By : DATO' SRI MOHD NAJIB TUN ABD RAZAK
Venue: RENAISSANCE KUALA LUMPUR
Date : 10-05-2004
Title: HACKERS HALTED 2004 SEMINAR

I would like to thank the Organisers for inviting me to officiate this inaugural Hacker Halted 2004 Seminar. I'm pleased to note that this Hacker Halted event held in Kuala Lumpur is the first to be organized by the EC Council anywhere in the world. I would like to extend a warm welcome to all participants, and in particular those from around the region who have traveled to Malaysia for this event.

Back in 1996, Malaysia took a huge leap into the digital world by establishing the Multimedia Super Corridor. The MSC was envisioned as a catalyst for Information and Communication Technology (ICT) development for the country. It was to be a second growth engine for the country, creating a new breed of entrepreneurs, while at the same time attracting global heavy weights of the IT world to use the MSC as a test bed for new ideas, products and services. The MSC was designed to put Malaysia firmly on the world map of ICT powerhouses. Some 8 years on, it is clear we have achieved much of this MSC vision. There are now over 1,000 companies with MSC status. By the end of this year, the MDC has estimated that these companies would have created close to 20,000 knowledge worker jobs and would have committed to approximately RM4.5 Billion in operating and capital expenditure. Cyberjaya is now home to some 200 companies with a working population of over 20,000. The MSC has come a long way for an idea that was once derided as nothing but an oil palm estate in the middle of nowhere.

The MSC also served another vital purpose, and that was to spur the pervasive use and adoption of ICT tools – products and services, hardware and software – among Malaysian companies as well as among Malaysians more generally. Here the clarion call was for Malaysia to transform itself into a Knowledge Economy, using technology, brain power and innovation to improve our competitiveness and create new sources of wealth. The vision is to works towards a "connected society" where computing would be ubiquitous and pervasive – at work, during our daily commute, in our homes and during our leisure.

The K-Economy revolution can only begin in earnest when we have adequate ICT infrastructure and penetration. At the end of 2003, Malaysia registered some 2.9 million internet dial-up subscribers. This is equivalent to an 11.4% penetration rate compared to a mere 1.8% in 1998. PC penetration also increased from 6.1 per 100 people to 16.6 over the same period. The number of broadband internet subscribers, while small, has shown a dramatic increase from 19,000 to 110,000 between 2002 to the end of last year. I believe we will see an acceleration of these trends as computing technology becomes more affordable, easier to use and most importantly, as companies begin to really compete to connect consumers to the Internet.

Apart from the ordinary consumer, the K-Economy is also having a great impact on the way the Government, companies and businesses operate. We have seen a boom in the growth of E-businesses and E-commerce. More and more organizations as well as governments are utilizing the virtual world to reach out to clients, partners, suppliers, and customers. The number of “business-to-business”, “business-to-customer” and “government-to-people” portals is growing, and is a reflection of how Malaysians are increasingly going online to seek information, conduct personal day-to-day transactions and deal with Government agencies.

While it is appropriate, and perhaps even inevitable for a developing economy like Malaysia that we seek to embrace these rapid and at times mind-boggling advances in ICT, we must be mindful of the dangers and challenges that are inherent in an increasingly interconnected world that is heavily reliant on technology. This vision of a truly networked society is not without pitfalls.

This morning’s seminar is all about providing participants with an understanding of this challenge and perhaps an early warning of things to come if we are not fully prepared. For those of us who use the Internet and email on a regular basis, you will have heard of spamming, viruses, web defacement, denial of service and a host of other attacks perpetrated by irresponsible parties. I suspect a large number of us are also likely to have been victims of such attacks. The perpetrators of these criminal acts are known as “hackers” – I have been told they are also known as “crackers” but this term is new to me. Before this morning, I knew only of cream crackers, Jacob of course

being the most famous of them all. The hacker community worldwide is a growing and thriving one. Some of the most brilliant minds in the ICT industry are part of this seedy underworld.

With each new attack, the damage inflicted by the activities of hackers escalates in sophistication, speed and costs. The US government estimated that the Code Red virus alone led to some US2.6 billion in losses to companies and computers users within the United States. A recent study by the UK Department of Trade and Industry revealed that 74% of all UK businesses – and 94% of large companies – reported IT security incidents last year, with an average of one security incident a month and once a week for large companies. The study also revealed that the average IT security incident costs large companies GBP120,000 a time.

Just last week, Malaysian users, along with millions of others around the world, experienced the latest attack by a new variant of an Internet worm called “SASSER” causing computers to shut down repeatedly. What is particularly lethal about this virus is that it can attack computers that are merely connected to the Internet, without having someone to download an email or open an attachment. Research also shows that the next generation of fast viruses such as Flash worms could infect an entire PC network within seconds. It is obvious that the financial costs of such attacks can only snowball as viruses spread faster, affect greater numbers of computers and cause more permanent damage.

Our own statistics reveal that we are seeing a surge in number of attacks this year. According to the National ICT Security and Emergency Response Centre (NISER) Quarterly Report published in April 2004, the number of web defacements has increased from 231 this quarter compared to only 6 in the last quarter of 2003. The big jump in number of attacks clearly demonstrates the vulnerability that exists within our government and corporate networks.

The threat of hackers is a real one. These attacks should not be seen as harmless pranks or a form of electronic graffiti. The very fact that systems and websites can be easily penetrated by hackers show that vulnerability exist. Given the widespread use of technology in business, the private sector is particularly vulnerable. Many of our

nation’s critical infrastructures are managed by the private sector - telecommunications, banks, ports, airports, power plants, refineries, water systems and roads. The communications networks of all these companies are potential targets for hackers and criminal elements.

There is also a national security dimension to this threat. These vulnerabilities have the potential to be exploited by elements bent on destabilising a country, an organization or the lives of ordinary individuals. It is not inconceivable for a terrorist group, a foreign government or a high tech criminal to further their cause by crippling an organization or country by destablising its strategic communications assets and networks. Our increasing reliance on the Internet, while bringing great benefits, has added further complexity to issues of national security and ultimately, political and social stability.

It is not my intention to be alarmist with my observations a moment ago. Rather, it is my hope that through forums and seminars such as this one today, organizations become more aware of such threats and develop a more comprehensive approach to information security. We need to move forward, and look beyond software and hardware approaches. Traditionally, information security has been the domain of the IT professionals. It has become abundantly clear that given the strategic impact of potential security threats, top management need to understand information security issues –as well as the technology solutions and process improvements necessary to minimize these threats.

Most CEOs today fail to understand the financial impact of unauthorized access into their information systems. Information security must become part of corporate strategy. Shareholders and management should ultimately realise that without effective information security policies and procedures, the competitive edge and efficiencies brought about by ICT can be undone by a single act of brilliance by a lone hacker.

In this regard, I would urge all government agencies and the private sector to equip relevant personnel with the latest knowledge, skills and tools to combat potential threats from hackers and their activities. Defensive, reactive approaches are no longer adequate. Organisations need to be proactive in handling information security issues. You will need to better understand the minds and

modus operandi used of hackers. You will need access to the same tools used by hackers so that you may be equally prepared to counter them. Organisations need to redefine the concept of security from being just guardianship of physical assets and movement of employees and visitors. The new role of a Chief Security Officer should be to fully integrate the control of access by any individual to an organisation's premises, assets as well as its networks.

Besides IT personnel, organisations must take steps to ensure ordinary employees are adequately educated on information security policies. Evidence show that most security breaches occur with non-IT personnel who are not fully aware of the consequences of their actions. Forwarded e-mails that are infected is often the major culprit. Unless everyone connected to the internet understands the impact of hacking and inadvertent security breaches, vulnerabilities will continue to exist for hackers to wreak havoc.

There is an urgent need to develop an integrated, collaborative approach to information security threats, failing which we will continue remain helpless victims of the hacking community. I would like to take this opportunity to suggest a permanent forum or platform to enable members of the IT security fraternity to share latest information, skills and technologies with one another. As we become more integrated with the global trading, commercial and investment environment, we will need to create a community of ethically trained IT security professionals who will be at the forefront of our war against hackers. For this forum or platform to be effective, the public and the private sector must form a balanced partnership – one that respects an individual organisation's right to privacy but at the same time, one that encourages a vital exchange of skills, knowledge and experience. I believe this platform will in time enable us to combat the network of hackers, many of whom belong to a forum of their own and are constantly exchanging ideas and tools worldwide.

The Government will continue to play its part to ensure greater security for all electronic-based activities and transactions. We have a responsibility to ensure a robust legal framework and enforcement approach that preserves and protects the information networks of this country. In this respect, three more Acts that will be tabled in Parliament:

the Privacy Protection Act; the Electronic Transaction Act and the Electronic Government Activities Act. In addition, the Government is examining the issue of spamming and we are currently studying existing legislation elsewhere. Once approved, these laws will provide greater protection to Internet users and facilitate the orderly growth of electronic commerce in Malaysia.

I have spoken at length about the challenges concerning information security and the steps we can all take to minimize the threats that confront us. I hope I have left you with enough food for thought. Let me end by congratulating the organizers – the EC Council and Wordware, as well as the National ICT Security and Emergency Response Centre, the MDC and the Malaysian National Computer Confederation for bringing such an important event to Malaysia.

I wish you all a successful meeting.

Office of the Deputy Prime Minister
Putrajaya