

# e-Security

Volume 10 -(Q1/2007)



**MOSTI**



**You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable to old-fashioned social-engineering manipulation**

*-Kevin Mitnick*

## Contributors

**MyCERT 1st Quarter 2007 Summary Report**  
CyberSecurity Malaysia

**Planning & Assessing the Need For Security Awareness for Organisations**

By Raj Kumar  
Senior Training & Outreach Executive  
CyberSecurity Malaysia  
[raj@cybersecurity.org.my](mailto:raj@cybersecurity.org.my)

**The Distributed, Web Enabled Enterprise**

By Lim Pün Kok  
Managing Director for Asean/ANZ  
Blue Coat Systems

**The Speed of Light Is Too Slow Again!**

By Nigel Hawthorne  
Vice President, International Marketing  
Blue Coat Systems

**Improving Internet Security in Organisations**

By Zahri Yunus & Shaharudin Ismail  
CyberSecurity Malaysia  
Islamic University College of Malaysia (KUIM)  
[zahri@cybersecurity.org.my](mailto:zahri@cybersecurity.org.my)

**Regulating Online Content: An Overview**

By Izwan Iskandar Ishak  
Policy Research Executive  
CyberSecurity Malaysia  
[izwan@cybersecurity.org.my](mailto:izwan@cybersecurity.org.my)

**Theft in The Digital World:  
Are We 'Legally' Ready?**

By Izwan Iskandar Ishak  
Policy Research Executive  
CyberSecurity Malaysia  
[izwan@cybersecurity.org.my](mailto:izwan@cybersecurity.org.my)

**Configuring Your Home Network (Wi-Fi)**

By Patrik Runald  
F-Secure  
[patrik.runald@f-secure.com](mailto:patrik.runald@f-secure.com)

**An Introduction to the Malaysian Cybercrime  
Legislative Framework**

By Deepak Pillai  
Partner  
HaryatiDeepak, Advocates & Solicitors  
[deepak@hdlaw.com.my](mailto:deepak@hdlaw.com.my)

**Data Theft**

By Aswami Fadillah  
Manager, Digital Forensics  
CyberSecurity Malaysia  
[aswami@cybersecurity.org.my](mailto:aswami@cybersecurity.org.my)

**Top Ten Predictions for 2007**  
By Fortinet

**Home Wireless:  
Connect Confidently**

By Noor Aida Idris  
Technical Writer  
CyberSecurity Malaysia  
[nooraida@cybersecurity.org.my](mailto:nooraida@cybersecurity.org.my)

**Integrated Threat Management –  
Protect Your Organisation from  
the Inside Out**

By CA

## From the Editor's Desk

vphilip@cybersecurity.org.my

Q1 2007 and we celebrate our 10th issue. Indeed, an incredible milestone and to further ride on that excitement, we are now known as CyberSecurity Malaysia.

Check out the latest MyCERT report in this issue and the latest threats and issues faced here in Malaysia. Also in this issue we have some great articles on Cyber Law. If you are ignorant of the cyber laws in Malaysia, check out our segment on this and know what we have and what the laws have to say.

In April 2007, we did our first INFOSEC.my Knowledge Sharing Session for this year and we had the privilege of having 4 Board of Directors from (ISC)2 present. Who were they? Well, we had our very own Lt Col (R) Husin Jazri, Dr Peter Berlich, Hord Tipton and Diana Lynn Contesti. We also had our team from Cyber Security Malaysia presenting on Wireless Security based on the War Driving conducted in KL recently.

We also conducted our first CISSP Course in May recently and we had an excellent trainer from the US, Lyron Andrews who did a marvelous job in delivering the class over 5 days. We hope to bring him down again in August for our next class. August will be the last CISSP class for 2007, so register quickly to avoid disappointment. Also, in August we will be launching the SSCP course targeted towards the technical community. Check out our website at <http://www.cybersecurity.org.my> for more details.

Once again, we invite more security professionals to contribute to our newsletter and remember that you can view our newsletter online from our website.

**Philip**

Philip Victor  
Editor

## Table of Contents

03	MyCERT 1st Quarter 2007 Summary Report CyberSecurity Malaysia
06	Planning & Assessing the Need For Security Awareness for Organisations
10	The Distributed, Web Enabled Enterprise
13	The Speed of Light Is Too Slow Again!
18	Improving Internet Security in Organisations
20	Regulating Online Content: An Overview
22	Theft in The Digital World: Are We 'Legally' Ready?
24	Configuring Your Home Network (Wi-Fi)
26	An Introduction to the Malaysian Cybercrime Legislative Framework
31	Data Theft
32	Top Ten Predictions for 2007

## A Message From the Head of CyberSecurity Malaysia

It gives me great pleasure to be able to communicate to all our e-Security readers. I'm glad to see this newsletter going into its 10th issue and also many appreciations to all those who have contributed. It is indeed great to have information security professionals and practitioners from both locally and internationally contributing their expertise to this newsletter.

We have recently changed our name to CyberSecurity Malaysia which we hope reflects more towards what we do and the services we offer. Formerly known as NISER, we have grown since and now playing an even more important role in securing our cyber space.

In February this year, the Malaysian Computer Emergency Response Centre (MyCERT), was appointed as the new chair for the Asia Pacific CERT (APCERT) and this has carved a great achievement for CyberSecurity Malaysia. The trust and confidence not only comes from our country but have been seen internationally and thus putting Malaysia as a key player in the Information Security arena.

In March this year, MyCERT together with the Japanese CERT/Coordination Centre (JPCERT/CC) had also conducted a 5-day Computer Security Incident Response Team (CSIRT) training for Cambodia, Laos & Myanmar. This training was held at Cambodia and participants from these 3 countries were trained on setting up National CERTs and managing these CERTs. The training was successful and participants benefited greatly from it.

As this is the first issue for 2007, I would like to say that cyber threats are growing as new technologies emerge. This will call for greater protection. The need for more Information Security Professionals is growing and we encourage more information security practitioners to embark on relevant information security professional certification and continuous competency building. This will lead to a bigger pool of security professionals and thus moving towards the nation's call for an increase in knowledge workers.

Awareness is the foundation and people are the key towards a secured and safer cyber environment. Together we need to build a culture of security and applying best practices in our daily lives so as the cyber crimes and attempt to commit any of them can be reduced effectively.

With that, I once again like to thank all contributors and look forward to more information sharing cooperation in making a cyberspace safe and a better place for everyone.

Best Regards  
Husin Jazri CISSP  
Acting CEO  
CyberSecurity Malaysia

34	Home Wireless: Connect Confidently
37	Integrated Threat Management – Protect Your Organisation from the Inside Out
39	13 Security Tips To Safe Internet Banking

### CORRECTION

The article "War Driving Analysis - Kuala Lumpur 2006" published in Volume 9 (Q4/2006) was written by Rozana Rusli ([rozana@cybersecurity.org.my](mailto:rozana@cybersecurity.org.my)) & Mohamad Nizam ([mnizam.kassim@cybersecurity.org.my](mailto:mnizam.kassim@cybersecurity.org.my)) of CyberSecurity Malaysia.

## READER ENQUIRY

Training & Outreach  
CyberSecurity Malaysia  
Ministry of Science, Technology and Innovation (MOSTI)  
Email: [training@cybersecurity.org.my](mailto:training@cybersecurity.org.my)

# MS-115.042007: MyCERT Quarterly Summary (Q1) 2007

## Original Issue Date: 12th April 2007

03.

The MyCERT Quarterly Summary includes some brief descriptions and analysis of major incidents observed during that quarter. This report highlights statistics of attacks or incidents reported to MyCERT, as well as other noteworthy incidents and new vulnerability information. MyCERT believes these statistics are only the tip of the iceberg. Internet users are encouraged to report computer security incidents to MyCERT in order to enable us to assist those affected.

In addition, this summary also directs to resources in dealing with problems related to security incidents, patches, service packs, upgrades and hardenings.

### Recent Activities

In this quarter, a total of 10680 incidents were received which is 2.98% decrease compared to Q4 2006. About 98.34% is contributed by spam reports. No major outbreak was observed this quarter. Incidents that had increased are spam, fraud and malicious. Other incidents that showed decrease in this quarter are intrusion, hack threat, denial of service and harassment.

Attached is the figure for Q1 2007 and Q4 2006:

	Q4 2006	Q1 2007	%
Intrusion	424	74	-82.55
Denial of Service	4	0	NIL
Malicious Code	11	13	18.18
Hack Threat	14	1	-92.86
Fraud	58	70	20.69
Harassment	25	19	-24
Spam	10472	10503	0.3
<b>Total</b>	<b>11008</b>	<b>10680</b>	<b>-2.98</b>

### Increase in Fraud Incidents

This quarter saw an increase in fraud incidents to 20.69%, which comprised of 70 reports compared to 58 reports in previous quarter. About 65.71% of fraud incidents reported were phishing incidents impersonating local and foreign financial institutions.

In this quarter, we also received reports of 9 phishing sites that targeted a single local bank, hosted on a single machine located in Korea, using a recent phishing technique called "ROCK PHISH". "ROCK PHISH" is a phishing tool kit that allows attackers to install phishing pages into non-web-server systems like the personal computers, desktops, workstations by installing small portion of the program that enables http service.

The respective ISPs, data centers and organizations have been alerted to remove the relevant websites and to investigate the affected machines and rectify them accordingly. In some cases, these hosts have been infected with bots and require thorough clean-up.

As was in the previous quarter, MyCERT continues to receive reports from local users regarding Internet scams. These include the Nigerian Scam, Cheatings, Illegal Online Gambling and Get Rich Scams. The mode of operations of the scams involves the use of spam to lure Internet users to visit specific websites and eventually request deposit of a certain amount of money to the fraudsters' accounts. Computer users should also be careful about disclosing confidential, personal or financial information online unless they know that the request for such is legitimate and users are also advised not to deposit or make payments to unknown third party's account.

**User may refer to the following guide on safeguarding against fraudulent emails and phishing attempts:**

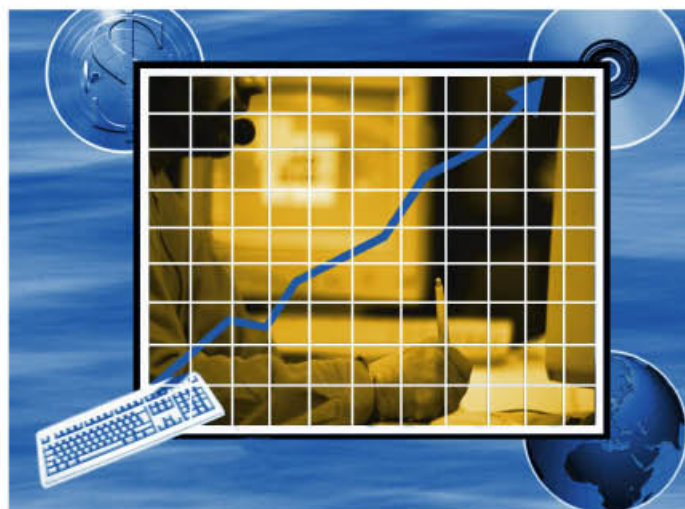


[http://www.mycert.org.my/other\\_resources/phishing.html](http://www.mycert.org.my/other_resources/phishing.html)

### Increase in Malicious Code Incidents

Malicious code incidents slightly increased compared to the previous quarter. A total of 13 incidents were reported compared to 11 in the previous quarter, which represents a 18.18% increase. In this quarter, we received several reports from foreign CERTs regarding Control & Command server of botnets running on local machines. The respective machines' Administrators were notified and advised to clean up the affected machines.

Besides reports on Control & Command servers, we also received reports from home users regarding their PCs being infected with the mass mailing worms, namely the W32.Nyxem worm, W32.Brntok worm and W32/VB-NIA Worm. The complainants were advised on removal procedures accordingly.



## We advise users to safe-guard their PCs against Trojan, backdoor and worm infections. Users may refer to the below guidelines:

**one**

Ensure computers are installed with anti-virus software and are frequently updated with the latest virus signatures. Users without anti-virus installed on their PCs may download commercial or free anti-virus from the following site:

<http://www.mycert.org.my/anti-virus.htm>

**two**

Ensure computers are always updated with the latest service packs and patches, as some worms propagate by exploiting unpatched programs present in computers.

**three**

Enable personal/host-based firewalls on PCs.

**four**

PC users are also advised not to view, open or execute any e-mail attachment unless it is expected or its purpose known to the recipient.

### Decrease in .MY Web Defacements

The first quarter of 2007 saw a decrease in number of .my web defacements by 82.55% compared to the previous quarter. We received 74 reports on intrusions; with majority of intrusion are web defacements.

Though the drop in number of reports received on Intrusion, MyCERT would like to urge all system administrators and virtual host administrators to upgrade and patch systems, services and applications they are currently using as and when new security are made available. In addition, it is also recommended to disable unnecessary or unneeded default services on the systems.

**More detail steps in securing UNIX and Windows Servers are available at**

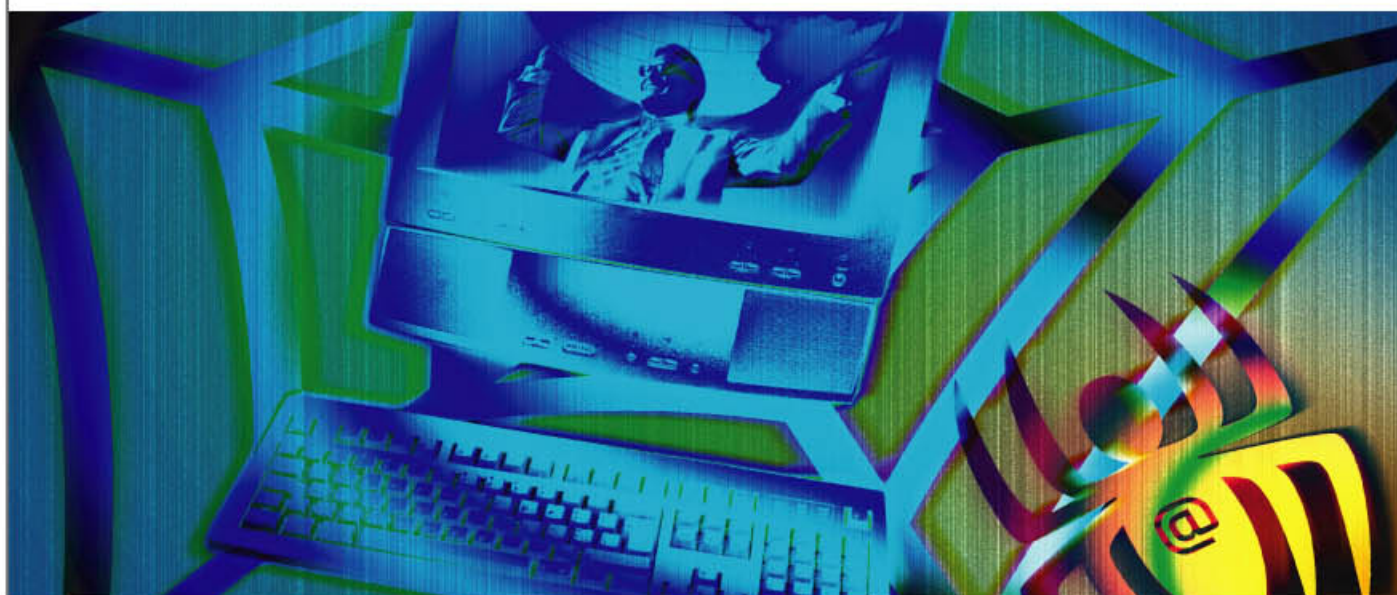


<http://www.mycert.org.my/resource.html>

### Slight Decrease in Harassment Incidents

Number of incidents received on harassment had decreased to 19 compared to 25 incidents which represents 24%. Majority of incidents involved harassments via blogs and web forums, in which false/misleading information were posted on web forums and blogs against a particular organization or individuals. The particular false/misleading information were removed within 1 – 3 days after MyCERT notified the respective ISPs where the blogs/forums hosted.

Other types of harassments we received were threatening/defamatory emails and SMS messages sent to victims with malicious intentions.



## Other Activities

### → Spam

Spam incidents had increased to 0.3% in this quarter compared to the previous quarter. A total of 10503 reports were received compared to 10472 reports in the previous quarter. Spam has developed from a mere nuisance into an epidemic that threatens end users and organizations. There are no perfect techniques or tools to completely eradicate spam, however there are techniques that end users and organizations can implement to minimize them, such as installing anti-spam filters at email gateways and applying appropriate email filters at end users' email clients. Users are also advised not to respond nor purchase products promoted via spam.

### → Denial of Service

During this quarter, no reports were received on denial of service.

### → Hack Threat

Incidents involving hack threat decreased to about 92.86% in this quarter. Only 1 report of hack threat consists of port scanning was received for this quarter compared to 14 in the previous quarter. The threat involved unauthorized scanning of network and system.



## Conclusion

Overall, the number of incidents reported to us had decreased by 2.98% compared to the previous quarter where incidents were mainly contributed from spam incidents.

Reports were the most for intrusion incidents with majority contribution from web defacements. Neither crisis nor outbreaks was observed this quarter.

Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats.

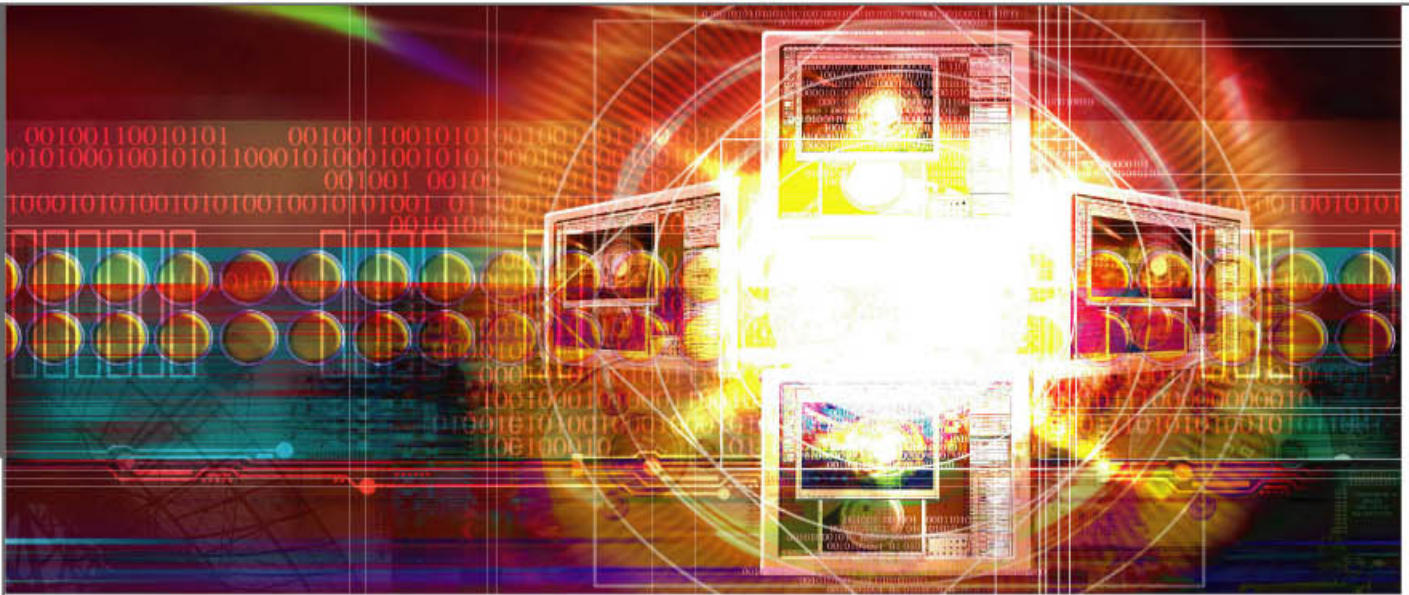
We strongly advise users/organizations to report and seek assistance from MyCERT in the event of any security incidents.

### MyCERT can be reached at:

E-mail : [mycert@mycert.org.my](mailto:mycert@mycert.org.my)  
 Phone : +603 89926969 (monitored during business hours)  
 Fax : +603 89453442 (monitored during business hours)  
 Handphone : +60 19 2665850 (24x7 call incident reporting)  
 SMS : +60 19 2813801 (24x7 SMS reporting)

### Business Hours : Mon - Fri 08:30 -17:30 MYT

Web : <http://www.mycert.org.my>  
 Postal : Malaysian Computer Emergency Response Team (MyCERT)  
 CyberSecurity Malaysia  
 Level 7, SAPURA@MINES  
 7, Jalan Tasik, The Mines Resort City  
 43300 Seri Kembangan  
 Selangor Darul Ehsan  
 MALAYSIA



# Planning and assessing the need for security awareness for organisations.

Having a world class security technology-based defenses and qualified security team does not raise the security readiness level in any organisation. The single most important element of security readiness is employee awareness.

User awareness is the first line of defense for any threat or risk that may be faced by an employee while using information systems or network systems. Without being aware of the dangers, an employee cannot be expected or prepared to safeguard themselves.

In every organisation, there will be users whom are completely not aware of the threats. It is known fact not many of the staff would have attended a formal training on security awareness or related course. Many would have heard of or faced viruses and spam email through experience but not all of the threats or most importantly, the best practices for defense. Although some of the staff may have an adequate knowledge of some of the more common types of information security threats, they may not be aware of relatively newer threats. For example, newer data transmission technologies such as Bluetooth are also affected by security and privacy issues. People are still unaware that someone can access their address book or make calls by connecting with their PDA or mobile phone through Bluetooth. Adults are failing to make financial transactions online (such as banking) due to the perception of lack of security.

A common understanding of the threats and safeguarding yourself and the organisation's information assets need to be established for all employees. To promote an effective information security

awareness programme, the message must be visible and understandable by all employees. The overall message is the same, but the delivery needs to be tailored to each level of individual in a manner that will cause them to support the vision. Therefore, planning and assessing the needs of each target group is vital for the success of the initiative.

Awareness and training programs must be designed with the organizations' mission in mind. It is important that the awareness and training program supports the business needs and be relevant to the organization's culture and IT infrastructure. The most successful programmes are those that users feel are relevant to the subject matter and issues are presented. Raising the awareness of employee knowledge of security and getting them to understand their own role in security cannot happen with a one-time event, it requires the development of a continuous process and therefore management support is crucial. The organisation leaders need to fully understand the directives that form the basis for security programme and need to exercise their leadership role to ensure commitment and compliance is exercised by all users in the organisation.

Some of the key questions that to be considered in order to meet the programme objective should include the following:



- Defining what is information security. Every employee must understand the term and the basic concept.
- What is the organisation's security strategy?
- What are the security policies and how it is practiced or applied in daily activities?
- What are the current processes related to business operations?
- What are the regulation that applies to business operations? It can be local, state or federal laws.
- How does security affect employee's daily activities?
- How would major security incidence affect the business?

## There are four (4) steps in creating a security awareness program

(refer to Fig.1.1, according to Mark Wilson and Joan Hash at NIST (National Institute of Standards and Technology, US): designing the programme, developing or purchasing the awareness materials, implementing the programme and post-implementation activities.

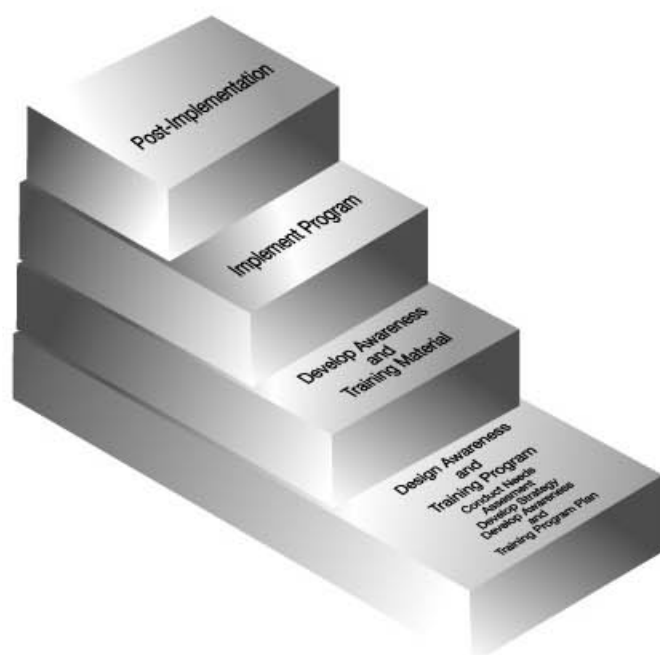


Fig.1.0 Steps in creation of Security awareness programme (Wilson and Hash, 2003)

The initial stage of awareness programme development is the design, where a training needs assessment is formulated in order to determine an organization's awareness and training needs (to Fig 1.0). The training needs assessment exercise is a strategy to be used for formulating the mechanisms for developing, implementing, and maintaining security awareness programmes.

### The awareness programme plan should discuss the following elements:

- To state and include any existing national and local policy that mentions the requirement for security awareness. This can be used as a form of directive, which can also come from the senior management.
- The mission and the scope of the awareness programme.
- The roles and responsibilities of personnel(s) who designs, develops, implements, and maintains the awareness programme and who should ensure that all users attend or view the applicable material or programme
- Goals to be accomplished for each aspect or activity of the program (e.g., awareness, training, education, certification) and the learning objectives to be clearly defined.
- Target audiences for each aspect of the program;
- Courses or awareness material for each target audience and topics to be determined. How the delivery of the topics and mode of communication should be determined.
- An evaluation mechanism should be determined to measure the success of the programme and also the frequency of exposure to the material should also be determined.

Part of the awareness programme development is the formulation of needs assessment which can be used to provide justification to the management for resource allocation, including funds and to meet the identified awareness and training initiatives for further development. It is crucial that the management support the initiative and its criticality to business is recognised. The following diagram (Fig.1.1) indicates the various inputs required for training need assessment.

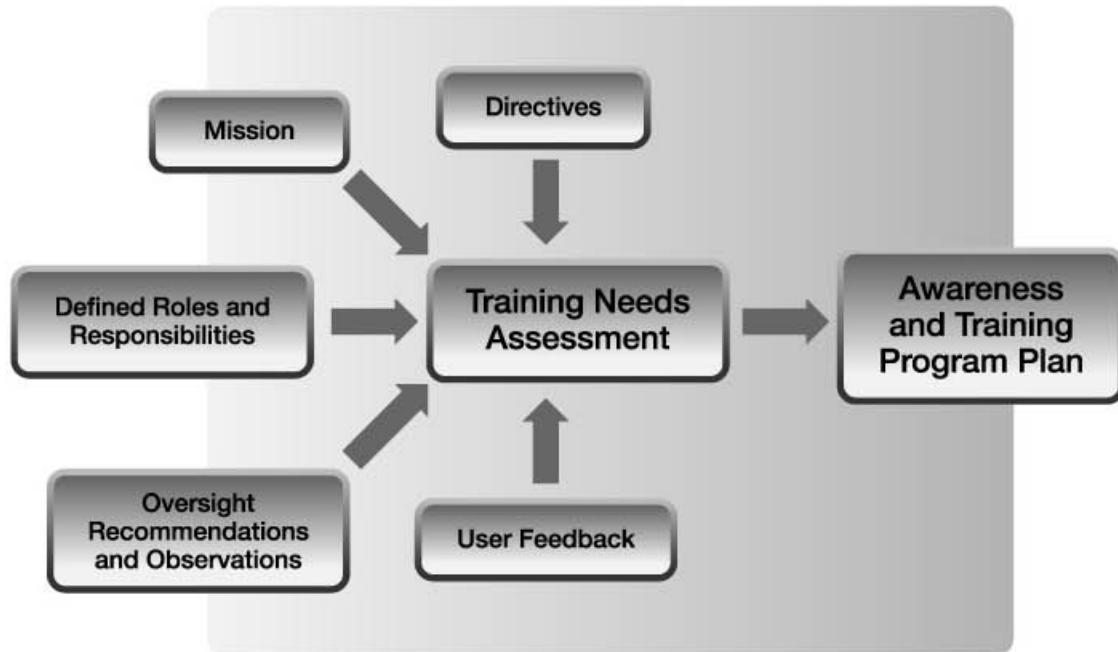


Fig 1.1 Inputs for the needs assessment process

The following are the key questions that need to be answered when conducting a training needs analysis:



1 What awareness or training is required to raise the current awareness level?



2 What is being done to meet these needs currently?



3 What is the current status of how these needs are being addressed and what is the progress?



4 Where are the gaps between the needs and what is being done, is there more to be done?



5 Which needs are most critical?



There are many sources of information or activities that can be performed to formulate the training needs assessment. The following are some of activities that would aid in the formulation:



**1 Conduct interviews with all key personnel from each level of management.**



**2 Conduct organization-wide survey to determine current state of awareness.**



**3 Conduct review and assessment of available resource material, such as current awareness and training material, training schedules, and lists of attendees**



**4 Analysis of metrics used related to awareness and training (e.g., percentage of users completing required awareness session or exposure, percentage of users with significant security responsibilities who have been trained in role-specific material)**



**5 Review of current security plans for general support systems and major applications, to identify system and application owners, and appointed security representatives**



**6 Review of system inventory and application user ID databases to determine all who have access.**



**7 Review of any findings and/or recommendations from reviews regarding the IT security program conducted in other organisations**



**8 Conversations and interviews with management, owners of general support systems and major applications, and other organization staff whose business functions rely on IT**



**9 Analysis of events (such as denial of service attacks, website defacements, hijacking of systems used in subsequent attacks, successful virus attacks) might indicate the need for training (or additional training) of specific groups of people**



**10 Reviews done when technical or infrastructure changes are made**



**11 The study of trends first identified in industry, academic, or government publications or by training/education organizations. The use of these "early warning systems" can provide insight into an issue within the organization that has yet to be seen as a problem.**

The needs assessment can and will be able to indicate the relationship between awareness and training requirements and an organization's current status. The gap between what is currently being done and what is required can be derived.

Another important aspect of a needs assessment is the related IT security awareness and training program requirements. For example, if awareness and training material is to be presented utilizing computer-based training (CBT) technology, a technical assessment should be conducted on the organization's hardware and software platform (e.g., local area network, workstations, video cards, speakers) to determine if the existing environment will be able to support awareness and training program. Similarly, if the organization plans to provide classroom training, the needs assessment should identify if adequate resources exists for an effective learning environment.

Once the needs assessment has been completed, the information needed to develop the awareness and training plan will be available. The plan should cover the entire organization and incorporate priorities identified by the needs assessment.

To successfully design a security awareness programme, support is needed from the senior management and the employees, including all those who have some degree of access to the computers, systems, and information of the organization. Employee participation at some level in the security awareness efforts is crucial as the first line of defense in security. The training needs assessment will provide an accurate measure for initiating the programme. As with any new initiative, you can expect issues. But by understanding the challenges and audience, you can effectively implement steps that will improve security in your company and help develop a cultural awareness for good security practices and successful awareness programme.

## References:

Wilson, M., Hash, J., October 2003. Building an Information Technology Security Awareness Program

Available from:



<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>

[Cited 18 December 2006]

European Network and Information Security Agency (ENISA), June 2006, A User Guide: How to Raise Information Security Awareness: ENISA publication

# WAN

## The Distributed, Web -

As organizations become more distributed and applications become more centralized, the corporate WAN is destined to play an increasingly important role in providing remote users with fast access to critical business applications. Optimizing the performance of applications over costly WAN links has become a critical issue and top priority for IT organizations.

To better understand the current state of the WAN, as well as plans that could affect WAN architectures and application performance in 2007, Blue Coat recently conducted a comprehensive survey of IT executives last December. Key findings and analysis of data were collected from more than 1,300 enterprise IT executives in 40 countries around the world.

### The survey results highlight certain key trends, including:

- Increasing consolidation of remote servers and applications into the data center
- Increasing application performance problems experienced by remote users
- Increasing integration of the Web into business processes
- Increasing amount of encrypted SSL application traffic
- Increasing Internet traffic as a percentage of overall WAN traffic
- Increasing number of mobile users working outside the WAN

# WWW enabled Enterprise

In today's global economy, ubiquitous network connectivity allows businesses to deploy facilities and employees wherever they can provide the most operational efficiency and economic value. Thus we're now seeing highly distributed organizations, with remote offices and mobile users often thousands of miles away from corporate headquarters. This shift is apparent in the results of the survey where 26% of respondents indicated they have more than 100 remote offices, and 70% of organizations have five or more remote sites.

Ironically, while organizations are becoming far more distributed, the trend toward server and application consolidation continues. Nearly 60% of respondents indicated that they are centralizing these resources away from remote offices and into corporate data centers. Indeed, consolidation of the data centers themselves is also underway, as IT organizations strive for tighter control and security of vital business information. Survey results indicated that 56% of all organizations are currently involved in data center consolidation projects, or have already completed the task.

As a result of both the consolidation of IT resources and the distribution of users, corporate WAN links and, increasingly, the Internet are providing the connectivity users need to get access to critical business applications. Today 36% of respondents are leveraging both WAN links and the Internet for application delivery to remote users. Moving forward, it will be critically important for IT organizations to ensure that all remote users experience optimized application delivery to their desktop – regardless of their location and regardless of how they access applications.

The latter point becomes more critical as the number of mobile users continue to grow. More than 90% of all respondents have mobile workers – including road warriors and home office users – that work outside the boundaries of the distributed enterprise network.

And 82% of these organizations expect the number of mobile users to increase in 2007. These users include executives, sales people, and support personnel, and their job functions are critical to the success of the business. The challenge for IT organizations, then, is to provide these users with same level of application performance and Web security as provided to users inside the corporate network.

In terms of the applications themselves, nearly 90% of all organizations host their business applications in the corporate data center. No surprise there. However, external application service providers (ASPs) are also being used by 23% of organizations, to host applications on the Internet and deliver them as a service to corporate users. ASPs will be used more broadly in 2007.

In either case, the Web browser is playing an increasingly important role in the way users access productivity applications, as well as content on the Internet. In 2006, more than 70% of organizations had already standardized on the Web browser as the primary application interface. In 2007, that trend will continue as more than 75% of all companies plan rollouts of new Web-based applications.

The integration of the Web with business-critical applications – whether hosted internally or externally – creates the need for application-level security. SSL has emerged as the standard protocol used to create secure, encrypted tunnels for Web-based applications. Survey results indicated that 53% of organizations have already deployed internal business applications that use SSL. In 2007, 45% of respondents plan to roll out new SSL applications, and 62% expect SSL traffic to increase as a percentage of overall WAN traffic. The percentage is obviously higher when you factor in external Web applications using SSL.

# Performance, Control, and Security Challenges

The evolution of the distributed enterprise, the integration of the Internet, and the consolidation of data centers and applications all offer tremendous business benefits. However, these trends also present new IT challenges related to WAN performance, application control, and Web user security.

For example, daily backup between data centers is critical to ensure business continuity in the event of a disaster. However, the volume of data that must be backed up increases every day. More data means more time and/or bandwidth required for this critical operation. Based on the results of the survey, more than 60% of survey respondents are feeling the pain of slow WAN performance caused by data center backups that consume too much time and/or bandwidth.

But the problem of slow WAN performance is by no means limited to data center backup. As noted earlier, the combination of centralized applications and distributed users means that more users must traverse the WAN to get the applications and files they need. Survey results indicate that remote users in 64% of all organizations are experiencing unacceptably slow application performance. This poor performance is associated with a broad set of applications, including client-server, Web, email, streaming media, and increasingly SSL applications.

With SSL applications, there is both good and bad news. The good news is that organizations are safely integrating the Web into their business operations, making their applications more secure and more accessible to remote users via corporate.

WAN links or the Internet. The bad news is that since SSL traffic is encrypted, its contents are not "visible" to IT, making it impossible to control and optimize delivery to remote users. With SSL traffic continuing to grow, this performance problem will only get worse.

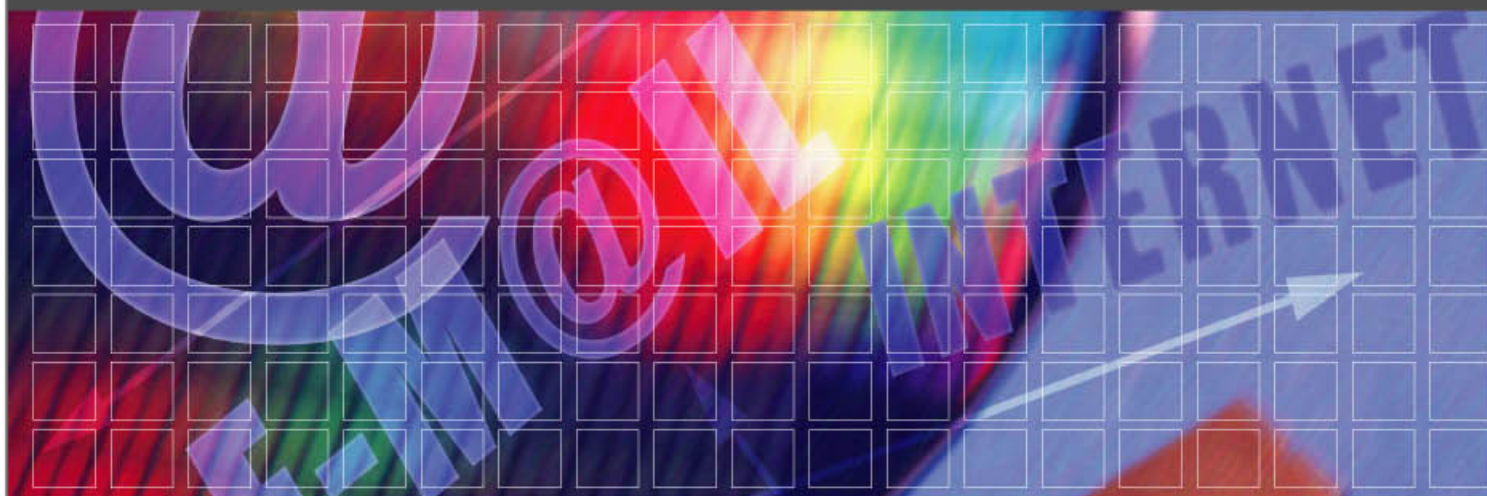
The total amount of Internet traffic continues to grow as a percentage of overall WAN traffic.

**Nearly 55% of survey respondents believe that Internet traffic now consumes more than 25% of all WAN bandwidth. In 2007, 77% of respondents expect Internet traffic to continue to increase. Some of that traffic is, of course, relevant to the business and important for user productivity. But much of it is likely non-essential, or worse, detrimental to the productivity of the business and individual users. Clearly there is a growing to control and manage Internet traffic and recover bandwidth lost to Web surfing.**

One of the reasons for all of the Internet traffic is that many companies still rely on a centralized Internet gateway at the headquarters site. With that type of architecture, all Internet traffic is then backhauled across WAN links to remote users. IT organizations can also address this problem by establishing additional Internet gateways in some larger branch offices. That would allow remote users to go directly to the Internet and would immediately reduce Internet traffic across the WAN.

About 26% of survey respondents are planning to adopt this strategy in 2007. Those organizations that are not planning to add more gateways expressed concerns that it would create additional security risks. This is a valid concern, but can easily be addressed by deploying the proper security capabilities in the remote location.

Clearly, there remain some critical performance (and security) problems that need to be addressed to ensure optimal productivity for all remote and mobile users across the distributed enterprise. When survey participants were asked how they intended to solve these problems, 45% indicated plans for more WAN bandwidth. This may help address some problems, but will not be effective in dealing with SSL traffic, increasing Internet traffic, streaming media, mobile users, or most importantly, the inherent latency that degrades the performance of many applications. Another 42% indicated plans to evaluate specialized appliances for acceleration WAN application delivery and providing remote users with Web security.



# The speed of light is too *s / o w* again!

In 1998, I wrote an article stating that the speed of light was too slow, and, until we fixed it, users would receive poor web performance due to the inefficiencies of the Internet protocols. Some people said "greater bandwidth will solve the issue" and promptly forgot about it.

Well, here we are, eight years later. We still haven't increased the speed of light, available WAN bandwidth has grown many times over and yet those of us remote from the data we need are still waiting for information; if anything the situation has got worse.

More users than ever are working remotely from corporate data, recent research from Nemertes Research states that "fewer than 10% of workers work at headquarters in the average company"<sup>a</sup>. At the same time, IT departments are consolidating servers to ease the management burden and comply with backup regulations, as an example Hewlett Packard announced it is cutting back from 85 worldwide data centers to 6<sup>b</sup>.

The last 8 years have also changed the way that applications are delivered to users; web-based applications being the norm, (often using SSL for encryption), streaming data for training and a wealth of rich content distributed around the standard organization. Web-based applications consume at least ten-times more bandwidth than traditional client-server applications.



## Greater bandwidth *is not equal to faster throughput*

There's no doubt that adding bandwidth helps delivery of data up to a point and the more users at the remote office, the greater the benefit from adding more bandwidth.

A simple analogy is to use the idea of a 65 mile length of freeway with a speed limit of 65MPH, when empty a single car can drive the distance in one hour. If development plans show that the freeway will be used by twice as many cars in eight years, then doubling the number of lanes will provide enough width for the new traffic. But what of the individual sitting in his or her car, does that individual car get there any quicker? The speed limit is still 65MPH so even though we have doubled the number of total cars, each individual car still takes the same hour to drive the distance.

To take this analogy further, if a car-owner was moving house eight years ago and it took him two trips to take his belongings along this same road, the total time to move house would be four hours (two round-trips). Today he is moving house again and has ten times as many belongings, now unless he hires a truck it will take twenty round-trips or a total of twenty hours and the total number of lanes on the road is irrelevant for that individual.

<sup>a</sup>[http://www.nemertes.com/columns/data\\_center\\_consolidation\\_and\\_stripping\\_the\\_branch\\_office](http://www.nemertes.com/columns/data_center_consolidation_and_stripping_the_branch_office)

<sup>b</sup>[http://utilitycomputing.itworld.com/4591/060517hpconsolidate/page\\_1.html](http://utilitycomputing.itworld.com/4591/060517hpconsolidate/page_1.html)



## The enemy of applications – distance

If the enemy of application delivery is not bandwidth, what is it? It is distance. To be more exact, the enemy is round-trip time. And round-trip time is defined by the following:

- The speed of light
- The real distance the data needs to travel (cables don't go direct from source to destination)
- Any delays from routers, firewalls and network latency
- The server and PC delays at each end
- The amount of data that can be transmitted at one time, defined by the protocol being used



## Our protocols are inefficient over the WAN

Now for some mathematics. Don't hide, it's not that bad.

The original design goal of TCP/IP was to create a protocol that was reliable over almost any network. A sender transmits small (maximum 64K) packets of information and then wait for an ACKs (acknowledgements of data) back from the recipient before sending more. The equivalent on the freeway is to take one box of belongings at a time along the 65mile route before driving back empty and collecting another box.

To make matters worse, other protocols reduce this maximum (for example MAPI, used by Microsoft Exchange, uses a maximum of 32K).

So, a single 5MB file needs a minimum of 78 round-trips (or 156 if using MAPI).

Even this assumes that TCP uses its highest window-size, however window-size is negotiated and adjusted between the devices based on response-time, TCP never gets to a 64KB window on long latency links.

## Isn't the speed of light so fast that this is all still only a theoretical problem?

OK, I admit, the speed of light in a vacuum is pretty fast – 299,792 Km/second or 186,282 miles/second. However, the speed of light in fiber or copper is around 70% of that in a vacuum<sup>o</sup>, roughly 210,000 Km/s.

So, to go back to our 5MB file that requires a minimum of 78 round-trips. Let's assume the server is in Boston, Massachusetts and the user is in London, a distance of 5279Km<sup>d</sup>. A single round-trip is double the distance: 10,558Km. 78 round-trips is therefore  $78 * 10,558$  or 823,524Km. Divide that distance by 210,000 and you have a minimum of 4 seconds to retrieve the file.

But this is all theoretical and assumes a direct link from the user to the server, no routing delays, no congestion and the optimal TCP window size.



## You can calculate it yourself – it's twice as bad as you think!

Most PCs have a utility called PING, this can be used to see the real round-trip time between devices across WAN links and the Internet. Before you start, make sure you are really testing to the destination you think you are, there are online utilities that will tell you where the server is hosted<sup>c</sup>.

In theory, our round-trip time between Boston and London could be as short as 50 milliseconds (10,558 divided by 210,000), however try it and you'll find it is always at least double. While writing this near London, I tested the round-trip to three websites hosted near Boston<sup>f</sup> (while most of the USA was asleep for minimum congestion) and received average round-trip times of 129 milliseconds. Now that 5MB will take a minimum of ten seconds to reach me, and this still assumes no server or firewall delays, congestion on the line, no slow-starts, maximum window-size and no additional packets to request the content and deliver approval from the server.

Let's remember, the round-trip between Boston and London is only 10,558 Km. The circumference of the earth is eight times that and the greater the distance, the worse the situation. Some examples using other round-trip times for the same 5MB file:

San Francisco – London	16 seconds
San Francisco – Sydney	23 seconds
Dallas – Beijing	21 seconds
Paris – New Delhi	12.5 seconds

**(Don't even think about using a satellite – geostationary satellites are based 35,000 Km above the earth introducing even greater delays).**

<sup>c</sup> [http://en.wikipedia.org/wiki/Speed\\_of\\_light](http://en.wikipedia.org/wiki/Speed_of_light)

<sup>d</sup> <http://www.indo.com/cgi-bin/dist/place1=@173964/place2=@67016>

<sup>e</sup> <http://www.parsec.it/whereis/index.php>

<sup>f</sup> <http://www.boston.com>, <http://www.fox25.com> and <http://www.umb.edu>

So, to show the real problem sometimes there's only one option. People based in HQ need to jump on an aeroplane and work in a remote office for a week, accessing all the same data that they do at HQ!

## What can be done?

In simple terms we need to reduce the number of round-trips that data needs to take to get from a server to a user. To go back to our analogy of moving house, we could:

- ✓ Through out some of our unwanted stuff – therefore reducing the number of trips.
- ✓ Optimize our delivery mechanism; hire a truck instead of using a car and get more items in one journey.
- ✓ Prioritize what gets sent first. Which is more important, the refrigerator or the curling tongs.

In the data world there are also a number of techniques that can work together to achieve faster data delivery.

## Object or file caching

Keep a copy of the object at the remote site, using object caching. When a user requests an object that has already been requested by another user, it can be delivered from the local cache (after checking with the server that the cached copy is still up to date). This reduces WAN bandwidth and latency to almost zero.

## Byte caching

When an object is not fully cached, techniques to recognize repeated patterns in the data can send tokens instead of the repeated data. This can send a few bytes instead of large amounts, thus increasing the apparent bandwidth and reducing the time to deliver the content.

## Protocol Optimization

Hide the inefficiencies of the protocols by sending large blocks of data before waiting for acknowledgements, fast-start those protocols that are slow to build up transmissions and even anticipate user requests for data (if a user requests the start of a file, these devices can anticipate that the user will request the rest of the file).

## Compression

Use compression technologies between the sites to reduce the bandwidth and round-trips needed.

## Bandwidth Management

To make sure the systems use the available bandwidth effectively, set priorities by user group, by server, by application etc.

## Remove inappropriate traffic

Let's not forget that business traffic is often competing with non-business traffic. Deploy devices that implement policies to block requests for inappropriate traffic.

# Conclusion

## Latency – the application killer

Bandwidth is not enough - distance is the real killer. Even with unlimited bandwidth, data still travels from server to user slowly due to the repeated trips taken before the full data arrives; we still have to wait. Organizations need to investigate solutions to solve this problem or applications will be unusable in remote offices.



# Improving Internet Security In

Cyberspace is an ever-expanding global digital network which speeds up many aspects of life. While new technologies allow for enormous gains in efficiency, productivity and communications, they also create new threats from those who have bad intentions towards us. Despite knowing the increase in the cyber threats, most CIOs and CSOs in many organisations do not even think about cyber incidents until after they have experienced of being attacked [1]. Most of the organisations feel relatively safe and they believe that perpetrators would not target them. Nowadays, there is no exception where most of cyber attacks are spread with the intent to damage everyone on the net. The recommended approach to manage cyber incidents within organisations is by setting up the Computer Security Incidents Response Team (CSIRT).



## What is a CSIRT?

CSIRT is an internal team within an organisation that is responsible for receiving, reviewing, and responding to computer security incidents and activities [2]. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, an educational organisation or a research network. Communication channels, data sharing agreements, and policies and procedures must be established before the internal CSIRT could operate effectively.

CSIRT provides support in responding to computer security incidents in an organisation. Since the incident handling is not a self-contained process, the CSIRT needs to have good relationship and communication with the business managers, representatives from various departments such as IT, legal, human resource and public relations. The relationship with these internal parties is crucial in order to deliver good operational process. This internal CSIRT also needs to establish relationship and create communication channels with external parties especially the CERT Coordination Center (CERT CC) or the national CERT. This relationship is important because alerts regarding the new threats always come from the national CERT.

In Malaysia, the Government has formed the Malaysian Cyber Security Centre (MCSC) to support the nation's cyber security initiatives covering both proactive and reactive measures. Through collaborations between private and public sector organisations, MCSC continuously identifies possible gaps that could be detrimental to national cyber security. MyCERT, a division under MCSC is a national CERT for Malaysia that provides incident response services. They have established a National Cyber Early Warning Centre that provides monitoring and detection of potential cyber threats in the country.

## The Importance of CSIRT

The number of intrusion reports grows each day and vary in different forms such as mailbombs, spams, forgeries, hack threats, viruses, denial of service (DoS) and intrusions.

Taking into account a case study on the Code Red virus alone revealed that the calculated global monetary losses caused by the virus runs into more than USD\$2.6 billion. Nimda, on the other hand, paralysed many organisations within an hour of its first public report on the 18 September 2001. At the end of the day, more than 100,000 computers were affected and tampered with [3].

The total incidents of cyber cases reported to MyCERT saw a significant rise from the year 2000 to 2005. There were only 347 cases reported in year 2000, but the number grew to 915 cases in year 2004 and 835 cases in year 2005.

The question is not whether "will I get hit?", but it is a matter of "WHEN will I get hit?" It must be noted that security prevention measures are not about eliminating threats, but rather on mitigating risks that are associated with it. Furthermore, incident handling measures will not prevent security breaches; however, it has the potential of minimising losses.

# Organisations



## Benefits of CSIRT

Why does organisation need a CSIRT? The direct benefit of establishing the CSIRT is the incident handling services to their organisation, which CSIRT could minimize and control the damage, provide effective response and recovery. CSIRT can be on site and able to conduct a rapid response to contain and recover from any computer security incidents.

CSIRT should be able to participate in information exchange either among department in the organisation or with other external CSIRTs. Their relationships with other CSIRTs can facilitate sharing of response strategies and cyber early alerts to potential problems.

Security Audit is another area where CSIRT could contribute their expertise to the organisation. CSIRT should be able to perform vulnerability assessments and incident detection and help identify vulnerable areas of the organisation.

The experience in handling incidents could benefit the organisation in a long run. The team may have wide experiences in handling security incidents and therefore is able to coordinate the recovery, mitigation and response strategies. By having these experiences, CSIRT could work to mitigate future events from happening.

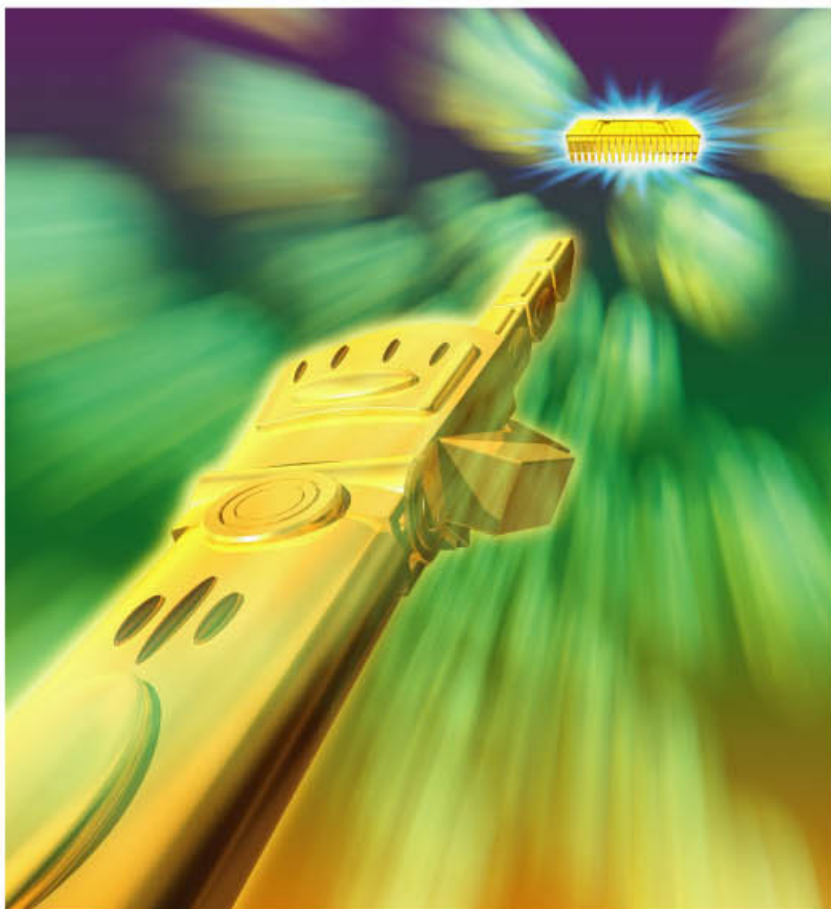
Providing capacity building to others would be one of the proactive works. These includes providing security awareness and education services, influencing policy makers, and coordinating workshops.

## Conclusion

The main goal of establishing CSIRT is to protect the crucial assets of the organisation. Using the experiences in handling incidents, they could work proactively to defend and protect the critical assets of organisations and the Internet community in general. The best way to protect the critical assets of the organisation is by having a dedicated team to look after security in the organisation.

## References

- [1] **Kaplan, S. 2003. When Bad Thing Happen to Good Companies.** (Online posting). 2 May 2006.  
 <<http://www.cyberincident.org>>
- [2] **Jaroszewski, P. 2003. Why do I need a CSIRT?**  
 9th TERENAs TF-CSIRT Meeting. 30 May.  
 (Online posting). 2 May 2006.  
 <<http://www.terena.nl/tech/task-forces/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf>>
- [3] **Lemos, R. 2001. Nimda winds down; companies recover.** (Online posting).  
 30 Jun 2006  
 <<http://news.com.com/2100-1001-273286.html>>
- [4] **MyCERT. 2006. MyCERT 2005 Annual Report.**  
 <<http://www.mycert.org.my>>



# Regulating Online Content: An Overview

*Published in New Straits Times, 30th April 2007*

One of the key points enunciated in the Malaysian Cyber Law is that there will be no censorship of the internet. This can be seen from Section 3 of the Communications and Multimedia Act 1998 where it says "Nothing in this Act shall be construed as permitting the censorship of the internet". However, this does not mean that the internet is above the law, and the users may use it by all means. It is, despite the freedoms it gives to the people, subject to the laws and regulations of the country. Certain areas are within the scope of the laws, especially when it is contrary to the local society's norms and acceptable practices.

One of the measures taken by the Malaysian government in regulating internet content is imposing the Internet Service Provider (ISP) and the telecommunications company to have optional filtering services for its users. This step however should not be construed as contravening the law, as it is definitely not censoring. It is only an option coming from the users to choose what they want to view.

The established traditional laws are always applicable to online content whenever the case permits. Such laws are designed to cater the subject matter, regardless where it is committed, whether online or in the real world. For instance, the Seditious Act 1948 and the Defamation Act 1957. The former Act provides punishment of sedition. The Act restricts any action which has seditious tendency, may it be words or publications. The Act empowers the authority to initiate a legal proceeding if the circumstance requires. Similarly, Defamation Act 1957 relates to the issue of libel, slander or malicious falsehood. It is humbly submitted that it can be used to regulate online defamatory content as well.

Although traditional laws may be used to regulate online content, it is advisable to look at our own cyber laws, merely because they were designed to handle the specific issues emerging from the internet. An example would be the Communications and Multimedia Act 1998 (CMA 1998). It is an Act to regulate the communications and multimedia industries in Malaysia.

When discussing about content, it is important to look at section 6 of the CMA 1998, where it states that content means any sound, text, still picture, moving picture, audio-visual or tactile representation, which can be manipulated, stored, retrieved or communicated. Further, in regulating online content, section 211(1) of the Act says:

**"No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person"**



By virtue of section 211(2) of the same Act, any person who contravenes the abovementioned section shall commit an offence and if convicted, shall be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both.

The Act further empowers a **Content Code** to be drafted to deal with offensive or indecent content. The Content Code will provide guidelines, standards and procedures of content by service providers through Self-Regulation. However, compliance to this code is voluntary.

According to the Content Code, a subscriber shall not provide a prohibited content online as this is contrary to the terms and conditions of the Internet Access Service Provider's (IASP's). In the event where a subscriber refused to follow the terms and conditions of the website by providing prohibited content as defined by the Code, the IASP has the right to withdraw or block the subscriber's access or even to remove the prohibited content. This must be done with the procedures laid down by the Code. It is encourage that the IASP should first ask the subscriber to remove the prohibited content by giving notice before terminating the subscriber's access account.



Similar situation in regulating online content may be seen in Australia and Singapore. In Australia, prohibited content shall be classified as such by a classification board. The development towards monitoring online content is also done by Self-Regulation, where the country develops her own Code of Conduct for Internet industries. In Singapore, An Internet Code of Practice has been produced to ensure that nothing is included in any broadcasting service which is against public interest or order, national harmony or which offends against good taste and decency. All Internet service providers together with Internet Content providers must ensure that prohibited material is not broadcast via the internet to users in Singapore.

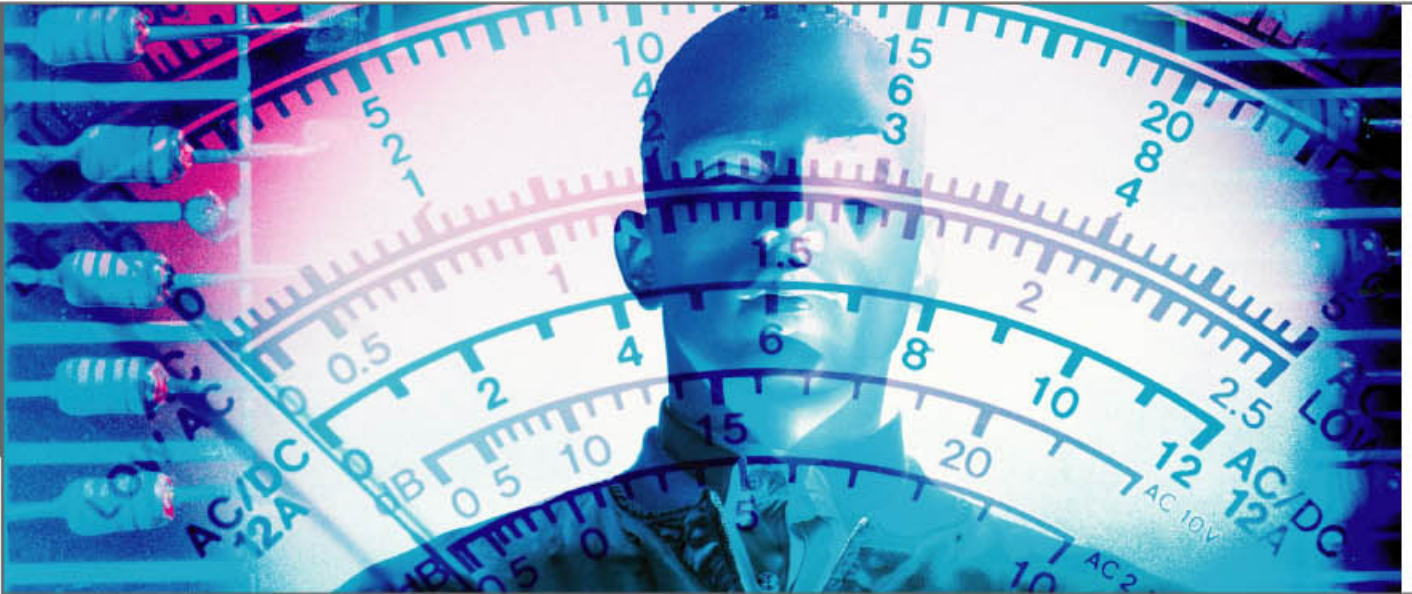
A rather strict approach may be observed in China where it implements access control for Internet Service Providers (ISP), Internet Content Provider (ICP), internet subscribers and cyber café's users. It has always been part of China's internet filtering system to supervise the internet. Under the State Council Order No 147, a regulation governing internet use was prepared. It is called the *Computer Information Network and Internet Security, Protection and Management Regulations*. Under the abovementioned regulation, Article 4 prohibits individual from using the internet to harm

internet security, disclosed state's secret, harm the interest of the state, or society or of a group or to take part in criminal activities.

One of the challenges in regulating online content relates to the borderless nature of the internet itself. The effect of legislation and regulations are territorial in nature. An act done outside the jurisdiction may not be controlled effectively. Among the ways to overcome this is to have collaboration at the international level so that regulating online content shall be more efficient. International regulations shall be able to cover the weaknesses of the territorial effects of national regulations.

**In conclusion, the foregoing paragraphs show that countries in the world have some measures on regulating internet content. Although what amounts to illegal or harmful content may differ from one country to another, the aim is to make the internet free from abuse by the irresponsible party. Regulating internet content may be one of the ways to deter the people from doing wrongful act in the cyber world, but the most important measure is to educate the society to use the internet wisely. The internet should be used for the greater good of the society, and not to be the platform to post illegal material or offensive to others.**





# THEFT IN THE DIGITAL WORLD:

Generally speaking, people have no concrete reason to commit crime. What they did was to satisfy their own desire. Perhaps the tendency to commit new crime supports the theory in criminological research on *homotypic continuity* or the continuity of similar behaviours over time. This theory focuses on the childhood misbehaviour and the adult outcome. It can be argued that criminals will continue to commit crime as the time goes by, showing why there is a progress on the issue of computer crimes. As always, the law is under pressure to cope with the growth of technology.

In the digital world, stealing information may be regarded as an offence. The online **Compact Oxford English Dictionary** defines information as facts or knowledge provided or learned or what is conveyed or represented by a particular sequence of symbols, impulses, etc. Information may be anything, whether personal, classified or even confidential. Information stolen can be used to impersonate other people, or simply using it for any gain.

According to section 378 of the Malaysian Penal Code, a person is said to commit theft if he intends to take dishonestly any movable property out of the possession of any person without the person's consent, moves that property in order to such taking. The challenge to this provision is whether theft committed in the digital world fits the definition of theft provided in the penal code.

The question that may come into picture is whether information stolen is considered as movable property. Apart from that, in the digital world, information may be copied, so there should be no question of 'moving' such information or 'taking' the information out of the possession of the owner.

At present, a well known type of theft of information is identity theft. Obtained through phishing, a method whereby fraudulent emails were sent to invite the public to a sham website requiring them to enter their personal particulars, especially financial information such as credit card details or banking account number. Information acquired from the victims may later be used to impersonate them.

Looking at this scenario, it seems like section 416 of the Penal Code may be applicable. A person is said to 'cheat by personation' if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is. However the applicability of this provision to the issue of online identity theft is yet to be tested in the court of law.

Although traditional law may be applicable whenever the situation permits, it is advisable to use cyber specific laws to cater cyber specific issues. With the aim to equip the country to face the new challenges in the cyber world, Malaysia has passed a number of cyber laws such as the Communications and Multimedia Act 1997, *Computer Crimes Act 1997*, *Digital Signature Act 1997*, *Telemedicine Act 1997*, the amendments to the *Copyright Act 1987* and the recent *Electronic Commerce Act 2006*.

# ARE WE 'LEGALLY' READY?

With regards to theft of information or phishing, a more appropriate legislation to handle this matter is the Computer Crimes Act 1997. Similar to the Computer Misuse Act in the UK, it is humbly submitted that the person who commits phishing may be prosecuted under Computer Crimes Act 1997. Section 3(1) one clearly spells the offence. According to section 3(1) of the Act:

- (1) A person shall be guilty of an offence if—
  - (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
  - (b) the access he intends to secure is unauthorized; and
  - (c) he knows at the time when he causes the computer to perform the function that is the case.

The whole act of phishing falls under section 3. This is because the phisher is using the computer to create a sham website, and using the computer to send an email, inviting the victim to provide their personal details. The phisher is intending to secure access to the victim's account for example and the access is absolutely unauthorized. According to *section 2(5) of the Act*, access of any kind by any person to any program or data held in a computer is unauthorized if:

- (a) he is not himself entitled to control access of the kind in question to the program or data; and
- (b) he does not have the consent or exceeds any right or consent to access by him of the kind in question to the program or data from any person who is so entitled.

Clearly the phisher is not entitled to control access of personal data of the victim, such as credit card details or passwords. Further, when he did an offence under section 3 with the intent to commit fraud, it is an offence under section 4 of the Act which provides:

- (1) A person shall be guilty of an offence under this section if he commits an offence referred to in section 3 with intent
  - (a) to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code.

**Axiomatically, technology will evolve and man will continue to commit crimes. The law will always be challenged to face new scenarios created by the online world. The law is required to be up-to-date and be able to cater the needs of the situation. Nevertheless, at the present moment, it is an important question to ask whether our laws are adequate to deal with online theft. After analyzing the provisions of the Act, it is argued that phishing is covered by the Computer Crimes Act 1997. Are we 'legally' ready? The answer would be in the affirmative.**

# Configuring your

## Home Network (Wi-Fi)

**Wireless routers are freeing more and more home users from trailing cables but are they also creating conditions suitable for hackers to jump in. Most people are delighted if they get their home wireless network up and running but this is not enough. Wi-Fi security threats are greater than for wired networks because the communications link cannot be made physically secure.**

An unsecured wireless network leaves the information on any PC connected to it open to theft. Not only that, but any connection from an unknown source can leave you vulnerable to any viruses that the unknown PC using your connection might have. For most people, however, the typical problem is surfers in range of their network who use up their Internet download limit and bandwidth for bit crunching downloads like films and other heavy media files. Without a secure encrypted signal, this can and does happen – especially in urban environments where the large volume of unsecured wireless networks offer a candy lane of choices for hackers and others keen to exploit bandwidth.



# network

## Plugging the gaps

Routers come with their own default security settings but since these are standard, the wiser policy is to configure your own – specifically these are the Service Set identification (SSID) or the name of your network and MAC address filtering to limit the number of users to the network.

The SSID is a unique identifier text string, up to 32-characters in length. It is attached to the header of data packets sent over a WLAN that acts as a password when a wireless device tries to connect to the WLAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.

MAC on the other hand is the acronym for Media Access Control address, a hardware address that uniquely identifies each node of a network. In 802.11 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sublayers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network medium. Accordingly, the MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it while the LLC layer controls frame synchronization, flow control and error checking.

Changing the SSID and enabling MAC address filtering via the router's web-based configuration utility and then matching those settings on any PC permitted to access the network provides a decent level of security. Even if a hacker should locate your SSID, if they are not on your MAC address list, access will be denied. If security is a bigger concern, typically for SMBs with confidential data and financial matters being handled on their wireless network, there is the possibility to enable either WPA or WEP encryption.

Despite the clear risks, many companies still fail to secure their Wi-Fi networks or encrypt data traffic. Hackers being typical opportunists will happily extract business critical data or use your WLAN for distributing illegal pornography – all activities with serious repercussions for a company's finances or reputation.

For most home wireless networks, however, the simple act of changing the basic default settings and setting up MAC address filtering is enough to stop your neighbor from accidentally or deliberately accessing your network or using your internet connection to download movies.

# An Introduction to the Malaysian Cybercrime Legislative Framework



## What is the legal definition of cybercrime?

There is no fixed definition of what may amount to cybercrime. The Oxford Reference Online defines cyber crime as crime committed over the Internet. The Encyclopaedia Britannica defines cyber crimes as any crime that is committed by means of special knowledge or expert use of computer technology. It also appears that the word 'cybercrime' is used interchangeably with the phrase 'computer crime'<sup>1</sup>.

The United Nations in its 'Manual on the prevention and Control of Computer-Related Crime'<sup>2</sup> has noted activities such as fraud by computer manipulation, computer forgery, damage to or modification of computer data or programs, unauthorised access to computer systems and services and unauthorised reproduction of legally protected computer programs, may amount to computer crime. The Australian Government have also identified other activities that may amount to cybercrime, which includes, offences against computer data and systems, computer related offences, content offences and copyright offences<sup>3</sup>.

In Malaysia, the **Computer Crimes Act 1997 ('CCA')** together with other legislation such as the **Communications and Multimedia Act 1998**, the **Digital Signature Act 1997** and the **Penal Code (Act 574)** provide for computer crime offences. The CCA was modelled after the **Computer Misuse Act 1990** of the United Kingdom and came into force on 1st June 2000.

us • trojan • adware  
-mail forgery • spo  
ojan • adware and  
us • trojan • adware  
-mail forgery • spo  
ojan • adware and  
us • trojan • adware  
-mail forgery • spo  
ojan • adware and  
us • trojan • adware  
-mail forgery • spo  
ojan • adware and

# Incidents that may amount to cybercrime

Cybercrime may occur in different ways. Viruses, worms and trojans are some of the more historically popular computer programmes that are used to commit crimes by using computers. The following is a non-exhaustive list of incidents which may amount to be a cybercrime in Malaysia:



**virus**



**trojan**



**adware and spyware**



**cookies**



**worms**



**mailbombs**



**e-mail forgery and**



**spoofing**

It should be noted that cybercrime is not limited to remote attacks on computers. It also very much includes gaining unauthorised access to computers and the data stored on them by physical means, e.g. by gaining unauthorised access to a computer and copying information from that computer's hard drive onto a floppy disk or a zip drive without authorisation.

It should be noted that cybercrime is not limited to remote attacks on computers. It also very much includes gaining unauthorised access to computers and the data stored on them by physical means, e.g. by gaining unauthorised access to a computer and copying information from that computer's hard drive onto a floppy disk or a zip drive without authorisation.

<sup>1</sup>Ibid and The State of the Law on Cyberjurisdiction and Cybercrime on the Internet by Gabriele Zeviar-Geese, California Pacific School of Law

<sup>2</sup>Both the above definition are quoted by NISER in (Is cyber crime reigning on a no man's land?)

<sup>3</sup>Cybercrime definitions, Australian Government, Australian Institute of criminology, <http://www.aic.gov.au/topics/cybercrime/definitions.html>



## The Malaysian Computer Crimes Act 1997

The CCA provides for the different offences that may be committed with a computer. The offences are:

- i) accessing computer material without authorisation;
- ii) accessing a computer without authorisation with the intent to commit or facilitate the commission of further offences;
- iii) modifying contents of any computer without authorisation;
- iv) wrongfully communicating a number, code, password or other means of access to a computer or person whom one is not duly authorised to communicate to; and
- v) abetting in a computer crime.

### ➤ (i) Accessing computer material without authorisation

This offence is provided for by **S.3 of the CCA**. A person may be guilty of such an offence if the person knowingly and without authorisation causes a computer to perform any function to secure access to any program or data held in any computer. The person need not intend to direct these acts to any particular program or data.

If found to be guilty of such an offence, the person may be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both.

For example a person that uses viruses, trojans and spyware to gain access to computers or programs of other people may have committed an offence as provided by **S.3 of the CCA** above. The hackers, when using such malicious programs, are gaining access to computers or programs that may belong to others, without authorisation from the owners of the computers or programs.

### ➤ (ii) Accessing a computer without authorisation with the intent to commit or facilitate the commission of further offences

This offence is provided for by **S.4 of the CCA**. A person may be guilty of such an offence if in the event a person commits an offence under **S.3 of the CCA** with the intent to either commit or facilitate the commission of such offence whether by himself or other person, involving fraud or dishonesty, thereby causing harm to any person, in body, mind, reputation or property. The further offences may not have to be committed at the same time as the offence for unauthorised access.

If found to be guilty of such an offence, the person may be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

A person may be liable for an offence as provided by this section if the person uses a virus, trojan, worm or spyware to commit fraud over the Internet. As such, these malicious programs are used to facilitate the commission of another offence that may either involve fraud or dishonesty.

### ➤ (iii) Modifying contents of any computer without authorisation

This offence is provided for by **S.5 of the CCA**. A person may be guilty of such an offence if in the event a person does an act that he knows will cause unauthorised modification of the contents of any computer. The person need not direct his act at any program or data. The unauthorised modification may be permanent or temporary.

If found to be guilty of such an offence, the person may be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both. However, a person may be liable for a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both if in the event such unauthorised modification is done with the intention to cause any harm to any person, in body, mind, reputation or unto the person's property.

A person may be liable for an offence as provided by this section if the person infects other computers with malicious programs that modifies the contents of the infected computer without the consent of the owner of the said computer. Such malicious programs may be viruses, spyware or worms which alter or modify the working mechanisms of the infected computers.

### ➤ (iv) Wrongfully communicating a number, code, password or other means of access to an unauthorised computer or unauthorised person

This offence is provided for by **S.6 of the CCA**. A person may be guilty of such an offence if in the event a person communicates a number, a code, a password or other means of access to a computer to any person not authorised to receive such information.

If found to be guilty of such an offence, the person may be liable to a fine not exceeding twenty five thousand ringgit or to imprisonment for a term not exceeding three years or to both.

A person may be liable for an offence as provided by this section if, for example, he is an employee of a web-based e-mail company and he forwards customers' passwords to rogues intending to steal information from the e-mail company's customers.

### ➤ (v) Abetting a computer crime

This is provided for by **S.7 of the CCA**. A person may be guilty of an offence if in the event a person abets another person in the commission of any offence within the **CCA**.

If found to be guilty of abetting the commission of an offence, the person may be liable to the sentence as provided for in the specific section that provides for the relevant offence.

Following that, a person who does any act in preparation of or in furtherance to the commission of any offence within the **CCA** may also be guilty of that offence within the **CCA**.

## Other matters provided by the CCA

The CCA also provides for other matters such as:

- presumption;
- the territorial scope of the CCA;
- the scope of the power of the police in relation to search, seizure and arrest within the ambit of the CCA; and
- obstructing a search exercise by the police.

### → Presumption

The CCA also provides the presumption that any person who has in his custody or control any program, data or other information held in a computer or retrieved from any computer which he is not authorised to have in his custody or control shall be deemed to have obtained unauthorised access to such program, data or information unless the contrary is proved. Therefore, any person who is caught in possession of a computer with information that he is not authorised to have, may be guilty of offences under Sections 3 and 4 of the CCA.

### → The territorial scope of the CCA

S.9 of the CCA provides Malaysia with jurisdiction over any offence as stated in the said act if in the event the affected computer, data or program was in Malaysia or is capable of being connected to or sent to or used with a computer in Malaysia at the time of the commission of the offences. The scope of this section is wide. Theoretically, perpetrators of cybercrime from outside of Malaysia may also be subjected to the provisions of the CCA. Offences committed by them will be dealt with as if the offence was committed in Malaysia. Therefore, in the event a foreigner was to unleash a virus on Malaysian computer systems, he may be guilty of committing an offence within the CCA. This is notwithstanding that he was not physically in Malaysia when he committed the relevant offence.

### → The power of the police in relation to search, seizure and arrest within the ambit of the CCA

S.10 of the CCA provides that a police officer above the rank of Inspector with a warrant, the power to enter, search, seize and detain any evidence such as computer peripherals, diskettes or other related materials that are of assistance to the suspected offence that is being investigated. Such police officer may also have the power to enter, search and seize without a warrant if in the event he has reasonable grounds for believing that the delay caused by waiting for the issuance of a warrant may frustrate the object of the search and seizure exercise. The said section also provides that such police officer may arrest any suspected perpetrator without any warrant.

### → Obstructing a search exercise by the police

S.11 of the CCA provides that a person may also be guilty of an offence if in the event he assaults, obstructs, hinders or delays any police officer from entering into any premises in the execution of their duties under the CCA. If in the event a person is guilty of such an offence, he may be liable to a fine not exceeding twenty five thousand ringgit or to imprisonment for a term not exceeding three years or to both.



## Other statutes applicable in computer crimes

Cybercrime is regulated in Malaysia by other acts in tandem with the **CCA**. These acts are the **Communication and Multimedia Act 1998 ('CMA')**, the **Digital Signature Act 1997 ('DSA')** and the **Penal Code (Act 574) of Malaysia ('PC')**. The following are some examples of the different types of crime against or via the use of computers that are governed by different legislation:

- **S.415 PC** – This relates to the offence of cheating and is relevant in the context of cybercrime for example where a person uses a stolen credit card to purchase goods online.
- **S.471 PC** – This relates to the offence of using as genuine a forged document. This section may be used in tandem with **S.4 of the CCA** in relation to incidences wherein a person hacks into an online merchant's website by using a trojan to obtain credit card particulars. These particulars are then used to manufacture forged credit cards. Such cards are then used by the person to purchase goods.
- **S.234 CMA** – This relates to the interception and disclosure of communication wherein a person who is caught conducting a wire-tap upon any part of the telecommunications infrastructure of Malaysia may be liable under this section.
- **S.72 DSA** – A person that manages to hack into the system of a repository thereby having access to confidential details of persons or companies using digital signatures may be liable under this section if in the event the person discloses any such information to another person or publishes it in a website.

## Powers of the authorities

The scope of the power of search and seizure of the relevant authorities in relation to the different computer crimes are dependent upon the respective statutes that provide for the specific offences. For example, if in the event a search is required to be conducted in relation to an offence within the **CMA**, the **CMA** provides for the scope and the power of enforcement of the authorities. The **CMA** provides that a police officer not below the rank of an inspector, an officer of the Malaysian Communications and Multimedia Commission ("MCMC") or a public officer authorised by the Minister of Energy, Water and Communications of Malaysia ("the Minister").

The **DSA** too has certain sections dedicated to the scope and power of the authorities when conducting search and seizure exercises. The **DSA** empowers the Minister to authorise any public officer to exercise the powers of enforcement under this Act. Following that, any police officer not below the rank of Inspector may exercise the powers of enforcement conferred by this Act.

As in relation to offences within the PC, the scope and the powers of the enforcement officers are governed by the **Criminal Procedure Code (F.M.S. Cap.6) ('CPC')**. Any police officer of any rank may conduct a search within the **CPC**, unless a search is to be conducted to locate an object that may be concealed upon the person (for example, to search for a microchip). In such an instance, a body search may only be conducted upon persons found within the premises of the search location in the presence of a magistrate, a Justice of Peace or a police officer not below the rank of Inspector.



## Computer Forensics

During the search, authorised officers are to collect information and evidence so as to produce the same during the prosecution of the perpetrators. There are certain guidelines that the authorised officers may adhere to in the collection and preservation of the evidence.

For example, during the search exercise, photographs will be taken of the crime scene. The suspect's computer will not be switched off in the usual way. The power plug is to be removed from the computer so as not to lose any information during the process of switching off the computer. The crime scene will also be dusted for fingerprints. When dusting for fingerprints, the authorised officer must be careful as to not polarise storage devices as the fingerprint powder is magnetic in nature. This may cause the data stored in the storage device to be irretrievable.

Evidence must be collected from the scene of crime to be stored in a special place by the authorised officers. When collecting such evidence, the authorised officers must be careful when packing and transporting the same. Generally, evidence are packed into labelled bags that will be sealed and labelled. A checklist of all evidence collected and details of the handling and management of the evidence after the collection exercise should be kept to avoid any questioning of the authenticity of the evidence.

## Conclusion

The **CCA** and other statutes such as the **DSA**, **CMA** and **PC** have provided a framework to deal with the basic cybercrime offences as addressed above. It is recommended that security or risk management systems take into account the requirements of the **CCA** and the other stated acts so as to be effective in:

- i) the providing assistance to the authorised officers in the collection of forensic evidence; and
- ii) the management of risk from any cyber crime;

The **CCA**, including the other abovementioned acts are tools to be used in curbing the occurrence of computer crime. However, these tools will be more effective if used in tandem with other tools such as good security systems and risk management systems. It is suggested that given the rate of advancement in today's technologies, a synergy of such tools may be more effective as compared to the use of only one of the mentioned tools in protecting oneself from being a victim of any cybercrime.



# Data theft

One of the main usages of IT system is to keep and maintain important data. The data can be anything from personal information, financial records and also Intellectual Property (IP). These data could also vary considerably from each individual organization depending on the type of service or business they provide.

In the case of financial sectors such as banking, the data stored in their IT systems is primarily on client's personal information including savings or loans. R&D companies might practice keeping confidential IP within the system. Whereas Universities might store data containing IP, examination questions and results.

Due to the significance and magnitude of such information, the information itself becomes the prime target for data theft. There could also be a general motivation for individuals to have access to it in order to copy or alter such information for their intended purpose.

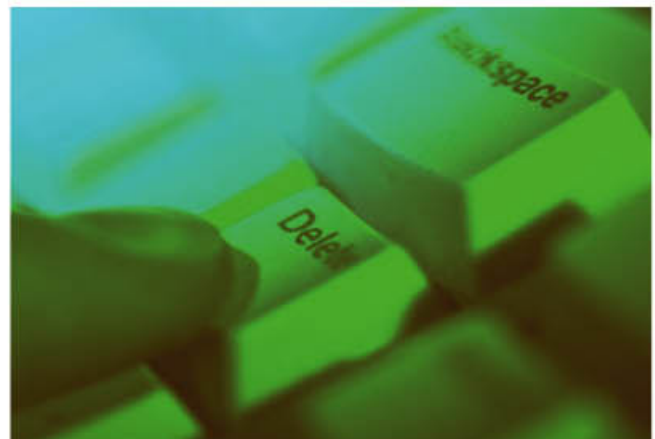
Nevertheless, with the emergence of sophisticated network security equipments for network perimeter defense such as Intrusion Detection System (IDS) or firewall, invasion from external network has become more complicated. Thus, intrusion cases from external parties are usually lower compared to internal breach.

Generally, data theft cases within the organization, is carried out by individuals (typically disgruntled employees, contractor or ex-employee) who are well aware of the company's network access.

With strict policies lacking in some companies, data theft becomes easier and in some cases goes unnoticed. The policy should state that whenever an employee has been given full authority (especially system administrator) to access important and confidential data, a monitoring mechanism must be engaged. The monitoring system can then be audited for any violation.

Data theft could also occur from lost, stolen or used laptops. Anyone having access to such may be able to retrieve confidential data and profit thereof. It is quite alarming that incidences such as this have gone unreported for the fear of repercussion towards the individuals.

Information/statistics on data theft from IT system is still very low. Not much information is currently available on the net.



# Top Ten Predic



As the drivers for cyber crime increase, there is a lack of inhibitors to counter the escalating threats. While escalating the use of technology, attackers are becoming more innovative in their development of lucrative business models. Now, more than ever, it is likely that these attackers – who were once satisfied with a paltry USD\$100 here and USD\$1,000 there – are gunning for the big boys. And in 2007, it is almost certain that they will pull out the stops in trying to get it.

In an interview with Richard Stiennon, network security industry expert and Fortinet chief marketing officer, 2007 could very well be the year that attackers get smart about attacking enterprise data caches in a fashion that could double their cyber crime revenue – moving their market to between USD\$4 billion and USD\$8 billion. Cyber extortion attempts, however, will no longer be limited to financial institutions or enterprises, and even local governments, schools and manufacturers could find themselves trying to protect against normally business-focused attacks.

**That said here is  
Stiennon's complete  
Top Ten Threat Prediction  
list for 2007:**



# tions for 2007

## ➤ 100 Percent Growth in Revenue for Cyber Crime:

The cyber crime industry will increase its focus on enterprise data stores and drive up its profitability. Stiennon's prediction is that the cyber crime industry revenue will come in between USD\$4 billion and USD\$6 billion next year, doubling their current overall take.

## ➤ More Attacks Against Wireless Networks:

Attackers will continue their pursuit of victims through text messaging, "vishing" and malware that infects Symbian phones and spreads via Bluetooth or MMS.

## ➤ DDoS in Support of Phishing Attacks

The cyber crime industry will increase its focus on enterprise data stores and drive up its profitability. Stiennon's prediction is that the cyber crime industry revenue will come in between USD\$4 billion and USD\$6 billion next year, doubling their current overall take.

## ➤ MySpace Grows Up and Gets Secure:

In 2007, the number of attacks from predators, criminals and hackers will get to the point that MySpace will be forced to tighten up its controls and monitoring. Unfortunately for MySpace, this will make it less appealing to its young adult audience.

## ➤ Successful DDoS Attacks Against Financial Services Firms:

Although DDoS attacks are already in progress, 2007 will be the year that attackers attempt more high-profile targets.

## ➤ YouTube Abuse:

Like network news, email and IM before it, the new video sharing trend will succumb to spammers who post ads, ad-backed videos and stealth marketing exploits

## ➤ "Threat of the Year" – Attacks Against DNS:

Whereas DNS servers are a part of the critical infrastructure of the Internet, they are also an easy attack target for DDoS DNS servers are exposed by their nature and, because they control where a browser is pointed, they could become the primary target for attackers that want to take down a web site.

## ➤ Network Infrastructure Shows Signs of Overloading:

The backbone providers have been resting on the excess bandwidth in which they invested during the dotcom bubble. Now that voice and video are really here, the infrastructure is showing signs of weakness. This could manifest itself in outages, slowdowns and a mad scramble to lay more fiber in 2007.

## ➤ Identity Theft Continues to Rise:

Markets are developing that could make it easier to monetize stolen identities thus increasing the value of stolen IDs while decreasing the cost of "moving" them.

## ➤ Spread of Windows Vista will have Zero Impact on the Overall Threatscape:

It may be several years before Vista represents more than 50 percent of all machines, and by then attackers will have likely matured and refined their tools. Zero-day exploits for Vista are already available for purchase on the Web

# Home Wireless: Co

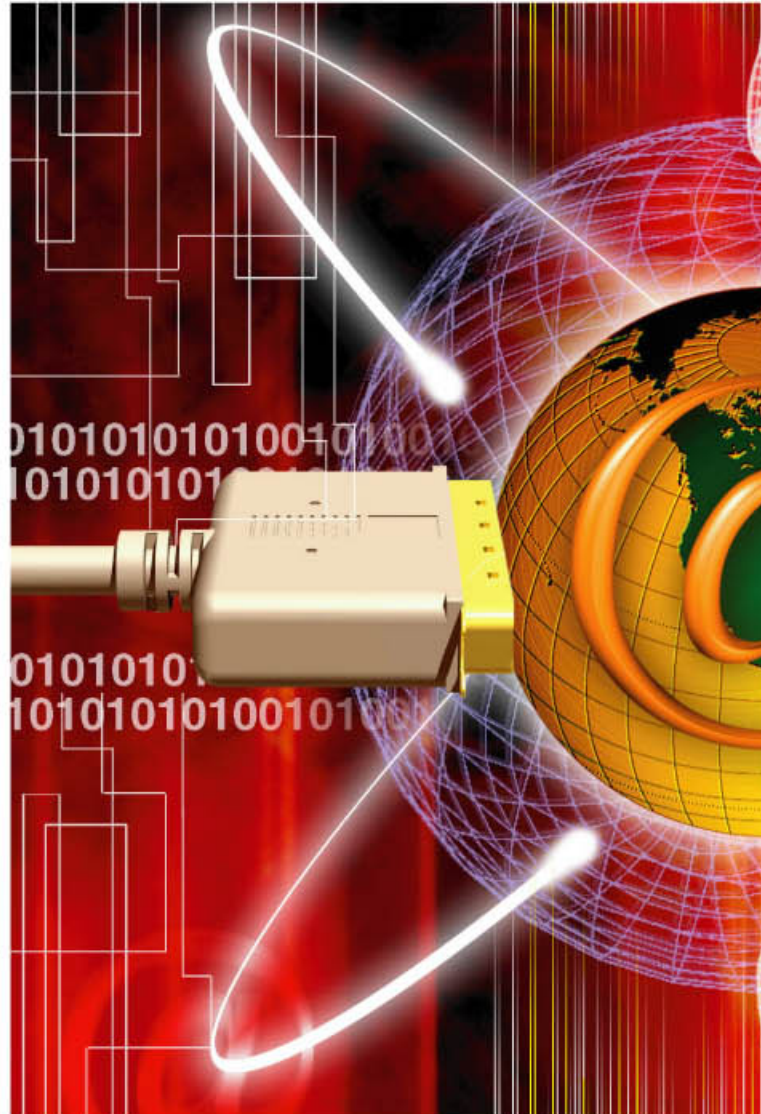
## Introduction

Wireless network enables you to connect to Internet from everywhere and anywhere. Going wireless from home usually requires an Internet connection into your house which then connects to a wireless router. This router converts signal through the air into wireless broadcast so that any computers equipped with wireless client card and within the network's coverage can easily receive it for Internet browsing.

The major problem of a home wireless network is that, any person with a wireless-equipped computer and in the network's range can use the same network. This means that, nearby hackers or even your neighbours could tap into your network unknown by you. If an unauthorised person uses your network to commit a cyberspace crime, it can be traced back to you.

Most home users have little consideration for securing their home wireless network simply because they find it too troublesome. From ITFacts.biz website, 38 percent of home users leave their connections completely open, without having any protection program in their computer at all. This is a sad fact as quite a number are still unaware of the importance of wireless security.

The trend for home wireless, meanwhile, is growing. According to BBC News, The Pew Internet and American Life Project survey indicates that the number of internet users with wireless at home nearly doubled, from 1 in 10 in January 2005 to 1 in 5 by December 2006. Wireless users are known to spend more time on Internet. The same survey shows 72 percent of wireless users check their e-mails daily as compared to 54 percent of internet users who check e-mails 'on the typical day'. The more time spend on Internet brings bigger risk as more time and attempts for hackers into your network.



## How to Strengthen Your Home Wireless Security

As it is very important to take basic precautions to a home wireless network, below are the simple points to strengthen its security:

### Protect your personal computer (PC) from external attacks

- Install and use anti-virus and firewall program. Ensure to always run these programs every time your PC is on. Update anti-virus program constantly with the latest patches and updates.
- Always update the operating system with the latest service pack provided by your operating system vendor.
- Disable remote access and file sharing on your PC.
- Create strong passwords for all important documents.
- Be careful when retrieving e-mails or downloading programs from the Internet. Verify its source to confirm it is from somebody or a site that you trust.
- Ensure to set your browser to the highest level of security notification and monitoring.

# Connect Confidently



## Immediately change the default password

- Change default 'Administrator' password (and username) provided by your router's manufacturer. Usually these are used to modify the router's configuration settings.
- Create strong password that only you know. A strong password must be a combination of various characters, signs, numbers, and lowercase and uppercase letters.
- Memorise your password and do not keep it in the computer.
- Do not disclose your password to anyone else especially close acquaintances.

## Use encryption

- All wireless equipments support some form of encryption. The popular ones are WPA (Wi-fi Protected Access) and WEP (Wired Equivalent Privacy). You need the encryption to prevent an unauthorised person from eavesdropping your transactions. Another version WPA2 is also available on newer wireless equipments.
- Ensure encryption setting is on because the default setting is usually off.

## Change the default SSID (Service Set Identifier/Network Name)

- Never use the default SSID for wireless router given by the manufacturer. SSID is used to identify your home network name. The default SSID normally is a standard, simple pre-defined name assigned for same hardware models.
- Create SSID that contains various characters, signs and numbers.
- Do not include your name or personal information as part of SSID.
- Change SSID frequently.

## Turn-off SSID broadcasting

- Disable SSID broadcasting mechanism. SSID broadcasting, which can be found in most wireless router, is responsible to send out SSID to any device in the vicinity. This feature is useful at public places, but for home environment, there is no need to announce this information because you already know it is there.

## Allow specific computers to access your wireless network

- Enable MAC (Media Access Control) address filtering. Set up an access control list by MAC addresses of every system you want to associate with wireless router. MAC address is unique and able to identify specific network adapters. Having access list stops an unidentified wireless device to use your network unknowingly.
- Set DHCP (Dynamic Host Configuration Protocol) to exact number of computers that you have. For example, if you have 3 computers, set it to 101-103.

## Strategically put wireless router in your house

- Place the wireless router in the centre of your home instead of near window. This is due to wireless signals which normally can reach across the streets and through your neighbour's house. If it is located near windows, stronger signal will be received outside your home making it easier for nearby unwelcome hackers.

## Turn off wireless network when you are not using it

- Turn off the wireless network when you are not using it or when you leave your house empty for an extended period of time. Wireless router does not suffer from power cycle wear-and-tear so rest assured that no damage is done when you turn it off frequently.

## Enable firewall on computers and routers

- Ensure to turn on the built-in firewall setting, which can be found on newer router.
- Read the manuals to configure either outgoing or incoming traffic, or both as needed by your specific requirement.
- Install and run personal firewall in every single computer that connects to the router.

## Reference

### [1] 4 steps to set up your home wireless network

Published: April 4, 2005



By Tony Northrup

(<http://www.microsoft.com/athome/moredone/wirelesssetup.mspix>)

### [2] WPA Wireless Security for Home Networks

Published: July 28, 2003



By Barb Bowman, Windows XP Expert Zone Community Columnist

[http://www.microsoft.com/windowsxp/using/networking/expert/bowman\\_03july28.mspix](http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.mspix)

### [3] Wireless users 'do more online'



<http://news.bbc.co.uk/1/hi/technology/6396665.stm>

### [4] Configuring Wireless Security for small network



[http://www.ezlan.net/Wireless\\_Security.html](http://www.ezlan.net/Wireless_Security.html)

### [5] Wireless Networking Basic Security Checklist Home User version



by Frank Thornton

[www.personalwireless.org/tools/docs/WLAN\\_Sec\\_Home.pdf](http://www.personalwireless.org/tools/docs/WLAN_Sec_Home.pdf)

## Conclusion

Overall, there is no denying the fact that we are all going wireless, at some point. We yearn for convenience and to be able to surf the Internet without long and messy cables. Nevertheless, we need to adhere to mentioned guidelines and procedures in order to connect confidently from home. Individually, we are responsible to guard our physical home from hacker or thief intrusion.



# Integrated Threat Management –

## Protect Your Organization From The Inside Out

***An effective strategy can improve operational efficiencies, increase business continuity and reduce security management costs***

Minimizing risk is tougher than ever. For security-focused IT managers in Asia Pacific the number and severity of threats continues to grow, with malware and spyware at the fore-front. Business continuity is an ever escalating challenge and core-concept for the region's increasingly 24/7 globally oriented business environment. To both manage the risks and meet ever tightening budgets, savvy IT managers in the region are realizing the benefits and value of integrated security management solutions. This article offers thoughts on the security needs and key innovations and trends impacting the evolution of threat management solutions in Asia Pacific.

### Complexity of Threats

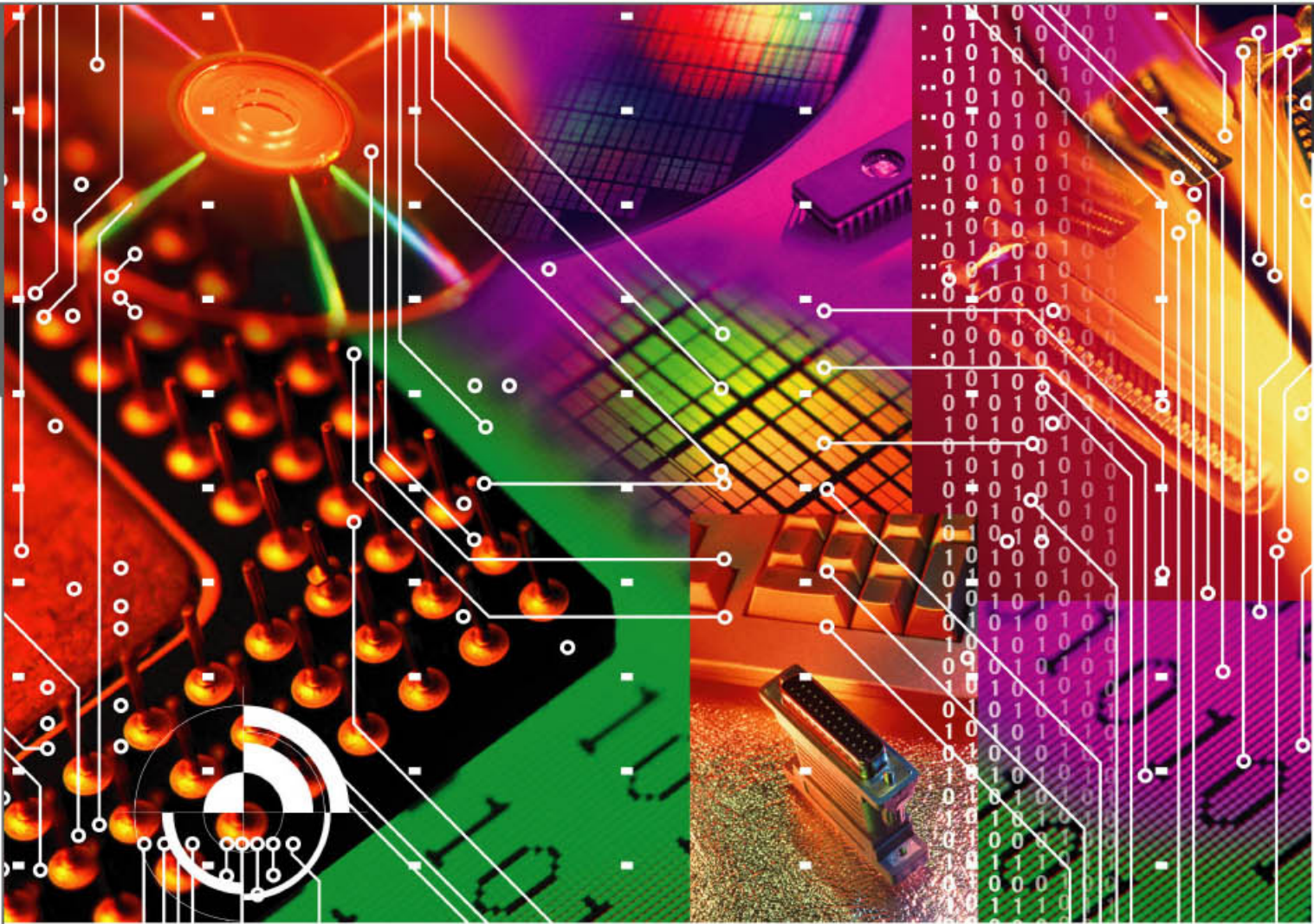
Today's corporation is at risk on all sides from a range of threats all varying in their nature and virulence. The pace of change is hard to keep up with, and new, more innovative, more destructive, and more undetectable threats are emerging on an almost daily basis. Pessimism pervades this fight, which for some is more of a grapple, mopping up after the damage is done. And the damage can be severe, going beyond the occasional irritating pop-up to the loss of revenue or reputation.

For enterprises in Asia-Pacific, virus attacks account for over three-quarters of security incidents<sup>1</sup>. However, particularly damaging for firms is the rising frequency of Denial of Service (DoS) attacks in Asia Pacific. The level and nature of this risk is unique to each organization, but in the worst cases, the temporary termination of vital processes can damage both a corporation's reputation and their bottom line. A recent report suggested DoS attacks can cause six times more financial damage than a virus<sup>1</sup>.

Anti-spyware solutions were the most purchased security tools in 2005, according to a recent Forrester report, with 80% of companies investing in such technology<sup>2</sup>. Spyware subverts a computer's operation for the benefits of a third party, with the scope of threat ranging from reduced productivity to identity and intellectual property theft. Spyware is quickly moving from being a mere hindrance to having the ability to seriously impact business performance and security. Network congestion due to increased

traffic is a threat to productivity, but particularly sinister is the potential for Malware to relay confidential information to an outside party, enabled for example, by key-logging and file-scanning. Such surveillance can impact all network spaces and can monitor email communications as well as web activity. Consequences could lead to data corruption and the theft of sensitive or confidential information, with severe financial costs, damaging lawsuits and a blemished reputation to boot.

The vague boundary between the legal and criminal installation of Spyware further complicates matters. Often bundled in with free download programs, users commonly consent to download such software, unaware of their actions due to the ambiguous wording contained in the End-User-Agreements, terms which many accept without even a glance. Educating and alerting internal users on security management issues is thus a vital step in combating Spyware, and indeed any other threats, from viruses and worms, to phishing and pharming activities.



## Knowledge is Power

Awareness is the very foundation of effective security management, and administration must be streamlined to enable organizations to respond quickly to an outbreak. To this end, centralized, policy-based management capabilities are essential.

Disparities in awareness and implementation of IT security solutions abound. Large enterprises place more importance on the protection of their IT environments than small-to-medium sized business' (SMBs), reflecting the determining influence of compliance requirements on IT security decisions. Currently, 27% of SMBs and 16% of enterprises do not use an anti-spyware product for example<sup>2</sup>.

Once an organization is attuned to its weaknesses and aware of its susceptibilities, it can then devise a strategy with confidence. Indeed, CIO and PricewaterhouseCoopers' recent annual report on the global state of information security highlighted the importance of strategy to tackling uncertainty<sup>4</sup>.

<sup>1</sup>CSI-Asia (2004) Cybercrime & Security Survey Report 2004

<sup>2</sup>Forrester (10/02/2005) Antispyware Adoption In 2005; IT Security Adoption And Trends

<sup>3</sup>IDC (May 2005) Asia / Pacific (excluding Japan) Security Software 2005-2009 Forecast; Market Analysis Report

## An Integrated Approach


As IT security architectures across Asia Pacific grow in complexity, there will be an increased need to manage and integrate multiple layers of security. Indeed, IDC forecast the region's security software market to reach US\$1.58 billion in 2009, representing an annual growth rate of 20.1%<sup>3</sup>. The days of point solutions, operating in isolation on a single vulnerability, are limited, mainly due to the difficulties and costs that hinder any attempt at effective central management.

The interconnected, over-lapping nature of threats to IT security requires a single management console for multiplatform enterprise environments. This is driving a major market consolidation; with stand-alone solutions becoming more and more embedded in integrated solution suites.

# 13 SECURITY TIPS TO SAFE INTERNET BANKING

1. Keep your password/PIN code safe and memorize them. Ensure you change them regularly (recommended every 3 months). If you conduct Internet transactions in a number of websites, use different passwords for each website. Create unique passwords that are difficult to guess, e.g. use a combination of letters and numbers.
2. How do you know the website is secured?
  - Look for https:// in the URL and not http:// when you login
  - Look at the status bar of the security icon (locked padlock) when you visit the bank site. Double click on the padlock and ensure that it has a valid digital certificate.

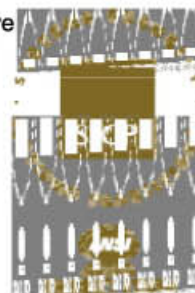
WEB BROWSER	SECURED	NOT SECURED
Microsoft Windows Platform		
Internet Explorer		
Netscape Navigator		
Firefox		

WEB BROWSER	SECURED	NOT SECURED
Apple MAC Platform		
Apple Safari		
Firefox		

3. Log out immediately after completing your Internet transaction. Then, clear the browser cache, cookies and history (refer to your bank's website for online guidance). Ensure that you log out properly after every Internet banking session and not just close the browser.
4. Never leave your computer unattended when you are conducting your Internet transactions.
5. If you are unsure of the security of the computer, do not use it for Internet transactions.
6. Use an anti-virus, anti-spyware and personal firewall and keep it updated. Some of this software are freely available on the Internet.
7. Ensure that your PC and browser are updated with the latest patches/fixes. Use the Automated Update feature of your Operating System (e.g. **Windows Update** for Windows users).
8. Do not be influenced by appealing offers, especially from unknown parties. Do not click on any links attached in your emails. Do not copy and paste any website address (URL). Retype the website address to surf or use your **Bookmark**.
9. Do not respond to emails asking for personal information, login information or on changing password notification. Report to your bank or CyberSecurity Malaysia.
10. If you decide to go to other websites linked via your Internet banking website, read the privacy and policy information of that website first before conducting any Internet transactions.
11. Always check your account balance/statement to ensure that no unauthorized withdrawal has taken place.
12. When visiting your Internet banking site, always check that the Date and Time, matches the date and time when you last signed in.
13. If your bank account has been compromised, act fast and inform the bank, or contact CyberSecurity Malaysia (<http://www.cybersecurity.org.my> or <http://www.mycert.org.my>)

# SSCP®: Systems Security Certified Practitioner

(ISC)²® Systems Security Certified Practitioner (SSCP®) credential offers an independent, vendor-neutral, and objective measure for information security tacticians to demonstrate their level of competence in the seven (ISC)² SSCP CBK® domains, the compendium of best practices for practitioner. The SSCP introduces and establishes the core concepts and understanding required for designing, developing and maintaining secure networks, applications and business processes. The SSCP credential requires candidates to:



- Possess one year of direct full time security work experience in one or more of the 7 SSCP CBK domains
- Subscribe to the (ISC)² Code of Ethics
- Pass the 3-hour, 125 multiple choice SSCP examination
- Complete the endorsement process
- Pay an annual maintenance fee
- Acquire 60 Continuing Professional Education (CPE) credits every 3 years
- Practitioners with inadequate work experience may achieve (ISC)² Associate for SSCP by passing the same SSCP examination. An associate has a maximum of 2 years to obtain the required experience and to submit the required endorsement form for certification as a SSCP.

FREE Candidate Information Bulletin is available at [www.isc2.org/studyguide](http://www.isc2.org/studyguide).

For FAQ on (ISC)² certifications, education services, examination information and registration, please visit [www.isc2.org/faq](http://www.isc2.org/faq) or email [isc2asia@isc2.org](mailto:isc2asia@isc2.org)

## (ISC)²® SSCP® CBK® REVIEW SEMINAR

The SSCP® CBK® Review Seminar is a three day program overviews the entire (ISC)² SSCP CBK. Attendees will benefit greatly from a broad, comprehensive and yet practical understanding of the important role that security plays in all of today's business processes. Attendees will learn how to integrate security principles into all projects, business processes and recovery and monitoring activities. This seminar will enable attendees with the ability to provide a skillful and effective level of support and leadership in their work environment as well as assist the attendees in study for the SSCP examination.

### Course Outline:

The SSCP CBK Review Seminar covers the CBK® as defined by (ISC)². The SSCP CBK is divided into seven domains, or topic areas as listed below:

- **Access Controls** – Concepts, Terms of Subjects and Objects, Implementation of Authentication Techniques
- **Analysis and Monitoring** – Principles, Practices, Mechanisms, Audits, Systems Maintenance, Analysis of Exploits
- **Cryptography** – Business and Security Requirements for Cryptography, Principles of Certificates and Key Management, Secure Protocols
- **Malicious Code** – Differentiate between Viruses, Trojan Horse, and Worms; Identification of Virus Activity; Differentiate between Trap Doors and Back Doors; Implication of Virus Hoaxes and Myths
- **Networks and Telecommunications** – Business & Security Requirements; Remote Access Architecture; Firewalls, Networks; Wireless
- **Risk, Response, and Recovery** – Risk Management Process; Security Assessments; Incident Handling Analysis; Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP)
- **Security Operations and Administration** – Change Management Concepts; System Development Life Cycle (SDLC); Security Evaluation and Assistance; Awareness Education; Code of Ethics; Security Infrastructure Evaluation; Security Policy Administration; Concepts of Certification and Accreditation Process; Implementation, Recommendation and Promotion of Security Best Practices

### Who Should Attend:

The SSCP® credential and the SSCP CBK® Review Seminar are ideal for those working toward or who have already attained positions as Senior Network Security Engineers, Network and System Administrators, Computer Systems Programmers and Analysts, Program Managers, Information Systems Auditors, Computer Operations Staff and Management, Database Administrators, Information Security Staff and Management, Business Analysts, and Help Desk Personnel.

### Pre-Requisites:

To attend the SSCP® CBK® Review Seminar the attendee does not need to have the pre-requisite experience for the examination. It is encouraged that all people working in the field of IT and Information Security attend the SSCP seminar to give them a thorough understanding of Information Security even if they do not intend to sit for the examination.

## Contact our education affiliate near you...

### Malaysia:

CyberSecurity Malaysia  
(formerly known as NISER)  
(P) +603.8992.6888  
(F) +603.8945.3205  
(E) [sscp@cybersecurity.org.my](mailto:sscp@cybersecurity.org.my)

Seminar Dates: **13-15 August, 2007**  
Registration Fee: RM2280 plus local tax where applicable  
Examination Dates: **8 Sept & 8 Dec, 2007**  
Exam Registration Fee: USD469 or USD369 for early registration  
16 days prior to the exam

30/F Bank of China Tower, 1 Garden Road, Central, Hong Kong.  
Tel: +852.8226.7798 Fax: +852.8226.7723 Email: [isc2asia@isc2.org](mailto:isc2asia@isc2.org) Website: [www.isc2.org/sscp](http://www.isc2.org/sscp)