ACPM
Audit Consulting Project Management
BUDAPEST • DUBAI • KIGALI • KUALA LUMPUR
NAIROBI • PRETORIA • SHANGHAI • WIEN

Malaysia Cyber Security Strategy 2020 -2024

On 12 Oct 2020, the Government of Malaysia launched the Malaysia Cyber Security Strategy (MCSS) 2020-2024 with an allocation of RM1.8 billion to step up national cyber security preparedness. It was noted that the equivalent authority in UK spent close to RM7.9 billion for its initial stage.

The Prime Minister of Malaysia Tan Sri Muhyiddin Yassin explained that the Communications and Multimedia Ministry (KKMM) and the National Cyber Security Agency (NACSA) would be tasked with formulating, implementing, monitoring and coordinating the medium-term action plan. The prime minister presented a strategy based on five pillars comprising 12 objectives, 35 actions plans and 113 programmes as the thrust of the cyber security approach required to combat today's cyber-attacks.

The MCSS outlines the pillars to be the guiding principles to improve the country's cyber security management in the next five years. Specifically, the pillars will address: -

- Enhancement of the management of national governance and cyber security by improving the country's critical information and communication technology (ICT) infrastructure as well as raising the ability to deal with cyber security issues effectively.
- Strengthening the enforcement of existing cyber security policies and standards by reviewing digital legislation as well as formulating specific laws to deal with cyber security.
- Empowering innovation and world-class technology for adopting cyber security tools and techniques.
- Improving development capacity as well as cyber security skills and capabilities to protect Malaysian interests.
- Enhancing international cooperation by activating regional and international cooperation to protect national digital interests and assets.

In early 2000, our team leader(s) in Malaysia was involved in the establishment of National Cyber Security Policy that anchored the establishment of the relevant government agency and provides the foundation for MCSS 2020-2024. We are particularly pleased to note that the MCSS is positioned to assist all parties to address the new and emerging threats.

- Data is the new oil, it's like black gold. If you don't respect it and don't protect it, it will slip through your fingers and land up in the wrong hands. Bad actors are no longer script kiddies de-facing websites - they are highly skilled and sometimes state-funded with the motivation of a whole nation state behind machine learning attacks – bots on the internet.
- For a long time, cyber security has languished as one of many risks and has struggled to take its rightful place in the boardroom. With pandemics such as Covid-19 will change all that. This pandemic has demonstrated how catastrophic events are inevitable – it's not a probability game, it's about being prepared for the worst case, it's about being a resilient nation.
- Cyber is one of those risks that are high impact and high likelihood – top right of the Board's 'risk quadrant'. There are two simple choices either land a Cyber expert into the Board or turn existing board members into experts. Board's need coaching and they need qualified cyber security professionals to peer with them and provide trusted expert advice.
- Today, businesses are still grappling with the basics – Spam, Ransomware, data theft and Malware. Companies will get wiped out – not because of their balance sheets, but their inability to withstand a Cyber breach. That may sound a little brutal, but it's a harsh reality and Boards need to wake up – NOW.
- Conversely, we saw success form those that have turned Cyber into an advantage. Organisations that put the security of their customers data at the heart of what they do will win trust, loyalty and respect. They will be agile and not suffer the inertia of endless testing in a DevSecOps world.
- Companies are still battling with today's technology controls will struggle to cope with what's coming up next. The brute force of quantum computing will be too much for some – it's set to obliterate current encryptions standards and controls. If that wasn't enough: whilst the internet and cloud shifted the perimeters of organisations, Edge Computing will make boundaries meaningless. This will drive the need for frictionless countermeasures – which means no more software-based agents and no more passive devices like firewalls.

How Can We Help?

We understand the cyber security challenges organizations facing are at both the Board and C-suite levels. Our **Enterprise Cyber Security Architecture (ECSA)** services will assist organizations in dealing with the Board and Top Management, to address the emerging cyber threats through structured governance, competent professionals, matured processes and effective technology.

We help organizations build or renovate an ECSA to meet their evolving business and cyber needs and to improve the organisation management and business operations. With our ECSA services, organisations can align their enterprise cyber security governance and strategy with business objectives, adapt to changes in business strategy, and bring assurance and efficiency to their overall cyber security management. Our services are both scalable and flexible to specific industry and technology requirements. We can design specific aspects of an architecture, or the whole architecture—at one site, or throughout the cyber insurance claims, pre risk analysis and table top exercises.

Our Approach

ECSA is ultimately driven by business strategy and will significantly influence that business and cyber strategy. It identifies opportunities for exploiting new enabling technologies and helps clarify the technology requirements—and therefore the major costs and risks—of specific business process designs or cyber risks or threats.

We establish models for an integrated set of cyber security capability components. When combined with the appropriate framework of standards and principles, these components can operate effectively together and adapt readily to the evolving needs of the business. The models can be used to guide the activities of the various project teams engaged in developing software, implementing commercial packages, and enhancing infrastructure capabilities, such as cyber security incident and response management, forensic technology and cyber security resilience and management processes.

We can focus on specific components within the enterprise security architecture, such as the technical architecture, policies and procedures, or corporate cyber security organization. It can also encompass a full enterprise architecture and identify interdependencies among specific technologies and all appropriate architectural components.

Our ECSA services offer many advantages to clients. Among the benefits, we:

- Develop an end-state vision of how an ECSA will support the organization
- Define the end-state architecture, including the integration and deployment across the enterprise's administration, management, applications, data, and technology areas
- Establish enterprise cyber security design principles, deployment standards, and management policies to help ensure the continued effectiveness of the security architecture as it evolves over time
- Plan the transition from the current environment to the end-state architecture, including digital, transformation change management and the establishment of a project or working with the insurance and brokering sector, we can help insureds understand their financial exposure. Running scenario modelling for instance.

CONTACT US

ACPMIT

HUNGARY – MALAYSIA – SOUTH-AFRICA – UAE – AUSTRIA

www.acpmit.com

SERVICE LEADERS:

Lim Huck Hai
Managing Director
Asia Pacific and Malaysia

Marton Miklos
Managing Director
International and EU

Nav Bahl
Managing Director
United Kingdom

Anuarul bin Dato' Ab. Halim
Head of Business Development
Asia Pacific

CONNECT WITH US:

ACPM IT

Head Office
Széchenyi István square 7-8.
1051 Budapest, HUNGARY
info@acpmit.com

Asia Regional Office
C-10-07, Sunway Nexis,
No.1, Jalan PJU 5/1, Kota Damansara
47810 Petaling Jaya, Selangor, Malaysia
info@acpmit.asia