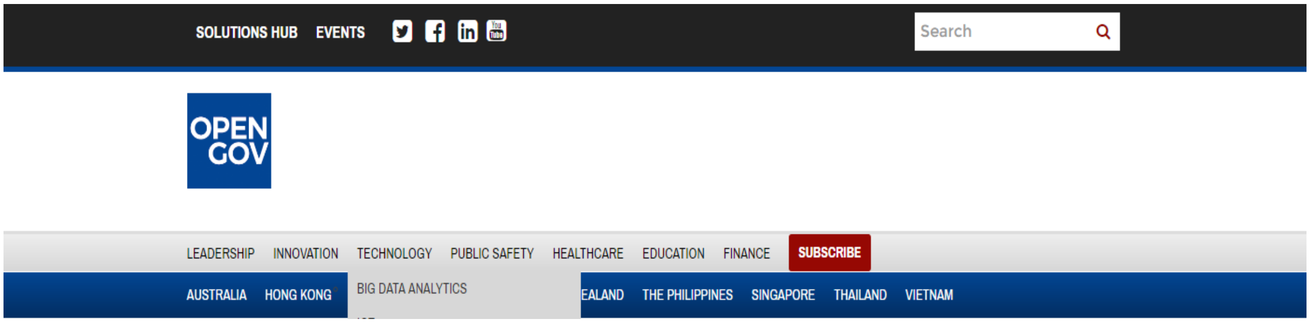

EXCLUSIVE- IoT and Big Data labs- Securing the future at CyberSecurity Malaysia

Dr. Solahuddin Bin Shamsuddin, CTO, CyberSecurity Malaysia, speaks to OpenGov about security going hand in hand with technology and dealing with IoT and Big data security.

03/08/2016

Dr. Solahuddin Bin Shamsuddin, CTO, CyberSecurity Malaysia (CSM), speaks to OpenGov about security going hand in hand with technology and the current focus areas of Big Data and IoT. CSM operates under the purview of the Malaysian Ministry of Science, Technology and Innovation (MOSTI).

Could you tell us about your role as CTO of CyberSecurity Malaysia?

My role is to lead and craft all technical related initiatives in CyberSecurity Malaysia to achieve the corporate agenda.

My jobs involve some strategic components amongst others, including planning and overseeing the development, implementation and management of the technology infrastructure, to support the delivery of CSM products and services and to identify as well as explore new research areas in cybersecurity.

In terms of operational components, I also oversee the preparation of proposals, implementation of the Government funded R&D projects carried out by CSM. In addition, I manage the technical advisory and advise on the adoption of latest technology by CSM that can provide the optimum ROI. All these activities are to be done in compliance with CSM’s objectives, policies, procedures and guidelines.

How do you evaluate the success of initiatives? What kind of return on investment (ROI) measures do you consider?

It depends. In CSM, when we propose a project to the government, we aim to provide the solutions to the evolving threats, and measure its benefits in ROIs in terms of values the project will give to the government, not necessarily quantified in dollars and cents.

For example, we provide our incident handling services for free. However, there are some costs involved in handling an incident such man/hour and mileage claims etc. Finding the ROI involves how much money has been spent and the value of services provided to mitigate the incident. All these can be quantified. Even though we don't bring dollars and cents to the government, the value of the services we provide is used to calculate the ROI.

What are the areas of focus for CSM in the next one year and on a longer scale of 3-5 years?

We are looking into the current strategic technology trend in order to analyse emerging cyber security challenges. Security and technology go hand-in-hand. With every new technology, there are new vulnerabilities and new security issues which come up.

The new trends predicted for this year by consulting firms include device mesh, smart machine, advanced machine learning, autonomous Agents and Things, Adaptive Security Architecture, Advanced System Architecture, Mesh App and Service Architecture and Internet of Things (IoT) platforms. We always look at what are the current and future technologies, what are the security issues that come with it.

For example, we are building an IoT lab, that will look into the security issues of IoT for the next five years and comes up with ways of addressing them.

We also have people looking into big data security. We are producing data scientists, who can look into the security issues of big data and produce useful results, predictive analytics for the company.

They can give us an edge compared to our competitors, the hackers, the bad guys. We always have to stay a few steps ahead of them.

Cybersecurity is necessarily pro-active. We look for possible threats. We will predict what is going to happen. So that we can be ready.

What kind of research will be done in the IoT lab?

It will be about the security aspect of IoT and also privacy. We are looking at anonymising the data, so that we can establish open community data. We should not waste any data that have been gathered. Government has a lot of data. This data shall be sharable with researchers and industries that might need to use the data for business purposes.

At the same time, we should be able to anonymise the data. We should be able to give them the right metadata that can be used that do not reveal the identity of the person.

All PII (Personally identifiable information) must be removed through anonymisation technology. This will come together with open community data sets.

From a security perspective, you have to look into it from all angles. You have to look at database security, network security, server security, if you are accessing it through app, then web security. Everything has to be addressed, not just one component.

You mentioned that data scientists are being trained. For all these projects, you will need experts with the requisite knowledge. Are there any ongoing initiatives for training professionals for these roles?

We are training our staff. For instance, for IoT, if we have a certain group or department which looks into it, we will send our staff for training there. This will ensure that they have up to date information and knowledge on the latest technologies. We send them for security professional certifications.

We do whatever it takes, so that they have the required knowledge.

If we don't have the right people in certain cases, we might get expert services from Subject Matter Experts (SMEs). We get them to come here and conduct trainings and transfer knowledge.

When and how do you collaborate with other government agencies?

Most of the big initiatives done by government require collaboration between agencies. Government agencies, government departments work together for certain projects.

For example, IoT is championed by MIMOS, which is under MOSTI. It requires collaboration. MIMOS, MDEC (Malaysia Digital Economy Corporation), MCMC(Malaysian Communications And Multimedia Commission), CSM, MAMPU, all work together. For IoT, we will come up with a IoT security framework for the whole project. CSM always contributes to the security aspects of a particular technology.

How do you see IoT evolving and what are the primary risks associated with it?

We are talking about Internet of Everything (IoE) now. Everything will be connected through the internet, through these IoT devices. IoT devices process data and then transfer data through the internet. If they keep the data, then it is not part of IoT. Our concern is about the security of the data. The data has to be protected so that, people cannot intercept or change it or replace the data, so that the CIA of the data is preserved, its Confidentiality, Integrity and Availability.

The security trend is to encrypt the data using PKIs (Public Key Infrastructure). But it has to be done at the manufacturer level, at the chip level. The big players in IoT, the ones who make the sensors, the processors, have to embed the PKI component on the chip itself during manufacturing. When it goes out into the production line, ready to be deployed, it has a corresponding public key and there must be a system for you to register that public key to an owner.

There has to be a repository that can map the ownership of the public key to a particular person. If a person owns an IoT device, and if something goes wrong, they have to take responsibility for it. There has to be accountability of all devices.

The handphone is the most common example of an IoT device. In Malaysia, you have to register your handphone by IC or passport. It cannot be anonymous. So, that at any point in time, we know who is the owner of that particular handphone.

We have to do that in IoT devices in the future. So that people cannot misuse IoT to commit a crime. In case a crime happens, PKI will facilitate forensic analysis. In order for this to be implemented successfully, in a timely manner, it should be an industry-driven initiative.