CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 34 - (1/2013)

The Need For Certification & Its Benefits

Transaksi e-dagang – Adakah Ia Selamat

Ensuring A Safer Regional Cyber Environment

"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems. "

Bruce Schneier, Secrets and Lies

ISSN 1985-1995

Your **cyber safety** is our **concern**

Securing Our Cyberspace

CyberSecurity Malaysia, an agency under Malaysia's Ministry of Science, Technology and Innovation was set up to be the national cyber security specialist centre. Its role is to achieve a safe and secure cyberspace environment by reducing the vulnerability of ICT systems and networks while nurturing a culture of cyber security. Feel secure in cyberspace with **CyberSecurity Malaysia.**

www.cybersecurity.my

Cyber999 Help Centre | Professional Development (Training & Certification) | Product Evaluation & Certification (MyCC) | Information Security Management System Audit and Certification (CSM27001) | Malaysia Trustmark | Security Assurance | Digital Forensic & Data Recovery | Malaysia Computer Emergency Response Team (MyCERT) | Security Management & Best Practices | Cyber Security Research | Cyber Security Awareness For Everyone (CyberSAFE)

CyberSecurity MALAYSIA

CyberSecurity Malaysia
(726630-U)

Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

T: +603 8992 6888
F: +603 8992 6841
E: info@cybersecurity.my

Customer Service Hotline:
1 300 88 2999
www.cybersecurity.my

People First, Performance Now

An agency under

MOSTI
Ministry of Science, Technology and Innovation

MSC MALAYSIA Status Company

A MESSAGE FROM CEO OF CYBERSECURITY MALAYSIA

Technology is an enabler and we are encouraging everyone to use it. At the same time, technology also introduces new risk and users need to know the risk associated with it, especially the internet. Criminals are also using technology to enable them to extend their reach to the whole connected world. Even security organisation like RSA, VeriSign, Lockheed Martin, NSA, FBI, and CIA were not spared.

This year rising trend in cyber incidents continues as the first half of 2013 has recorded, on average, nearly 100 more incident per month as compared to 832 incidents per month in 2012. Content related incident for the first six month has more than doubled and Spam recorded 16% higher from the whole of last year's total. Cyber Harassments, Malicious Codes, and Frauds in the first six month of 2013 are already more that 60% (77.7%, 68.5%, and 62% respectively) of last year total incident.

We have to equip ourselves with knowledge to enable us to protect ourselves better. Even for none techies, they should at least be aware of the current cyber threats like Spam, Love Scams, Parcel Scams, Identity Theft, and Cyber Stalking to name a few. Then there are the international standards like ISO 27001 that organisation can adopt into their operations in a structured manner to protect their investment.

With the connected world, information or news travels very fast and not all information are true. All of us need to do our due diligence and verify the information especially before we shared it with our online friends.

This eSecurity Bulletin enables us to share, highlight, and discuss concepts, approaches, trends and best practises in the field of cyber security and we hope you benefit from it.

See you at our Cyber Security Malaysia – Awards, Conference and Exhibition (CSM-ACE) 2013 in November.

Thank you and warmest regards,

Dr. Amirudin Abdul Wahab
Chief Executive Officer, CyberSecurity Malaysia

EDITOR'S DESK

Greetings to all!

It is with great pleasure that we bring you the eSecurity Bulletin 2013. As you are aware there are tons of information on the internet and sometime we are not sure about the accuracy or the integrity of these information, especially pictures which could fool our eyes. Well in this digital age the cliché of "seeing is believing" is not true anymore as our Digital Forensic expert share with us about image forensics techniques that would benefit you especially the "UFO in Putrajaya..." article.

Also in this issue the Bring-Your-Own-Device (BYOB) article which is currently a much discussed topic as it brings along it own sets of operational and legal issues.

And I take this opportunity to convey a big 'Thank You' to all the articles contributors for sharing their knowledge.

Be Smart! Be Safe!

Best regards,

Rosly Yahil, Editor

TABLE OF CONTENTS

READER ENQUIRY
Security Managment and Best Practices, CyberSecurity Malaysia, Ministry of Science, Technology and Innovation (MOSTI) • E-mail: smbp@cybersecurity.my

PUBLISHED AND DESIGNED BY
CyberSecurity Malaysia (726630-U)
Block A, Level 8, Mines Waterfront Business Park, No 3,
Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan.

MyCERT 2nd Quarter 2013 Summary Report

6 August 2013

Introduction

The MyCERT Quarterly Summary Report provides an overview of activities carried out by the Malaysian Computer Emergency Response Team (hereinafter referred to as MyCERT), a department within CyberSecurity Malaysia. These activities are related to computer security incidents and trends based on security incidents handled by MyCERT. The summary highlights statistics of incidents according to categories handled by MyCERT in Q2 2013, security advisories and other activities carried out by MyCERT personnel. The statistics provided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussions of the incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian constituency. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q2 2013

Incidents were reported to MyCERT by various parties within the constituency as well as from foreign, which include home users, private sectors, government sectors, security teams from abroad, foreign CERTs, Special Interest Groups including MyCERT.s proactive monitoring on several cyber incidents.

From April to June 2013, MyCERT, via its Cyber999 service, handled a total of 3093 incidents representing 23.77 percent increase compared to Q1 2013. In Q2 2013, incidents such as Fraud, Content Related, Malicious Codes, Intrusion, DOS and Cyber Harassment had increased while other incidents had decreased moderately.

Figure 1 illustrates the incidents received in Q2 2013 classified according to the type of incidents handled by MyCERT and its comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Quarter		Percentage
	Q1 2013	Q2 2013	
Content Related	16	26	62.5
Cyber Harassment	100	133	33
DoS	2	8	300
Fraud	1116	1374	23.12
Intrusion	862	864	0.23
Intrusion Attempts	16	8	50
Malicious Codes	49	393	72.04
Spam	331	283	14.50
Vulnerability Reports	7	4	42.86

Figure 1: *Comparison of Incidents between Q1 2013 and Q2 2013*

Figure 2 illustrates incidents received in Q2 2013 classified according to the type of incidents handled by MyCERT.

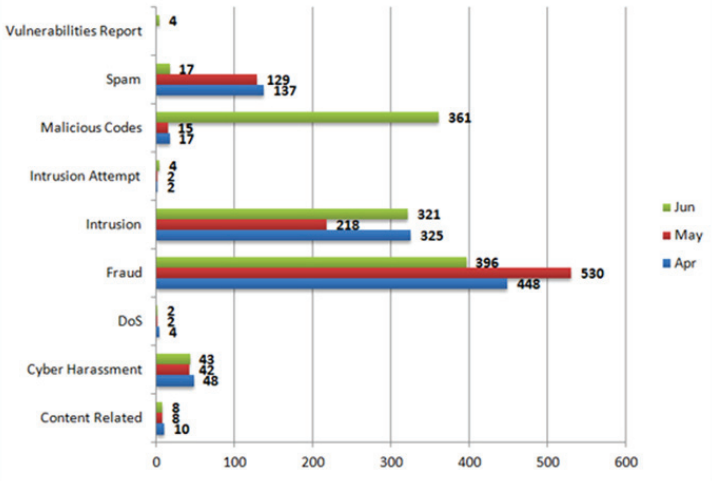


Figure 2: *Breakdown of Incidents by Clas sification in Q2 2013*

Figure 3 : Shows the percentage of incidents handled according to categories in Q2 2013.

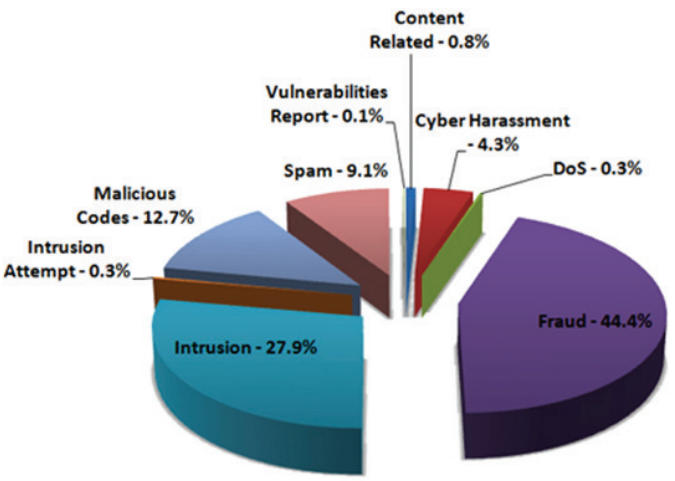


Figure 3: *Percentage of Incidents in Q2 2013*

In Q1 2013, a total of 864 incidents were received on Intrusion representing a 0.23 percent decrease compared to previous quarter. As was in the previous quarters, web defacements or web vandalism is still continuous. Based on our findings, majority of the web defacements were due to vulnerable web applications or unpatched servers involving web servers running on IIS and Apache. Majority of the defacements were using SQL Injection and Cross site scripting methods.

In this quarter, we received a total of 707 .MY domains defaced belonging to various sectors such as private, educational, government sectors compared to 750 .MY defaced domains in Q1 2013. MyCERT had responded to web defacement incidents by notifying respective Web Administrators to rectify the defaced websites by following our recommendations and the defaced websites were managed to be rectified accordingly by the respective Administrators.

Figure 4 shows the breakdown of domains defaced in Q2 2013.

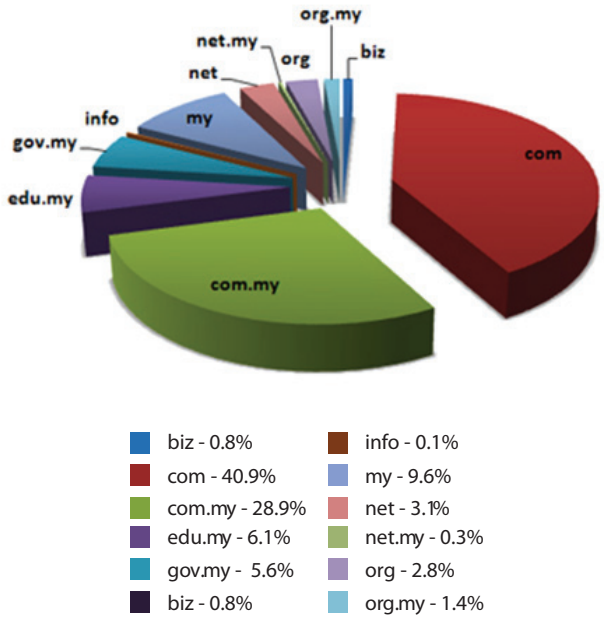


Figure 4: *Percentage of Web Defacement by Domain in Q2 2013*

Account compromise incidents still prevails in this quarter as was in previous quarter. The same trend we observed in Q2 2013 as was in Q1 2013 in which perpetrators are taking advantage of various techniques to compromise accounts belonging to other Internet users. Majority of account compromise incidents involved free web based emails and social networking accounts such as Facebook. Account compromise incidents could be prevented if users practice good password management such as using strong passwords and safeguard their passwords.

Users may refer to the below URL on good password management practise:
http://www.auscert.org.au/render.html?it=2260
http://www.us-cert.gov/cas/tips/ST04-002.html

A total of 1374 Fraud incidents were received in this quarter, from

organizations and home users. Some of the fraud incidents that usually users report to us are phishing, job scams, fraud purchase and Nigerian scam. Phishing incidents involving foreign and local brands continues to increase in this quarter along with other types of frauds. A total of 720 phishing websites targeted local brands and 1085 phishing websites targeted foreign brands were handled by MyCERT in this quarter.
Incidents on job scams, Nigerian scams, fraud purchase continues to increase as was in previous quarter. We advise Internet users to be precautious and always adhere to best practices when they purchase goods online. They must make sure they are dealing with trusted parties and never simply transfer money to seller without prior checking on the status of the seller.

Some of the tips users can follow are as in the below links:

- http://msisac.cisecurity.org/newsletters/2011-11.cfm
- http://www.actionfraud.police.uk/fraud-az-online-shopping-fraud

Cyber harassment incidents had increased in this quarter with a total of 133 incidents representing 33% increase. Harassment incidents generally involved cyber stalking, cyber bullying and threatening. Social networking sites such as Facebook, emails and chat programs such as Yahoo Messenger, Skype have become popular avenues for cyber harassment as they are becoming popular communicating channels on the net. We advise users to be very precautious with whom they communicate on the net especially with unknown people and be ethical on the net.

In this quarter, we observed a trend in cyber harassment that targets Malaysian, male victims. The Modus Operandi is the perpetrator, posing as a young, beautiful, single Japanese or Filipino female requesting to be friend with potential victim over the social networking site namely Facebook. After being friends with potential victims for some time, the perpetrator will invite the victim to video chat with her on skype. During video chat, perpetrator will lure victims and will take videos of victims in unpleasant position and situation using video cam. Victims will not realize that their video had been recorded and perpetrator will start to threaten victim to pay certain amount of money otherwise the video will be posted on the net such as on YouTube or on Facebook.

We advise Internet users to be very carfeul with whom they be friends with on the net as there maybe irresponsible users on the net with malicious purpose to threaten other Internet users into giving money to them. If victims are threaten by somebody, we advise them to lodge a police report immediately at a nearby police station together with evident to support the police report.

In Q2 2013, MyCERT had handled 393 incidents on malicious codes, which represents more than 100 percent increase compared to previous quarter. Some of the malicious code incidents we handled are active botnet controller, hosting of malware or malware configuration files on compromised machines and malware infections to computers.

In this quarter, we also received reports from Security Feeds regarding the Nitol Botnet activities involving many IP addresses originating from our constituency. MyCERT had analysed the activities and notified the respective ISP for further investigation and to clean up the infected machines.

More information on Nitol Botnet is available at:

- http://blogs.mcafee.com/mcafee-labs/digging-into-the-nitol-ddos-botnet
- http://www.csoonline.com/article/716188/microsoft-downs-botnet-that-infiltrated-chinese-pc-supply-chain

Advisories and Alerts

In Q2 2013, MyCERT had issued a total of 5 advisories and alerts for its constituency which involved Critical Vulnerability in Microsoft Internet Explorer 8, Oracle Java SE Critical Patch Update, Critical Vulnerability in Adobe ColdFusion, Multiple updates from Oracle for Java SE, Microsoft Security Bulletin Summary, alert on Redirection of Several .COM. MY and .MY Domains to Defacement Page. The Alert and Advisory comes with descriptions, recommendations and references.

Readers can visit the following URL on advisories and alerts released by MyCERT

- http://www.mycert.org.my/en/services/advisories/mycert/2013/main/index.html

Other Activities

IIn Q2 2013, MyCERT personnel had conducted several talks, presentations and trainings in local and in overseas for example in April 2013, MyCERT personnel had conducted a presentation during the FIRST Technical Colloquim held in Amsterdam, Netherlands. The presentation was on In-house Developed Tools to Enhance Incident Response - Sharing MyCERT's Experience.

Besides International presentation, MyCERT staff had also conducted several talks onSecurity Awareness, Cyber Trends, Social Media Security in various corporate organizations and Government Agencies.

Besides the talks/presentations, MyCERT personnel had also conducted several Incident Handling Training for System Administrators from corporate and Government organizations in this quarter.

Conclusion

In conclusion, overall the number of computer security incidents reported to us in this quarter had increased by 23.77% compared to the previous quarter. Spam, Vulnerabilities report and Intrusion attempts had decreased in this quarter however majority of categories of incidents had increased. No severe incidents were reported to us in this quarter and we did not observe any crisis or outbreak in our constituencies. Nevertheless, users and organizations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from these threats.

Internet users and organizations may contact MyCERT for assistance at the below contact:

Malaysia Computer Emergency Response Team (MyCERT)

E-Mail: cyber999@cybersecurity.my
Cyber999 Hotline: 1 300 88 2999
Fax: (603) 8945 3442
24x7 Mobile: 019-266 5850
SMS: Type CYBER999 report <email> <report> & SMS to 15888
http://www.mycert.org.my/

Online Version: http://www.mycert.org.my/en/services/advisories/mycert/2013/main/detail/931/index.html■

The Council for Security Cooperation in the Asia Pacific (CSCAP) Study Group on Cyber Security - Ensuring a Safer Regional Cyber Environment

By | Lt Col Sazali Sukardi (Retired)

It is beyond doubt that enterprise and government users must be part of the solution while pursuing two objectives of cybersecurity policy-making - preserving the openness of the Internet as a platform for innovation and new sources of growth.

Background

The Council for Security Cooperation in the Asia Pacific (CSCAP) membership includes almost all the major countries in the Asia Pacific. It has 21 full members (Australia, Brunei, Cambodia, Canada, China, Europe, India, Indonesia, Japan, DPR Korea, Korea, Malaysia, Mongolia, New Zealand, Papua New Guinea, Philippines, Russia, Singapore, Thailand, United States of America and Vietnam) and one associate member (Pacific Islands Forum Secretariat). CSCAP is a non-governmental (second track) process for dialogue on security issues in the Asia Pacific that provides an informal mechanism for scholars, officials and other professionals in their private capacities to discuss political and security issues and challenges facing the region. It also provides policy recommendations to various inter-governmental bodies, convenes regional and international meetings and establishes linkages with institutions and organisations in other parts of the world to exchange information, insights and experiences in the area of regional political-security cooperation.

CSCAP Study Group on Cyber Security

On June 2nd, 2010, the CSCAP Steering Committee approved the establishment of the CSCAP Study Group (CSCAP SG) Co-Chaired by CSCAP Australia, CSCAP India, CSCAP Malaysia and CSCAP Singapore. The CSCAP Study Group is to examine the various cyber security issues and challenges that are relevant to the Asia Pacific region, and their likely security risks. Based on these findings, CSCAP Study Group proposed an effective strategy to accommodate cyber security challenges in the region. The CSCAP Study Group has convened two meetings to carry out the study:

- First Meeting on 21st – 23rd March 2011 in Kuala Lumpur, Malaysia; and
- Second Meeting on 10th – 12th October 2011 in Bengaluru, India.

The First Meeting of CSCAP Study Group

The first meeting of CSCAP Study Group on Cyber Security was convened on 21st – 23rd March 2011 in Putrajaya, Malaysia. The meeting was attended by 20 delegates from 12 member committees (Australia, Brunei, Cambodia, China, India, Japan, Malaysia, Mongolia, New Zealand, Singapore, South Korea, USA, and Vietnam), and a non-member from Chinese Taipei. The meeting was aimed at providing an avenue for the delegates to share their ideas about various cyber security issues and challenges that are relevant to the Asia Pacific region, and potential security risks. The meeting discussed the various issues and challenges facing the Asia Pacific Region that covered the following areas:

- Cyber Security Issues and Challenges In The Asia Pacific
- Cyber Security Partnerships: the Roles and Responsibilities of the Government, the

Private Sector, and Civil Society
- Legal Policy and Framework: Territorial and Universal Jurisdictional Challenges in Cyber Security; and
- Multinational Cyber Security Cooperation: Possible Cooperative Measures in the Asia Pacific Region

Based on the discussions, the Study Group has identified several major considerations as follows:

- **ICT in the Asia Pacific Region**
  The rapid development of ICT in the Asia Pacific region has resulted in enhanced prosperity amongst regional nations. Cyber security that ensures a secure, trusted and resilient ICT domain is a critical factor in underwriting that prosperity.

- **Nations' Roles and Responsibilities**
  The first priority for each regional nation is to implement an effective domestic cyber security strategy and policies, and to extend all possible support to other nations in their legitimate search for cyber security cooperation.

- **Regional Cooperation – The Requirement**
  Concurrent with the development of national strategies and policies, it is vital that regional nations cooperate in establishing effective collective measures to ensure that cyber security across the whole region meets their mutual interests.

- **Regional Cooperation – What Can Be Done?**
  Regional nations are to identify areas of mutual concern that will enable collective cooperation, the setting and measuring of goals and actions within those areas, and related priorities.

- **Terms and Definitions**
  Regional nations should not define terms because of problems of reaching a collective agreement, and instead work on the basis of a general understanding of the meaning of the terms currently used.

- **Legal Approaches**
  The possibility of a cyber security treaty amongst regional nations should be considered using a soft law approach to address illegal activities that can be expanded over time. This treaty route can help in removing legal hurdles in cooperation among nations in the Asia Pacific region.

- **Non-Legal Approaches**
  There is a vital need to adopt non-legal approaches as an immediate cyber security strategy. Regional cooperation may need to establish initially on a bilateral or multinational basis amongst a limited group of regional nations but with the opportunity for others to join at a later date. The activities include Cyber Security Awareness and Education, Sharing of Information and Experience, Technical Assistance, Capacity Building, Regional Cyber Crisis Management and Coordination through Asia Pacific Computer Emergency Response Teams (APCERTs), and references to other similar studies i.e. by APEC, ITU, EU, OECD, etc.

The CSCAP Study Group agreed to proceed with development of the Draft Memorandum to be submitted to the CSCAP Steering Committee and the ASEAN Regional Forum (ARF) for further consideration. The Draft Memorandum was discussed deliberately in the second meeting.

The Second Meeting of CSCAP Study Group

The **second meeting** was convened on 10th – 12th October 2011 in Bengaluru, India. The meeting was attended by 15 delegates from 10 member committees (Australia, Brunei, China, India, Japan, Malaysia, New Zealand, Russia, Singapore and Vietnam), and a non-member from Chinese Taipei. This meeting was to deliberate the Draft Memorandum by the CSCAP Study Group that should lead to amenable proposals that have a potential to be accepted at the ARF Steering Committee. The Draft Memorandum will then be taken forward to the respective governments.

The first part of the meeting discussed the proposed structure of the Draft Memorandum, whereas the second part of the meeting

deliberated other similar studies conducted by other regional and global organisations. There are fifteen distinct study considerations which are grouped into Significance of Cyber Security, Cyber Security as a Domestic Security Issue, and Cyber Security as a Regional Security Issue. The meeting also had focused sessions on the other regional arrangements which are to be reflected in the Draft Memorandum. These arrangements are namely Study of Shanghai Cooperation Organisation, Council of European Convention on Cyber Crime, and UN Global Cyber Security Agenda.

The Study Group also acknowledged the existence of hostile activities and aggression conducted by nation states, state-sponsored and non-state actors. The Study Group recommended these issues could be the subject for separate considerations and CSCAP should elaborate these issues further within an appropriate format. Based on the discussions, the recommendations of the CSCAP Study Group are grouped under National Responsibility and Regional Cooperation.

The Draft Memorandum recommends that a nation state to have in place a domestic cyber security strategy. The national role towards cyber security in the context of ARF regional cooperation was stated as responsibility of an ARF member country in ensuring cyber security, and its contributions to an ecosystem for cyber security in the Asia Pacific region. The members of the study group added the national responsibility element that reflects on three dimensions namely Cyber Security as a National Responsibility, Enabling Legal Frameworks to Enhance Cyber Security, and Ensuring Participation in Multilateral Cooperation. The Draft Memorandum delves on a need in establishing a Computer Emergency Response Team (CERT), and the memorandum was amended with these suggestions.

The deliberations and outcome of the discussion on regional cooperation was summarised as follows:

- Cyber Security Awareness and Education;
- Sharing of Information and Experience;
- Capacity Building and Technical Assistance;
- Development and Expansion of Asia Pacific Computer Emergency Response Team (APCERT);
- Legal Approach and inclusion of Harmonization of Laws; and
- Creation of a Regional Cyber Security Action Task Force (CSATF) to develop recommended standards, mechanisms, and policies to assist in the harmonization of laws.

The Draft CSCAP Memorandum to ARF

An effective regional cyber security strategy is an essential requirement for ensuring that all ARF nations are able to operate within and benefit from the advantages of a secure, resilient and trusted electronic operating environment. The CSCAP Memorandum is intended to recommend to ARF those measures required to implement such a strategy. The report by CSCAP Study Group serves as the basis for the preparation of CSCAP Memorandum and it is to be submitted as a separate document to ARF Steering Committee for further consideration

Conclusion

The CSCAP Study Group on Cyber Security has successfully brought together cyber security experts from all over the Asia Pacific region, in order to share, elaborate and debate various regional and global cyber security issues and challenges, and their potential security risks. The study has achieved its objectives in identifying these issues and challenges as well as in recommending effective cyber security recommendations for Asia Pacific Region. The report is also intended to serve as the basis for regional nations to further explore cyber security collaborative efforts and to identify suitable cooperative programmes towards protecting our common interests in cyber security. It is the view of the CSCAP Study Group that the report should be further translated into appropriate actions to ensure its continuity.■

The Story in Your Eyes – The Experiment

By | Nazri Ahmad Zamani, Mohamad Firham Efendy Md. Senan

Introduction

Nowadays, technology improves the quality of photography. With variety of devices available in the market, thousands of photos can be captured in extremely high quality.

There is an interesting article written by Mr Hany Farid from Dartmouth College, New Hampshire, United States. He wrote about forensics on a photo based on the reflection of the eyes. From the photo, we can see lights reflecting from the eyes, and such lights contained information that can be extracted. However, reading is not enough. Some sort of experiment is needed to clear our doubts.

Therefore, we conducted a simple experiment to prove whether the stated claim is true. Thus, armed with a Nikon D3100 DSLR, Adobe Photoshop and a Super-Resolution coding (which we wrote from the library provided by the EPFL) we started our own Myth Buster Test. Finally yet importantly, Nazri managed to get his supportive eight-year old son to be the model for our experiment. We laid out four simple steps that we adhered strictly.

The Experiment

Step 1: Snap a picture

The setup was simple: Nazri asked his son to sit on a sofa right under the living room's fluorescent lights while Nazri snapped his smiley face.

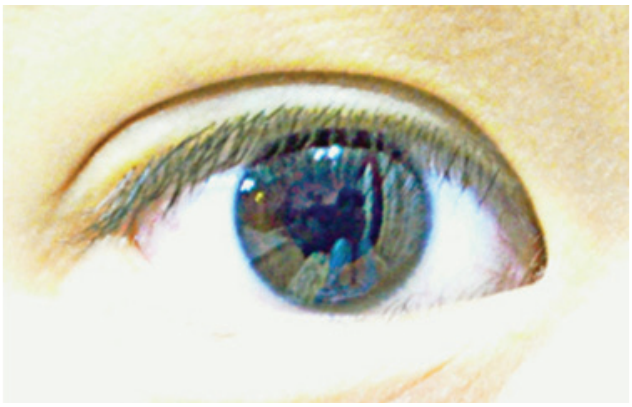
Step 2: Enhance the photo

The next step is setting up the photo for the analysis. The image is sized about 4608×3072 resolution. It is truly a concern if we try to enlarge the whole image to get a better zoom on the pupil as it will consume a lot of computing time and memory. Therefore, it is better to just crop out the right eye and use it for the analysis.

Here the size of the image is about 1240×920 resolution.

By using Adobe Photoshop, we enhanced the brightness of the image, hue and saturation in order to enhance the clarity of the reflection on the subject's right eye.

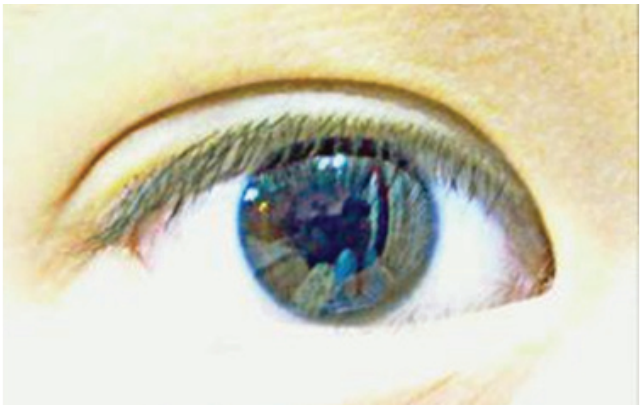
Here you can observe that several objects were clearly mirrored on the eye.



Step 3: Super-Resolution

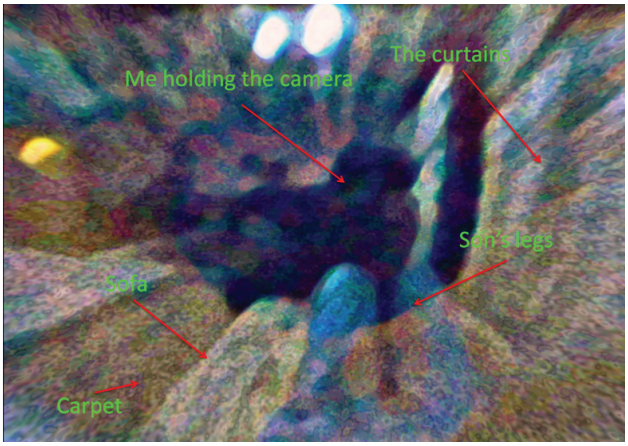
We loaded up the image to the Super-Resolution coding that we have previously written. We set the zoom level at x3; with Vanderwall selection for estimating the rotation/shift and Robust Super-Resolution for the interpolation. The original code of the EPFL can only call TIFF images as to take advantage of the SamplePerPixel information from the image metadata for the SR algorithm (a structure-preserving algorithm for computing the spectrum of Hamiltonian matrices).

As we were using a JPEG format image, we had to make small changes in the coding to override the SamplePerPixel's call. The result was a good quality enlarged image at 3720×2760 resolution. As you can see from the image below, the quality is very much similar to the previous photo. From this point on, we will only use the pupil to get the reflection information.



Step 4: Second round of enhancement

This is the final step – we cropped out the pupil and conducted the lens distortion correction. After that, we enhanced the image with another round of hue/saturation, brightness correction and de-blurring. Voila! The result are as follows:



Please note that this work was carried out using a DSLR image. Therefore, this is a very good quality source to begin with. We did not expect that it would work on lower quality sources such as webcams or surveillance cameras. However, this is a brilliant idea indeed! Thanks to FourAndSix for sharing their thoughts on this matter. ■

References:

1. *Ecole Polytechnique Fédérale de Lausanne. "Super-Resolution" http://lcav.epfl.ch/software/superresolution*
2. *Hany Farid. "The Story In Your Eyes" http://www.fourandsix.com/blog/2012/6/4/the-story-in-your-eyes.html*

UFO in Putrajaya...Really?

By | Nazri Ahmad Zamani, MohdZaharudin Ahmad Darus

There is every reason to think there are actually more things in the sky these days to be concerned about.

What's the Story?

A recent picture of a UFO taken in Putrajaya has caught the attention of Malaysia's local blogs and UFO enthusiasts. The photo was taken by an individual who claimed that he napped that photo of the UFO while he was in Putrajaya using his Samsung smart phone.

The following are pictures that were retrieved from emails together with other images on the same event. These emails were circulated among peers and then from there the photos were distributed to the public at large. The photos even managed to get the attention of a few independent news websites.

Could there really be a UFO in Putrajaya?

In debunking the UFO myth, we have conducted a few analysis on the retrieved photos. We will explain to you how the analysis was conducted, and at the end of this paper, we will summarise our findings on the authenticity of the said UFO sighting. algorithm and is closely modelled after that algorithm. When a message of any length less than 264 bits act as input, the SHA produces a 160-bit output (message digest). Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message.

Let's Conduct A Few Analysis

The analyses were divided into three parts:

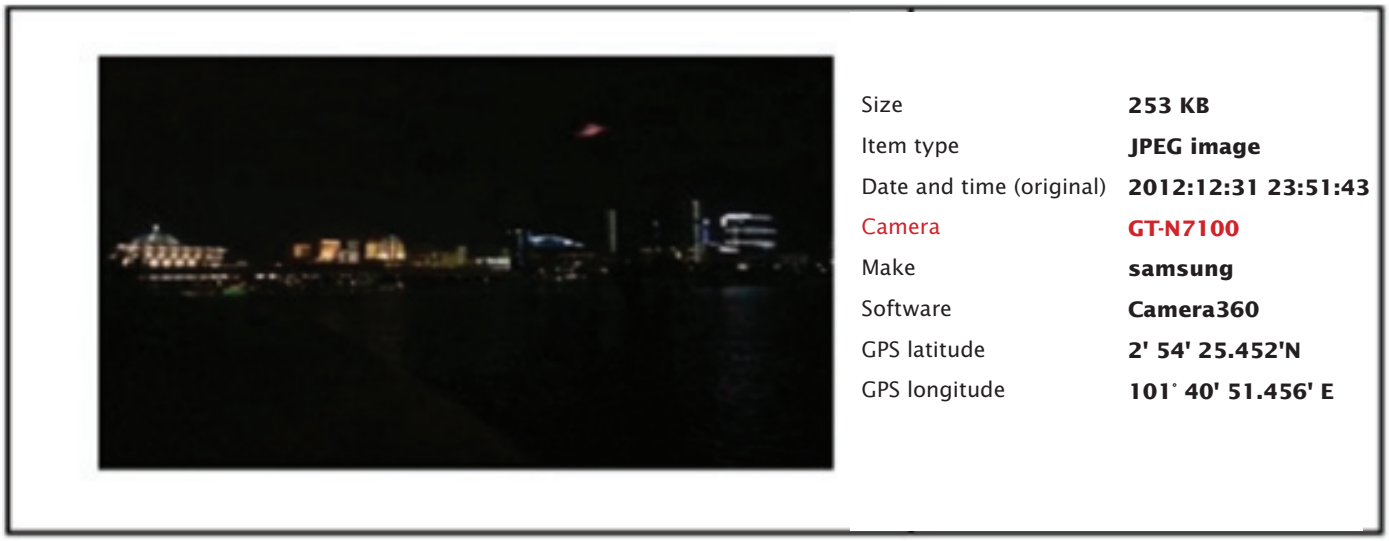
1. EXIF data analysis
2. Structural Similarity Index Measurement (SSIM) analysis
3. Blur & Light direction analysis

Phase 1: EXIF data analysis

The EXIF data analysis was used to check the metadata of a digital photo. That includes the timestamp of the photo, the device used to capture the photo and the GPS coordinates of where the photo was captured.

The metadata pointed out that these photos were taken using an application called Camera360. Camera360 is an application that can be installed on Android devices to capture photos. This application offers thousands of special effects that can be used to modify an image and that includes aliens and UFOs.

Further analysis on Google (Yes, Google is a powerful analysis tool!) revealed that the photo of the flying saucer, was the same photo as in the claimed captured UFO photo!



Size	**253 KB**
Item type	**JPEG image**
Date and time (original)	**2012:12:31 23:51:43**
Camera	**GT-N7100**
Make	**samsung**
Software	**Camera360**
GPS latitude	**2' 54' 25.452'N**
GPS longitude	**101° 40' 51.456' E**

From Google search, we discovered these images:

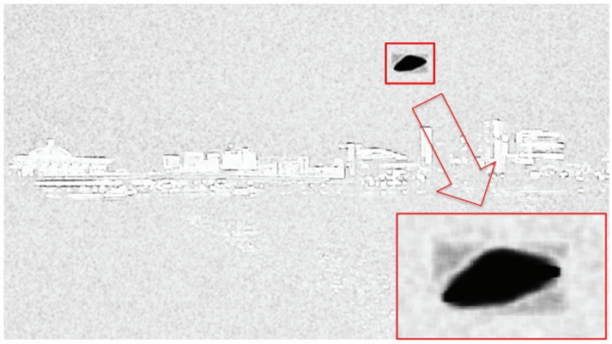
HaHa! busted!

We were not even in the second phase of the analysis yet and we have solved this mystery! However, let us make this more CSI-like, and continue to the next analysis.

Phase 2: The Structural Similarity Index Measurement (SSIM) analysis

The SSIM is traditionally used for assessing the quality of an image. It is usually used to assess the similarity between before and after processing of an image. This kind of assessment is popularly applied on image compression assessments.
In this case, from the total numbers of photos supplied to us, one was very much similar to the picture of the UFO which we had previously Googled over the Internet.

Feel free to observe for yourself the following figure.



The SSIM result is 99.7 percent similar. This indicates that the two images are highly similar to each other. The highest score of SSIM is at 100 percent while the lowest is at 0 percent.

The pixels surrounding the UFO are seen in contrast in term of brightness to the rest of the image. The pixels are also in a rectangular shape, which describes the manner of how the image was pasted on the original image.

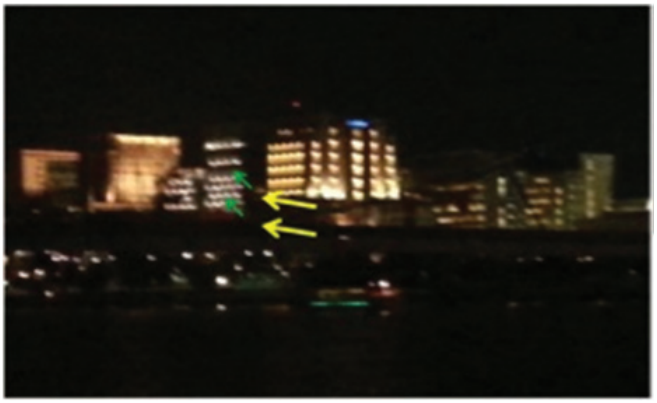
Phase 3: Blur & Light Direction Analysis

This method was used to check the consistency in terms of blurring and light directions from the photo. Usually, a tampered photo contains object blurring and light direction that is not aligned to the overall photo blurring and light direction.

In this case study, the light direction is supposed to be positioned at the direction of the movement of the hands that snapped the photo.

Looking at the photo at hand, the building lights at the background were found to be in a sort of a direction (which is shown in the following figure). The UFO object, on the other hand, has no similar movements.

This indicates the UFO was never in the picture when the photo was taken.



Let Us Conclude Our Analysis, Please!

From the three simple analyses shown here, we can conclude that the photos are fake, and someone has certainly doctored the photos. A UFO was never there at Putrajaya, at least at the date and time when the photos were taken.

Modifying or tampering with digital photos is fun but to prove it is another matter altogether. You need to present a scientific analysis before you can conclude your findings.

In the digital forensics field, photo authentication analysis can be a challenging task. Due to advance image processing and editing technology, it is getting more difficult from time to time to differentiate and to prove the originality of a photo. For example, Adobe Photoshop and other CGI applications can produce very realistic outcomes. A good knowledge and right techniques might help you to overcome this dilemma.■

References:

1. *"UFO Spotted in Putrajaya, Malaysia". http://www.malaysia-kini.com/2013/01/ufo-spotted-in-putrajaya-malaysia/.*
2. *"Super-Resolution". http://lcav.epfl.ch/software/superresolution.*
3. *Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, Apr. 2004.*
4. *Loza et al., "Structural Similarity-Based Object Tracking in Video Sequences", Proc. of the 9th International Conf. on Information Fusion, 2006.*

BYOD: Should It Be Allowed?

By | Noor Aida Idris

Can the establishment of a foundation for a proactive and highly responsive mobility strategy be maximised with a simple solution?

Introduction

The Information Security Forum (ISF) announced on 29th November 2012 the five most prevalent security threats that organisations will face in 2013[1] . One of them, is securing personal devices in workplace[2] . Personal devices in workplace or bring-your-own-device (BYOD) refers to employees who bring their own computing devices (e.g. tablets, smartphones, laptops and PDAs) to the workplace for use and connectivity on the organisational network.

BYOD is a growing trend for many countries. According to a BYOD survey conducted by Ovum[3] across 17 different countries (including Malaysia), 57.1 percent of employees engage in some form of BYOD; and when broken down by market, it seems that 75 percent of employees in the emerging, high-growth markets (e.g. Brazil, Russia, India, UAE, and Malaysia) demonstrate a much higher tendency to BYOD to work. This survey was conducted in Q4 of 2012 with the purpose to learn about behaviours and attitudes of employees who BYOD.

Employees usually are more satisfied at work if they are able to use their own or preferred devices. However, when employees bring their own mobile devices to work without any appropriate planning in BYOD implementation, security risks are introduced that can threaten the security posture of the organisation. The survey by Ovum[4] revealed that 18 percent of organisations' IT department is unaware of BYOD activity, while a further 28 percent of organisations' IT department actively ignore it as it happens. Figure 1 shows that management of BYOD is an issue in many countries[5] , at an average of only 20.1 percent of BYOD being managed. However, some countries, e.g. United States, did demonstrate a higher level of management in comparison to the rest.

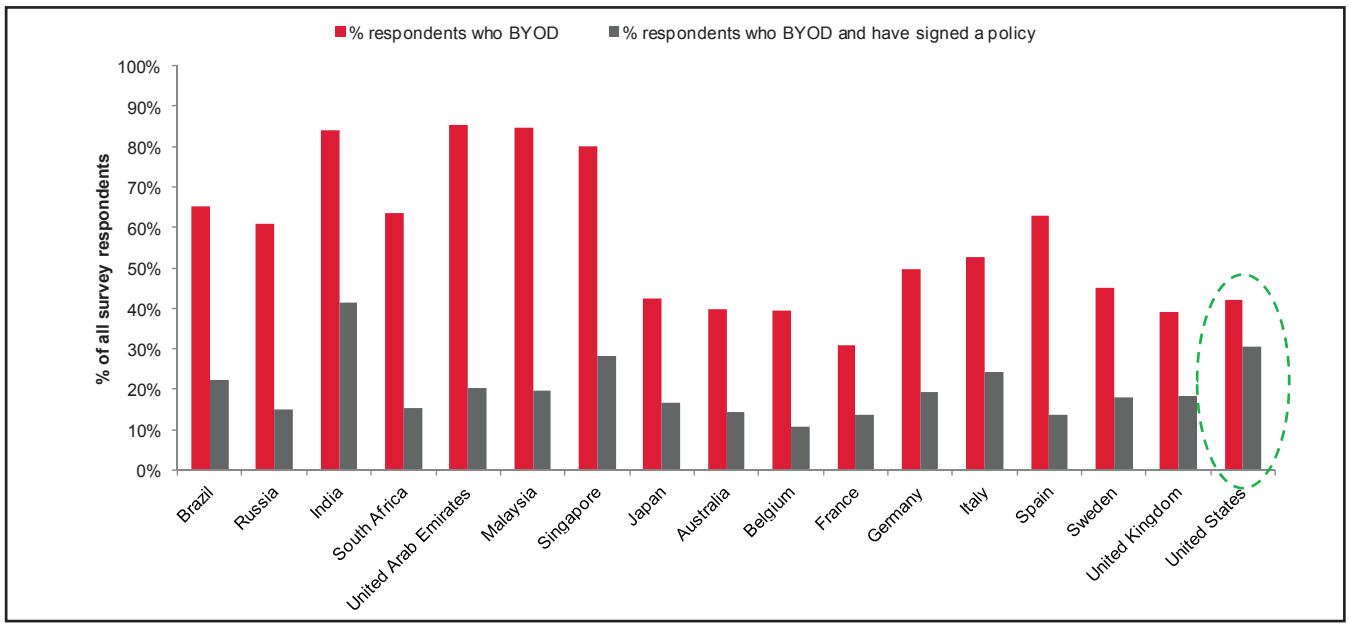


Figure 1: *BYOD management*

[1]Top 5 security threats for 2013 (source: http://www.net-security.org/secworld.php?id=14033)

[2]The securing mobile devices threat, however, is not mutually exclusive. This threat can be combined with other threats to create even greater threat profiles; furthermore other threats will emerge in 2013.

[3]BYOD – Research findings released, (source: http://www.cxounplugged.com/2012/11/ovum_byod_research-findings-released/)

[4]BYOD – Research findings released, (source: http://www.cxounplugged.com/2012/11/ovum_byod_research-findings-released/)

[5]BYOD: an emerging market trend in more ways than one (source: www.logicalis.com/news-and-events/news/logicalis-white-paper-byod.aspx#.UVklGRdkP4W)

In February 2013, Varonis conducted an online survey to examine the impact of BYOD on work habits and data security[6] . Several key findings of the survey are:

- 50 percent of employees reported that someone at their organisation has lost a device with important data in it
- 22 percent said the lost device had security implications for the organisation

Organisations should weigh the pros and cons of BYOD; and not just ignore employees who BYOD or simply disallow BYOD at workplace. BYOD can be an enabler for organisations, thus, organisations should take advantage of BYOD and allow for it. Nevertheless, they should develop a strategy to reduce security risks by planning and managing the BYOD implementation, through the implementation of ISO/IEC 27001:2005 Information Security Management System (ISMS) - Requirements.

ISO/IEC 27001:2005 ISMS – Requirements is an international standard published by International Organisation for Standardisation (ISO). The standard specifies requirements for an Information Security Management System (ISMS) that an organisation can develop and operate to protect its information assets and manage its information security risks. As a whole, ISMS can assist in the holistic and systematic management of information security within the organisation. Thus, ISMS is valuable in the planning and managing of the BYOD implementation to organisations in an effective manner.

This article describes the necessary requirements in ISMS that organisations can undertake in order to plan and manage their BYOD implementation.

Assessing BYOD risks

Risk assessment is a systematic process for identifying and evaluating events[7] (i.e. possible risks and opportunities) that could affect the achievement of objectives, positively or negatively. Risk assessment is one of the requirements in ISO/IEC 27001:2005 ISMS under clause 4.2.1 c). Risk assessment process in ISMS usually includes other sub-processes such as identifying, analysing and evaluating the risks.

When conducting risk assessment, organisations should be able to identify security risks associated with BYOD. Some of the risks associated with BYOD are information disclosure due to stolen or lost personal device or confidential and sensitive business information stored in mobile devices without sufficient protection. Another type of security risk occurs when an employee leaves the organisation, for whatever reasons, and applications and confidential data may become unavailable to organisation as they still reside in the employee's personal device. This possibility will occur when there is no procedure in place to safeguard the organisational confidential data.

Other risks introduced by BYOD are[8]:

- Introduction of Malware to the network through mobile devices that come pre-installed with malware;
- Trojanised applications that may be downloaded from third-party application stores that steal sensitive business information stored in mobile devices;
- Social engineering tactics that lead employees to click malicious URLs spammed by trusted sources via text messages, social media, emails;
- Virus infection of the network-connected jail-broken smartphones.

These risks need to be analysed and evaluated to determine whether security controls need to be implemented to reduce the risks to acceptable level. Organisations will need to design the security controls for the risks associated with BYOD. On the other hand, organisations may also decide to disallow BYOD if they realise the risks associated with BYOD are too high or the cost of security controls does not commensurate with the risks.

Figure 2 provides options on security controls that organisations may apply in BYOD implementation. They are; password protection, remote wipe, encryption and disallow BYOD. These options have been implemented by organisations in the Varonis online survey[9].

[6]BYOD online survey (source:www.varonis.com)

[7]ISO/IEC 27005:2011 Information security risk management

[8]Bring your own risk (source: www.trendmicro.com/us/enterprise/challenges/it-consumerization/infographic/index.html)

[9]BYOD online survey (source:www.varonis.com)

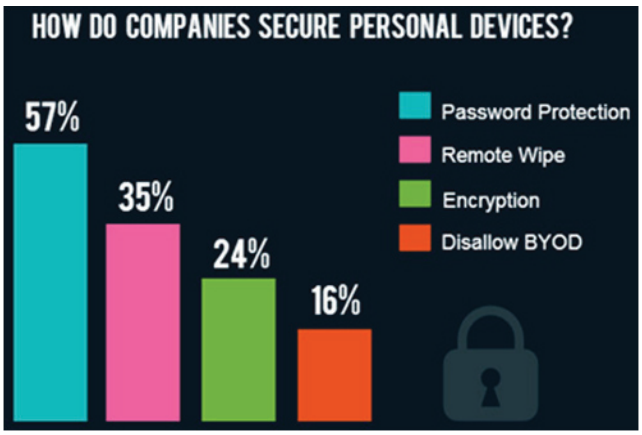


Figure 2: *Security controls for Securing Personal Devices*

Developing BYOD policies and procedures

Organisations should develop policies and procedures related to BYOD. Several controls in ISO/IEC 27001:2005 ISMS are relevant to the development of BYOD policies and procedures. They are:

- A.5.1 Information security policy; Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations;
- A.11.7 Mobile computing and teleworking; Objective: To ensure information security when using mobile computing and teleworking facilities.

BYOD policies and procedures should basically tell the employees the dos and don'ts of BYOD. The policies and procedures should have the following contents[10] :

- **Specify what devices are permitted**
  There are various types of devices available currently. Organisations should specify what devices are allowed and will be supported in the workplace; this includes brand, operating systems (OS) etc.

- **Establish security controls for mobile devices**
  Employees tend to resist security controls (e.g. passwords or lock screens) on their personal mobile devices. However, organisations should establish security controls for personal mobile devices as there can be sensitive information in the devices, when the devices connect to organisational network. Nevertheless, organisations may discuss with the employees to find appropriate security controls that will not burden them.

- **Define service/support level for devices under BYOD criteria**
  Organisations should define what type and level of support that will be rendered to the personal mobile devices. Examples are in terms of broken devices, application (i.e. email, network issues), data loss etc.

- **Clarify who owns data, applications, devices**
  While it seems logical that organisations owns information stored on the servers that the employees access with their devices, it becomes a problem when the issue of wiping the device (e.g. in the event the device is lost or the employee resigns). Wiping a device usually involve deleting all contents in the device, including personal pictures, music and applications that in many cases the employee, not the organisation, has paid for. Thus, organisations should clarify with employees the right to wipe devices brought onto the organisation's premise. Organisations, should provide guidance on how employees can secure and back up their personal content and applications.

- **Specify what applications will be allowed or banned**
  Organisations should specify whether employees are allowed to download, install and use applications that present security or legal risks on mobile devices that have access to organisational network and resources. Major considerations typically include applications for social media browsing, replacement email applications and VPNs or other remote-access software.

- **Integrate BYOD implementation plan with organisational acceptable use policy**
  Organisations should ensure requirements in the existing acceptable use policy are covered in the BYOD implementation plan. This means the requirements for BYOD implementation should be aligned with the acceptable use policy. For example, is it a violation of acceptable use policy if the employees:
  - Post on Facebook or other social media sites using their personal devices?

[10]7 tips for establishing a successful BYOD policy, www.cio.com/article/706560/7_Tips_for_Establishing_a_Successful_BYOD_Policy

- Browse offensive websites via personal devices, which later inadvertently download malware and affect the organisational network?
- Transmit, unintentionally or not, inappropriate material over organisational network, using personal devices' VPN?

- **Indicate methods for employee exit strategy**
  Organisations should clearly spell out the employees exit strategy in the BYOD procedure. The detailed procedures of the removal of access rights, e-mail access, data and other proprietary applications on these personal mobile devices should be described. Disciplinary actions and/or enforcement should also be stated in the procedure as well.

The BYOD policies and procedures should be approved and communicated to all employees and relevant parties. Enforcement of the policies and procedures should also be in place. Lastly, the policies and procedures should be reviewed at planned intervals to ensure the validity and accuracy of the policies and procedures.

Monitoring security incidents related to BYOD

Organisations should monitor any security incidents which may occur due to BYOD. ISO/IEC 27001:2005 ISMS specifies few controls for managing security incident which are A.13.1 Reporting information security events and weaknesses and A.13.2 Management of information security incidents and improvements.

The objectives of these two controls is to ensure information security events and weaknesses associated with information systems are communicated in a manner that allows for timely corrective action to be taken and ensure a consistent and effective approach is applied to the management of information security. This will help organisations in managing security incidents related to BYOD effectively.

In addition, internal ISMS audit (clause 6 of ISO/IEC 27001:2005) is another requirement in ISMS that can assist organisations in managing and monitoring their BYOD security incidents. The internal ISMS audits will ensure organisations conduct audits periodically to find non-conformities in terms of violation of BYOD policies and procedures.

Conclusion

BYOD has created tremendous opportunity for organisations to allow their employees to work in new, innovative and productive ways. The old ways of prohibiting access to organisational network and data from personal devices, or insisting that employees use organisation-owned devices at workplace will not work in the consumerisation era. Thus, organisations should be flexible and allow BYOD in their organisations. However, they need to equip themselves with the knowledge and how-tos in managing the BYOD effectively. As described in this article, ISO/IEC 27001:2005 ISMS implementation will help organisations to understand BYOD risks, develop policies and procedures related to BYOD and monitor the security incidents related to BYOD. Other efforts should also be made to ensure the BYOD implementation is successful and managed effectively. ■

References:

1. *ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems – Requirements.*
2. *ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management.*
3. *BYOD – Research findings released, 28 November 2012, http://www.cxounplugged.com/2012/11/ovum_byod_research-findings-released/, accessed on 27 March 2013.*
4. *Adrian Drury, Richard Absalom, BYOD: an emerging market trend in more ways than one, http://www.logicalis.com/news-and-events/news/logicalis-white-paper-byod.aspx#.UVklGRdkP4W, accessed on 27 March 2013.*
5. *BYOD online survey by Varonis System, www.varonis.com, accessed on 27 March 2013.*
6. *Top 5 security threats for 2013, Information Security Forum, www.net-security.org/secworld.php?id=14033, accessed on 27 March 2013.*
7. *Jonathan Hassel, 7 Tips for Establishing a Successful BYOD Policy, May 17, 2012, http://www.cio.com/article/706560/7_Tips_for_Establishing_a_Successful_BYOD_Policy?page=3&taxonomyId=600013, accessed on 27 March 2013.*
8. *Bring Your Own Risks, www.trendmicro.com/us/enterprise/challenges/it-consumerisation/infographic/index.html, accessed on 27 March 2013.*

Transaksi e-Dagang: Adakah ianya selamat?

By | Azrul Ehsan Ahmad & Norhazimah Abdul Malek

JOHOR BAHRU: Seorang kakitangan swasta yang membeli tiga telefon bimbit dengan harga RM3,250 secara dalam talian terkejut apabila hanya menerima lesung batu berharga RM14.50, sehari selepas melunaskan pembayaran.

Lebih menyakitkan hati, tulisan RM14.50 berkenaan masih ada pada lesung batu berkenaan dan mangsa tergamam ketika menerimanya.

"Saya membuat pembelian itu selepas melayari satu laman web dan tertarik dengan tawaran telefon bimbit Samsung Galaxy S bernilai RM1,100 seunit berbanding harga pasaran semasa iaitu RM1,900.

"Saya membeli tiga telefon bimbit berkenaan secara talian pada 6 Disember lalu dan membuat bayaran ke akaun seorang lelaki." kata mangsa semalam.

Menurut mangsa, dia kemudian menerima SMS daripada kakitangan sebuah syarikat menjual peralatan komunikasi yang menawarkan barangan percuma atau diskaun RM50.

Mangsa memilih tawaran diskaun berkenaan dan sehari kemudian, dia menerima bungkusan barangan dibeli.

"Saya gembira kerana telefon bimbit berkenaan tiba tepat pada masanya, tetapi terkejut apabila mendapati kotak bungkusan berkenaan cuma mengandungi lesung batu.

"Saya menghubungi nombor telefon tertera seperti dalam SMS diterima sehari sebelum itu, tetapi individu terbabit enggan menjawab panggilan saya," katanya.

Mangsa kemudian melakukan pemeriksaan di Suruhanjaya Syarikat Malaysia (SSM) dan mendapati syarikat terbabit tidak wujud.

Laporan diatas adalah antara kes penipuan perniagaan Internet yang pernah disiarkan oleh suratkhabar Harian Metro bertarikh 10 Januari 2012.

Dalam arus paskal pemodenan dunia tanpa sempadan hari ini, kita sememangnya tidak dapat lari dari perubahan terhadap gaya hidup yang berorientasikan teknologi maklumat. Penggunaan Internet telah menjadi salah satu sumber utama dalam kehidupan harian kita semua. Istilah "dunia di hujung jari" sering digunakan bagi menggambarkan situasi tersebut. Menerusi penggunaan Internet, segala urusan harian boleh dilakukan secara dalam talian (online). Antaranya, urusan pembayaran bil dan cukai, kemudahan laman sosial bagi menghubungkan individu dengan dunia luar, dan tidak kurang hebatnya juga urusan jual-beli yang dijalankan secara dalam talian.

e-Dagang merupakan aktiviti yang kian mendapat tempat di kalangan para peniaga dan pembeli di negara ini. Antara produk-produk yang ditawarkan termasuklah peralatan komunikasi, produk kesihatan, kecantikan, pakaian, sukan, aksesori dan lain-lain lagi. Perniagaan e-Dagang mempunyai kebaikan di mana ianya dapat menjimatkan masa dan juga kos. Para peniaga juga dapat mempromosikan barangan mereka tanpa sempadan.

Walaubagaimanapun sejak akhir-akhir ini, kita sering membaca kes-kes penipuan berkenaan e-Dagang. Di antaranya, barangan yang diterima tidak menepati ciri sebenar barangan yang dilihat di laman e-Dagang dan paling malang, jika barang berkenaan bukan barang yang dipesan atau barangan yang dipesan tidak kunjung tiba walaupun bayaran telah dibuat sepenuhnya.

Pada tahun 2012, sebanyak 9,986 insiden berkaitan keselamatan siber telah dilaporkan kepada Pasukan Tindakan Kecemasan Komputer Malaysia (MyCERT), CyberSecurity Malaysia. Sebanyak 4,001 laporan adalah berkaitan penipuan Internet. Pada tahun 2010, sebanyak 2,212 kes penipuan Internet dilaporkan dan 5,328 kes dilaporkan pada tahun 2011. Istilah penipuan Internet secara amnya merujuk kepada mana-mana jenis skim penipuan yang menggunakan satu atau lebih perkhidmatan dalam talian. Penipuan Internet boleh dilaksanakan menggunakan aplikasi komputer seperti forum, e-mel, atau laman sesawang. Perkara ini jelas memperlihatkan peningkatan kes sehingga ke satu paras yang amat membimbangkan selain memberi petunjuk yang kini semakin ramai membeli-belah secara dalam talian.

Lantaran itu, pihak kerajaan telah mengambil langkah proaktif dengan memperkenalkan Malaysia Trustmark bagi menangani kesulitan dan masalah-masalah yang berbangkit akibat kes penipuan perniagaan Internet ini.

Apa itu Malaysia Trustmark ?

Malaysia Trustmark merupakan hasil inisiatif Kerajaan Malaysia dalam usaha untuk merangsang perniagaan e-Dagang, meningkatkan keyakinan pengguna untuk melakukan transaksi e-Dagang dan seterusnya mengurangkan risiko penipuan Internet.

Malaysia Trustmark adalah perkhidmatan menilai dan mengesahkan sesebuah laman e-Dagang tempatan dari segi:

1. Pendedahan maklumat (Disclosure of Information), memerlukan setiap organisasi yang menjalankan perniagaan e-Dagang untuk memaparkan segala maklumat perniagaan dengan tepat dan terkini di laman sesawang e-Dagang mereka;

2. Amalan perniagaan (Practices) berdasarkan polisi serta prosedur yang diamalkan oleh sesebuah organisasi dalam menjalankan urusan jual beli dalam talian;

3. Keselamatan (Security), yang memerlukan sesebuah organisasi untuk memastikan tahap keselamatan laman sesawang e-Dagang mereka supaya data pelanggan serta sebarang transaksi elektronik yang terlibat di dalam urusan jual-beli dalam talian terjamin;

4. Privasi atau Perlindungan Data Peribadi (Personal Data Protection) yang memerlukan sesebuah organisasi itu mematuhi Akta Perlindungan Data Peribadi 2010 bagi memastikan data pelanggan mereka dilindungi;

5. Penyelesaian Pertikaian Alternatif (Alternative Dispute Resolution), setiap organisasi yang menjalankan perniagaan e-Dagang perlu mempunyai prosedur pengendalian aduan atau pertikaian pelanggan. Prosedur ini haruslah dipaparkan di laman sesawang e-Dagang mereka.

Sesebuah organisasi akan dapat menggunakan logo Malaysia Trustmark di laman sesawang e-Dagang mereka jika mereka mematuhi keperluan di atas.

Antara faedah-faedah Malaysia Trustmark adalah:

1. Membina keyakinan para pengguna terhadap transaksi e-Dagang tempatan;
2. Menggalakkan amalan perniagaan e-Dagang yang teratur dan selamat;
3. Mengurangkan risiko dan kes penipuan Internet;
4. Organisasi yang mempunyai logo Malaysia Trustmark akan lebih dipercayai seterusnya akan meningkatkan jualan mereka;
5. Memperluaskan peluang-peluang perniagaan di peringkat tempatan dan antarabangsa.

Untuk merealisasikan inisiatif ini, Kerajaan Malaysia telah melantik CyberSecurity Malaysia sebagai agensi Pengendali (Operator) dan Pengesah (Certifier) Malaysia Trustmark bagi sektor swasta manakala Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) pula dilantik sebagai agensi Pengendali (Operator) dan Pengesah (Certifier) Malaysia Trustmark bagi sektor awam.

Jika melihat kepada situasi di luar Malaysia, pendekatan yang sama juga dilaksanakan di negara-negara maju di mana terdapat badan atau organisasi yang diiktiraf untuk mengeluarkan logo Trustmark seperti VeriSign, TRUSTe dan TrustSg. Dengan adanya logo tersebut, jelas menggambarkan kesan positif di mana ianya membantu meningkatkan kepercayaan dan keyakinan para pembeli terhadap organisasi yang menjalankan perniagaan e-Dagang.

World Trustmark Alliance (WTA)

World Trustmark Alliance
Global Trust Innovation

World Trustmark Alliance (WTA), gabungan di antara Asia Pacific Trustmark Alliance (ATA), eConfianza.org dan Euro-Label Trust Mark, adalah satu perikatan kerjasama antarabangsa di antara organisasi-organisasi yang mengeluarkan logo Trustmark. Ahli-ahli WTA adalah organisasi-organisasi yang aktif dalam meningkatkan

keyakinan para pengguna dalam e-Dagang di negara mereka seperti CyberSecurity Malaysia (Malaysia), Commerce Net Singapore (CNSG) dan Consumer Association Singapore (CASE) (Singapura), NIPA (Korea Selatan), TRUSTe (Amerika Syarikat), Trade Safe dan EC Network (Jepun), SOSA (Taiwan), Qartas Corporation (Filipina), Eropah, Thailand, Mexico, dan China. Objektif WTA adalah:

1. Memperluaskan peluang perniagaan melangkaui pasaran tempatan;
2. Menggalakkan amalan baik dalam transaksi-transaksi serantau;
3. Membina keyakinan dalam pasaran e-Dagang; dan
4. Menjadi model pertama bagi kerjasama serantau yang merupakan langkah pertama kearah perikatan global.

Ahli-ahli WTA menggunakan Garis Panduan Pengendali Trustmark (GTO) yang merangkumi keperluan pendedahan maklumat (Disclosure of Information), amalan perniagaan (Practices), keselamatan (Security), privasi atau perlindungan data peribadi (Personal Data Protection), Penyelesaian Pertikaian Alternatif (Alternative Dispute Resolution), dan pemantauan (Monitoring) untuk mengaudit organisasi yang menjalankan perniagaan e-Dagang.

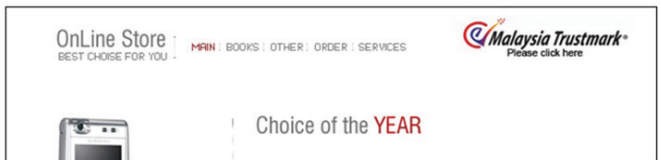
Tips kepada Pengguna

Para pengguna atau pembeli di negara ini adalah dinasihatkan untuk melakukan transaksi hanya melalui laman e-Dagang yang selamat dan dipercayai sebelum meneruskan urusan jual beli secara dalam talian. Dengan adanya logo Malaysia Trustmark pada laman sesawang e-Dagang yang dilawati, ianya menunjukkan organisasi tersebut telah mengambil pendekatan program keselamatan.

Para pengguna juga boleh merujuk kepada garisan panduan yang ada berkenaan transaksi elektronik seperti yang disediakan oleh Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan (KPDNKK). Garis panduan tersebut boleh dimuat turun di laman sesawang KPDNKK.

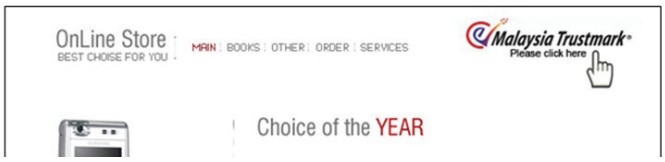
Di bawah ini juga disediakan langkah-langkah yang perlu diikuti bagi mengenalpasti laman sesawang yang telah mendapat pengesahan Malaysia Trustmark. Sila pastikan:

1. Logo Malaysia Trustmark terletak di bahagian kanan atas sesebuah laman sesawang.



2. Sebelum melakukan sebarang transaksi jual beli, pembeli atau pengguna haruslah memeriksa kesahihan logo Malaysia Trustmark tersebut:

   - Langkah 1: Gerakkan tetikus ke arah logo Malaysia Trustmark yang terletak di bahagian kanan atas.
   - Langkah 2: Klik pada logo Malaysia Trustmark atau perkataan "Please Click Here" yang terdapat di bawah logo Malaysia Trustmark.



   - Satu paparan sijil bagi Malaysia Trustmark akan muncul.
   - Langkah 3: Periksa status yang terdapat di dalam paparan sijil Malaysia Trustmark tersebut.

   - Jika status Malaysia Trustmark tersebut adalah 'VALID' (sahih), ini bermakna organisasi tersebut masih mematuhi keperluan Malaysia Trustmark. Jika tidak, ianya menunjukkan organisasi tersebut tidak lagi memberi komitmen terhadap pendekatan rancangan keselamatan Malaysia Trustmark.

Diharapkan dengan sedikit perkongsian mengenai Malaysia Trustmark ini dapat meningkatkan keyakinan pengguna untuk melakukan transaksi e-Dagang dan seterusnya merangsang perniagaan e-Dagang di Malaysia. Di samping itu, mengurangkan risiko dan kes penipuan internet yang kini kian menjadi-jadi.

Untuk mengetahui lebih lanjut mengenai Malaysia Trustmark bagi sektor swasta (MTPS), sila lawati Malaysia Trustmark.■

A Glimpse of ISO 22301– Business Continuity Management Systems

By | Ida Rajemee Bt Ramlee

Background

The new international standard for Business Continuity Management System (BCMS) "Societal security - Business continuity management systems – Requirements" i.e. ISO 22301 was officially launched in May 2012. This new global standard for business continuity management (BCM) specifies requirements to **plan, establish, implement, operate, monitor, review, maintain and continually improve on a documented management system.** The standard aims to protect against, reduce the likelihood of occurrence, prepare for, respond to and recover from disruptive incidents when they arise.

This is the first international standard for BCM using the British Standard BS 25999 - Business Continuity Management Part 2 as its primary input. Other standards referred to include the NFPA 1600:2010, ASIS SPC 1-2009, ISO 27031, ISO Guide 73, ISO PAS 22399 and other national BCM standards (e.g. Australia, New Zealand, Singapore, Japan, Singapore and Canada).

The new standard was developed according to the ISO Guide 83, with a new high-level structure which specifies the common headings and standardises text as agreed in ISO. The guide states several principles, definitions, standard words and a fixed format that ensure consistency with all future and revised management system standards. This will also allow easier integration and interface for organisations implementing various management systems like the ISO 27001, ISO 14001 and ISO 9001.

Why Implement BCM?

The birth of the global standard will eventually cater to the needs for a consistent approach to BCM implementation. This is especially important for multinational firms that operate in different countries and have to comply with each country's BCM standards and statutory obligations. Similar to other management systems, the standard is also easily scalable so it can be adapted to organisations of almost all sizes. By adopting to this new standard, organisations are able to measure itself against good BCM practice.

For service oriented organisations, BCM practices should be embedded into their business operations and become part of corporate culture to ensure availability of their critical services. In Malaysia, the implementation of BCM at the organisation level is mainly due to regulatory and statutory obligations. For instance in the Financial and Banking sector, Bank Negara Malaysia has issued BCM Guidelines with the main objective *"to outline and enforce minimum BCM requirements on the institution so as to ensure the continuity of critical business functions and essential services within a specified timeframe in the event of a major disruption."*

Another major contributing factor to BCM implementation is the Cabinet mandate for Malaysia's Critical National Information Infrastructure (CNII) organisations to obtain the ISO 27001 Information Security Management System (ISMS). The certification needs to be obtained within three years from the date of the mandate i.e. 24th February 2010. As BCM is specifically defined in Control A.14 of the ISO 27001 requirements, this has indirectly boosted the implementation of BCM and fulfilling

the ISMS requirements at the same time.

Furthermore, the control is described in general and fulfills the basic requirements of BCM. The existence of the ISO 22301 provides the best methodology to support the implementation of this specific clause. By complying with the 27001 BCM controls, it will be easier for organisations to expand their BCM implementation to meet the requirements of ISO 22301.

Comparison with BS 25999

Considering BS 25999 has been the main reference most popular for business continuity standards ever since it was published in November 2007, some significance comparisons are highlighted in this sub-topic.

In general the ISO 22301 requirements are similar to the BS 25999-2 which includes the core components of BCM i.e. business continuity policy, business impact analysis, risk assessment, business continuity strategy and business continuity plans, exercising and testing, internal audit, management review and non-conformity and corrective action. Moreover, the new standard also includes improvement over 25999-2 in areas such as disaster response and crisis communications, and gives more emphasis on the planning of the BCMS and the engagement of the management throughout the phases.

Compared to BS 25999, major changes are observed in these following new areas - understanding the organisation, understanding the needs and expectations, management commitment, monitoring measurement, analysis and evaluation and communication and warning system. These requirements are new in ISO 22301 and were not covered in BS 25999.

Another new aspect introduced in this new standard is the Top Management Commitment. In ISO 22301, the top management are given clearer BCM leadership responsibilities and ways to demonstrate their commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the BCMS.

BS 25999 only describes the management's review in general and is based on Review Input and Output whereas management review requirements are also emphasised in greater detail in ISO 22301.

In the aspect of performance evaluation in terms of monitoring, measurement, analysis and evaluation, these areas are not covered significantly in BS 25999 compared to ISO 22301.

The former only described brief requirements in maintaining and reviewing BCM arrangements while the ISO 22301 requires organisations to determine what needs to be measured and monitored, methods to be used and when monitoring should be performed and when the analysis evaluation of measurement results should be performed. Procedures for monitoring performance are also clearly described.

Other new areas covered under the scope of BCMS are the interested parties' needs and interests, such as customers, investors, shareholders, the supply chain, public and/or community input and needs, expectations and interests.

BCM practitioners are also exposed to new definitions introduced in this standard. Some of the new terms are listed in the table below:

Terms	Definition
Correction	An action to eliminate a detected non-conformity
Disruptive Incidents	An event that stops the business operations
Documented Information	Information required to be controlled and maintained by an organisation and the medium on which it is contained

Maximum Acceptable Outage (MAO)	Time it would take for adverse impacts, which may arise as a result of not providing a product/service or performing an activity, to become unacceptable
Maximum data loss	The point to which information used by an activity must be restored to enable the activity to operate upon resumption – also referred to as Recovery Point Objective
Minimum Business Continuity objective (MBCO)	Minimum level of services and/or products that is acceptable to the organisation to achieve its business objectives during a disruption

Application of the PDCA model

Organisations which have implemented other management systems standards such as ISO 9001, ISO 14001 or ISO/IEC 27001 will be familiar with the Plan-Do-Check-Act (PDCA) model applied in the ISO 22301. The PDCA model is used in planning, establishing, implementing, operating, monitoring, reviewing, maintaining and improving the effectiveness of an organisation's BCMS. At the same time, consistency with other management system standards that are already in place can also be obtained through integrated implementation and operation.

The ISO 22301 is designed to be compatible with other management system standards. For instance, ISO 27001 and ISO 22301 are highly compatible and are very easy to implement jointly. Similarities between the two standards are in the areas of Document and records management, Human resources management, Internal Audit, Management Review, Corrective and preventive actions, Setting objectives and measurement and the PDCA cycle. There are also overlapping areas in Incident Management and Risk Management.

The diagram summarises the PDCA cycle in the BCMS context.

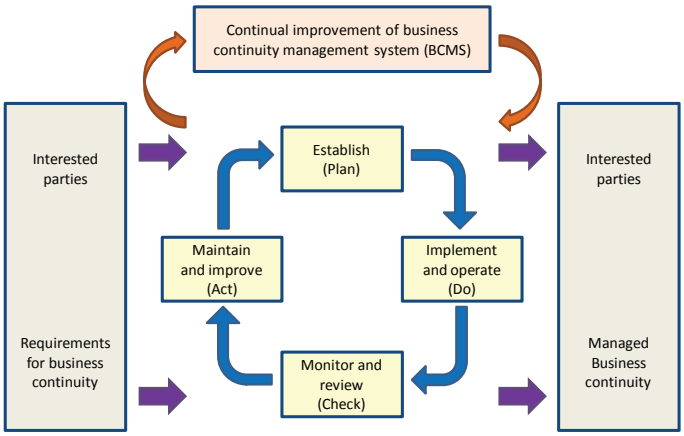


Figure 1: *PDCA model applied to BCMS*
Source: http://www.bsigroup.it/

For the ISO 22301 requirements, the Planning activities include Clause 4: Context of the organisation, Clause 5: Leadership, Clause 6: Planning and Clause 7: Support. The DO phase covers Clause 8: Operation. Clause 9: Performance Evaluation represents the Check Phase and lastly Clause 10: Improvement is covered under the ACT phase. All these clauses are discussed in brief in the following section.

The Requirements & Clauses

This standard comprises of 10 main clauses initiated by the Scope, Normative Reference, Terms and Definitions, as followed by the standard's requirements from Clause 4 to Clause 10.

a - Clause 4: Context of the organisation

This clause introduces the requirements necessary to establish the context and determine the scope of the BCMS. This is obtained by getting the internal and

external needs of relevant interested parties such as regulators, staff, customers and other related stakeholders. Other considerations are the organisation's strategic objectives, key products and services, risk tolerance as well as the regulatory, contractual and stakeholders' obligations and other interested parties (i.e. customers, investors, shareholders, the supply chain and public/community) needs and interests. The scope is also defined based on the size, nature and complexity of the organisation.

b - Clause 5: Leadership

It summarises the requirements specific to top management's role in the BCMS and how leadership demonstrates its expectations to the organisation via a business continuity policy statement, providing sufficient resources to support, implement and maintain BCMS.

Top management are also responsible to ensure the BCMS achieves its expected outcome, BCMS objectives and plans are established as well as responsibilities and authorities for relevant roles are assigned accordingly.

c - Clause 6: Planning

Clause 6 describes requirements as it relates to establishing strategic objectives and guiding principles. This is achieved by identifying the risks to the BCMS implementation, treating the risks identified and complying with the organisational needs. Business continuity objectives must be established and communicated within the organisation and plans need to be developed to achieve these objectives.

d - Clause 7: Support

This clause addresses specific resources and staff competency for BCMS implementation. It also covers the need for both internal and external communications relevant to the BCMS. Additionally, all requirements for documented information to support BCMS operations are explained during document creation, update and document control.

e - Clause 8: Operation

Clause 8 includes the requirements for Business Impact Analysis, Risk Assessment, the development of Business Continuity strategy, procedures, exercising and testing. It also stresses on the importance of a well-defined incident response structure to support timely response and escalation of incident.

f - Clause 9: Performance evaluation

Performance evaluation requirements are in terms of BCM performance measurement, BCMS compliance with International Standards and management's expectation and feedback from management with regards to expectations. Evaluation of continuity procedures and capabilities shall be conducted along with management review to ensure the organisation's BCMS continue with suitability, adequacy and effectiveness. Internal audit shall also be conducted at planned intervals to determine conformance to the standard and the organisation's requirements for its BCMS.

g - Clause 10: Improvement

This clause identifies and acts on BCMS non-conformance through corrective action. Organisations complying to the standard shall evaluate the need for action to eliminate the causes of non-conformities and corrective actions appropriate to these non-conformities. The continual improvement for suitability, adequacy or effectiveness of the BCMS is also required.

Looking Forward

The new standard ISO 2230 is auditable as organisations are able to obtain accredited

certification for this standard similarly to BS 25999-2. Since the standard is a major revision from the previous BS 25999, organisations previously certified with the BS 25999-2 are given a two year transition period to comply with ISO 22301, which is due by May 2014.

Existing organisations that are currently certified with BS 25999-2 will have to 'upgrade' to ISO 22301. Some of the certification bodies e.g. UK Accreditation Service (UKAS) provide transition guidelines and timescales to organisations currently certified with BS 25999-2:2007. The same goes to other countries with national BCM standards like the UK which has announced the withdrawal of their national standard.

In the efforts to support the adaptation of this new standard, the ISO/TC 223 Societal Security published a complementing guideline in December 2012. The ISO 22313 Business Continuity Management Systems – Guidance clarifies the intent of all the ISO 22301 requirements and provides detail explanations and relevant samples to assist with the implementation of ISO 22301.

Other BCM family guidelines and procedures which are in the pipeline to be published are ISO 22316 - Organisational resilience - Guidance and principles, ISO 22322 – Inter/Intra organisational warning procedures , ISO 22324 – Emergency Management- Colour-coded alert, ISO 22325 - Guidelines for emergency capability assessment for organisations , ISO 22351 – Disaster and emergency management - Shared situation awareness, ISO 22323 – Organisational Resilience Management Systems – Requirements with guidance for use and ISO 22398 – Guidelines for exercises and testing. With the BCM standards and guidelines, it is hoped that the implementation of BCM will be more systematic, structured and easy.

Although adoption to standards is a voluntary 'act', the existence of the ISO BCM standard may be a good reason for better compliance in BCM implementation. The founding of this global BCM standard may be a triggering factor for Malaysia's CNII to adopt this standard.

Although it is too early to determine the adoption level of ISO 22301 in Malaysia, it is possible for the standard to be next in line to be mandated for compliance at all CNII agencies. Adoption to this new standard will definitely ensure better organisational resilience against disruption, preparedness in facing the unexpected and to ensure continuity of significant services across the critical sectors in Malaysia. ■

References:

1. *ISO 22301 – Societal Security – Business Continuity Management System – Requirements*
2. *Whitepaper ISO22301 - http://www.pecb.org/iso22301*
3. *http://www.bsigroup.co.in/upload/Standard/ISO-22301-Presentation.pdf*
4. *http://www.continuityandresilience.com/core-approach-note-ISO22301.pdf*
5. *http://www.iso27001standard.com/webinars/ ISO 27001 & ISO 22301/BS 25999-2: Why is it better to implement them together?*
6. *Business continuity - ISO 22301 when things go seriously wrong http://www.iso.org/iso/news.htm?Refid=Ref1602*
7. *Making the move from BS 25999-2 to ISO 22301 - http://www.bsigroup.com.my/bs25999-transition-iso22301*
8. *Bank Negara Malaysia – Guidelines on Business Continuity Management*

The Need For Certification and Its Benefits

Local SMEs that are ICT developers are urged to certify their products with CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI).

If you are an SME involved in developing ICT products, you might want to take note of the local services provided by CyberSecurity Malaysia in terms of getting your products verified and recognised by international standards. Once a product is verified, it will also be able to connect to global markets with the right certification and verification needed.

Information As An Assurance

Information can be considered as a collection of data and knowledge about a topic; processed and presented in an understandable format for its intended audience. Information exists in a variety of different formats such as in printed form or written on paper, electronically stored, and spoken in conversation. Information such as trade secrets, intellectual property, future business plans and strategies, personnel and customer records, and business intelligence are valuable data.

Loss of information could disrupt business operations, tarnish the organisation's reputation, and result in fines or penalties. Today, most information are stored and transmitted electronically, processed daily, and accessible from almost anywhere. Therefore, information owners would require some form of 'control' on the type of information that could be shared, and with whom. They also need some form of 'assurance' that the information would be accessible, accurate and usable upon demand.

This relates to the information securityissues, which calls for the preservationof confidentiality, integrity and availability of the information. Most organisations rely on technology to store, process, and transfer information. They need to identify context, determine the threats, consider their impact to the organisation if the threat is realised, and determine those risks that require control. However, most organisations have limited resources to focus on information security problem.

Business structures and operating models differ from one organisation to another. Controls may be implemented in technology, facilities and infrastructure, policies and procedures, and people. But, how can an organisation know that the security controls are effective? The organisation needs a culture of security at levels appropriate to the business, and continuously test the security implementation. This is the basis for assurance, and it provides confidence in implementing security controls.

Assurance is the basis for confidence or trust in something tangible. In information security, assurance means confidence that the organisation is protected against security threats, confidence in the implementation of security controls, and confidence in the security functions implemented by a product or system.

Information technology (IT) security evaluation and certification is a method of gaining confidence in the security functions implemented by the information, communication and technology (ICT) product or system. IT security evaluation and certification seeks to provide ground for confidence that the ICT product or system meets consumer's security needs, function as specified by the developers, possesses adequate guidance, operates securely, correctly built, and delivered securely as requested. It also assures that the ICT product or system has been tested thoroughly. However, it does not mean that the evaluated and certified product is totally free from exploitable vulnerabilities. There will remain a residual level of risk that exploitable vulnerabilities remain undiscovered in an ICT product's claimed security functionality. This residual risk is reduced as the certified level of assurance increases for such ICT products and systems.

The Perks of It All

For an ICT product developer, independent IT security evaluation and certification benefits them because they have developed a product that meets the consumer's requirements. Their certified products are marketable with the internationally recognised certification mark. Additionally, certification gives additional value

to the product because it provides comparability, which serves as a market differentiator against similar categories of products in the global ICT market. In addition, IT security evaluation improves the security engineering practices of the ICT products developers.

Nowadays, most of the countries in the world have developed their own policy on acquiring ICT products particularly those intended for the critical sectors. Certified products that have undergone the IT security evaluation using the international recognised standards and methodology such as Common Criteria (CC) or ISO/IEC 15408 are preferred. Hence, to fulfil this requirement, it is crucial for developers to ensure their ICT products are evaluated and certified.

As for consumers of ICT products who may have insufficient knowledge, expertise, or resources to critically evaluate security features of such ICT products, but do not wish to rely solely on the promises made by the developers, then these consumers may benefit from independent security evaluation.

Common Criteria provides a mechanism for ICT consumers to express their security needs to developers for various types of ICT products such as firewall, operating systems and others in an unambiguous manner. This is what we refer to as a Protection Profile (PP). A PP develop by a consumer define a minimum set of security functionality that must be implemented in a type of product. The PP needs to be evaluated and certified to ensure that it is complete, consistent, and technically sound and suitable for use as a template on which to build another PP or an ICT product.

During acquisition, consumers just need to check whether an ICT product has been successfully evaluated, and whether it is developed based on the consumer's requirements or PP. By using a PP, customers can make the right decision in procuring the right ICT product. It also builds consumers' confidence towards the quality and security of ICT products and systems through rigorous independent security evaluation.

Recognition is Key

Recognising the importance of security assurance of ICT products, and the benefits for local ICT developers and consumers, the Malaysian Government through CyberSecurity Malaysia, an agency under the purview of the Ministry of Science, Technology and Innovation (MOSTI), has established an evaluation and certification scheme, known as the Malaysian Common Criteria Evaluation and Certification Scheme or in short MyCC Scheme.

MyCC Scheme is a systematic process for evaluating and certifying the security functionality of ICT products and systems against ISO/IEC 15408 standard, which is also known as Common Criteria (CC). The mission of the scheme is to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria standard and to build consumers' confidence towards Malaysian Information Security products.

The MyCC Scheme is managed and administered by a Certification Body, a unit within Information Security Certification Body Department in CyberSecurity Malaysia, which is known as Malaysian Common Criteria Certification Body (MyCB). It provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against the Common Criteria standard.

In order to recognise the certificates and countries that use CC and Common Evaluation Methodology in their IT security evaluation and certification process, an arrangement called Common Criteria Recognition Agreement (CCRA) has been established between interested countries. Details of the arrangement can be found at www.commoncriteriaportal.org.

There are two types of memberships in this arrangement, Certificate Consuming Participant and Certificate Authorising Participant. Certificate Consuming Participant countries recognise the results of security evaluations and certifications from Certificate Authorising Participant countries. As of March 2012, there are 10 countries which have been recognised as Certificate Consuming Participant including Austria, Czech Republic, Denmark, Finland, Greece, Hungry, India, Israel, Pakistan and Singapore. ICT products certified under these countries are not yet recognised globally until they become Certificate Authorising Participant.

In Tandem with the Growth of Malaysia's ICT Initiative

Countries known as Certificate Authorising Participant are the countries that have IT security evaluation and certification scheme that will

be accessed by CCRA and compliant to CCRA requirements. The security evaluation and certification results are accepted and recognised by all CCRA participating countries. Certificate Authorising Participant countries consisting of Australia, Canada, France, Germany, Italy, Japan, Korea, Malaysia, New Zealand, Norway, Spain, Sweden, The Netherlands, Turkey, UK, and USA.

Malaysia (through CyberSecurity Malaysia) has been accepted as a Certificate Consuming Participant on 28 March 2007. After four years developing the scheme and its components under the 9th Malaysian Plan, on 27 September 2011, **Malaysia has been accepted as the CCRA Certificate Authorising Participant, the first for ASEAN and for a developing country.** With this recognition, Malaysia, through its MyCC Scheme, is able to issue Common Criteria certificates on ICT products.

Malaysia is now well positioned to gain access to international markets and will have immediate recognition across all CCRA member countries. This would further bolster Malaysia's competitiveness in quality assurance of information security based on the Common Criteria standard and build end-user confidence towards Malaysian information security solutions. Furthermore, Malaysia through MyCC Scheme can offer its services related to product security evaluation and certification to the world. This will definitely spur the growth of Malaysia's ICT industry.

Through the Second Economic Stimulus Package, the Malaysian Government has provided special grants for local companies to have their ICT products certified under the MyCC Scheme. More than 20 products have been certified including access control devices and systems, data protection, and a range of other systems.

Certification shows that the security functionalities of an ICT product or system have been evaluated based on defined scope and verified against developer's claims. Therefore, the deployment of certified products or systems can increase the confidence level of consumer security needs; function as specified; have adequate guidance; operate securely; built correctly; thoroughly tested and have reduced the potential for exploitable vulnerabilities. Both consumers and developers will benefits from this exercise. For more information, visit www.cybersecurity.my/mycc or email to mycc@cybersecurity.my.

Answers that local SME ICT developers need to know about:

Why should your ICT products and systems be evaluated?

As the demand for ICT products have been increasing, in some organisations, it is fast becoming one of the criteria in the procurement process. Your clients can benefit from independent security evaluation that provides a degree of assurance that an ICT product correctly performs its functions, while reducing the likelihood of security flaws being present. In addition to the benefits for all consumers of ICT products, ICT security evaluation delivers a number of strategic benefits for Malaysia as follows;

- Improve the competitiveness of Malaysian ICT products in a global ICT market
- Enhance Malaysia's reputation as a provider of ICT assurance services globally
- Gain access to international markets for Malaysia ICT products
- Enhance the security of Malaysian information infrastructure by making available a suite of independently secured ICT products
- Enhance the security of Malaysian ICT products through rigorous independent security analysis.

What type of product or system can be evaluated?

Any ICT product or system including software, hardware and firmware that claims to have a security capability can be evaluated like an operating system, database management system, firewall, communication system, smartcards, data separators, setc.

How much does it cost to get my product or system certified?

Cost for evaluation and certification can be divided into three:

- Evidence development - if the Sponsor is unable to develop the evaluation evidence, they need to acquire a consultant.
- Evaluation - cost for MySEF to perform the evaluation. This fee is dependent on the scope of the evaluation, the complexity of the product, the assurance level and

whether any evidence can be reused from previous evaluations of the same product.
- Certification - cost for MyCB to perform the certification. This fee can be found at www.cybersecurity.my/mycc

How much does it cost to get my product or system certified?

The evaluation duration is depending on the scope of evaluation from the Security Target (ST), assurance level, complexity of the product, Sponsor experience in supporting the evaluation and reuse of previous evaluation results.

Is the evaluation expensive and time-consuming?

Every sort of examination requires resources, but it is a common misconception that evaluation must always demand a great deal of resources. The cost lay predominantly with the developer. However, using a well-organised development process with the necessary regard to the security aspects, an improved level of security can be attained. The evaluation itself also costs money and takes time.

The two most important factors affecting cost and duration are:

- Evaluation assurance level
- The complexity of the product or system (with respect to security functions)

What evaluation documentation is required?

For Common Criteria evaluations, the developer is required to provide at least Security Target, design documentation, guidance documentation, configuration management documentation, and the IT product to be tested. Common Criteria Part 3 - Security Assurance Requirements details the documentation required for Common Criteria evaluations.

Can one use the Common Criteria without planning for an evaluation?

Yes, Part 2 of the CC (Functional Requirements) serves as an excellent basis for specifying functional requirements. Through the use of the component requirements in the CC, stringent and consistently formulated requirements are obtained. The CC also demonstrated the interdependence of the components, e.g. the requirement for logging would also normally demand confirmed timing information and information on user ID, etc.

How do you maintain certification for new products or systems?

Once a product or system has been successfully evaluated, Common Criteria and the alternative approaches operate assurance maintenance methodology for maintaining certification without having to undergo separate evaluations for each new version of software. The concept is to ensure that TOE continues to meet its security target as changes are made to the software or its environment.

Who do I talk to if I am considering evaluation?

A good place to start is with the Certification Body itself who will be pleased to give further advice. You may also wish to contact the MySEFs who will be willing to give appropriate advice.

How do I get a product evaluated?

The majority of activity in the early stagesof an evaluation takes place between the sponsor of the evaluation and the MySEF. The sponsor is responsible for providing the security target (ST) and the associated IT product that will become the target of evaluation (TOE). The sponsor must ensure that all essential documentation to be provided to the MySEF is available. The sponsor then contacts a MySEF to negotiate a contract and initiate the security evaluation.

Get your product evaluated and certified under the MyCC Scheme?

Evaluation services are conducted under contract by MySEFs; MyCB provides the certification oversight at minimal charge (certification fees) to the evaluation sponsors. To have a product evaluated, sponsors should contact MySEF. MySEF will assess the product and advise on its acceptance potential by providing the Evaluation Project Plan (EPP) and other supporting evidence to MyCB. Once accepted by MyCB, MySEF will host the evaluation kick-off meeting to execute the evaluation.

What is the expiry date of a certificate?

There is no limiting validity date on a certificate. It is a measure of the security of one version of a product, with regard to the state of the art on the date on which the product was certified.■

Training Programs

CyberSecurity MALAYSIA

Professional Development Schedules in CyberSecurity Malaysia Calendar 2013

No.		Program Duration	Standard Fees (RM)	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Fundamental/Introduction															
1	Critical Infrastructure Protection	2 days	1500		20-21					9-10					
2	Digital Forensics Essentials	3 days	1950				2-4						1-3		
3	Malaysia Common Criteria (MyCC 1.0) - Understanding Security Target, Protection Profile & Supporting Evaluation	1 day	790				2						21		
4	Introduction to ISO 27001 & ISO 27002:2005 Information Security Management System	1 day	650	8	6	4	5	6	10	5	26	2	3	11	9
5	Business Continuity Management for Essentials	1 day	1000		27		9		11		24			26	17
6	Data Encryption for Beginners	1 day	790		19						1				
7	Cryptography for Beginners	1 day	890			25						2			
8	CSM Security Essential Training	2 days	1590	9-10				28-29				10-11			
9	Google-Fu Power Search Technique	2 days	1400					20-21							2-3
10	Wireless Security	2 days	1350						19-20						5-6
11	Internet Banking Security	1 day	650						3				28		
12	Customize Training Package for groups and companies (Fundamental Courses Item 1-12)	1-5 days	Negotiable												
Intermediate															
1	Malaysia Common Criteria (MyCC 2.0) - Foundation Evaluator Training	3 days	3290				3-5						22-24		
2	Incident Response & Handling for Computer Security & Incident Response Team (CSIRTS)	3 days	3590			12-14						24-26			
3	Cryptography for Information Security Professional	3 days	3590			26-28						3-5			
4	ISO 27001 Implementation	3 days	3200	29-31	25-27	5-7	8-10	7-9	11-13	8-10	14-16	3-5	7-9	12-14	2-4
5	Incident Handling and Network Security Training (IHNS)	3 days	3590				15-18							11-14	
6	Network Security Assessment Training	2 days	1300					7-9					29-30		
7	Server and Desktop Security Assessment Training	2 days	1300						4-5						3-4
8	Web Application Security Assessment Training	1 day	750						18				2		
9	Digital Forensics for First Responder	4 days	3200				15-19						7-10		
10	Customize Training Package for groups and companies (Intermdiate Courses Item 1-8)	1-5 days	Negotiable												
Specialization/Specific Domains															
1	ISMS Internal Auditor Course (ISO 27001)	2 days	2850			26-27				30-31		9-10		26-27	
2	Digital Forensics for Law Practioner	2 days	1500					13-14				18-19			
3	Forensics on Internet Application	1 day	900						5					19	
Professional Certification															
1	Certified Information System Security Professional (CISSP) CBK Review Seminar	5 days	4705												
2	System Security Certified Practitioner (SSCP) CBK Review Seminar	5 days	4372												
3	Certified Secure System Lifecycle Professional (CSSLP)	5 days	4180									30 - 4			
4	Business Continuity Management Professional Certification (BCLE2000)	5 days	8900			4-8		6-10		1-5					2-6
5	ISO 27001 Lead Auditor (External Auditors)	5 days	5000	14-18	18-22	18-22	22-26	27-31	17-21	15-19	19-23	23-27	21-25	18-22	16-20

*Subject to change

Venue

CyberSecurity Malaysia, Training Centre, Level 4, Block C, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia. | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0844 (ISPD)

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4656

MS ISO/IEC 17025 TESTING SAMM NO. 456 (MySEF LABORATORY)

MSC MALAYSIA Status Company

CyberSecurity MALAYSIA
Agensi di bawah MOSTI

1 Malaysia
Rakyat Didahulukan, Pencapaian Diutamakan

MOSTI
Kementerian Sains, Teknologi dan Inovasi

VIRUS SENTIASA MENUNGGU UNTUK DIMUAT TURUN

Sentiasa bijak. Sentiasa selamat

layari www.CyberSAFE.my untuk maklumat lebih lanjut

cybersafe.malaysia

Pejabat Korporat:
CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8992 6888 | Fax: +603 8992 6841
Email: info@cybersecurity.my | Talian Khidmat Pelanggan: 1300-88-2999 | www.cybersecurity.my

csm-ace 2013

CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

13-14 November@The Royale Chulan, Kuala Lumpur

The 2013 Cyber Security Malaysia Awards, Conference & Exhibition (CSM-ACE 2013) is a public-private-partnership driven event to be held in The Royale Chulan, Kuala Lumpur, Malaysia from the 13th to 14th November 2013.

CSM-ACE 2013 gathers cyber security industry experts and community to exchange ideas on security management, policy and technology.

It is an annual industry gathering organised by CyberSecurity Malaysia, the National cyber security specialist centre under the purview of the Ministry of Science, Technology and Innovation (MOSTI).

"SECURING CYBERSPACE FOR ECONOMIC GROWTH"

Organised by:

CyberSecurity MALAYSIA

Endorsed by:

MOSTI Ministry of Science, Technology and Innovation

SKMM MCMC

Official Awards Evaluator:

Deloitte.

Gold Sponsors:

Deloitte. BAE SYSTEMS IBDO

Supporting Organisations:

National Security Council

(ISC)²

MIS TRAINING INSTITUTE

APCERT Asia Pacific Computer Emergency Response Team

ISF Information Security Forum

OBJECTIVES

- CSM-ACE aims to catalyse innovation and growth in the cyber security industry.
- CSM-ACE helps to educate information security managers and professionals, hence strengthen Malaysian self-reliance in terms of technology and human resources.
- CSM-ACE nurtures and inculcates cyber security awareness at National level.

"SECURING CYBERSPACE FOR ECONOMIC GROWTH"

AWARDS:

The Malaysia Cyber Security Awards are presented to distinguished individuals and organisations in recognition of their significant contributions to the cyber security, safety and well-being of the Malaysian cyberspace.

CONFERENCE:

The Conference provides a knowledge-sharing platform for cyber security industry experts and community to deliberate on the latest trends in cyber security. It is expected to attract 300 participants from the industry players, the academia, the government / regulatory bodies, and the Critical National Information Infrastructure (CNII) organisations.

EXHIBITION:

The CSM-ACE 2013 exhibition showcases trade and investment opportunities by assisting and allowing industry players to promote their products and services.

TARGET PARTICIPANTS

WHO SHOULD REGISTER

- Chief Executive Officers
- Chief Technology Officers
- Chief Financial Officers
- Chief Information Officers
- Chief Marketing Officers
- Chief Operating Officers
- Chief Security Officers
- Legal Officers
- IT Officers
- Senior Government Officials
- Management Consultants
- Industry Analysts
- Research Scientists
- Academicians
- Venture Capitalists

"SECURING CYBERSPACE FOR ECONOMIC GROWTH"

CSM-ACE 2013 PROGRAM

Day 1 : 13th November 2013

TRACK 1: Governance & Risk Management	
Time	**Topics**
0800 – 0850	Registration
0850 – 0900	Welcome Address by Emcee & Scene Setting
0900 – 0930	Presentation 1: *Cyber Security Threat Landscape* **Drew William,** President, Condition Zebra
0930 – 1000	Presentation 1: *Mobile Application Security - Understand Your Threats and Vulnerabilities* **Dr. Jeffrey Bannister,**Co-Founder, Orbitage
1000 – 1030	Networking Break
Opening Ceremony	
1030 – 1040	Welcome Address by Emcee, Negaraku & Doa Recital
1040 – 1045	Welcoming Remarks Speaker: **Dr. Amirudin Abdul Wahab,** CEO of CyberSecurity Malaysia
1045 – 1055	Opening Address Speaker: **Y.B. Datuk Dr. Ewon Ebin,** Minister, Ministry of Science, Technology & Innovation, Malaysia
1055 – 1100	Opening Ceremony & Launching Ceremony
1100 – 1130	Keynote 1: Speaker: BAE SYSTEMS DETICA
	Keynote 2: Speaker: **Lt. Gen.(R) Kenneth A. Minihan,** Paladin Capital Group
1130 – 1230	Plenary Session : *Cyber Security for Economic Growth: Malaysia Industry Going Global* Moderator: **Datuk Badlisham Ghazali,** CEO, Multimedia Development Corporation (MDec)
1200 – 1300	VIP Exhibition Walk-About & Opening Press Conference
1230 – 1400	Lunch & Networking
1400 – 1430	Presentation 3: *Social Media – Its Impact on Economic and Social Well-Being*
1430 – 1600	Panel Discussion 1: *Cyber Security as a Proxy for Trade Protection* Moderator: **Prof. Khaeruddin Sudharmin,** Managing Director, MRC Malaysia Panelist 1: **Thaib Mustafa,** Vice President, IT Strategy, Telekom Malaysia Panelist 2: **Pierre Noel,** Chief Security Officer, Microsoft Asia
1600 – 1630	Networking Break
1630 – 1700	Presentation 4: *Legal Challenges in Cyber Environment* **Dr. Hartini Saripan,** Ketua Pusat Pengajian Undang-Undang, UiTM Shah Alam
1700 – 1730	Presentation 5: *Being the Target of a Cyber Attack - Lessons Learnt* **Richard Watson,** Managing Director, Asia Pacific and Middle East BAE Systems Detica

TRACK 2: Technical	
Time	**Topics**
1400 – 1430	Presentation 6: *Inside Euro Grabber - Anatomy of a Malware* **Mohammed Fadzil Haron,** CTO, Accrete Technologies Sdn Bhd
1430 – 1600	Panel Discussion 2: *Surviving the Cloud Computing* Panelist 1: **Aloysius Cheang,** Managing Director APAC, Cloud Security Alliance Panelist 2: **Dr. Jamalul-lail Ab Manan,** Senior Director (Advanced Information Security Cluster), MIMOS Berhad Panelist 3: **Dr. Koji Nakao,** Information Security Fellow and Distinguished Researcher, NICT, Japan Panelist 4: **Salmah binti Khairuddin,** Perunding ICT Unit Perunding Pengurusan Pusat Data, The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)
1600 – 1630	Networking Break
1630 – 1700	Presentation 7: *PKI and Digital Certificates* **Lester Soo,** CTO, eVault Technologies SB
1700 – 1730	Presentation 8: *Being the Target of a Cyber Attack - Building an Effective Response* **Ganesh Narayanan,** Senior Regional Sales Manager, IXIA Breaking Point

Note : *The agenda is subject to change without prior notice*

CSM-ACE 2013 PROGRAM

Day 2 : 14th November 2013

TRACK 1: Governance & Risk Management	
Time	**Topics**
0900 – 0930	Presentation 9: *Cyber Security Through ROI Approach*
0930 – 1000	Presentation 10: *Financial Management of Cyber Risk - Mitigating Cyber Threats* **Steve Durbin,** Global Vice President Information Security Forum
1000 – 1030	Networking Break
1030 – 1100	Presentation 11: *Does Compliance to Standards Contribute to Your Bottomline?* **Douglas Brown,** Executive Director Risk Advisory Services, BDO Consulting Sdn Bhd
1100 – 1230	Panel Discussion 3: *Truth and Consequences: Clouds and Virtualization* Panelist 1: **Steven Rosen,** CTO, YTL Communications Panelist 2: **Myla Pilao,** Director ,TrendMicro
1230 – 1400	Lunch Networking & Exhibition
1400 – 1430	Presentation 12: *Conflict in Cyber Space – The Trend of Future Challenges*
1430 – 1600	Panel Discussion 4: *Social Media : New Reality or a Perception?*
1600 – 1630	Networking Break
1630 – 1700	Presentation 13: *The Internet Health Model for Cyber Security*
1700 – 1730	Presentation 14: *Mega-Trends in Information Risk Management for 2013 and Beyond: CISO Views*
	End of Track 1

TRACK 2: Technical	
Time	**Topics**
0900 – 0930	Presentation 15: *BYOD – Secure Zoning Between Enterprise and Personal Data on Mobile Devices* **Rozana Rusli,** Executive Director,KPMG Management & Risk Consulting Sdn Bhd **Meling Mudin,** Associate Director,KPMG Management & Risk Consulting Sdn Bhd
0930 – 1000	Presentation 16: *Embedded Systems Under Fire - Fault Injection on Secure Boot* **Zabri Adil,** Head, Digital Forensic, CyberSecurity Malaysia
1000 – 1030	Networking Break
1030 – 1100	Presentation 17: *Wireless Security Issues, Known Vulnerability, Nothing Been Done* **Brandy Rotters,** Chairman, Air Patrol
1100 – 1230	Panel of Discussion 5: *The Cyber Security Industry: Survival in the Age of Cyber Warfare* Moderator: **Zahri Yunos,** COO, CyberSecurity Malaysia Panelist 1: **Dato' Seri George Chang,** Regional Director, Fortinet Panelist 2: **Peter Lilley,** Australasian Region Director, BAE Systems Detica Panelist 3: **Vikas Desai,** Advisory Consultant, RSA Panelist 4: **Lt. Col. (R) Asmuni Yusof,** Director of Malaysian Communications and Multimedia Commission (MCMC)
1230 – 1400	Lunch Networking & Exhibition
1400 – 1430	Presentation 18: *Big Data Analytics – Take it to the Next Level in Building Innovation, Differentiation and Growth* **Neal Meikle,** Associate Director, Forensic Technology, PwC
1430 – 1600	Panel of Discussion 6: *Security at the Industrial Control System – The Bigger Picture.* Moderator: **Ir. Md. Shah Nuri Md. Zain,** Under Secretary Cyber & Space Security Div.,National Security Council Prime Minister's Department
1600 – 1630	Networking Break
1630 – 1700	Presentation 19: *Countering DDOS Attack Against Layer 7 : A Case Study* **Oliver Kwan,** VP for Prolexic in Asia,Prolexic
1700 – 1730	Presentation 20: *IPv6 -The Naked Truth of Migration, Implementation and Usage* **Dr. Omar Amer Abuuabdalla,** CTO, IPv6 Global Sdn Bhd
	End of Track 2

Note : *The agenda is subject to change without prior notice*

INVITED SPEAKERS

Drew William
President, Condition Zebra

Dr. Jeffrey Bannister
Co-Founder, Orbitage

Lt. Gen.(R) Kenneth A. Minihan
Managing Director, Paladin Capital Group

Datuk Badlisham Ghazali
CEO, Multimedia Development Corporation (MDec)

Prof. Khaeruddin Sudharmin
Managing Director, MRC Malaysia

Thaib Mustafa
Vice President of IT Strategy, Telekom Malaysia

Pierre Noel
Chief Security Officer, Microsoft Asia

Dr. Hartini Saripan
Ketua Pusat Pengajian Undang-Undang, UiTM Shah Alam

Richard Watson
Managing Director, Asia Pasific and Middle East,
BAE System Detica

Steve Durbin
Global Vice President, Information Security Forum (ISF)

Douglas Brown
Executive Director Risk Advisory Services,
BDO Consulting Sdn Bhd

Dr. Suhazimah Dzazali
IT Security Consultant, MAMPU

Steven Rosen
Chief Technology Officer, YTL Communications

Myla Pilao
Director, TrendMicro

Mohammed Fadzil Haron
Chief Technology Officer, Accrete Technology

Aloysius Cheang
Managing Director APAC, Cloud Security Alliance

Dr. Jamalul-lail Ab Manan
Senior Director, Advanced Information Security Cluster,
Information Security Fellow and Distinguished Researcher
MIMOS

Dr. Koji Nakao
Information Security Fellow and Distinguished Researcher,
NICT, Japan

Salmah binti Khairuddin
Consultant, ICT Unit Perunding Pengurusan Pusat Data,
MAMPU

Dr. Chang Cheong Swee
Director, Heitech Managed Services

Lester Soo
Chief Technology Officer, eVault Technologies SB

Ganesh Narayanan
Senior Regional Sales Manager, IXIA Breaking Point

Ruzana Rusli/ Meling Mudin
Executive Director/ Associate Director, KPMG

Zabri Adil
Head, Digital Forensic, CyberSecurity Malaysia

Brandy Rotters
Chairman, Air Patrol

Zahri Yunos
Chief Operating Officer, CyberSecurity Malaysia

Dato' Seri George Chang
Regional Director, Fortinet

Peter Lilley
Australasian Region Director, BAE System Detica

Vikas Desai
Advisory Consultant, RSA

Lt. Col.(R) Asmuni Yusof
Director, Malaysian Communications and Multimedia Commission (MCMC)

Neal Meikle
Associate Director, Forensic Technology, PwC

Ir. Md. Shah Nuri Md. Zain
Under Secretary Cyber & Space Security Division, National Security Council

Oliver Kwan
Vice President Asia, Prolexic

Dr. Omar Amer Abuuabdalla
Chief Technology Officer, IPv6

CSM-ACE 2013 CONFERENCE FEES

Registration	Fee (RM)
Early Bird Registration within 16 May 2013 – 31 July 2013	RM 699 per person
Normal Registration within 1 August 2013 – 8 November 2013	RM 899 per person

HRDF CLAIMABLE

CSM-ACE 2013 CONFERENCE REGISTRATION

Register now at www.csm-ace.my/register.html. For assistance or more information, please contact our event organiser:

Tel: +603 8946 0999 Fax: +603 8946 0831 E-mail: secretariat@csm-ace.my

AWARD CATEGORIES

MALAYSIA CYBER SECURITY AWARDS

- CYBER SECURITY PROFESSIONAL OF THE YEAR
- CYBER SECURITY COMPANY OF THE YEAR
- CYBER SECURITY ORGANISATION OF THE YEAR
- CYBER SECURITY EDUCATION & TRAINING PROVIDER OF THE YEAR
- CYBER SECURITY OUTREACH PROVIDER OF THE YEAR
- CYBER SECURITY PROJECT OF THE YEAR
- CYBERSAFE AMBASSADOR OF THE YEAR

Official Awards Evaluator:

Deloitte.

For more information about CSM-ACE 2013, go to **www.csm-ace.my**

For more information about CyberSecurity Malaysia, please go to www.cybersecurity.my

Corporate Office:
CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8992 6888 | Fax: +603 8992 6841
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my

CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

Safeguard Your Money !

AGAINST

[SMISHING]
SMS SCAMS

[VISHING]
CALLER SCAMS

[PHISHING]
EMAIL SCAMS

If you receive this, immediately contact your bank!

logon to www.CyberSAFE.my to find out more

cybersafe.malaysia

Corporate Office:
CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8992 6888 | Fax: +603 8992 6841
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my

CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

Account Balance:
RM 0.00

According to the experts, if you routinely check your bank balance over public networks, the odds are good that eventually you're going to run into someone who's looking for people who do just that.

Be smart. Be safe

logon to www.CyberSAFE.my to find out more

cybersafe.malaysia

Corporate Office:
CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8992 6888 | Fax: +603 8992 6841
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my