Interview with the CEO of Cybersecurity Malaysia

"The only thing that's constant is change", says Dr. Amirudin Bin Abdul Wahab, CEO of Cybersecurity Malaysia. When tackling fast evolving cyber threats, the country's only option is to grow and continually advance its cyber strategies.

"You have to be adaptive, rather than responsive", Amirudin says. The agency he leads sets the cybersecurity framework for the whole country. It educates the public, trains professionals and works with government to adopt the best guidelines in tackling cyber attacks.

GovInsider spoke to Amirudin about how he addresses this complex problem, the bigger challenges and his vision for the industry.

Drawing from the skills pool

Amirudin believes that there is a skills shortage in cybersecurity. Working as a team, the agency identifies the skills gaps and builds the expertise needed. He sees the Internet of Things (IoT) as an emerging sector that will require specialist skills, but "no one can be an expert in everything", Amirudin admits; so it is important for his team to first recognise the vulnerabilities faced, in order to build a pipeline of talent as best they can.

To plug the skills shortage, Cybersecurity Malaysia (CSM) has established close relationships with universities across the country. The agency drafts

class modules with universities, for instance, by providing Master programmes in the National University of Malaysia. Besides focusing on public universities, CSM is “also working with some private colleges to build training programmes on basic information security skills”, he says.

Amirudin wants each university to define their own niche in the cybersecurity arena. It’s a huge sector, and he wants each of them to play a “vertical role”. When CSM collaborates with these universities, it leverages on the strength of each university. The team works with University Putra Malaysia to specialise in cryptography, because it “has a very strong cryptography association”, and is also the country’s lead research centre, he explains. “If your forte is warfare defence, then that is the area that you should go in”.

The employees in CSM also serve as professors in the universities. Amiruddin himself is an adjunct professor in two local universities, and he encourages his employees to act as visiting lecturers or professors, in order to “share industry knowledge with academia”.

The relationship the agency has with tertiary educations is two way: Amirudin’s colleagues are not only professors, some of them are also PhD students researching cybersecurity issues. He sends them to universities to expand their knowledge. “I cannot produce… graduates, so I send them to do research.” This is part of building the national capacity, he explains.

He wants local companies to develop more competitive products in cybersecurity, reducing the reliance of the country on foreign products. “The challenge now is to move up to the next level”, to provide products and services that can be used locally, and exported globally to create a new industry, Amirudin says. “Cybersecurity is not just about the issue of security”, but it can also be linked to economic interests. It’s an opportunity to tap into as an economic growth area, he notes.

CSM also has the responsibility to manage private sector talent. Professionals need to be trained and retrained in their jobs. Amirudin admits that some of the IT specialists are not aware of the latest threats; and yet they are the ones that the public depend on for security. Experts need to acquire technical skills needed in different areas, understand how to fortify cyber infrastructures, and how to respond to attacks, he explains.

Working with government

CSM helps other government agencies bring cyber criminals to justice. It provides specialist expertise in digital forensics to law enforcement agencies, working with the anti-corruption commission, police, customs, domestic trade, the consumer group, communications, and the central bank to provide digital evidence. CSM analysts will go through the digital evidence provided, and they will testify in courts, Amirudin explains.

The agency has also drafted a cybersecurity framework for the public sector. It worked with the Malaysian Administrative Modernization and Management Planning (MAMPU). “We are currently assisting them on that”, he says. The framework, called RAKKSSA, will be used as a guide by the public sector to enhance cybersecurity protection and manage government ICT assets. It sets a standard on how to identify, detect, respond and recover from cyber attacks and system failures.

At the same time, CSM also has a role to play in strengthening and enforcing the laws. “We can’t cope with the changes because [they] are fast”, but the agency tries to minimise the threats faced. The agency “reviews the existing laws”, and through these efforts it hopes to implement “stronger ways of prosecution”. “If there is a need to create certain policies or guidelines to strengthen protection, then we have to do it”, he asserts.

Reaching out to citizens

Amirudin understands that having specialist skills are not enough. “We could cover the loopholes that attackers are trying to exploit”, but the fix doesn’t always lie in fortifying computer infrastructures. It’s not just about setting up firewalls and antivirus softwares. Sometimes, “it’s also the peoples’ vulnerability”, he admits.

“We need to look into the aspects of people”, Amirudin says. CSM has set up an awareness programme called Cybersafe to educate kids, youth, and parents on cybersecurity measures. For instance, educating the public about privacy settings, sharing of personal information online and basic dont’s such as avoiding clicking unknown attachments. The programme oversees awareness talks and tests citizens on their cyber knowledge.

The agency also has a computer emergency response team that responds to citizens’ reports. Set up in 1997, the platform allows Internet users to escalate or report computer security incidents. Reports can be submitted through email, phone calls, text message or through a mobile app. Cyber999 “is not only for the government sector but also for the public”, he says. It is one way to “be closer to the people with regards to cybersecurity issues”.

CSM has analysed incident reports to find out what the top threats in the country are: fraud, intrusion and malicious code. Amirudin points out that these have been the top three hits in the past five years. Industries facing intrusion attacks are typically government, finance, and telecommunications, whereas citizens tend to fall prey to financial fraud.

To greener pastures

Amirudin has bigger plans for the agency. “We have to engage into new areas; the list of portfolios has to be deepened”, he says. For example, his team is looking into biometric forensics, embedded device forensics and IoT security.

As cybersecurity measures evolve, his team will have to constantly refine their skills. And Amirudin captures the sentiment well: “We have to change, or else we’ll be irrelevant”.