

**Mission Statement of the NSC**  
 To reduce and mitigate the probability of cyber security risks from crystallizing by disseminating early warnings and to share information among the stakeholders thus minimizing any adverse impact to the overall network infrastructure in Malaysia



# The SKMM Network Security Centre

Shamsul Jafni Shafie shares how the centre is ensuring information security and reliability of the network.

**W**e are living in a converged communications environment. Security in the converged environment is essential. Its importance cannot be stressed as what is seen from the endless surveillance and attacks from malicious hackers and other intruders.

Security in the digital world is also imperative as a business enabler. It is about mitigating the risks of the networks interconnected to each other. No network is a stand-alone compartment. It is not an island by itself. All networks are interdependent and are interconnected. Hence information sharing is not only encouraged but is an important element.

As it is with other network infrastructure found in most parts of the world, the infrastructure in Malaysia is privately owned. They service consumers; the private sectors, businesses and organizations such as the

government and other critical national infrastructures.

End terminals (PCs, mobile phones etc) have also become an active element in the network architecture and can be connected to different networks. A significant part of today's communication is also cross border or transits through third countries.

Networks are systems on which data are stored, processed and through which they circulate. They are composed of transmission components (cable, wireless link, satellites, routers, gateways, switches, etc) and support services (domain name system including the root servers, caller identification service, authentication services, etc). Attached to networks is an increasingly wide range of applications (e-mail delivery system, browsers, etc) and terminal equipment (telephone set, host computers, PCs, mobile phones, personal organizers or PDAs, domestic appliances, industrial machines, etc)

The marriage and convergence of technology between communications and the multimedia industry has allowed other forms of data and voice to be transmitted seamlessly using the same network through various forms of medium. Over and above that, we can also store information virtually, eliminating costs of storage in the physical world. All of the above require that the network be secured.

The Internet itself was born from the marriage between communications and multimedia. It allows people from all over the world to sample communications where data, text, pictures, voice and multimedia features is easily transmitted across the continent with ease and with little cost too.

Businesses and governments have seen the promises of such convergence. It is a cheap and easy way of communication. The benefits have presented multiple platforms upon which businesses transact and governments communicate. The proposition

## Network Thermometer



**Figure 1:** In the future and with different entities or stakeholders in the NSC, the NSC would be able to measure the threats faced in the networks within Malaysia.

is very attractive: the ability to knock down geographical barriers to reach unthought-of customers the world over.

The use of electronic communications and the related issues of security are not new. As the Internet and other info-communication networks become an ever-increasing part of Malaysian's daily lives, so does our dependency upon their underlying infrastructure. Unfortunately, so too have hostile attacks on infrastructures by network predators.

In developing and initiating plans for the development of the communications and multimedia industry in Malaysia, it was also realised that, to ensure that Malaysia achieved such goals, it needs to ensure consumers, businesses, industry players, investors, venture capitalist (VCs) and the global fraternity that it is a "safe" and "secure" place to do business.

Given the present dependence and the overall vision that communications and business in Malaysia will be fully digitised, securing the information and network systems in Malaysia is imperative and cannot be relegated to second place in terms of having the right strategies, policies and action plans. Every country has taken steps to prepare in terms of capacity building, policies and strategies to face any consequential effects. Issues concerning security have gradually come up; as a top policy issue in the later part of the years and it will not be one that will go away. It will continue

to play a major role in any decisions relating to the development of technology in the communications and multimedia environment.

Malaysia has set itself goals to achieve in the ICT, communications and multimedia world. It has set itself to become a global centre and hub for the communications and multimedia industry, understanding and realising that the future of a country will be built upon these factors. As a nation, it understands that it must not be left behind as it strives towards realising vision 2020.

Taking into account all of the above matters, the Malaysian Communications and Multimedia Commission (SKMM) initiated the setting up of the Network Security Centre (NSC).

### Background

Section 3 (2) (j) provides for the 10th National Policy Objective of the Communications and Multimedia Act (CMA) 1998, which is to ensure information security and the reliability and integrity of the network. Therefore, it is incumbent upon SKMM to establish a regulatory framework in support of the 10th national policy objectives.

The concept of establishing a network security centre was first mooted under SKMM's Framework for Industry Development (FID) Plan 2001 – 2006. The plan to set up the NSC was in line with the growing challenges that SKMM saw in the communications and multimedia industry and the need for a body that can function

to coordinate incident response to the ever-growing threats to the network.

The NSC will serve as the national Internet network thermometer to provide overall understanding of macro cyber threat level with the involvement and cooperation of both public and private sectors (**Figure 1**).

The first phase of the NSC will include the seven major Internet Service Providers (ISPs) namely TM, Jaring, Time, NTT MSC (Arc.Net), Celcom, Maxis and DiGi. Later, the NSC will be further extended to other ISPs.

By formalising the NSC, it will be the platform for SKMM to reaffirm its commitment to achieve the policy objective of information and network security under the CMA.

### The Need for the NSC

SKMM expects that all owners of network have in place security precautions in order to ensure that risks are mitigated and their network secure.

However, one of the challenges in addressing cyber security is the lack of a culture among organisations to share information on incidents and threats experienced, with each other. In short, the threats that organisation "A" is facing are not known to organisation "B" whereas organisation "B" may be subjected to the same source of threats that organisation "A" is facing. As such, there is a need for a trusted third party that can fill the gap that will then be able to ensure that threat information is shared with other third parties

without disclosing the current party that is being threatened. By sharing the information, other organisations can then take protective and corrective measures to secure themselves.

The NSC provides for the supervision, monitoring and early warning measures to all relevant stakeholders, as well as mass-scale security threats and attacks entering Malaysia through the international gateways.

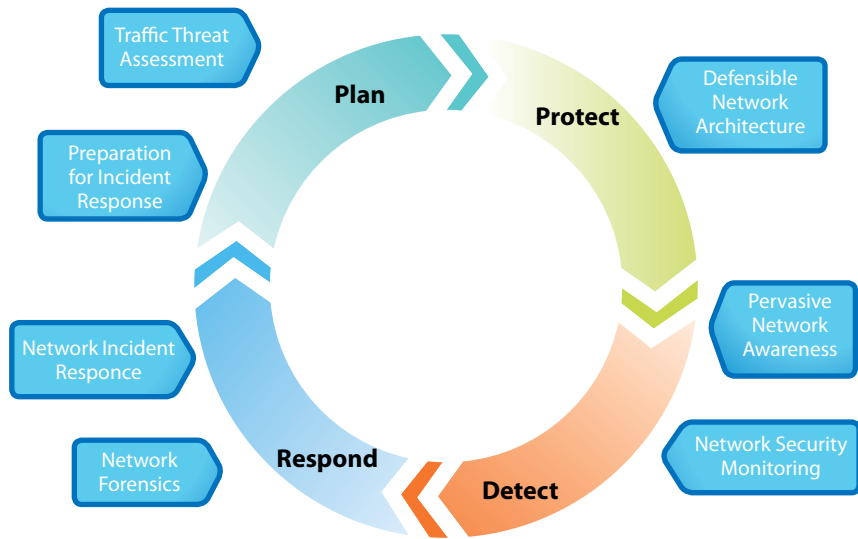
The NSC provides information and advisories about global threats, vulnerabilities and security issues affecting ISPs in Malaysia. It collects and analyses malicious traffic entering Malaysia and coordinates with ISPs to prevent damage caused by large-scale attacks. It will also facilitate information sharing and disseminate results of real-time analyses among ISPs and all relevant stakeholders in Malaysia.

It will also serve as a central point of contact for reporting of major incidents through a Centralised Abuse Reporting Portal. Through this, reliable trusted information on cyber attacks, incidents and malicious code affecting one ISP will be known to the others, so they will be able to act to pre-empt them from affecting them as well.

From the national and CMA perspective, the NSC will ensure the security of the information and network infrastructure of the communications and multimedia industry from the national level (i.e. above individual networks of service providers and critical users). Benefits obtained from such assurance include:

- Ensuring network reliability (and availability), integrity and the protection of the information system
- Ensuring that all critical national infrastructure sectors will be advised on to ensure that they are secured against any cyber intrusion, vulnerabilities, equipment failure and human error. This can be achieved by forming cooperative relationships among all local relevant stakeholders and international coordination.

## Network Security Processes



**Figure 2**

- Assuring the credibility and integrity of the nation's information system that is crucial to drive the economy which is based on ICT.

The NSC would give the ability to detect/spot early warning against cyber attacks before they spread and become a nationwide problem and would use aggregated data to model the effects of a virus or cyber attacks on key networks. However, it should be stressed that the NSC will not be a substitute for the security team for each organisation. It does not assume responsibility to ensure the security of the networks and it will not replace internal teams. What the NSC does is that it complements and supports the activities of internal teams by ensuring that information sharing between two or more different organisations are enabled and facilitated.

### The Roles and Functions of the NSC

There will be a host of responsibilities that the proposed NSC will take upon. These responsibilities will ensure that SKMM strategically plan and initiate policies and action items to ensure the security of the information and network systems in Malaysia, whilst positioning Malaysia as a Centre of Excellence in the field of information and network security. The roles and

responsibilities include but are not limited to:

- a. Work in partnership with the owners of critical systems to ensure that appropriate levels of protection are in place;
- b. Provide service of alerts and briefings of electronic attack;
- c. Encourage and facilitate information sharing on incidents, vulnerabilities and countermeasures;
- d. Assist the owners of critical systems in responding to electronic attacks;
- e. Investigate and access the threat of electronic attack and make available as much information as possible about the origins and nature of this threat;
- f. Cooperate fully with other national and international organisations engaged in work complementary to the Centre's role;
- g. Advancing work on raising information and network security awareness in both the public and private sectors;
- h. Ensuring that international activities in information and network security are properly coordinated;
- i. Address information and network security skills and R & D issues;
- j. Defining and ensuring information and network security including identifying potential incidents of a critical nature;

- k. Encouraging private sector leadership and self-regulation where possible;
- l. Lead and coordinate international efforts in relation to information and network security;
- m. Undertake incident analysis and provide a response capability for law enforcement purposes;
- n. Provide analysis, intelligence and threat assessment advice;
- o. Work closely with the public and private sector, academia, law enforcement agencies and international bodies/agencies;
- p. To position Malaysia as a centre of excellence for information and network security and as a training hub in the Asia Pacific region;
- q. Publicising security best-practice procedures and standards;
- r. Analyse trends of information and network security markets at both home and overseas;
- s. To work with critical infrastructure organizations and other sectors nationally and internationally to improve awareness and communications regarding information and network security.

In summary, the NSC will have 3 main tasks and functions. They are:

- a. Network Threat Monitoring and Management;
- b. Vulnerability Management; and
- c. Incident Management, Warnings, Response and Network Forensic.

It is to be noted that ISPs and organisations will already have some form of network monitoring activity within its own network. These activities will however only be limited to what happens within their own network. Thus a top-level multi-network monitor such as the NSC is necessary to ensure overall security across all networks. With this, a security breach on one network could be detected early and counter action/measures coordinated and shared with the industry and other relevant stakeholders curbing the problem before it becomes widespread.

The NSC coordinates three main activities:

### **Network Threat Monitoring and Management**

- a. The proposed threat monitoring and early warning will generate early warning of massive attacks or malicious propagation through threat monitoring. This is to ensure continued protection of networks and ICT systems of ISPs and other key organizations from the security infringements.
- b. It also provides direct analytical support for information and network security investigations and will serve as an information database for network analysis and unlawful acts on the nation's infrastructures. Early detection will reduce any widespread attack or propagation that may bring down the infrastructure and cause downtime and cripple the service.
- c. One of the means to protect is to get early warnings on such incidents and advise the ISPs and related organizations to take preventive measures on the threats.

### **Vulnerability Management**

- a. The objective of this activity is to ensure continued ICT infrastructure of ISPs through periodic identification and mitigation of vulnerabilities in a cost effective manner.
- b. One of the means to protect is to identify the vulnerabilities in the network devices, operating system, databases and applications and mitigating these vulnerabilities. This can be done through internal and external penetration testing.
- c. As new vulnerabilities keep emerging worldwide on regular basis, such testing should be undertaken on a periodic basis.
- d. The vulnerability testing results and recommendation reports will have greater impact and higher potential for action amongst ISP. This ensures that each ISP takes up mitigation action in a timely fashion.

- e. There is a need to keep track of security status amongst ISPs and conduct network security audit and benchmarking study. The NSC will generate the required vulnerability status data for such statistics and benchmarking.

### **Incident Management, Warnings, Response and Network Forensic**

- a. The objective of this activity is to provide timely and efficient information and recommendations to manage security incidents, to contain the damage and conduct forensics activities. This will achieve through tools, processes and skilled personnel as well as sharing of information among the stakeholders.
- b. Any security incidents, which can cause extended downtime, should be managed in a proper manner in order to contain the damage and to restore the functionality to normal status.
- c. One of the means to protect is to have a rapid response team with necessary tools and processes to investigate reported incidents and further to take remedial action.
- d. The incident management and forensics activity will be manned with skilled personnel and necessary tools to act as a rapid response team. Any incidents reported to SKMM will be investigated, remedial actions recommended, reports sent to the relevant parties and lessons learned shared among other stakeholders.

In short, threat monitoring and management will provide early warning of massive attacks and malicious code so that ISPs can take preventive measures to defend against them.

Vulnerability management will conduct periodic tests to identify vulnerabilities as early as possible, so that ISPs can take remedial measures in the spirit of "prevention being better and cheaper overall than cure."

Incident management and forensics will provide timely information and recommendations to manage security incidents and contain the damage. Its

rapid response team will use tools and processes to investigate reported incidents to effectively manage and contain the damage.

Besides providing timely remedies, it will provide advice on recent events to all relevant stakeholders and all bodies critical to the security of the national information infrastructure. It will advise on how to counter them. There are also monthly reports on how they can secure themselves against the latest threats, vulnerabilities and international trends in threats.

### NSC Operations

The NSC's security professionals monitor the ISPs' networks 24 x 7, all year round, with teams of 20 to 25 staff working in groups of four to five, in three shifts, checking on any known threats and anomalies.

### Pre-empting Attacks

The NSC's intelligent attack management team will also be able to drill down on information to provide details on incidents. However, since watching out for known threats will only help detect already known dangers, relying on them alone for identification of threats will not be able to detect new and unknown threats.

Thus the NSC team also looks for anomalies in signatures that have not been flagged as suspected malicious traffic so that they can nab unknown or new threats as these emerge. The NSC will create its own database of these threats, which will be shared with other cyber security organisations.

### The Future of the NSC

The NSC's future plans are to link up to different sectors critical to the economy and national security, including healthcare, emergency services, government, defence and security, transport, energy, telecommunications and to more international information sources, security agencies



Figure 3: NSC in the Future

and computer emergency response teams (Figure 3).

The NSC plans to be the hub for information sharing, warning, alerts and advisories on network threats for the country. By doing so, it is foreseeable that the culture of information sharing will be spread widely throughout the country and that there will be improvement and enhancement to information sharing involving cyber attacks, threats and vulnerabilities within the public and private sector.

### Conclusion

The first national policy objective of the CMA is for Malaysia to become a major global centre and hub. To do so, it must also initiate strategic plans and policies to promote a high level of consumer confidence in service delivery from the industry. To support all of the above initiatives, Malaysia must also demonstrate a high level of security in its information and network systems.

All of the above factors hinges upon the initiatives and plans that the SKMM has. The setting up of the NSC will coordinate not only the SKMM's efforts towards securing the nation's information and network systems but will also effectively coordinate other efforts in Malaysia. [.my](http://www.gov.my)

Shamsul Jafni Shafie is the Director of Security, Trust and Governance Department of SKMM. He can be contacted at [sam@cmc.gov.my](mailto:sam@cmc.gov.my).