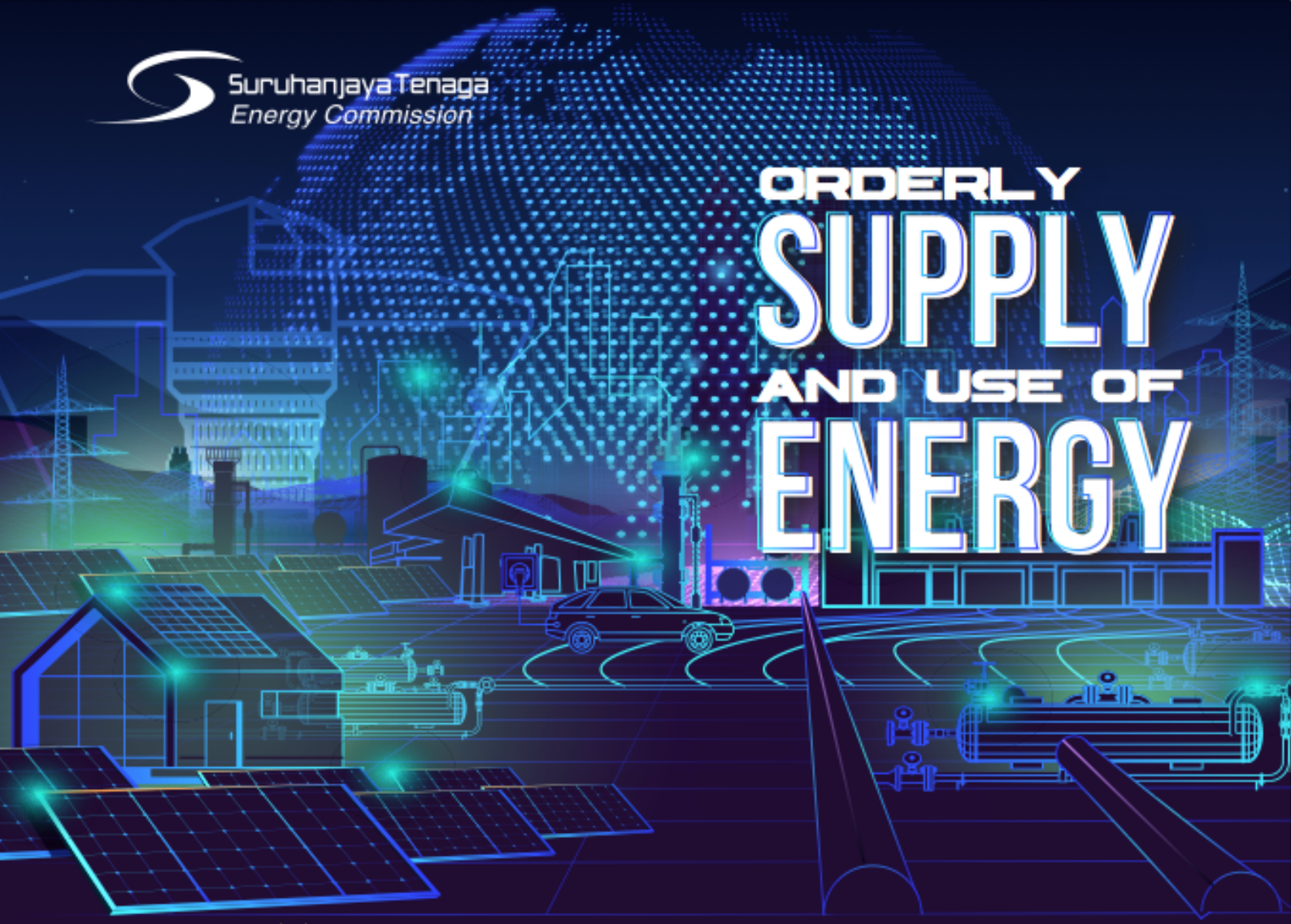


FREE DOWNLOAD

www.st.gov.my

Suruhanjaya Tenaga
Energy Commission

ORDERLY SUPPLY AND USE OF ENERGY



Suruhanjaya Tenaga (ST), a statutory body established under the Energy Commission Act 2001, is responsible for regulating the energy sector, specifically the electricity supply and piped gas supply industries in Peninsular Malaysia and the Federal Territory of Labuan.

THE ENERGY COMMISSION

ADVISES
Ministers on all matters concerning the national policy objectives for energy supply activities, the supply and use of electricity, the supply of gas through pipelines and the use of gas.

REGULATES
electricity and piped gas tariffs and the quality of supply services, as well as promotes competition and prevents misuse of monopoly power.

PROMOTES
good practices, as well as research, development and innovation in the electricity and piped gas industries.

PLANS AND DEVELOPS
laws, regulations, rules, guidelines and programmes for the orderly development and functioning of the electricity and piped gas industries.

LICENSES AND CERTIFIES
electricity and piped gas suppliers, competent electricity and gas personnel, training providers, contractors, equipment and installations, energy service companies and energy managers.

MONITORS AND AUDITS
performance and compliance of licensed and certified suppliers, service providers, installations, equipment importers, manufacturers and retailers.

INVESTIGATES
complaints, accidents, offences and industry issues; and enforces compliance.

Suruhanjaya Tenaga (Energy Commission of Malaysia) | st_malaysia | ST_Malaysia | Portal ST | st_malaysia

No. 12, Jalan Tun Hussein, Precinct 2, 62100, Putrajaya

Tel: 03 8870 8500 • Fax: 03 8870 8637 • www.st.gov.my