

# eSecurity

www.cybersecurity.my

The First Line of Digital Defense Begins with Knowledge

Vol 37 - (2/2014)

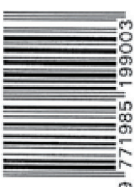


How To Overcome the Website affected by Cracker  
Security Threats Overview in 4G LTE Mobile Networks  
Trend Analysis on Fraud Purchase in 2014

*"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**.



**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](mailto:info@cybersecurity.my)

Customer Service Hotline:  
1 300 88 2999  
[www.cybersecurity.my](http://www.cybersecurity.my)

An agency under





## ***A MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA***



Welcome to the 37th Edition of the E-Security Bulletin!

We hope the knowledge imparted through our numerous articles would in some way help in raising the adoption of essential cyber security practices among Internet users.

It is very important for us to continuously preach and share valuable knowledge about positive and ethical ways of using the Internet, especially on social media platforms. This is vital as in the long run, we would like to ensure our Digital Citizens maintain an ethical and courteous culture that Malaysians are known for globally.

We believe positive societal culture like working together to imagine a better future and collaborating across traditional silos to design that future together through the power of story-telling and sharing should remain intact no matter how high we move up the rank in terms of socio-economy and digital sophistication.

Thank you for your continuous support.

**Dr. Amirudin Abdul Wahab**

Chief Executive Officer, CyberSecurity Malaysia

## **EDITORIAL BOARD**

### **Chief Editor**

Dr. Zahri bin Yunos

### **Editor**

Lt. Col Mustaffa bin Ahmad ( Retired )

### **Internal Reviewers**

1. Dr. Solahuddin bin Shamsuddin
2. Col. Sazali bin Sukardi (Retired)
3. Pn. Sabariah binti Ahmad
4. Pn. Zaleha binti Abd Rahim
5. En. Rosly bin Yahil
6. En. Ruhama bin Mohammed Zain
7. Pn. Ramona Susanty Ab Hamid
8. Pn. Azira Abd Rahim

### **Designer & Illustrator**

1. Zaihasrul bin Ariffin
2. Nurul Ain Zakariah

### **READERS' ENQUIRY**

Outreach and Corporate Communications, Level 5, Sapura@Mines, No.7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan

### **PUBLISHED AND DESIGNED BY**

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



## TABLE OF CONTENTS

1. Staying Away from Spam .....	1
2. ISO/IEC 27001 A Clause A Day: Clause 7.2 Competence.....	3
3. Capacity Building for the Development of National Cyber Security .....	4
4. Updated Personnel Records – Is It Necessary?.....	6
5. Cyber Drill Exercise among OIC Networks in Fight against Cyber-Attacks .....	8
6. Retinal Scanning VS Iris Recognition .....	11
7. Security Threats Overview in 4G LTE Mobile Networks .....	13
8. Why Social Networking Sites? .....	16
9. The History of Cryptography.....	19
10. INFOGRAPHIC: PKCS - Public Key Cryptography Standards.....	21
11. Email Account Compromise and Security Best Practices: A Case Study.....	25
12. Automated Incident Response Process .....	30
13. What we can learn from Online Fraud in 2014 .....	31
14. The Rise of Cyber Espionage In The Digital World.....	33
15. MH370 Cyber Crisis Management .....	36
16. Documented Information in ISO/IEC 27001:2013 Information Security Management Systems (ISMS) .....	44

# Staying Away from Spam

By | Noraziah Anini Mohd Rashid

## Why Spam is still an issue?

It might be 2015 but spam mails still exist and remain an issue. Research by SecureList (Figure 1) shows a high percentage of spam mails throughout Q1 of 2014.



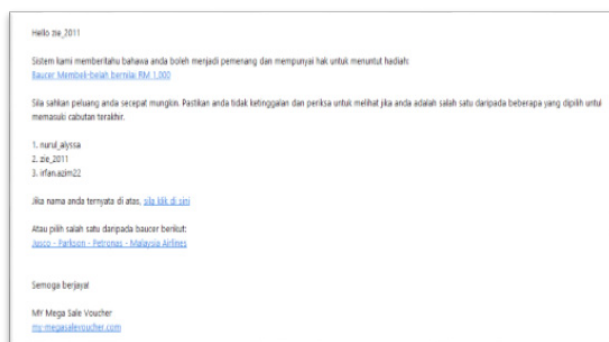
Figure 1: Statistic for Quarter 1 2014 by SecureList.com

Spam can come from any sector or industry usually for advertising purposes. They can also disguise as scam, manipulating receivers for illegal profit-making. While

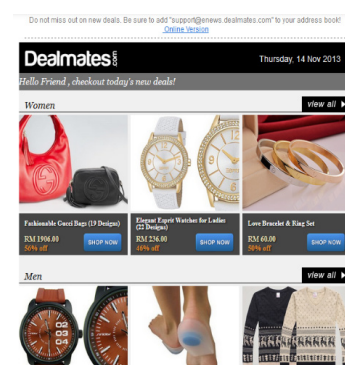
it. While there are many solutions and tools introduced to end-users, the best is self-awareness and constant reminders to secure personal information. It is as simple as paying attention to details when changing passwords, giving out bank account numbers and transferring money online.

## How to identify Scammers & Spammers?

Before it was called 'Spam', businesses sent emails to businesses or individuals identified as potential clients, with intent to advertise their products or services. They were not malicious in their intent. A person can receive these emails through newsletter subscriptions. In some cases, the recipient might have agreed to receive updates on products or solutions advertised online. It is important to note that scam emails can appear as spam. The only difference is the mode of operation, the scammers intend to steal. Figure 2 explains the difference between spam and scam emails. Scam emails



Scam mail



Spam mail

Figure 2: Scam mail vs Spam mail

this issue has been discussed time and again, there is no one easy solution to completely and permanently prevent

usually provides recipients "too good to be true" deals and requires them to

2

respond immediately or click on the links provided.

Some scam cases require recipients to disclose their bank account and credit card details. Scam mails can also disguise as letters from troubled entities or individuals from Middle Eastern countries, asking for recipients' help with their financial situation. This would require online money transaction between the recipient and scammer. These emails would induce recipients' sympathy and ask for their kindness. Although email scams are widely known, there are people who are still cheated for their money.

### Smart Tips to avoid Scammers

The best practice is not to reply to these emails or click any of the links as this may cause malware infection to receiver's machine. Unsubscribing to the email may draw scammers' attention further. They would know that the account is active and will continue sending scam emails. Instead, recipients can configure their spam setting to filter these emails. Recipients should avoid money transaction with unverified sources, especially providing them access to personal information. If unsure, recipients should call the company to verify the details of the transaction.

Awareness is important. Recipient can stay informed by keeping up with the latest online security news and developments. One of the simplest and easiest ways to identify spam is by using Google's search engine. Searching for the sender's email address online can help recipients to determine its validity. Sometimes paying close attention to the email address would do. For example, a Jusco promotion that came through from reply@mx249.wonderiswonderful.com. Legitimate organisations would only use email addresses with accurate company name or representation.

To avoid spams or scams, online users should avoid sharing their email addresses on public forums or websites. Online users should also change their setting to hide their email addresses when creating accounts on websites. Spammers may send an email asking the recipient if he or she is interested in the products or services they have just viewed. The best approach is to ignore these emails.

Malaysians who come across scams can lodge complaints to the Malaysian Communication and Multimedia Commission (MCMC). ■

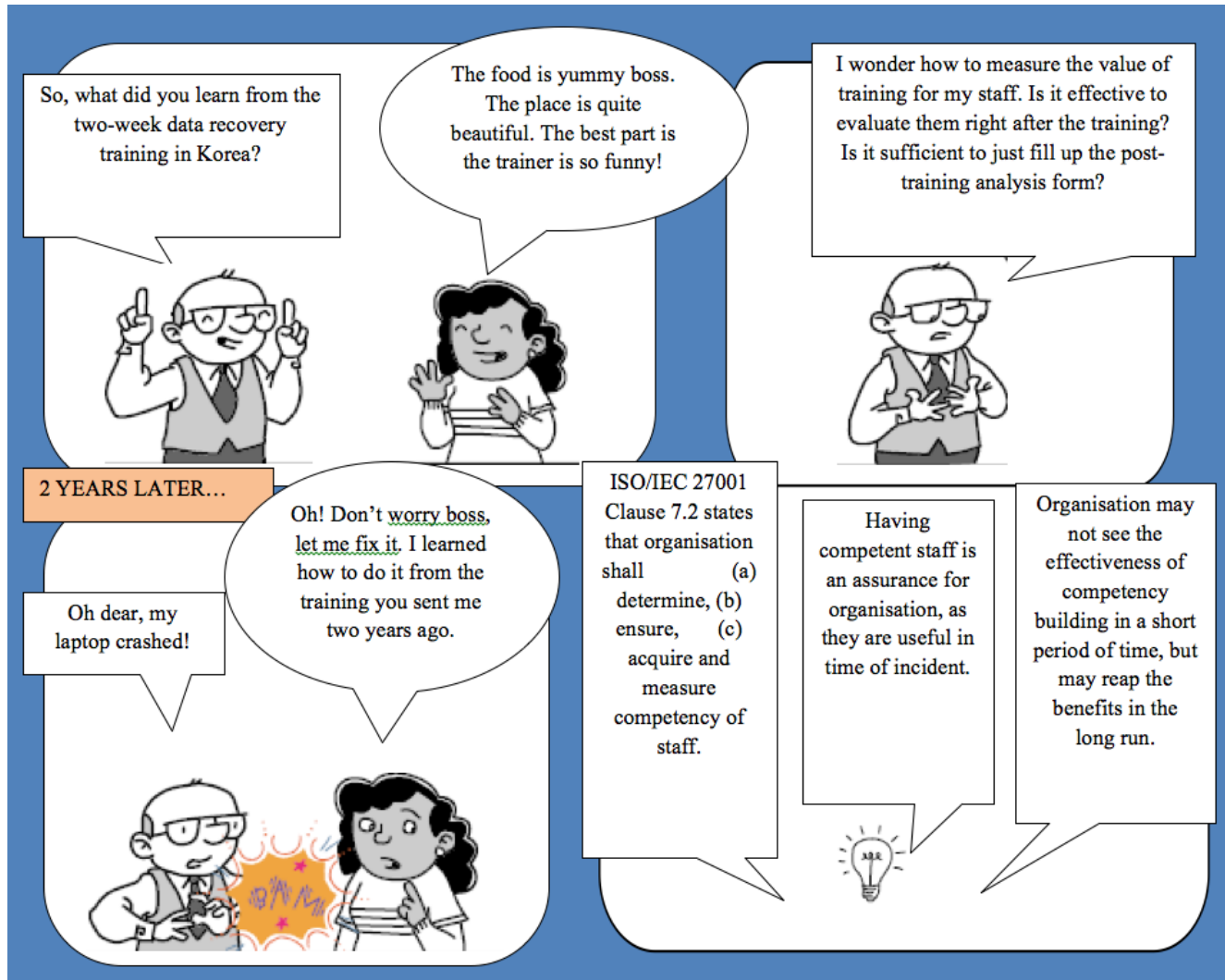
### References

1. *Malaysian Communications And Multimedia Commission (MCMC) | Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) - Regulatory Approach to Spam.* (n.d.). Retrieved November 11, 2013, from <http://www.skmm.gov.my/FAQs/SPAM/Regulatory-Approach-to-Spam.aspx>.
2. *Spam Trends and Statistics Report Q2 2013 | Kaspersky Lab | Kaspersky Lab US.* (n.d.). Retrieved November 14, 2013, from <http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q2-2013#.UoQUIOJj560>



# ISO/IEC 27001 A Clause A Day: Clause 7.2 Competence

By | Razana Md Salleh



## Summary

While employers understand the importance of staff competency building, they may not necessarily see the benefits of training right away. This unnecessary stress can be avoided with post-training evaluation and even, candid conversations on the training. ■

# Capacity Building for the Development of National Cyber Security

By | Hafiz Ambar, Rahayu Azlina Ahmad, Siti Hazwah binti Abd Karim

The world is reliant on the Internet these days, especially with the many new and exciting digital offerings by governments, corporations, businesses and individuals. This rapid digital development also attracts cybercrimes. This has raised concerns among the governments, organisations, groups and individuals entrusted in the cyber security space. It also calls for capacity building and paradigm shifts in the legislations involving cyber security. There is a growing need for cyber security professionals with the right skills, knowledge and expertise; and establishment of specific authorities to oversee and steer cyber security initiatives and efforts.

## The Importance of Capacity Building

Governments, international organisations and the private sector have been placing importance in building their cyber security capacities. Cyber-attacks on Estonia, Georgia and Iran serves as a grim reminder to the rest of the world on the potential damages from cyber-threats and its impact to the economic, political and social state of nations.

Technology is transforming the way nations and societies work, interact and transact. Governance systems are keeping pace with the cyber space development that usually requires secure infrastructures. Building capacity in the cyber space is not only about the security, but also end-user demand for digital governance and delivery of services like e-Government facilities, e-Health provisions, online-based education systems, online banking services and more.

## Capacity Building Measures

Strategic capacity building measures can only be effectively and properly implemented at the topmost of the governance hierarchy, i.e. the government. These are three crucial capacity building measures:

### 1. Legal Measures

Legislation plays a critical role in providing a harmonised framework accepted by all relevant parties. There is a need for adequate legislations in place – for example, the enactment of a dedicated act of law that caters to local cyber security issues and harmonises with other similar international legislations as well. This facilitates positive international efforts in cyber security and combating cybercrime.

### 2. Technical Measures

Entities without adequate capabilities to identify cyber-related issues will be vulnerable to cyber threats. Technology companies need to be at the forefront of cyber space – gluing the pieces together. Concerned nations need to adopting security measures and accreditation schemes for software applications and systems.

It is important to establish a national entity, governed by a national framework, dedicated to cyber-related issues on a nationwide level over the Critical National Information Infrastructures (CNIIs). For example, the national Computer Incident Response Team (CIRT), Computer Emergency Response Team (CERT) or the Computer Security Incident Response Team (CSIRT).

### 3. Organisational Measures

Organisational measures are essential for a successful implementation of a national strategy accompanied and an all-inclusive plan to govern the implementation, delivery and measurement aspects. A national strategy can match commitments and efforts by cyber security stakeholders and players. An underlying national strategy is required for the creation of related sub strategies, structures, institutions, roles and more, necessary for the development of national capabilities.

## Capacity Building General Framework

The International Telecommunication Union (ITU) in its Global Strategic Report argued

that capacity building to promote cyber security remains complex and considered a technical, specialised fields. The ITU has also proposed a capacity building framework to promote cyber security (see Figure 1).

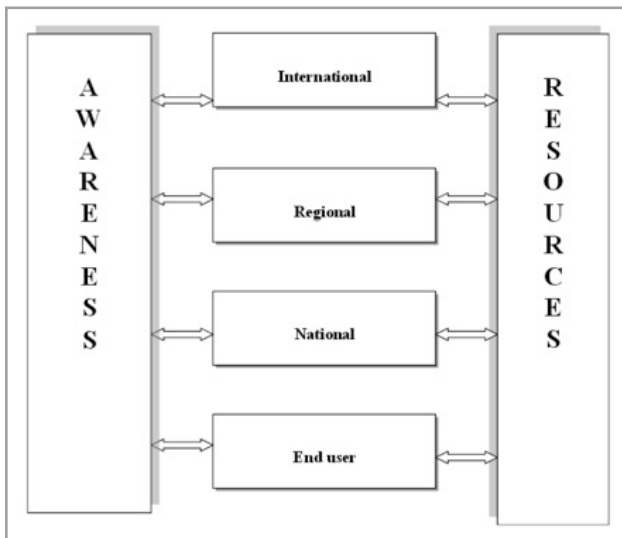


Figure 1: Capacity Building General Framework

The framework was based upon the raising awareness levels and the availability of resources. Raising awareness is important to ensure a functioning and sustainable framework for international cooperation to safeguard the cyber space.

## Cyber Skills Capacity Building

*"Organisation doesn't really accomplish anything. Plans don't accomplish anything, either. Theories of management don't much matter. Endeavours succeed or fail because of the people involved. Only by attracting the best people will you accomplish great deeds" -- former US Secretary of State, Collin Powell*

Cyber skills capacity building is the epitome of any established entity that can move with the evolving cyber security industry. This requires an adequate number of cyber security professionals to sustain the efforts and to meet the goals of their cyber security strategies.

A well-planned training roadmap can produce highly-skilled professionals and identify the right candidates for specialisation paths at an early stage. Stakeholders input must be considered when formulating and deciding the training roadmap.

The CSIRT is a platform where professionals can hone their skills and enrich their experiences by dealing with real-life cyber security issues, incidents and escalations.

It is important to foster international collaborations with other CSIRTs and organisations all around the world. Discussions, exchange of information and ideas through forums, seminars, conferences and attachment programmes will benefit all.

The government can also begin incorporating cyber security lessons into school curricula to nurture cyber-awareness among the young generations way they choose, the nation will only end up with a society that are fully aware of the perils of the cyber space and ideally can also protect themselves, thanks to the cultivated good cyber security practices over the years prior.

The Internet Society's anticipates three billion Internet users by early 2014. Malaysians require capacity building efforts properly in place to accommodate for such a heavily-connected world.

## References

1. *Cyber Capacity Building in Ten Points*. European Union Institute for Security Studies. Retrieved from [http://www.iss.europa.eu/uploads/media/EUISS\\_Conference-Capacity\\_building\\_in\\_ten\\_points-0414.pdf](http://www.iss.europa.eu/uploads/media/EUISS_Conference-Capacity_building_in_ten_points-0414.pdf)
2. *Cybersecurity Readiness Study*. Ponemon Institute. Retrieved from <http://www.hp.com/h20195/v2/GetDocument.aspx?docname=4AA2-9963EEW>
3. *Global Cybersecurity Index: Conceptual Framework*. International Telecommunication Union & ABI Research. Retrieved from [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI\\_Conceptual\\_Framework.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Conceptual_Framework.pdf)
4. *Internet Society Global Internet Report 2014: Open and Sustainable Access for All*. Internet Society. Retrieved from [http://www.internetsociety.org/sites/default/files/Global\\_Internet\\_Report\\_2014\\_0.pdf](http://www.internetsociety.org/sites/default/files/Global_Internet_Report_2014_0.pdf)
5. *ITU Global Cybersecurity Agenda (GCA) A Framework for International Cooperation in Cybersecurity*. International Telecommunication Union. Retrieved from [http://intgovforum.org/Substantive\\_2nd\\_IGF/ITU\\_GCA\\_E.pdf](http://intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf)
6. *ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) Global Strategic Report*. International Telecommunication Union. Retrieved from [http://www.cybersecurity-gateway.org/pdf/global\\_strategic\\_report.pdf](http://www.cybersecurity-gateway.org/pdf/global_strategic_report.pdf)
7. Probert, David E. (2010). *Cybersecurity Capacity Building & International Collaboration*. International Telecommunication Union. Retrieved from [http://www.itu.int/ITU-D/cyb/app/docs/Salta\\_101101/Session4/Probert\\_Presentation.pdf](http://www.itu.int/ITU-D/cyb/app/docs/Salta_101101/Session4/Probert_Presentation.pdf)



# Updated Personnel Records – Is It Necessary?

By | Norlela binti Mohamed Yunan

Employees are the biggest asset of any company. Proper management of personnel records is important to ensure updated information are available to make a right decision and to protect both rights of the state and individuals. The information held in personnel records is usually used to make decisions about suitability for promotion, transfer or in some cases disciplinary action and termination. The records also will be used to determine pay and other benefits for the employee and dependent family members.

## What Belongs In A Personnel Record?

Personnel records document stores the contractual relationship between employer and employee and the employee's career history in the organisation. Information that is sensitive and personal will be categorised as Secret or Private and Confidential and labelled accordingly. These type of information are accessible by authorised personnel only. Information kept in the Personnel Records includes the following:

- The job application and resume of the employee
- Letter of Appointment to the employee
- A job description for the position that the employee holds
- Academic Qualification or acquisition of new educational or professional qualifications
- Emergency contacts or next-of-kin contact number
- Beneficiary information
- Competency / Expertise Areas
- Professional Membership
- Publication / Presentation
- Career History or previous employment details
- Achievements
- Certifications
- Training History
- Medical report
- Background check
- Periodic performance evaluations
- Any forms relating to benefits that the employee enjoys
- Evidence records and notes of any disciplinary proceedings taken against the employee
- Any employment contracts, written agreements, or acknowledgments between

the employee and the employer (e.g. Non-Disclosure Agreement, Code of Conduct)

- Any documents that relate to employee mobility (e.g. transfer, re-designation, promotion, resignation, termination etc.)

## Where Are They Kept?

Personnel records can be maintained either in paper form, or electronically. Traditionally can be extremely time consuming especially when it comes to extracting data. With technology and globalisation, many organisations have moved from paper-based systems to computer-based systems. They deploy Human Resource Information Systems (HRIS) with various functions to simplify tasks. Computerised personnel record system allows easy analysis for reporting purpose.

## Who Is Responsible?

The HR department is responsible to maintain records of each employee's work history in the organisation. However, some organisations allow the employees to key-in, review and update his/her personal profile electronically via Employee Self Service (ESS) system. HR will receive notification on the changes. Employees will have to submit supporting documents to HR for verification.

## Why Is It Crucial To Update Data?

Any record keeping system is only useful if it fulfil certain principles. It must be:

- Up-to-date
- Accurate and reliable
- Confidential with regards to personal details
- Adaptable, so that it can cater for future developments and changes
- Economical in its introduction, use and maintenance

Employers have the option to implement the security management standard i.e. ISO/IEC 27001 and will need to comply with the standard's security requirements. The Information System Management Systems (ISMS) needs to achieve an overall information security assurance through the preservation of the following:

- Confidentiality: Assurance that information is shared only among authorised persons or organisations
- Integrity: Assurance that the information is authentic, complete and can be relied upon to be sufficiently accurate for its purpose
- Availability: Assurance that the systems responsible for delivering, storing and processing information are readily accessible when needed, and/or by those who need them

In addition, employers also need to address the following implications:

- business continuity
- minimisation of damages and losses
- competitive edge
- profitability and cash-flow
- respected organisation image
- legal compliance

## Business Continuity Management (BCM)

Organisations may encounter the possibility of disruptive and unplanned events that have impacts on the business operations. Examples of these events are natural disaster, power outages, cyber-attacks, security breaches, pandemic illness, loss of key staff etc. Although it is impossible to predict crises, it is possible to prevent them from becoming a disaster or reduce the impact, so organisation can continue its operation with minimal disruptions.

HR plays a crucial role in the organisation's preparations and responses to crisis. When a crisis occurs, HR will take the lead to resolve any human issues and protect the welfare and safety of the affected employees. Accurate and complete personnel records are invaluable source of information which will assist HR to respond readily before, during and after a crisis. For instance, if a building collapses from a fire and employees are trapped in the building, HR will need to refer to the employees' personnel records to contact and notify the employees' next-of-kin and the insurance agency, if necessary. The records are also useful for HR to identify employees who have First Aid skills that would benefit the situation.

Having accurate personnel records is crucial for complying with the legal requirements:

Section 61 of Employment Act 1955 (Part XIII: Registers, Returns and Notice Boards) mandates:

*"(1) Every employer shall prepare and keep one or more registers containing such information regarding each employee employed by him as may be prescribed by regulations made under this Act.*

*(2) Every such register shall be preserved for such period that every particular recorded therein shall be available for inspection for not less than six years after the recording thereof".*

The particular points to note in the Personal Data Protection Act (PDPA) 2010 are:

### Data Integrity Principle

*11. A data user shall take reasonable steps to ensure that the personal data is accurate, complete, and not misleading and kept up-to-date by having the purpose, including any directly related purpose, for which the personal data was collected and further processed.*

### Access Principle

*12. A data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this Act.*

Periodic maintenance of the personnel records will ensure all important documents and information are complete, accurate, updated and easily accessible by an authorised personnel at any time. Employees must be reminded to review and update their particulars as and when there are changes to their profile. Updated information will help the organisation in making efficient decisions, as well as to protect the rights of the organisation and individual employees.

## References

1. [http://www.academia.edu/3159363/THE\\_ROLE\\_OF\\_PERSONNEL\\_RECORDS\\_IN\\_PROTECTING\\_THE\\_RIGHTS\\_OF\\_THE\\_CITIZENS](http://www.academia.edu/3159363/THE_ROLE_OF_PERSONNEL_RECORDS_IN_PROTECTING_THE_RIGHTS_OF_THE_CITIZENS)
2. [http://en.wikipedia.org/wiki/Information\\_security\\_management\\_system](http://en.wikipedia.org/wiki/Information_security_management_system)
3. <http://humanresources.about.com/>
4. <http://www.managementstudyguide.com/personnel-records.htm>
5. <http://www.infoentrepreneurs.org/en/guides/crisis-management-and-business-continuity-planning/>
6. <http://www.epa.gov/records/tools/vital.htm>
7. <http://www.wbiconpro.com/432Rupak.pdf>
8. [http://www.arimi.org/hr\\_contribution\\_to\\_crisis\\_management](http://www.arimi.org/hr_contribution_to_crisis_management)
9. <http://www.shrm.org/research/articles/articles/documents/1205rquartpdf.pdf>
10. <http://www.isoqsltd.com/iso-certification/iso-27001/>
11. Malaysia Employment Act 1955
12. Personal Data Protection Act 2010 LAW OF MALAYSIA Act 709
13. PWC | Personal Data Protection Act (PDPA) 2010: "Data Protection: It's getting personal"
14. [www.irmt.org/documents/educ\\_training/.../IRMT\\_personnel\\_recs.doc](http://www.irmt.org/documents/educ_training/.../IRMT_personnel_recs.doc)

# Cyber Drill Exercise among OIC Networks in Fight against Cyber-Attacks

By | Hafiz Ambar, Rahayu Azlina Ahmad, Siti Hazwah binti Abd Karim

## OIC Networks Fight against Cyber-attacks

The Organisation of The Islamic Cooperation-Computer Emergency Response Team (OIC-CERT) provides a platform for OIC member countries to explore and develop collaborative initiatives and partnerships in cyber security. It aims to strengthen their self-reliance in the cyber space.

The OIC-CERT comprises of 23 CERTs and cyber security-related agencies from 19 OIC member countries. The organisation has been working hard to forge partnership and build strategic alliances with OIC member countries and other CERTs to mitigate cyber threats which includes annual cyber drill exercises. The first OIC-CERT Cyber Drill began in February 2012, followed by its participation in the Asia Pacific Computer Emergency Response Team (APCERT) Drill in January 2013 and most recently, in February 2014.

## Sophistication behind Cyber Incidents

The increase in cloud and mobile computing has introduced more complex cyber-attacks. These attacks have been attempted on governments, businesses and individual users, more than ever before. Some experts even argue that it is no longer about whether an attack is going to happen, but rather when it is going to happen.

Nowadays, sophisticated attacks are taking place in the IT infrastructures. Attackers continuously refine their methods to beat any systems' security improvements applied. They consolidate assets to create global networks that can support coordinated criminal activities. There has also been a rise in cyber spying and targeted attacks on organisations and individuals.

The other trend making headlines is the continuous mapping of targeted networks and probing for the systems' weaknesses and vulnerabilities. Malware propagation through website intrusions and spam are on the rise, as well as large-scaled Structured Query Language (SQL) Injection attacks. Phishing cases are increasing, particularly through the fast flux method and domain phishing.

## Preparing for the Worst: Cyber Drill Exercises

The cyber drill exercises are important in enhancing capabilities, improving preparedness and communication, and encouraging collaboration of the participating CERTs and economies. These exercises help develop the capabilities of OIC member countries to protect their Critical National Information Infrastructures (CNIIs). They also help acquire and enhance the capacity to protect against cyber threats. Participation in the drills will enhance a country's expertise and experiences in cyber security, reduce the skills gap and allow sharing of valuable knowledge and experience with participants from other member countries.

These exercises also improve the preparedness of OIC countries in the identification, prevention, response and resolution of cyber security incidents. The drills provide the opportunity to train professionals from participating economies on how to handle cyber-related incidents according to internationally accepted standards and best practices, and to effectively collaborate with others within the same ecosystem and area of interest.

These drill exercises emphasise on how effective communication and collaboration between governments can succeed in the fight against cyber threats and crime. Participants from diverse economies will be



aware of cross-border cooperation in cyber space, in their response to developing countries' needs. Participants can test the existing communication capability to gauge the actual ability to communicate and relay information across physical borders and different time zones. These exercises enable effective decision-making and help coordinate swift response that can assist other economies to mitigate cyber-attacks.

## How does it work?

During a cyber drill exercise, participating teams will be divided into two roles, the player and the observer. The player is tasked to execute the 'incident handling' process, analyse threats and mitigate simulated cyber-attacks, while the observer is required to perform communication roles that assists the player in mitigating the simulated attacks. The drill scenarios are created by cyber security experts and coordinated by the organiser.

## The Issue with Cyber Drill Exercises

Organising a cyber drill exercise is a huge challenge that requires meticulous planning. The organiser is required to outline the exercise objectives. They will need to decide the size of the drill (manpower, systems, networks etc.), the type and amount of technical hands-on required and the preparation/training required for the participants (and the organising committee) for a smooth-sailing drill.

It is also a challenge to get the support and participation of major organisations such as banks and government agencies – the biggest targets in cyber-attacks. While they understand the benefits of cyber drill exercises, it is complicated to plan and execute a hands-on simulated cyber-attacks because their operations are much larger and dispersed. They also find it difficult to conduct cyber drill exercises over concerns that they may affect their day-to-day operations.

Another challenge is to simulate what is considered as a typical cyber-attack. There are also concerns that drills will be more

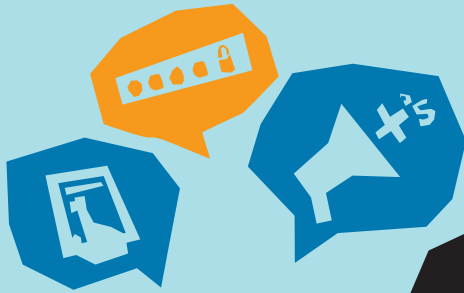
focused on operational issues (e.g. business continuity, recovery of systems and services, media handling etc.) and not on the cause of attacks and how to stay protected. Even worse, there are also concerns of drill "data" accidentally getting out of hand. For example, the malware or virus intended for the drill is accidentally leaked out of isolated network and into live systems.

## Conclusion

Given the borderless nature and dangers of constantly evolving cyber-attacks, it is vital that every CERT and CIRT continues to share their knowledge, information and experience with one another to successfully mitigate cyber threats.

## References

1. APCERT drill on countering cyber attacks. *Sunday Observer*. Retrieved from <http://www.sundayobserver.lk/2014/03/02/fin10.asp>
2. APCERT Embarks on Global Coordination to Mitigate Large Scale Denial of Service Attack. Asia Pacific Computer Emergency Response Team. Retrieved from [http://www.apcert.org/documents/pdf/APCERTDrill2013PressRelease\\_AP.pdf](http://www.apcert.org/documents/pdf/APCERTDrill2013PressRelease_AP.pdf)
3. APCERT Stops Cyber Attacks During Drill Exercise. Asia Pacific Computer Emergency Response Team. Retrieved from <http://www.apcert.org/documents/pdf/APCERT-drill-2007.pdf>
4. Coughlan, Sean (2014). Cyber-attacks increase leads to jobs boom. *BBC News Business*. Retrieved from <http://www.bbc.com/news/business-26647795>
5. Kumar, Avanti (2013). CyberSecurity Malaysia appointed OIC-CERT permanent secretariat. *Computerworld Malaysia*. Retrieved from <http://www.computerworld.com.my/resource/security/cybersecurity-malaysia-appointed-oic-cert-permanent-secretariat/>
6. OIC-CERT Cyber Drill Coordination Successful In Addressing Targeted Cyber Crisis. BERNAMA. Retrieved from [http://www.cybersecurity.my/bahasa/knowledge\\_bank/news/2012/main/detail/2160/index.html](http://www.cybersecurity.my/bahasa/knowledge_bank/news/2012/main/detail/2160/index.html)
7. Phneah, Ellyne (2011). Cybersecurity drills useful but risky. *ZDNet Asia Edition*. Retrieved from <http://www.zdnet.com/cybersecurity-drills-useful-but-risky-2062302569/>
8. Workshop Report: Value Cyber Security Exercises. Asia-Pacific Economic Cooperation. Retrieved from [http://www.mtc.gob.pe/portal/apectel38/spsg/08\\_tel38\\_spsg\\_013\\_APEC\\_Draft\\_Exercise\\_Report%5B1%5D.pdf](http://www.mtc.gob.pe/portal/apectel38/spsg/08_tel38_spsg_013_APEC_Draft_Exercise_Report%5B1%5D.pdf)



#LittleBigThing #SID2015




**CARE BEFORE SHARE**

WHEN IN DOUBT, LEAVE IT OUT

THE BLUE TICK

OVERSHARING

**Be smart. Be safe**

logon to [www.CyberSAFE . my](http://www.CyberSAFE.my) to find out more  [cybersafe.malaysia](https://www.facebook.com/cybersafe.malaysia)

# Retinal Scanning VS Iris Recognition

By | Nurul Izratul Imrah Zolkafle

11

## Introduction

Most people assume that Retinal Scanning and Iris Recognition are similar identification methods. They are both categorised as 'eye biometrics' that leaves people confused between the function of iris recognition and retinal scanning.

Retinal scanning involves the use of a scan that surveys the blood vessel patterns on the retina using infrared light. This biometric vein retinal technology looks at the back of the eye that has nerve tissue, and this includes blood vessels that come with a unique retinal pattern. Whereas, iris recognition involves scanning the iris specifically, focusing on the flat, coloured, ring-shaped membrane behind the cornea of the eye; whilst with an adjustable circular opening (pupil) in the centre. Figure 1 illustrates the difference between iris and retina.

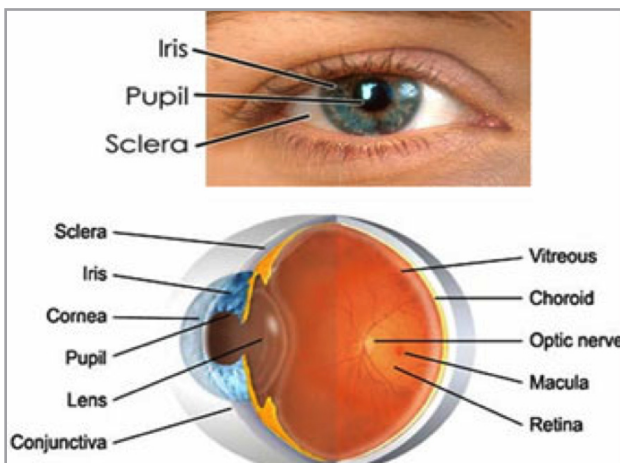


Figure 1<sup>1</sup>

## Retinal Scanning

This technology was founded by Robert Hill in the 1970s. Hill was an electrical engineer discovered the idea of using retinal scans as a form of identification when he was helping his father, an ophthalmologist, to detect eye

disease through photographs.

The retina is the innermost coating of the eye, containing light-sensitive nerve cells and fibres connecting with the brain through the optic nerve<sup>1</sup>. Nerve cells are tissue that require blood to function properly and possess an intricate blood vessel system called 'choroidal vasculature'. To scan the retina, a light beam needs to be exposed directly in the eyes for 10 to 15 seconds for the image to be converted to digital format.

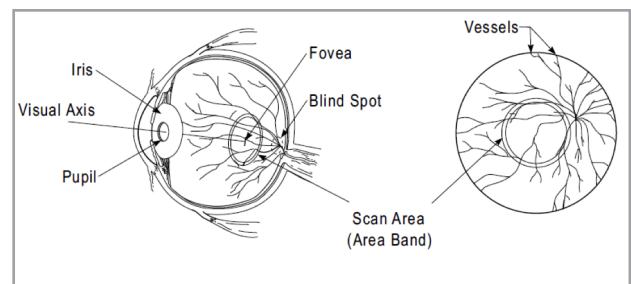


Figure 2 Eyes structure<sup>1</sup>

Figure 2 illustrates the image captured by a retinal scanner. The image on the left is a cross section of an eye with the retina. The ring can be seen on the right image is a cross section of the eye straight up and down.

Retinal scanning technology is the most accurate for biometric identification. In just 20 seconds, the retinal scanner scans about 400 reference points used for identification processes. The biggest disadvantage to this technology is certain diseases that can affect the choroidal vasculature and cannot be authenticated by the scanner.

A retinal scanner is considered more intrusive and slower. Users are required to be three inches from the scanner and focus on a red light point to clearly capture the retina. The red light is not good for the eyes as it can cause cataracts. Scan more than one time can cause dizziness to the user.



## Iris Recognition

This technology was patented back in the 1980s. It was used by a Pennsylvania prison to help identify prisoners. Today, many airports are beginning to use this technology, including London's Heathrow Airport and Germany's Frankfurt Airport. In 1963, ophthalmologist Frank Burch proposed using iris patterns to recognise an individual. In 1985, Drs. Leonard Flom and Aran Safir, ophthalmologists, proposed discovered that no two irises are alike. In 1993, the Defense Nuclear Agency began testing a prototype unit, successfully completed by 1995.

Iris is a thin, circular structure of the eye, responsible for controlling the diameter and size of the pupils and the amount of light reaching the retina. Iris recognition is a particular type of biometric system that can be used to reliably identify a person by analysing the patterns found in the iris<sup>4</sup>.

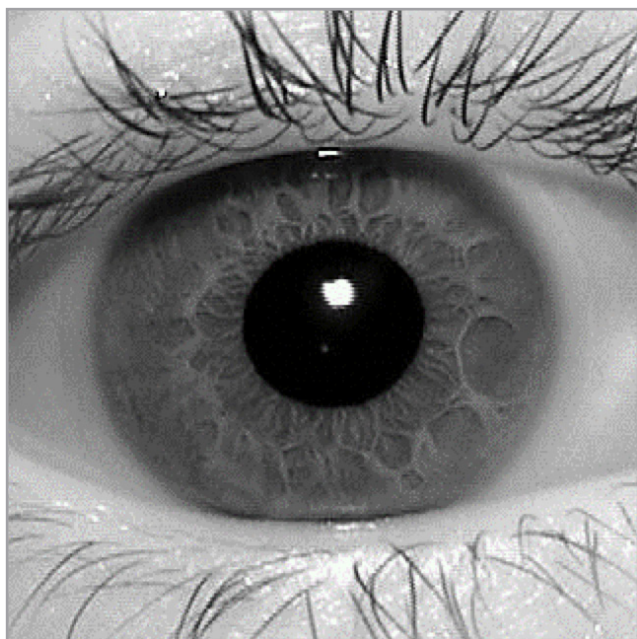


Figure 3 Iris Pattern <sup>5</sup>

Iris recognition uses high-quality camera technology with subtle infrared illumination to acquire images of the detail-rich, intricate structures of the iris. Most of the researchers classify the methodology in three steps: capture the pattern of the iris, calculate patterns by mathematical and statistical algorithms, and run a search through matcher engines in databases of enrolled iris

templates. Basically, before the recognition process, localisation of the iris must be performed to identify resultant noise like eyelashes, reflections, pupils and eyelids in the captured image. The iris scanner can be utilised from a much farther distance of up to two feet and uses about 240 reference points.

The advantage of using iris recognition is its ability to search at speeds measured in millions of templates per second per (single-core) CPU, and with infinitesimally small False Match rates and extremely resistant to False Matches.

## Conclusion

Although both technologies have different methods of identification, they are highly reliable because no two people have the same iris or retina. However, retinal scanning measurement accuracy can be affected by disease like diabetic and not suitable for pregnant women.

For those who interested with iris recognition can review the currents standards of iris recognition such as "ANSI/INCITS 379-2004 Iris Interchange Format" and "ISO/IEC 19794-6: 2005 Biometric Data Interchange Format – Part 6: Iris image data"<sup>3</sup>.

## References:

1. Carlos, *Iris vs. Retina*, <http://scanmein.blogspot.com/2011/04/iris-vs-retina.html>, accessed on 26 December 2013.
2. *Pediatric Visual Diagnosis Fact Sheet, RETINAL\_DISEASES\_DEFINITION\_DIAGNOSIS*. Pdf
3. *NSTC Subcommittee on Biometric, Iris Recognition*.pdf
4. *Iris Recognition*.pdf by Michale Boyd
5. Luigi Rosa's, *Real-Time Iris Identification*, <http://www.advancedsourcecode.com/irismovingaverage.asp> accessed on 28 December 2013.

# Security Threats Overview in 4G LTE Mobile Networks

By | Alifa Ilyana Chong Binti Abdullah

## Introduction

In an era of mobile broadband communication at work and at home, mobile network security is more pivotal than ever. With the introduction of 4G LTE networks and the IEEE standardisation for mobile networks, the secure, “walled garden” days are over. Mobile networks are becoming very similar to common IP-based networks. The move to IP-flat architecture in 4G LTE networks means that networks are now susceptible to IP-based security attacks from the Internet and RAN, subsequently presenting a security challenge to MNOs that previously did not exist, and demanding new methods for network protection.

## Key components of 4G LTE mobile network

To realise the security concerns or threats in 4G LTE mobile network, one must first understand the key network elements involved in 4G LTE mobile network. 4G LTE mobile network still contains the same basic network elements as per the previous 2G GSM to 3G WCDMA generation of mobile network.

### User Equipment (UE)

The device used by a person or system to access external service networks (voice and data traffic) via the mobile network. User equipment can also be referred to mobile station. To gain benefit of LTE access, UE must be able to support LTE frequency bands such as 900 or 1800 or 2100 Mhz.

### Radio Access Network (RAN)

The radio network which connects subscribers to their service provider. Each generation of mobile network consist of their own radio technology such 2G, 3G and LTE. They have been designed to be access-compatible to each other.

### Backhaul

The physical network connections used to carry data between the Radio Access Network and the Mobile Core Network.

### Core Network

The network which controls and authenticates users and devices, generates charging data records for billing purposes and provides agreed quality of services to subscribers. The LTE mobile core network is also referred to EPC or SAE.

### External Service Networks

The services provided by the mobile operators and may include connection to PSTN, VoIP, VoLTE networks, Internet or Public Data Network (PDN), roaming partners, enterprise or corporate specific networks and many other services.

These five key network components could be the potential target by attackers or hackers to gain entry and subsequently abusing the mobile network.

## Potential security threats and their impacts in 4G LTE mobile network

Among the five key network components, UE and core network remain the most potential targeted parts for security threats of the mobile network, while RAN and backhaul have attracted fewer security concerns (Figure 1). There is still potential increase of security threats on RAN and backhaul but they are likely to be more confined because of complex deployment configurations specifically tailored to operator based on location from specific vendor. Therefore, attacks would be difficult as they require complex preparation together with on-site access. However, security measures should

be considered from time to time, especially with the presence of small/femto cells and the integration of Wifi-hotspot with cellular network as these would allow attacks on mobile networks easier to plan and carry out.

Security threats associated with mobile network can be divided into two main categories:

### Intrusion

Network is more open to intruders unless protective security measures are taken such as passwords, encryptions and granular authentication as these could lead to misuse of information, unauthorised modification or deletion of data and network capacity abuse.

### Exploitation

Attackers gain access to mobile network and launch DoS attacks which could jeopardise the core network system.

UE such as smartphones can generate excessive signalling traffic in the mobile

core network during the busy hour periods if they are already compromised by malware. Nowadays, there are a number of mobile malwares can be found, especially Android malware and vulnerable for smartphone users. Examples of Android malwares are Andr/PJApps-C, Andr/BBridge-A, Andr/BatteryD-A, Andr/Generic-S and Andr/DrSheep-A.

The growing demands of OTT player such Facebook, Whatsapp and Twitter can also be a factor in excessive signalling traffic generated by UE, especially smartphones and could raise a potential of congestion in the core network. Therefore, protective measures should be adopted by MNOs to prevent their network from being jammed-up by signalling storm.

By year 2020, there will be 50 billion connected devices on the internet and almost 90 per cent of the world's population will have mobile broadband subscriptions, according to telecommunication giants Ericsson. With the increasing growth of mobile broadband, mobile operators will

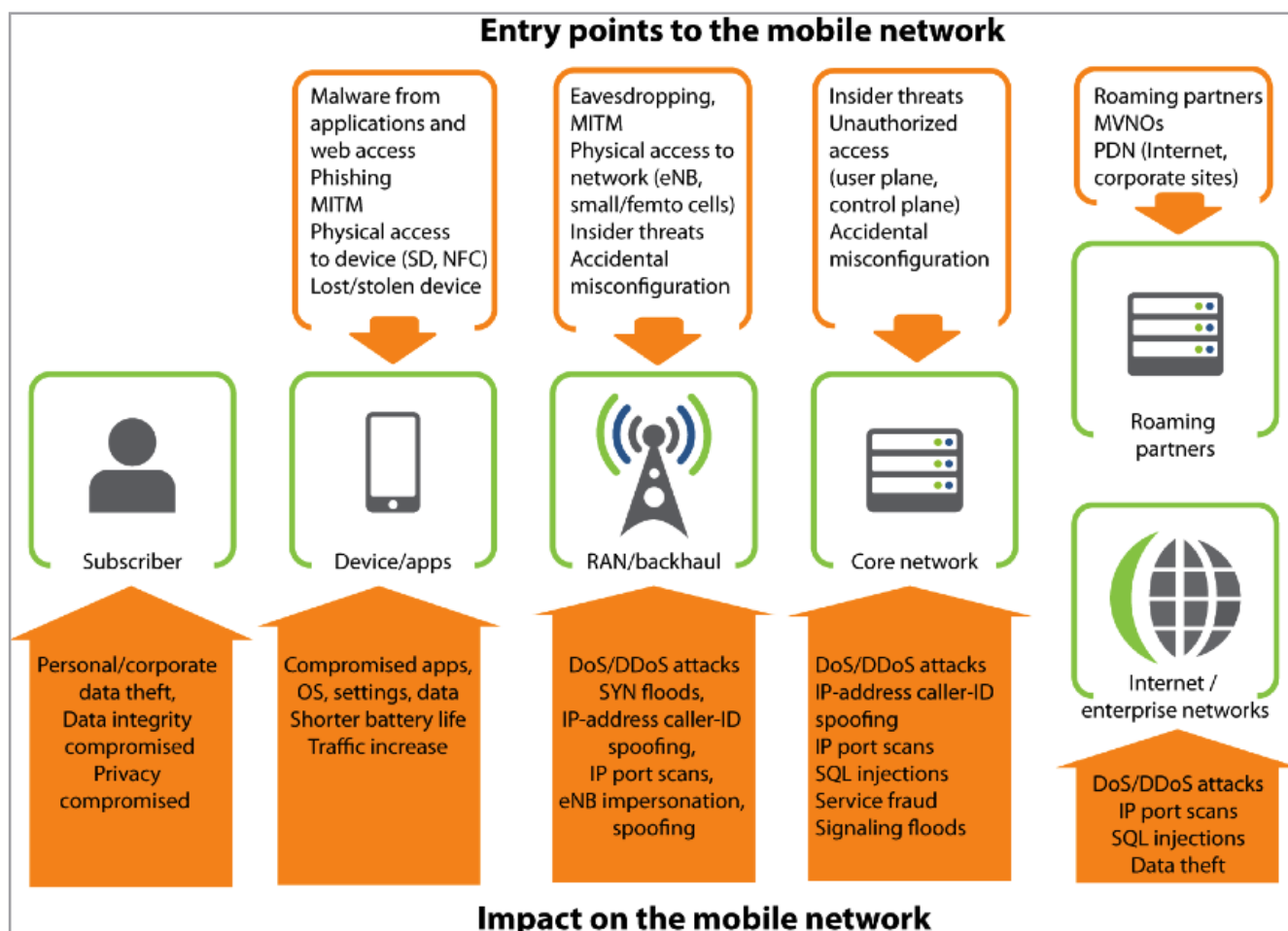


Figure 1. Overview of mobile security: entry points and impact of security threat. Source Senza Fili

face many challenges to protect their 4G LTE mobile networks from any security threats and provide their best services to customers.

4G	Fourth Generation Mobile Communication
DDoS	Distributed denial of service
DoS	Denial of service
eNB	eNodeB
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LTE	Long term evolution
MITM	Man in the middle
MNO	Mobile network operator
MVNO	Mobile virtual network operator
NFC	Near field communication
OS	Operating System
PDN	Packet data network
PSTN	Public System Telephone Network
RAN	Radio access network
SD	Secure Digital
SMS	Short message service
SQL	Structured query language
Syn Floods	TCP syn attack
VoIP	Voice over IP
VoLTE	Voice over LTE
EPC	Evolved Packet Core
SAE	System Architecture Evolution
UE	User Equipment
OTT	Over the Top

## References

1. *Mobile Network Security – Availability Risks in Mobile Networks*. ERT Lab Security Researcher. Retrieved from [http://security.radware.com/uploadedFiles/Resources\\_and\\_Content/Attack\\_Tools/Mobile\\_Networks\\_Security\\_Research\\_Paper.pdf](http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/Mobile_Networks_Security_Research_Paper.pdf)
2. *Wireless Security in LTE Networks*. Senza Fili Consulting. Retrieved from [http://www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili\\_WirelessSecurity\\_121029\\_FINAL.pdf](http://www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_WirelessSecurity_121029_FINAL.pdf)
3. *Media Vision 2020*. Ericsson. <http://www.ericsson.com/tv-media/media-vision-2020/>



# Why Social Networking Sites?









By | Nor Radziah Jusoh and Yuzida Md Yazid

Social networking sites (SNS) have become the most popular mode of communication. A social networking site is usually a web-based service that allows individuals and businesses to create public profiles, share information and views with their connections. It is a media that we use to update our daily statuses, share photos and interesting places with family and friends, as well as promoting, selling and buying merchandises. Some people are even addicted to SNSs where they completely

emerge themselves. Days without SNSs would seem incomplete to them. What really motivate people to use SNSs?

## Popular Social Networking Sites

Based on [www.ebizmba.com](http://www.ebizmba.com), the top 15 sites globally was dominated by Facebook, Twitter, LinkedIn, Pinterest, Google and others, as of November 2014. User population on Facebook is larger than the population of some countries.

<p>Rank : 1 900,000,000</p>  <p>A Social utility that connects people with friends and others who work, study and live around them.</p>	<p>Rank : 2 310,000,000</p>  <p>Connects with friends and other fascinating people. Users can get live updates on their areas of interest.</p>	<p>Rank : 3 255,000,000</p>  <p>A tool to help users manage their professional identity. They can also build and engage their professional network.</p>	<p>Rank : 4 250,000,000</p>  <p>A visual discovery tool that users can use to find ideas for their projects and interests.</p>
<p>Rank : 5 120,000,000</p>  <p>Users can search the world's information, including webpages, images, videos and more.</p>	<p>Rank : 6 110,000,000</p>  <p>Users can post anything (from anywhere), customise everything, and find and follow what they love.</p>	<p>Rank : 7 100,000,000</p>  <p>Users can capture and share important moments in their life with friends and family.</p>	<p>Rank : 8 80,000,000</p>  <p>VK is the largest European social network site.</p>








<p>Rank : 9 65,000,000</p>  <p>Users can share and connect with the Flickr Community and place all their photos in one place.</p>	<p>Rank : 10 42,000,000</p>  <p>Vine is the best way to see and share life in motion through short, beautiful, looping videos created for friends and family.</p>	<p>Rank : 11 40,000,000</p>  <p>This tool helps groups of people with shared interests plan events and facilitates off line group meetings in various localities around the world.</p>	<p>Rank : 12 38,000,000</p>  <p>Tagged makes it easy to meet and socialise with new people through games, shared interests, friend suggestions and browsing profiles.</p>
<p>Rank : 13 37,000,000</p>  <p>A tool to find out what people want to know about the users.</p>	<p>Rank : 14 15,500,000</p>  <p>A tool that helps users meet new people near them.</p>	<p>Rank : 15 15,000,000</p>  <p>This sites offers users access to nostalgic content, yearbooks and connect with people.</p>	

Table 1: User population in Social Networking Sites

Source: <http://www.ebizmba.com/articles/social-networking-websites>

These SNSs are not only popular among youth but also all ages from all walks of life. According to Pew Research Centre, as of January 2014, 74% of online population use SNSs. Divided by age group, 89% of users were between the age of 18 and 29.

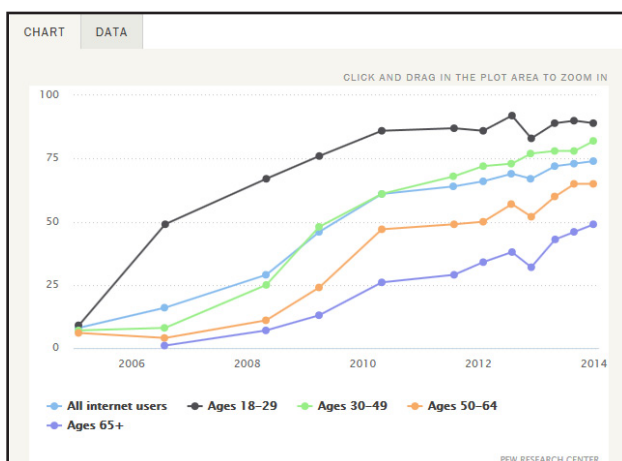


Diagram 1: Social Media Use by Age Group over Time

## Why Social Networking Sites?

Many researchers are trying to understand why people use SNS. Research by Petter Bae Brandtzæg and Jan Heim shows that, the list of motivational factors includes to create new relations, maintain relationship with friends, socialise, access information, debate, get free SMS, kill time and others.

In China, Renren.com survey with college students listed 'social interaction, 'self-image building', information-seeking' are the motivational factors in using SNS. Another study (table 2) shows students from Malaysia, Iran, UK and South Africa choosing 'peer pressure', 'keeping in touch' and 'finding classmates' as top motivation in using SNS.

User's Motivations in Joining SNSs	Malaysia	Iran	UK	South Africa
Everyone I know using SNS	78%	81%	84%	73%
Keeping in touch with others	62%	66%	55%	44%
Find classmates	53%	51%	43%	45%
Received a promotional e-mail	30%	20%	25%	10%
Network in general	25%	18%	20%	26%
Find jobs	19%	17%	14%	16%
Find course information	18%	20%	15%	19%
Friend suggested it	12%	8%	7%	18%
Find dates	11%	3%	10%	22%
Get to know more people	9%	4%	6%	4%
Find people with mutual interests	9%	4%	11%	8%

Table 2: User's Motivations in Joining SNSs

## Need to belong

Across all cultures of people, there is one major motivational factor that encourages people to join/use SNSs – the need to belong. It is the need to be accepted by others from the same group. Researchers believe that this need relates to self-esteem, attachment and self-presentation to impress others.

## Marketing

SNSs are used as powerful marketing tools used by companies to sell products and services. Brand communities are a special form of consumer communities that bind brand and community together. Social interactions between community members profoundly influence customers' relationship with, and attitude towards, the brand. In such virtual environments, users often gather together in sub-groups with a specific brand in its centre, a brand-related community; consumers share their interest for a brand, exchange information and knowledge, or they simply express their affection for this specific brand.

## Social Gap

Parents have extra motives to use SNS - bonding and bridging the social gap between them and their children. Children tend to be closer to their friends than their

parents. Parents use SNSs to communicate with their children, their children's friends, and the parents of their children's friends. Adolescents are more open and expressive in social networking sites. Hence, parents consider SNS as a good platform for them to know more about their children.

## Campaign

Usage of SNSs among politicians, especially during election campaigns, is becoming a trend. Candidates running for presidential and parliament posts use micro-blogging and online social networks such as Twitter and Facebook to communicate and connect with the citizens. Traditional campaign involves only one-way communication. However, SNSs campaigns convey messages to people, that has an 'amplifying' effect. Politicians can create a mass connection and respond to more people.

## References

1. Petter Bae Brandtzaeg and Jan Heim, (2009), *Why People Use Social Networking Sites*, pp. 143–152, © Springer-Verlag Berlin Heidelberg 2009
2. *Population of Countries in the World*. Worldometers, 2014. (<http://www.worldometers.info/world-population/population-by-country/>)
3. Manzoor Ali Mirani, (2011), *Motives for Students Using Social Networking Sites: Findings from Sukkur, Pakistan*, IPEDR (22)
4. *Social Media Use by Age Group Over Time*, Pew Research Internet Project, (2014) (<http://www.pewinternet.org/data-trend/social-media/social-media-use-by-age-group/>)
5. Schaefer, Cora. (2008). *Motivations and Usage Patterns on Social Network Sites*.
6. Joan DiMicco, David R. Millen, Werner Geyer, Casey Dugan, Beth Brownholtz, Michael Muller, (2008), *Motivations for Social Networking at Work*, CSCW'08 .
7. Leila Karimi, Rouhollah Khodabandelou, Maryam Ehsani, Muhammad Ahmad, (2014), *Applying the Uses and Gratifications Theory to Compare Higher Education Students' Motivation for Using Social Networking Sites: Experiences from Iran, Malaysia, United Kingdom, and South Africa*, *Contemporary Educational Technology*, 5(1), 53-72.
8. Zhang Wei Wei, Huang Pei Yi, (2011) *How Motivations of SNSs Use and Offline Social Trust Affect College Students' Self-disclosure on SNSs: An Investigation in China*.
9. Jennifer Doty, Jodi Dworkin (2014). *Parents' of adolescents use of social networking sites*, *Computers in Human Behaviour*.
10. Maurice Vergeer, Liesbeth Hermans and Steven Sams (2013), *Online social networks and micro-blogging in political campaigning, The exploration of a new campaign tool and a new campaign style*, *Party Politics Journal*
11. Mushera Frehat, Emad Abu-Shanab (2014). *The Role of Social Networking in the Social Reform on Young Society*.
12. Melanie E. Zaglia (2013). *Brand communities embedded in social networks*.

# The History of Cryptography

By | Liyana Chew bt Nizam Chew & Isma Norshahila Mohd Shah

19

## Introduction

Cryptography is so advanced that people don't even notice using them in their daily lives. Have you ever wondered how cryptography came about?

500 BC ATBASH CIPHER	Atbash is a simple substitution cipher for the Hebrew alphabet. This cipher substitute the first letter of the alphabet for the last letter and the second letter for the second last letter and so on.
50 BC CAESAR CIPHER	Caesar cipher is one of the oldest types of ciphers. It is the simplest and widely known encryption technique that is often incorporated as part of a more complex scheme, such as Vigenere Cipher. Caesar cipher is a type of substitution cipher in which each letter in the plaintext is rotated left or right by some fixed number of positions down the alphabet.
7 C SKYTALE	Skytale is one of the tools used to perform a transposition cipher, consisting of a wooden rod that acts as a key. Both sender and recipient need to own a wooden rod with the exact same diameter and length. A strip of parchment will be wound around the rod and message will be written on it. Then, the strip of parchment is sent as a cipher text. The recipient uses a similar rod, wraps the parchment to decrypt and reads the message. This cipher is said to be used by the Spartan military to communicate during battle times.
9 C FREQUENCY ANALYSIS	Frequency analysis is the study of the frequency of letter or groups of letters in a ciphertext that is useful in cryptanalysis. The method is used as an aid to break classical ciphers such as Caesar Cipher and other substitution ciphers. In substitution ciphers, each plaintext letter is encoded to the same cipher letter or symbol. To start deciphering the encryption, it is useful to get a frequency count of all the letters in ciphertext. The most frequent letter may represent the most common letter in English which is E followed by T, A, O and I whereas the least frequent are Q, Z and X. This method was first documented by an Arabic mathematician, Abu al-Kindi.
1920s ENIGMA MACHINE	Enigma machine was used by Britain's code breakers for enciphering and deciphering secret messages during World War II. It was invented by Arthur Scherbius, the German engineer at the end of World War I. It has been claimed that as a result of the information gained through the device, hostilities between Germany and the Allied forces were curtailed by two years. Before and during World War II, Enigma has been the inspiration for many other designs of rotor cipher machines, such as the British Typex and the American Sigaba.
1977 DATA ENCRYPTION STANDARD (DES)	Data Encryption Standard (DES) is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards (now called NIST – National Institute of Standards and Technology) as an official Federal Information Processing Standard (FIPS) for the United States and which has subsequently enjoyed widespread used internationally. It is based on a symmetric-key algorithm that uses a 56-bit key to each 64-bit block of data.
2001 ADVANCED ENCRYPTION STANDARDS (AES)	Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. The cryptographic algorithm used block encryption of 128 bits in size, supporting three variants of key sizes which are 128, 192, and 256 bits. It was developed by Joan Daemen and Vincent Rijmen. This algorithm is fast in both software and hardware due to the design principles known as substitution-permutation network.






# KNOW PRIVACY SETTINGS

PRIVATE ACCOUNT

GEO-LOCATION

PHOTO TAGGING

## Be smart. Be safe

logon to [www.CyberSAFE.my](http://www.CyberSAFE.my) to find out more  [cybersafe.malaysia](https://www.facebook.com/cybersafe.malaysia)

# INFOGRAPHIC: PKCS - Public Key Cryptography Standards

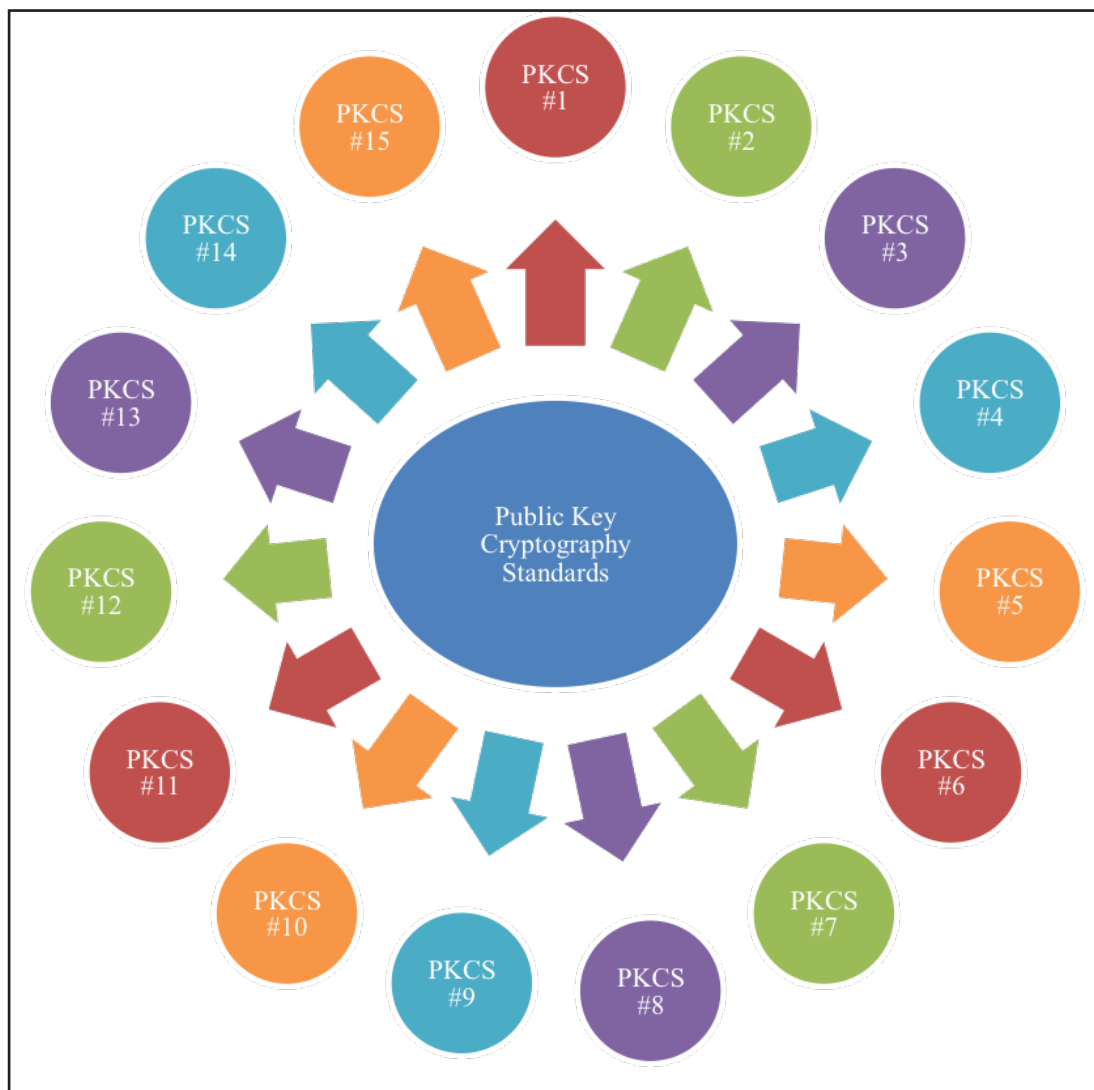
By | Nik Azura Nik Abdullah & Norul Hidayah Ahmad Zawawi

## What is Public Key Cryptography Standards (PKCS)?

- A set of standards for implementation of public-key cryptography developed by RSA Laboratories (a Division of RSA Data Security Inc.) starting in early 1990s in cooperation with Apple, Microsoft, DEC, Lotus, Sun, and MIT.
- PKCS#1, #3, #5, #6, #7, #8, #9, #10, #11, #12 and #15 have been published.

PKCS#13 and #14 are currently being developed, whereas PKCS#2 and #4 are no longer active as of 2010.

- The purpose of these standards is to accelerate the deployment of public-key cryptography when we work with public key cryptography and digital certificates.
- Some of these standards have become part of many formal standards including ANSI X9 and IEEE P1363.



## Who uses PKCS and how it is used?

1. International Organisation for Standardisation and International Electrotechnical Commission (ISO/IEC) developed standards for application independent cryptographic techniques and bank security standards.
  - ISO/IEC 9798-3: Information technology-Security techniques-Entity Authentication - Part 3: Mechanisms using digital signature techniques which defines seven protocols based on cryptographic signatures.
  - ISO/IEC 7816-15: Identification cards - Integrated circuit cards with contacts.
  - ISO/IEC 9796: Information technology - Security techniques - Digital signature schemes giving message recovery.
2. American National Standards Institute (ANSI) developed ANSI X9 standards for financial service specifically for personal identification number (PIN) management, check processing and electronic transfer of funds.
  - ANSI X9.9 is a banking standard for authentication of financial transactions which focuses on message formatting and the particular message authentication algorithm.
  - ANSI X9.17 is the Financial Institution Key Management standard which defines the protocols to be used by financial institutions to transfer encryption keys.
3. National Institute of Standards and Technology (NIST) developed standards for use by US federal government department.
  - FIPS PUB 186-3: Digital Signature Standard (DSS) specifies a suite of algorithms that can be used to generate a digital signature.
  - NIST Special Publication 800-3: Establishing a computer security incident response capability.
4. Internet Engineering Task Force (IETF) developed standards for use by Internet community.
  - RFC 2048: Multipurpose Internet Mail Extensions (MIME)
  - RFC 2246: The TLS Protocol
  - RFC 2376: XML Media Types
  - RFC 2518: HTTP Extensions for Distributed Authority
5. Institute of Electric and Electronic Engineers (IEEE) developed IEEE P1363: Standards Specifications For Public Key Cryptography
  - IEEE P1363-2000 & 1363a-2004: Traditional Public-Key Cryptography includes digital signature and key establishment schemes based on integer factorization (e.g RSA), discrete logarithm (e.g Diffie-Helman, DSA) and elliptic curve discrete logarithm (e.g MQV) problems.
  - IEEE P1363.1: Lattice-Based Public-Key Cryptography includes encryption (e.g NTRUEncrypt) and digital signatures (e.g NTRUSign) schemes.
  - IEEE P1363.2: Password-Based Public Key Cryptography includes password-authenticated key agreement (e.g EKE, SPEKE, SRP) and password-authenticated key retrieval (e.g Ford & Kaliski) schemes.
  - IEEE P1363.3: Identity-Based Public Key Cryptography using Pairings includes techniques for identity-based cryptography using pairings.

### PKCS #1: RSA Cryptography Standard

Presents the recommendations for implementing the RSA algorithm for public-key cryptography which defines:

- The mathematical properties of RSA key pair (public key and private key).
- Data conversion primitive (Integer-to-Octet-String and Octet-String-to-Integer).
- Cryptographic primitives (encryption-decryption and signature-verification).
- OAEP-based encryption scheme and PSS-based signatures schemes.

### PKCS #2

Covers RSA encryption of message digests, but was withdrawn in 2010 to be merged in PKCS #1.

### PKCS #3: Diffie-Hellman Key Agreement Standard

Describes a cryptographic protocol which enables two parties, who have no prior arrangements, to agree on a secret key only known by them, but will not be available to eavesdropper.

### PKCS #4

Covers RSA key syntax, but was withdrawn in 2010 to be merged in PKCS #1.

### PKCS #5: Password-based Encryption Standard

Presents the recommendations for implementing password-based cryptography which defines:

- Key derivation functions which produced a derived key from a base key (password) and other parameters (salt value and iteration count).
- Two symmetric encryption schemes; PBES1 with an underlying block cipher (DES or RC2) and PBES2 which is recommended for new applications.
- Message-authentication schemes which consist of MAC generation operation and MAC verification operation.

### PKCS #6: Extended-Certificate Syntax Standard

Presents the syntax of extended certificates which consists of an X.509 public-key certificate and a set of attributes, collectively signed by the issuer of this certificate. The intention of this standard is to extend the certification process beyond just the public key to include other information about a given entity.

### PKCS #7: Cryptographic Message Syntax Standard

- Describes a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes. The syntax admits recursion (one envelope can be nested inside another, or one party can sign some previously enveloped digital data) and allows arbitrary attributes (signing time to be authenticated along with the content of a message and countersignatures to be associated with a signature).
- Compatible with Privacy-Enhanced Mail (PEM); signed-data and signed-and-enveloped-data content constructed in PEM-compatible mode can be converted into PEM messages, and vice-versa, without any cryptographic operations.

### PKCS #8: Private-Key Information Syntax Standard

- Describes syntax for private-key information (which includes a private key for some public-key algorithm and a set of attributes) and describes syntax for encrypted private keys. A password-based encryption algorithm could be used to encrypt the private-key information.
- Private-Key Information Syntax and Encrypted Private-Key Information Syntax shall have ASN.1 type PrivateKeyInfo and ASN.1 type EncryptedPrivateKeyInfo respectively. Encryption process for both involves the private-key information is BER encoded yielding an octet string as step one. To differentiate between these two syntax, the result of step one in the Encrypted Private-Key Information Syntax, is encrypted with the key to give an octet string, the result of the encryption process.



### PKCS #9: Select Attribute Types

Presents certain attribute types for use in PKCS#6 extended certificates, PKCS#7 digitally signed messages, PKCS#8 private-key information, and PKCS#10 certificate-signing request. This standard provides in more details about syntax (what is syntax, how it is to be used and where it is to be used).

### PKCS #10: Certificate Request Standard

Describes the syntax for certification request of a public key, a name and optionally a set of attributes. The process of certification request is defined as following below:

- A CertificationRequestInfo value which consist of a distinguishing name, a public key, and optionally a set of attributes which is constructed by an entity.
- The CertificationRequestInfo is then signed with the entity's private key.
- The CertificationRequestInfo value, a signature algorithm identifier, and the entity's signature are collected together into CertificationRequest value.

### PKCS #11: Cryptographic Token Interface

Describes an application programming interface (API) which is known as "Cryptoki" (pronounced "crypto-key") and short for "cryptographic token interface". This standard is defined as an API platform to cryptographic tokens including hardware security modules (HSM) and smart cards. The PKCS#11 most commonly use the cryptographic object types such as RSA keys, X.509 Certificates and DES/Triple DES keys.

### PKCS #12: Personal Information Exchange Syntax Standard

Describes a format for storing and transporting personal information including private keys, certificates, miscellaneous secrets, and extensions. Machines, applications and browsers that support this standard will allow users to import, and export a single set of personal identity information.

### PKCS #13: Elliptic Curve Cryptography Standard

The elliptic curve cryptography standard is currently being developed. This standard will concentrate on the elliptic curve cryptography aspects which consist of parameter and key generation and validation, digital signature, public-key encryption, key agreement, and ASN.1 syntax.

### PKCS #14: Pseudo- random Number Generation

The pseudo-random number generation standard is currently being developed. At this moment, there are a lot of methods of creating pseudo-random number generator, but there is no one outstanding method to become a standard yet.

### PKCS #15: Cryptographic Token Information Format Standard

Describes a standard that users are able to use cryptographic tokens to identify themselves to applications, independent of the application's Cryptoki implementation (PKCS#11) or other API. The aim of this standard is to enable:

- Interoperability among components running on various platforms.
- Application to take advantage of products and components from multiple manufactures.
- Use of advances in technology without rewriting application level software
- Maintaining consistency with existing, related standards while expanding upon them only where necessary and practical.

# Email Account Compromise and Security Best Practices: A Case Study

By | Md Sahrom Bin Abu

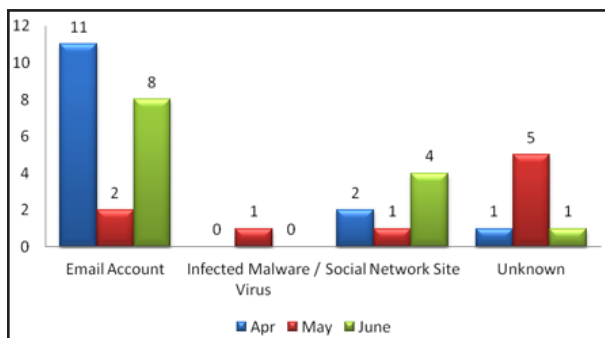
## Email Account Compromise cases in Malaysia

When an account is compromised, it is exposed to serious data loss, data theft or theft of services. Compromise at the end user access level can be contained, however the same can't be said for a root-level (high administrative level) access. Account compromise can be classified into email account intrusion, malware/virus infection, social networking (social engineering), keylogging malware (Command and Control) and others.

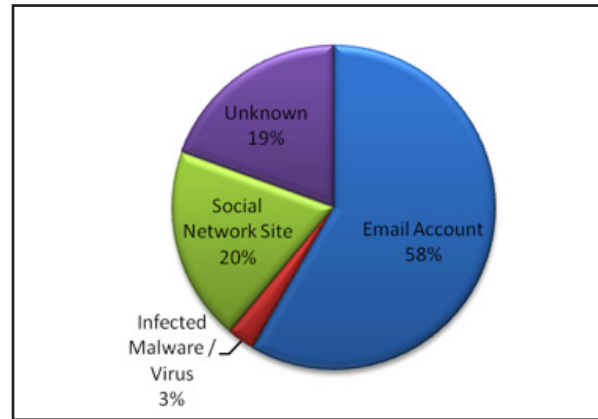
'Compromised account' incidents usually comes from account owners and seldom from third parties, with the highest number of cases involving personal emails or social networking accounts. In the second quarter of 2014, 36 incidents on 'account compromise' were reported, as shown in table 1 and graphic 1.

Types of Account Compromise	April	May	June	Total
Email account	11	2	8	21
Malware/virus infection	0	1	0	1
Social networking site	2	1	4	7
Unknown	1	5	1	7
Total	14	9	13	36

Table 1: Number of Account Compromise Incidents in Q2/2014



Graph 1: Number of Account Compromise Incidents in Q2/2014



Graph 2: Types of Account Compromise Incidents

## What happens when your email gets hacked?

"A Malaysian IP address hacked my account and sent emails to people all over the world as well as those in my address book. I have since changed the password but they have tried to hack into my personal account again. Please see log below."

The IP address for 14th April is 60.49.70.46

The IP address for 31st March is 175.145.196.101

Date	Event	Location
Date? 12:42 PM	Signed in from Internet Explorer (Windows)	Carrick-On-Shannon, Leitrim, Ireland
Date? 10:02 AM	Signed in from IE (Windows)	Carrick-On-Shannon, Leitrim, Ireland
April 15	Changed password	Carrick-On-Shannon, Leitrim, Ireland
April 16	Signed in from IE (Windows)	Carrick-On-Shannon, Leitrim, Ireland

Table 3: Snippet of log activity for my email account

## Analysis

Based on WHOIS information, both IP belong to TMNET.

Queried whois.apnic.net with  
"60.49.70.46"...

% Information related to '60.49.0.0 - 60.49.255.255'

inetnum: 60.49.0.0 - 60.49.255.255  
netname: ADSL-STREAMYX  
descr: TMNST  
country: MY  
admin-c: EAK2-AP  
tech-c: EAK2-AP  
status: ASSIGNED NON-PORTABLE  
mnt-by: MAINT-AP-STREAMYX  
mnt-lower: MAINT-AP-STREAMYX  
mnt-routes: MAINT-AP-STREAMYX  
mnt-irt: IRT-TMNST-MY  
notify: tmcops@tm.net.my  
changed: nuralwani@tm.com.my 20130412  
changed: hm-changed@apnic.net 20140515  
source: APNIC

irt: IRT-TMNST-MY  
address: TELEKOM MALAYSIA BERHAD  
address: TM BRICKFIELD  
address: Jalan Tun Sambanthan  
address: 43200 KUALA LUMPUR  
e-mail: ipmc\_ipcore@tm.com.my  
abuse-mailbox: abuse@tm.com.my  
admin-c: TIA7-AP  
tech-c: TIA7-AP  
auth: # Filtered  
mnt-by: MAINT-AP-STREAMYX  
changed: abuse@tm.com.my 20140211  
source: APNIC

person: EMRAN AHMED KAMAL  
nic-hdl: EAK2-AP  
e-mail: abuse@tm.com.my  
address: Telekom Malaysia  
address: Jalan Pantai Baru, Kuala Lumpur.  
phone: +6-03-83185434  
fax-no: +6-03-22402126  
country: MY  
changed: fuwaizah@tm.net.my 20080918  
mnt-by: TM-NET-AP  
abuse-mailbox: abuse@tm.com.my  
source: APNIC

Queried whois.apnic.net with  
"175.145.196.101"...

% Information related to '175.145.0.0 - 175.145.255.255'

inetnum: 175.145.0.0 - 175.145.255.255  
netname: ADSL-STREAMYX  
descr: TMNST  
country: MY  
admin-c: EAK2-AP  
tech-c: Eak2-AP  
status: ASSIGNED NON-PORTABLE  
mnt-by: MAINT-AP-STREAMYX  
mnt-lower: MAINT-AP-STREAMYX  
mnt-routes: MAINT-AP-STREAMYX  
mnt-irt: IRT-TMNST-MY  
notify: ssc@tmnet.com.my  
changed: fuwaizah@tm.com.my 20130404  
changed: hm-changed@apnic.net 20140515  
source: APNIC

irt: IRT-TMNST-MY  
address: TELEKOM MALAYSIA BERHAD  
address: TM BRICKFIELD  
address: Jalan Tun Sambanthan  
address: 43200 KUALA LUMPUR  
e-mail: ipmc\_ipcore@tm.com.my  
abuse-mailbox: abuse@tm.com.my  
admin-c: TIA7-AP  
tech-c: TIA7-AP  
auth: # Filtered  
mnt-by: MAINT-AP-STREAMYX  
changed: abuse@tm.com.my 20140211  
source: APNIC

person: EMRAN AHMED KAMAL  
nic-hdl: EAK2-AP  
e-mail: abuse@tm.com.my  
address: Telekom Malaysia  
address: Jalan Pantai Baru, Kuala Lumpur.  
phone: +6-03-83185434  
fax-no: +6-03-22402126  
country: MY  
changed: fuwaizah@tm.net.my 20080918  
mnt-by: TM-NET-AP  
abuse-mailbox: abuse@tm.com.my  
source: APNIC

An email notification was sent to inform the ISP involved on the unauthorised activity for its further action.



Graph 3: Email notification to the ISP

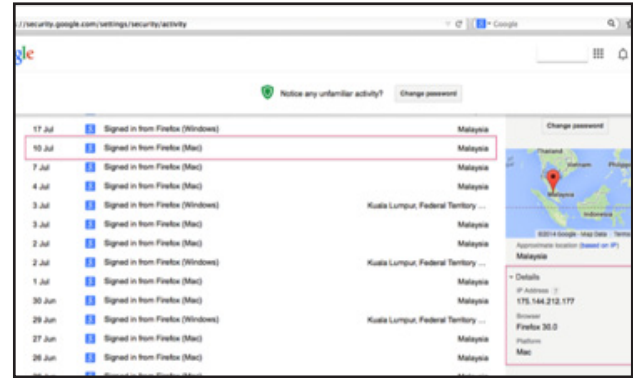
## What to do when your email is hacked?

Once the email account has been marked as 'compromised', the account can be recovered using the Password Recovery Tool (PRT). However, if there are insufficient information (e.g. forgotten security question) to use the PRT, the account can no longer be used.

The table below shows the recovery process for scenario 1 and scenario 2.

Scenario	Recovery and Mitigation Process
Able to recover password using PRT	<p>Step 1: Check if you can login and change the password</p> <ul style="list-style-type: none"> <li>Try recovering the password using PRT. Once you've successfully logged in to the account, change the current password to a long one with multiple cases, numbers and special characters.</li> <li>Send a message to all contacts in the owner's email account, to inform that the problem has been rectified.</li> </ul> <p>Step 2: Reset all the passwords in related accounts</p> <ul style="list-style-type: none"> <li>Find all services registered using this email account by searching the inbox for confirmation emails. Then, change the passwords accordingly.</li> </ul> <p>Step 3: Reset all the accounts with the same password used in the hacked account</p> <p>Step 4: Investigate how the account was hacked</p> <ul style="list-style-type: none"> <li>Check the activity log for unfamiliar activities and perform WHOIS to IPs used by hacker to find the location. Refer to Graph 4.</li> <li>Make a police report and liaise with the Investigation Officer to get more information of the IP.</li> </ul>
Unable to recover password using PRT	Send a letter or email to the relevant service provider such as Google, Yahoo or Microsoft to either request for account termination or recover the account.

Table 4: Email recovery and mitigation process



Graph 4: Gmail's recent activity log

## Best Practices in Password Creation

Passwords can be cracked using of a word list or dictionary programme. Instead of manually keying in these combinations, hackers use bots to automatically compare lists of words or character combinations against the password until they find a match. Table 5 lists some common passwords used by end-users:

Common Passwords
123456, 234567, 789456258753951, yourname-computer, yourbirthday, yourphone, name1234, Gankster1234, sushi1111, hummerkller, youremail, abc123, password

Table 5: List of common passwords

Users can apply the following best practices to develop a secure, unique password:

- Do not use passwords that are based on personal information easily accessed or guessed.
- Do not use words that can be found in any dictionary of any language.
- Develop a mnemonic to remember complex passwords.
- Use both lowercase and capital letters.
- Use a combination of letters, numbers and special characters.
- Use passphrases when you can.
- Use different passwords on different systems.



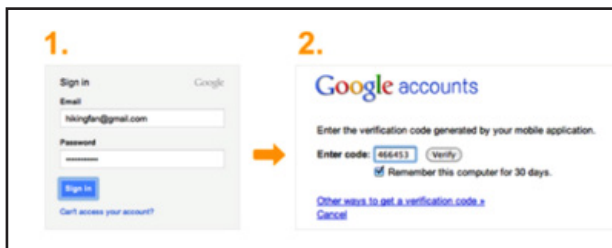
## Double Protection with 2-factor Authentication

In 2011, Google introduced the two-factor authentication to provide its users a more protection. The two-factor authentication is used in banks either for credit card usage or ATM machine access. This method requires users to enter a code number to verify the validity of the card before using it.

With this method, users now have another form of identification, usually a code generated by a key fob or a smartphone app. The code must be keyed in at the time of login as it changes after a certain period of time.

How it works on Gmail:

- Sign in to Google using the usual username and password.
- You are required to key in a code that will be sent to you via text, voice call or mobile app.
- If you are using a home computer, you may come across a Google pop-up asking you if you'd like to enable this authentication feature. Even if you do enable, Google will still prompt for codes when you or anyone else tries to sign in from other computers.



Graph 5: Google two-factor authentication (credit: googleblog.blogspot.com)

Though the number of cases is not alarming, email or social network account owners should always be aware of the threats caused by account compromise. Information can be manipulated by irresponsible parties for malicious reasons. Account owners must change their passwords regularly and use only strong, secure passwords. They also must make sure that their machines and applications are regularly patched or updated to keep the computer from malware or viruses.

## Reference:


1. <http://www.mycert.org.my>
2. <http://www.sans.org>
3. <http://www.us-cert.gov/ncas/tips/ST04-002>
4. <http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html>
5. <http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/>

#LittleBigThing #SID2015

# STRONG PASSWORDS

UPPER & LOWER CASE   SYMBOLS   NUMBERS   8 OR MORE CHARACTERS

## Be smart. Be safe

logon to [www. CyberSAFE . my](http://www.CyberSAFE.my) to find out more  [cybersafe.malaysia](https://www.facebook.com/cybersafe.malaysia)

# Automated Incident Response Process

By | Sharifah Roziah Mohd Kassim

## Malaysia's Computer Emergency Response Team – Before & After Incident Response Process Automation

Cyber security incidents reported to Malaysia's Computer Emergency Response Team, MyCERT of CyberSecurity Malaysia come from various sources such as government agencies, private sectors, foreign security organisations, foreign CERTs, Security Feeds, Special Interest Groups (SIG) and home users. In 2014, 11,918 incidents were reported to MyCERT, representing a 12 per cent increase compared to year 2013. Statistics (table 1) show that fraud, intrusions and malicious codes were among the highest incidents reported to Cyber999, the cyber incidents helpline centre managed by MyCERT.

Types of Incident	2012	2013	2014
Content Related	20	54	35
Cyber Harassment	300	512	550
Denial of Service	23	19	29
Fraud	4,001	4,485	4,477
Intrusion	4,326	2,770	1,125
Intrusion Attempt	67	76	1,302
Malicious Code	645	1,751	716
Spam	526	950	3,650
Vulnerabilities Report	78	19	34
<b>TOTAL</b>	<b>9,986</b>	<b>10,636</b>	<b>11,918</b>

Table 1. 2012 – 2014 Incident statistics

As the number of cyber incidents increases year-on-year, more organisations and individuals have started paying attention to data security. More than ever, it is also critical for the authority to respond to these security incidents efficiently and in a timely manner. For example, attacks classified as 'critical' such as the Distributed Denial of Service (DDoS) can make information unavailable to users. Critical attacks must be responded within 6 hours or less, whereas Malware outbreaks must be responded within 24 hours depending on its criticality.

## Issues with Manual Incident Response processes

Given the short deadlines for incident responses, the right tool can make or break the effort behind any incident. When My CERT started operation, manual process and response to cyber incidents presented several challenges to the team. Firstly, it required additional cost required to employ and train new CERT staff. The lack of resources and necessary skillsets affected the efficient and speed to process data. Secondly, manually-processing data involving network flows, network packets, logs and files, was often tedious and required time to analyse. Lastly, there were possibilities for human error.

## Moving toward Automated Tools

MyCERT developed two set of tools to automate the analysis and processing of incident data on a daily basis. The tools consist of a set of scripts written in Python programming language, developed in a simple structure to promote flexibility and ease of use. The tools have assisted MyCERT in the analysis and escalation of security incidents to relevant Internet Service Providers (ISPs) and System Administrators. Today, these tools can process big incident data that are related to intrusion, malware activities, phishing websites and DDoS activities.

Automated tools developed by MyCERT will help analyse big data from various Security Feed organisations that collect and distribute data to MyCERT. The data reveals botnet activities from Malaysia IP addresses. Collected data will be sent to a Customer Relation Management (CRM) system that issues a Parent Ticket. The tool will query and assign the data with a Child Ticket number. Once the tool completes auto-analysing and processing the data at the Child Ticket level, the Parent Ticket will be closed.

These data contains information such as aate, tme, timestamp, source IP Address, destination IP address and even, malicious links. All IPs related to the malicious activities will be auto-queried using an in-house developed WHOIS database. After the WHOIS queries are completed, the tool will auto-notify the respective ISPs using a pre-set Reply Template, urging action to rectify the botnet-infected IPs. Once notified, the tool will auto-close the Ticket in the CRM System.

## Did it work?

After the implementation of the automated tool, MyCERT's Incident Response showed an increase in efficiency, reduction in time to analysis and process data and minimal human-related errors. As the automated tool as developed in-house, the cost of maintenance was low as well. The tool is also easily customisable, especially when a new requirement arises in the Incident Response process.

Cyber incidents are increasing daily not just in scale, but in sophistication of attack techniques. MyCERT's new milestone in Incident Response processes will potentially have a big impact towards addressing and resolving security incidents in Malaysia.

## References

1. MyCERT Incident Statistics for the Year 2013 [online], <http://www.mycert.org.my/en/services/statistic/mycert/2013/main/detail/914/index.html>
2. Shadowserver, <http://www.shadowserver.org>

# What we can learn from Online Fraud in 2014

By | Norlinda Jaafar

Purchase fraud occurs when a criminal approaches a merchant and proposes a business transaction, and uses fraudulent means to pay for it. As a result, the merchant does not get paid for his products/service. On the reverse side, purchase fraud also happens when a fraudulent merchant dupes a legitimate buyer. In this case, the buyer will lose his money and the merchandise. Today, purchase fraud can happen online as well.

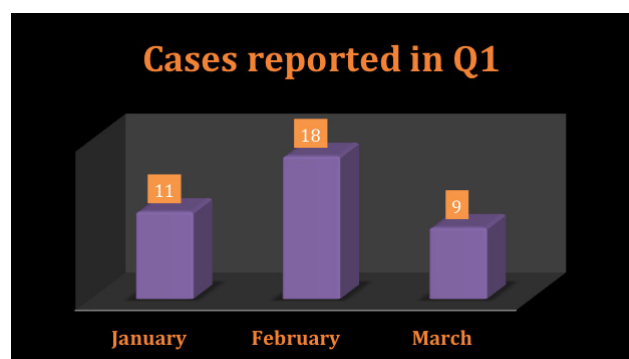


Figure 1 – Breakdown of Fraud Purchase Incidents in Q1

The statistics show purchase fraud incidents reported to MyCERT through its Cyber999 help centre. In the first quarter of 2014, 38 incidents were reported to Cyber999. The number of incidents reported in February, was the highest, whereas March recorded the lowest with 9 incidents. Most fraud incidents reported wore a similar pattern – both buyers and sellers have been duped during the transaction.

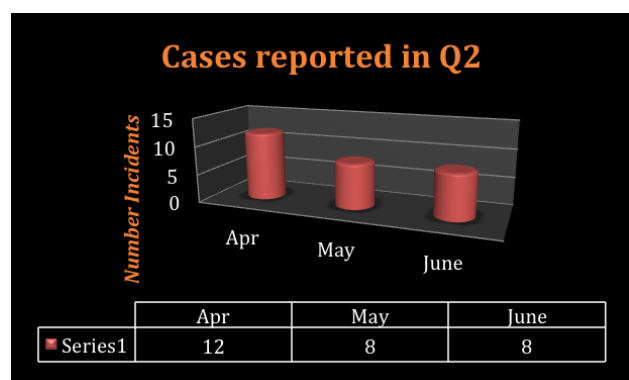


Figure 2 – Breakdown of Fraud Purchase Incidents in Q2

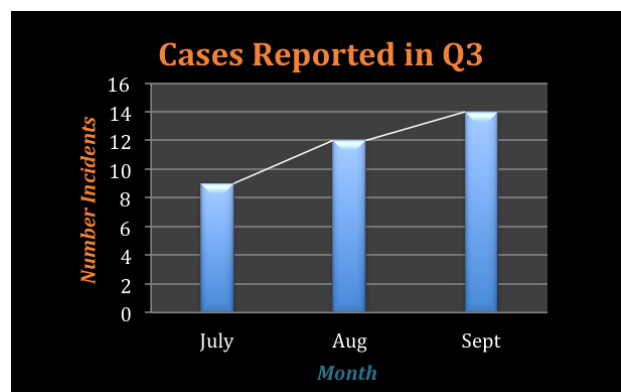


Figure 3 – Breakdown of Fraud Purchase Incidents in Q3

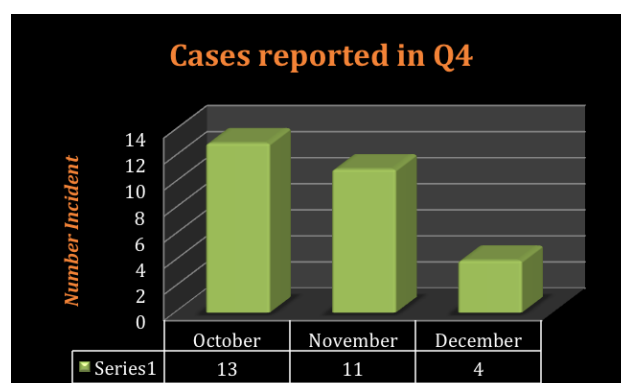


Figure 4 – Breakdown of Fraud Purchase Incidents in Q4

Figures 1 to 4 show no sudden spikes in purchase fraud incidents throughout the year.

## The People behind Purchase Fraud

In any purchase fraud, the seller advertises goods that may not even exist. The advertisement usually uses today's popular social networking sites such as Facebook. Some may even call their buyers over the phone to convince them.

As the Internet shopping and online auctions grow in size and popularity, the number of complaints on purchase fraud also increases. Besides loss of money and goods, buyers sometimes receive goods that are less valuable than the one advertised and even, goods that are significantly different from its original description. Some buyers have



complained on sellers who fail to disclose the full information on the product.

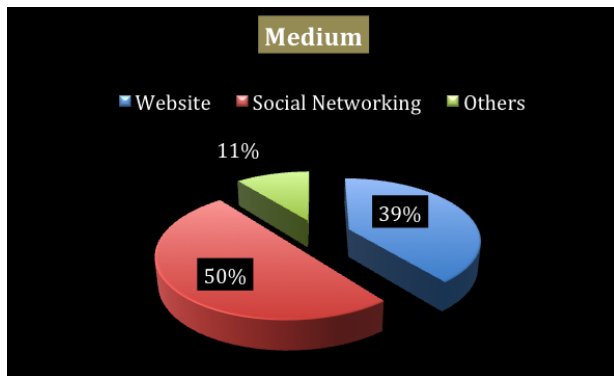


Figure 5 – Fraud Purchase by Medium Used in 2014

Half of the fraud incidents (50 per cent) happened on social networking sites. The most common social network site used by the criminals is Facebook. Almost 40 per cent of the cases occurred over websites such as mudah.my, lelong.com and others.

However, some of the complainants did not provide sufficient information for a complete analysis when reporting to Cyber999. As a result, some cases had to be closed unsuccessfully – this makes up 11 per cent of the incidents.

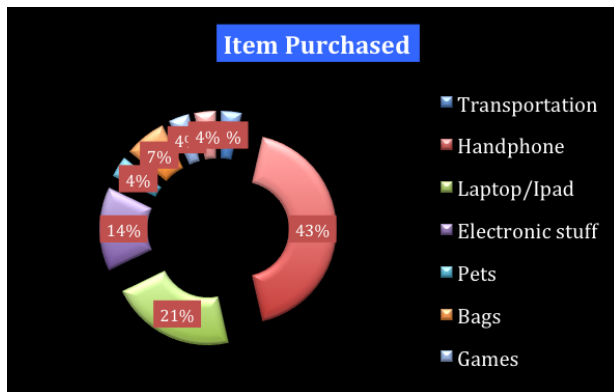


Figure 6 - Percentage of Fraud Purchase by Affected Component in 2014

The most common item involved in last year's cases were handphones. They were advertised heavily on Facebook by these fraudster. Cyber999 regularly lodges reports to Facebook, urging investigation on those pages. Facebook will then investigate these incidents and even, terminate accounts that violate service terms. As for fraudsters who use websites to advertise their merchandise, Cyber999 notifies the website administrators and

Law Enforcement Agencies to take necessary action on the respective sites.



Figure 7 – Percentage of Fraud Purchase by Target

Cyber999 finds that majority of the complainants are local Internet users. Locals are advised to lodge a police report and foreigners can report to the Malaysian Embassy in their respective countries. Complainants are required to provide supporting documents, which will be extended to the respective Law Enforcement Agencies for further investigation.

Internet users are advised to be more careful when buying, selling or dealing with unknown merchants online. Internet user should exercise caution when dealing with online merchants, especially when the person is acting suspiciously. Tips and guidelines on fraud purchase preventions are found on [www.mycert.org.my](http://www.mycert.org.my).

## References:

1. <http://www.mycert.org.my>
2. <http://www.esecurity.org.my>

# The Rise of Cyber Espionage In The Digital World

By | Zaleha Abd Rahim and Zahri Yunos

33

## Introduction

Rapid technology advancement in today's digital world has opened up many opportunities in our daily life such as inspiring creativities, enhance relationships, improving the quality of life and opportunity for wealth creation. However, technology has also created negative activities such as distributed denial of service (DDoS) attacks, defacement attacks, malicious software infections, system intrusion and cyber espionage.

Cyber espionage is defined as the act or practice of obtaining secrets without permission from the holder of the information. It is the hottest topic ever discussed worldwide since Wikileaks and the PRISM programme. In February 2014, Kaspersky Lab Security research team announced the discovery of 'The Mask' also known as Careto, an advanced Spanish language speaking threat actor that has been involved in the global cyber espionage operations since 2007. In March 2014, BAE Systems Applied Intelligence disclosed a Russian cyber espionage campaign code-named as SNAKE that targeted governments and military networks.

## Cyber Espionage Methods and Threats

Examples of cyber espionage is the use of cracking techniques and malicious software including Trojan horses and spyware. It may wholly be perpetrated online from computer desks of professionals on bases in faraway countries or may involve infiltration at home by technically competent conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and unethical software programmers.

The main objective of the cyber espionage attackers is to gather sensitive and valuable data from the infected systems. This include not only office documents, but also various encryption keys, VPN configuration, SSH

keys (serving as a means of identifying a user to a SSH server) and RDP files (used by the Remote Desktop Client to automatically open a connection to a reserved computer).

Cyber espionage operations are well organised and their primary targets are government institutions, diplomatic offices and embassies, energy, oil and gas companies, research organisations and NGOs. Several cyber espionage incidents should be a wakeup call to organisations that underestimate these threats. Organisations that rely on outdated technology for protection should beef up their IT security systems and staff awareness on cyber espionage.

In the case of cyber-attacks against Estonia in 2007 and Georgia in 2008, it was reported that the Russian utilised cyber espionage before conducting the cyber-attacks. During the cyber espionage operations, the actors launched a series of denial of service attacks against the Critical National Information Infrastructure organisations that provide critical services to the country. Government employees' computers, passwords and email accounts were infiltrated. They disrupted, destroyed and stole information from the Critical National Information Infrastructure organisations.

According to Mark Russinovich (RSA Conference 2013), author of Zero Day and Trojan Horse, there are several reasons for States to maintain and utilise aggressive cyber capabilities:

- to deter other States by infiltrating their critical infrastructure
- to gain knowledge, which makes it possible for State to advance more quickly in their military development
- to make economic gains where technological progress has been achieved
- to be able to paralyse an adversary's capability or the adversary's ability to control its own forces in a conflict

## Cyber Espionage Case Studies

### Sponsored State-Actor Activities

Cyber espionage is seen as rivalry process by harassing or provocative actions. The objective is to achieve gains through non-conventional means. An example is the cyber espionage campaigns which had been reported between China and USA, where sensitive documents pertinent to national security were stolen.

### WikiLeaks

WikiLeaks is a non-profit and anti-secrecy media organisation headed by Julian Assange and its modus operandi is to publish both the news stories and the original source material so that readers are able to analyse the story and see the evidence of the truth. WikiLeaks believes everyone has the right to freedom of opinion and expression which includes freedom to hold opinion without interference and to seek, receive and impart information and ideas through any media. The case of Private Bradley Manning, a U.S Army who had digitally copied and released more than 470,000 classified U.S documents to WikiLeaks is an example of cyber espionage.

### PRISM

Another example of cyber espionage is the exposure of PRISM programme by Edward Snowden, a former private contractor for the United States National Security Agency (NSA). Snowden revealed that PRISM is an internet and telephone surveillance program where NSA is given the privilege to access all communications by default. "In other words, you are being watched and recorded even if you are not doing anything wrong", according to Snowden.

### CARETO

The Mask, also known as Careto, is an advanced threat actor that has been involved in cyber espionage operations since 2007. The word 'MASK' comes from Spanish language 'Careto' which means ugly face or mask that was included in some of the malware modules. Careto intercepts all communication channels and collects the most vital information from the infected system. Detection is extremely difficult because of its stealth rootkit capabilities, built-in functionalities and additional cyber espionage modules.

## Tips to Stay Secure

Below are some guidelines to secure against cyber espionage:

### Hide in the network.

Implement hidden services. The less obvious you are, the safer you are.

### Encrypt your communications.

You need to do your best to ensure that your communications are encrypted. You are much better protected than if you communicate in the clear.

### Be suspicious of commercial free software.

Most free encryption products have back doors. It is wise to assume that freeware products also have foreign-installed backdoors. There is no such thing as free lunch. So, be suspicious whenever someone offers you a free package!

### Continuously perform security audit.

One of the methods to improve the security of your network is by having continuous IT Security Audit as well as Vulnerability Assessment of your critical applications, hardware and software. It is also recommended to follow best IT security practices so that you are in compliance with the standard IT security guidelines.

### Monitor your network.

Invest on monitoring the networks for anomalies and security incidents.

### Knowledge sharing.


Sharing information about incoming cyber-attacks to help other networks stay protected. Computer analyst can use the information to understand the attack, who launched it, origin of the attack and how to protect against other similar attack.

Cyber espionage is highly-targeted cyber operation. Therefore, protection to the sensitive information and intellectual property that have the highest value to outsiders should be taken seriously. Those involved in a cyber-espionage usually eavesdrop on communications in the computer network. What sort of defensive mechanism do we have for thwarting against cyber espionage campaign? If our computer networks are unsecured, there is a high probability for us to fall prey to cyber espionage.



1. STRONG PASSWORDS
2. KNOW PRIVACY SETTINGS
3. CARE BEFORE SHARE

**Be smart. Be safe**

logon to [www.CyberSAFE . my](http://www.CyberSAFE.my) to find out more  [cybersafe.malaysia](https://www.facebook.com/cybersafe.malaysia)

# MH370 Cyber Crisis Management

By | Mohd Rizal Abu Bakar

I remember checking my phone for news before going to bed that night on 7th March 2014, when I saw a tweet from Bernama that flight MH370 bound to Beijing was missing. To confirm this news, I switched on the television. Strangely, I found only one station covering the news.

Disappointed, I turned to other sources for more information: the Internet, specifically the social media. On Facebook and Twitter, the timelines were loaded with unverified news, questions, re-sharing of posts and re-tweets on the incident.

Postings on official channels on social media were understandably vague, as authorities organised search and rescue operations with international counterparts. Many turned to social media for information.

Social media postings found on Facebook and Twitter consisted of various emotions:

- *"Where is the plane?"*
- *"Does Hallmark make a card for 'Where the heck is that plane?'"*
- *"Could Malaysia Airlines Flight 370 have been stolen to be used in the future as a terrorist weapon? Hmmm."*
- *"Theory 45: The aircraft was hijacked using a mobile phone."*

In the following weeks and months, various conspiracy theories, speculations and comments were posted on social media related to the missing flight.

## Crowdsourcing to Locate MH370: Did It Really Help or Made It Worse?

Netizens also turned to crowdsourcing to investigate and obtain information on the missing airline. Crowdsourcing is the process of obtaining needed services, ideas or content by soliciting contributions

from a large group of people in online communities for a greater purpose. Among the crowdsourcing websites used were:

1. **Tomnod** – owned by DigitalGlobe, a satellite services and digital mapping provider, gets millions of its users (approximately eight million) to help with the search using high resolution satellite images to scour the 1,007,750km<sup>2</sup> of land and sea [1] for any signs of debris. Each user is given a certain amount of land or sea area to search. Users can tag areas that has characteristics of the missing aircraft and share with others. Images with multiple tags are provided to satellite imagery experts for analysis.

According to a research done by Beutler Ink [2], within the first week of the crisis, a staggering 2.3 million users signed up for the search for MH370 at Tomnod.com, and users had tagged 650,000 objects within a 24,000 square kilometres, viewed 98 million times. By the second week, 14,000 square kilometres of satellite based map of the Straits of Malacca was added to the website.

On the second day of the incident, the website received 100,000 unique visitors per hour. The enormous amount of traffic to the website disrupted its service on one or more occasions. However, the data gathered by Tomnod users was not used by the authorities mainly because data from the Inmarsat satellite and other satellites owned by countries involved in the search and rescue (SAR) operations were already being used.

Among the images tagged by Tomnod users include plane wreckage or debris, rafts and oil slicks. None of the above was verified as authentic and used by the SAR teams.



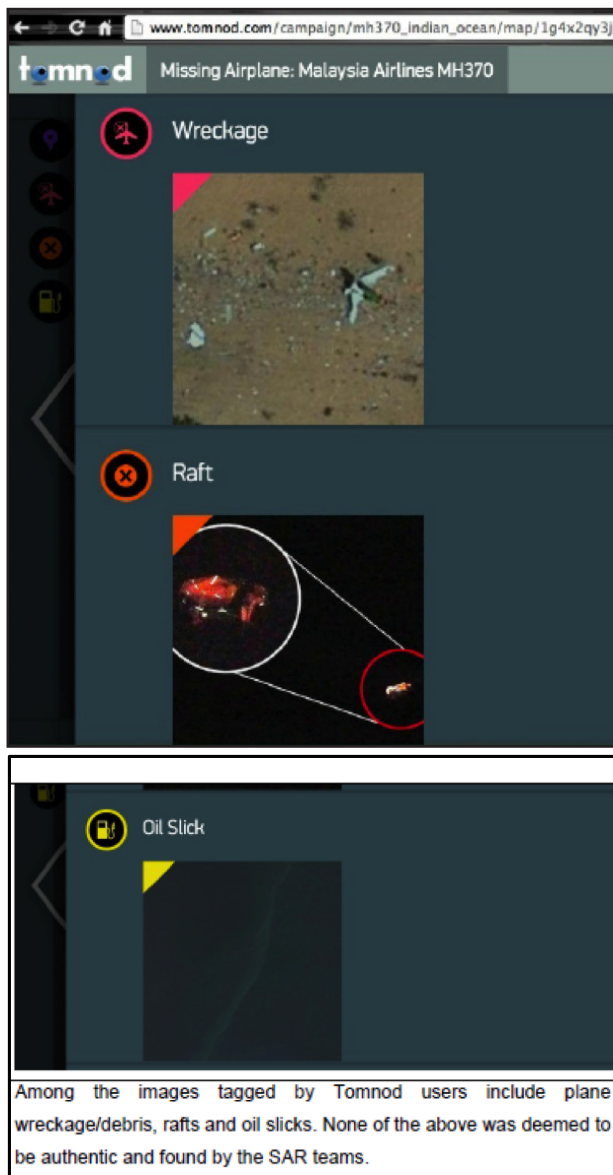


Image 1: Screen capture of Tomnod.com MH370 crowdsourcing campaign

## 2. FlightRadar24 – Provided flight radar playback for the public.



Image 2: Screen capture of MH370 flight playback on FlightRadar24.com

## 3. BlackBridge – The company's website, mapbox.com, provided similar features to Tomnod.com.

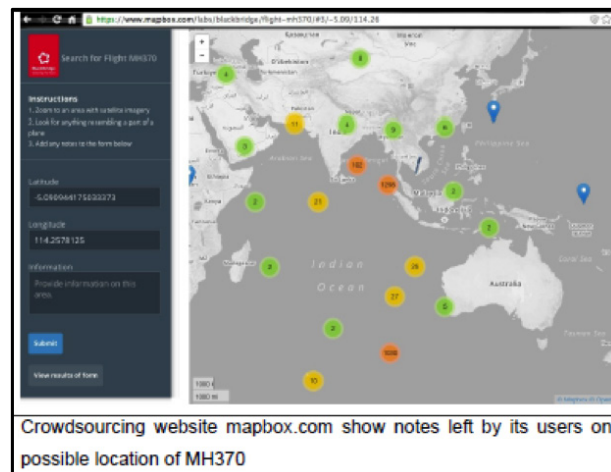


Image 3: Crowdsourcing website, mapbox.com, allows users to leave notes on the possible location of MH370

4. **Twitter** – Over four million tweets with the hash tag #MH370, #Pray4MH370 and #MASalert were posted within two weeks after the incident.
5. **Facebook** – Nexgate.com reported an increase from roughly 50 to 680 social media accounts on the incident, a couple of days after.
6. **Reddit** – *Redditors* moved their focus to daily posts or threads on the crisis, which includes discussions on the updates and speculations.

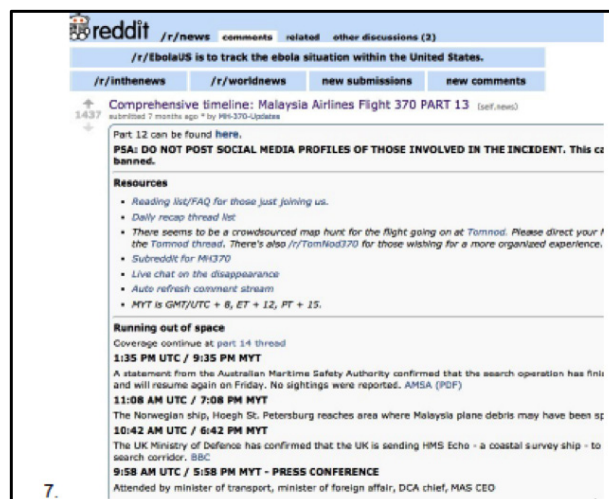


Image 4: Screen capture of Reddit.com posts on MH370

7. **Wikipedia** – The first Wikipedia post was created at 12.37 AM, 8th March 2014. As of 30th October 2014, the number of revisions grew to 10,042, from 2,108 edits.[3]

Malaysia Airlines Flight 370 • en.wikipedia.org			
Page history • LanguageTool Wikicheck • Revisions (Wikipedia)			
General statistics [hide]			
ID:	42140303	First edit:	Mar 8, 2014, 12:37 AM • 6P111
Wikipedia ID:	Q15936324 - 50 items	Latest edit:	Oct 30, 2014, 12:30 AM • Tot1080
Page size:	203,576 Bytes	Max. text added:	Oct 28, 2014, 3:53 PM • Grandmaster • +267,801
Total revisions:	10,842	Max. text deleted:	Oct 29, 2014, 3:27 AM • Magarsia • -29,745
Number of editors:	2,186		

Image 5: MH370 Wikipedia Statistics

The growing popularity of crowdsourcing websites helped in neutralising the information and curiosity of the public, but it did also sparked more conspiracy theories and speculations on the incident. The information compiled by the users of crowdsourcing was not synchronised and verified with the SAR teams on the ground.

Apart from direct officials (Malaysia Airlines, Ministry of Home Affairs, and Ministry of Transportation) involved in the MH370 crisis management, other government agencies need to take part to assist in curbing unlawful Internet related activities using the MH370 crisis as a motive.

## General Consensus

### MH370 Crisis: Social Media or Internet Activities OR Era of the 'anywhere' Newsroom

The Internet is crowded by attention seeking individuals and groups as well as hackers who rely on the number of Facebook, Twitter and Instagram 'likes', 're-tweets' and 'shares' to gain followers and victims.

#### I. Facebook

As of 20th October 2014, Facebook has over a million accounts dedicated to MH370 (these include personal accounts and pages). Survey by Birdsong, social media analytics engine, shows an increase from two per cent to slightly over 16 per cent 'engagement rate' from 8th March to 17th March 2014. The result shows how social media is used to seek and discuss real world issues, specifically MH370 and Malaysia Airlines. However, cyber criminals were also taking advantage of online users by misleading and defraud them.

A report by the International Business Times on 14th March 2014 [4] revealed a Facebook malware that had surfaced on the site, using a video by the title "*Malaysia Airlines*

*Missing Plane MH370 Has Been Spotted Somewhere Near Bermuda Triangle*". Users who clicked on the link are redirected to a malicious phishing site where users will have to share the video to watch it. This gives the hacker access to users' account and continue spreading the link to their connections.

#### II. Twitter

Over 4 million tweets with the hash tag (#MH370) were posted in just two weeks after the incident. It also recorded a 20 per cent increase in followers just two days after. On day five of the search (12th March 2014), over one million tweets were posted by an estimated 360,000 users, not including re-tweets. Tracked tweets were based on three main hash tags:

- #MH370
- #Pray4MH370
- #PrayForMH370
- #DoaUntukMH370
- #MASalert

The *tweets* made by users consisted of messages of prayer and hope for the rescue of the passengers, its crew and passengers as well as SAR teams. The topics that were absent in the tweets compiled by Day Five of the search:

- i. Information on the search and rescue progress
- ii. Criticism of the search efforts
- iii. Deliberate misinformation on search efforts
- iv. Conspiracy theories
- v. Criticism of BN leaders, the media and PR leaders (for remarks made)

The Twitter heat maps below show tweets were made mainly from Malaysia, although there was a high concentration made from Bangkok, Thailand as well.

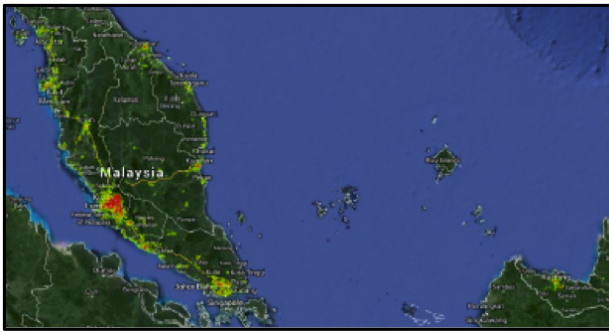


Image 6: Red signified High Concentration, yellow signified medium and green, few.

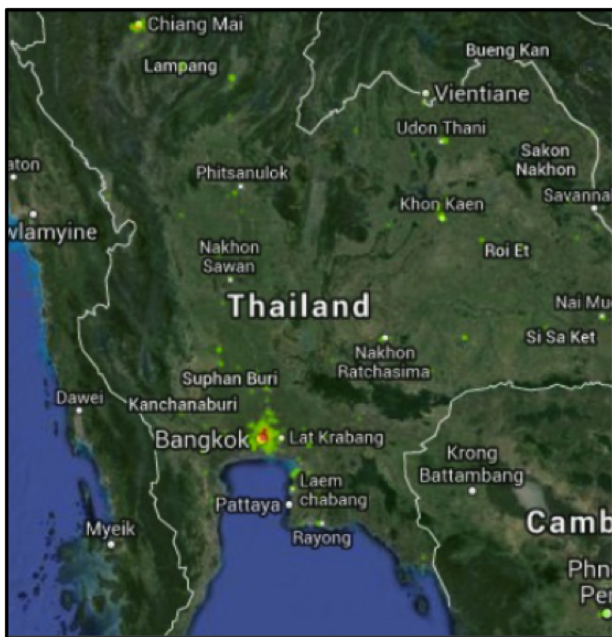


Image 7: Thailand Tweets concentration for MH370

Using link-shortener services, scammers and hackers also used Twitter to send malicious links to victim's friends. Worse still, adult content, hate speech and other non-related content now litter the Internet, specifically in the social media platforms. Nexgate's survey shows an increase from 0 to 3,900 instances of 'bad content' in the period of nine days after the incident. [3]

### III. Instagram

Out of respect to the flight crew, passengers and families of MH370, Malaysia Airlines did not upload posts on the incident on Instagram between 27th March and 20th May 2014.

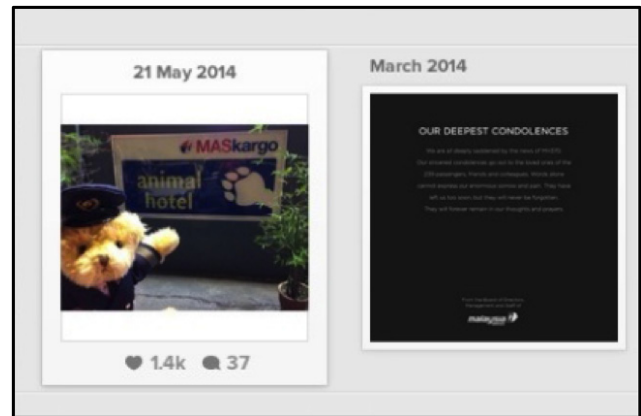


Image 8: Malaysia Airlines Instagram account posting gap out of respect to the loss of MH370

Examples of unethical usage of social media on the crisis:

1. Sharifah Sofia Syed Rashid (MAS employee)
  - Posted conspiracy theories on the missing MH370 on her Facebook. She claimed that the Malaysian government and media was instructed by the US government to deny allegations that the flight was last seen in the Maldives. Her account was deactivated shortly after and someone claiming to be her relative said she was sick.



Image 9: Sharifah Sofia's Facebook post on MH370



## 2. Krish Jeendira (Air Asia pilot)

- Accused the Malaysian government of hiding the truth behind the flight's disappearance. The senior first officer was later suspended by the management of Air Asia.



Image 10: Krish Jeendira, a senior First Officer with Air Asia, criticised the government for 'hiding the truth'

## 3. Alex Chow - individual

- Incited racism, insulted Islam and Prophet Muhammad and blamed the government for MH370 on Facebook.

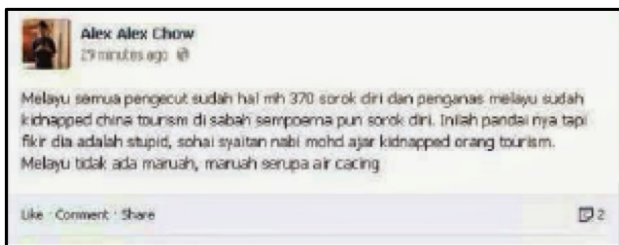


Image 11: Alex Chow's hate speech on Facebook

- The author published an article on the allegations of MH370 hijacked using the 'Red Switch Autopilot' to crash into Petronas Twin Towers.



Image 11: Theory on MH370 hijacked using a system called 'Red Switch Autopilot'

## Managing Information: Classification or Categorisation

When managing information during a crisis, information can be categorised as:

- Official Medium (Television, radio, social media, websites)
  - Official Information – reports, press statements, social media posts, articles
- Unofficial Medium (Television, radio, social media, websites)
  - Unofficial Information – social media posts, articles

These are the methods used by both official and unofficial media to relay information on the MH370 crisis:

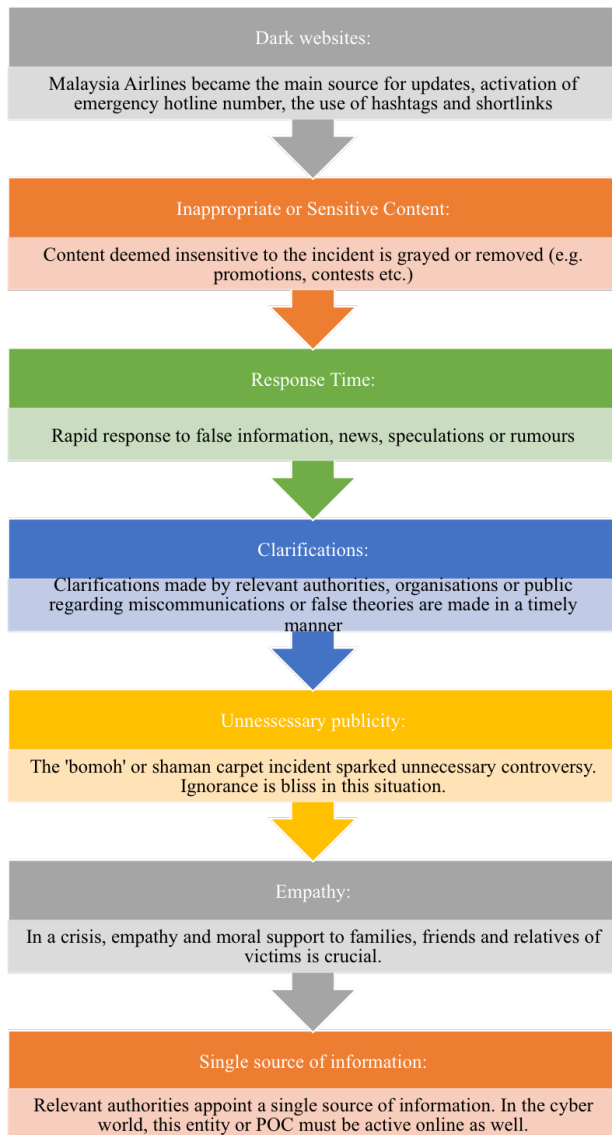


Figure 1: Steps to be taken in a crisis

## What is a Dark Site?

When a crisis strikes an organisation, its website is normally the first point of contact for the public. A prebuilt Dark Site can be used or activated quickly during a crisis. The purpose of a *Dark Site* is primarily strategic. Positioning the organisations involved as the primary source for information will help in suppressing and controlling dangerous speculations and rumours.

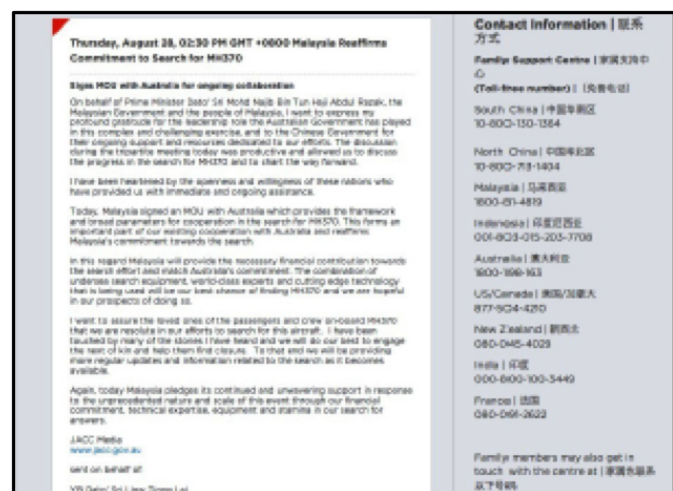


Image 12: Screen capture of Malaysia Airlines' Dark Site

The purpose of a *dark site* is to show the media and public the importance organisation places in providing accurate and timely information on the crisis.

Ways to activate and use the '*dark site*':

- The current everyday website is completely removed and replaced with the dark site.
- A link to the Dark Site is displayed prominently on the everyday website to redirect users.
- A separate URL is created based on specific search terms.





Image 13: Greyed out logo and profile photo on Malaysia Airline Facebook page

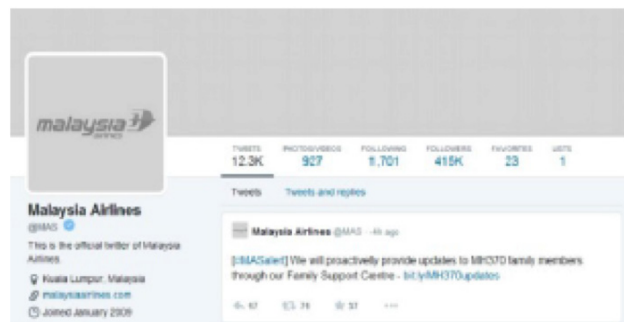


Image 14: Greyed out logo and profile photo of Malaysia Airlines' Twitter page

The main issues that surfaced during the initial phases of the crisis were information accuracy and timing. The relevant authorities were deeply criticised mainly for the following reasons:

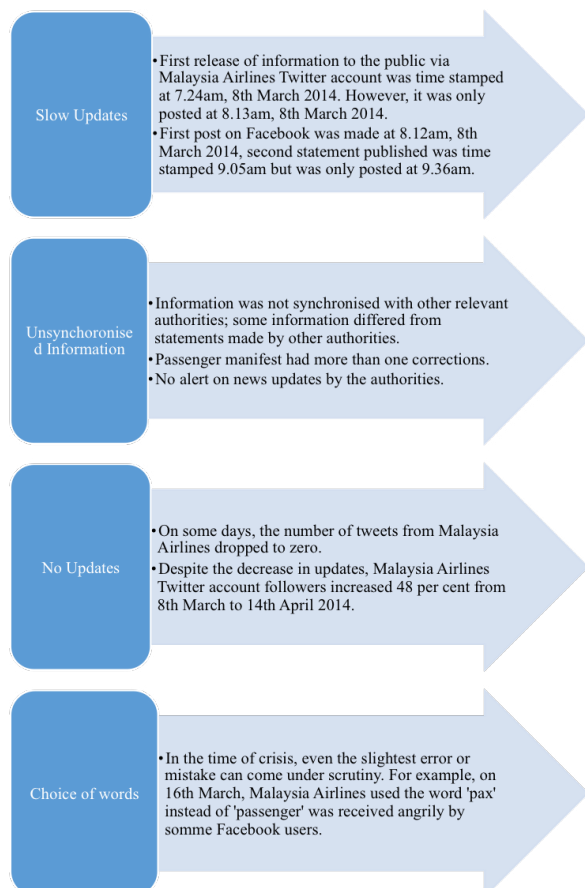


Figure 2: Main issues with social media management by relevant authorities for MH370

## Why and how to address these issues?

A crisis of large magnitude requires training and specialty. Efforts have to synchronised and cyber related issues must be taken into consideration.

The slow updates were probably due to uncertainty. In this case, information relayed from one country to another took time because of the following factors:

- Time differences – not everyone was awake when the news broke over the media or Internet. Although SAR teams and relevant organisations involved in the crisis worked non-stop, they need rest and time to recover.
- Telecommunications problems – SAR team used radio and satellite telecommunications to communicate information. Information received for the team needs to be confirmed before delivering to the organisations involved.
- Language barrier – as the first search area was in Vietnam waters, this could also cause delay.
- Limitation in resources – vague or unconfirmed or unsynchronised data from each country involved

## What we need to learn

- Do not use Social Media used to spread inaccurate information. It is crucial to check facts and correct misinterpretations, before spreading it.
- Get your strategies right. In a crisis, relevant authorities must understand their cyber tactics and maintain an active online presence.

Organisations should invest in a good crisis management plan, especially one with a cyber-perspective. Our five recommendations for a successful crisis management:

## Step 1: Preparation

Setting up mitigation measures:

- i. Establish a central cross-functional Crisis Communication Team consisting of:
  - a. CyberSecurity Malaysia (an agency under the Ministry of Science, Technology and Innovation) – to lead in the detection, monitoring and advice relevant authorities during crises from a cyber-security standpoint. Other members of the team include Royal Malaysian Police (PDRM), Royal Malaysian Army, Ministry of Transportation, Ministry of Internal Affairs and External Affairs as well as major transportation companies.
- ii. Ensure all transportation companies, government agencies have a ‘*Dark Site*’ updated regularly during crises and a toll free number to be activated.
- iii. Cultivate *influencers* and advocates in all social media platforms with the task of managing and monitoring crowd reactions during crises.

## Step 2: Identify the type of crisis

There are three types of crisis:

- i. Sudden – unexpected
- ii. ‘Volcanic’ – on-going or in the process
- iii. Bizarre – unexpected

## Step 3: Respond, Respond and Respond

Updating is key.

- i. Convene with the crisis communication team
- ii. Research for references similar to crisis situation
- iii. Activate *dark sites* and hotline
- iv. Prepare official statements with accurate information *before* releasing it to the media and public
- v. Address viral reports from the media and the public immediately.

## Step 4: Assessment

- i. Evaluate and reassess the scenario and issues *honestly*
- ii. De-brief internal, external parties involved as well as the customers (other flight passengers, vendors)
- iii. Prepare for the future

## Step 5: Integration of awareness with traditional and alternative media

- i. Use key channels and appointed influencers to target:
  - a. Employees
  - b. Media
  - c. Customers
  - d. Other influencers
- v. Try *not to control* the message or situation, but influence it.
- vi. Be transparent – if it’s a mistake, apologise. This reduces rumours and speculations.
- vii. Collaborate with other airlines (OneWorld Alliance for Malaysia Airlines), airports and authorities to send the message across to the public.

## References

1. [1]<http://nexgate.com/blog/malaysian-airlines-mh370-plays-out-in-socialmedia/>
2. [2]<http://www.beutlerink.com/blog/thin-air-internet-responds-malaysia-airflight-370/>
3. [3][http://tools.wmflabs.org/xtools/articleinfo/index.php?article=Malaysia\\_Airlines\\_Flight\\_370&lang=en&wiki=Wikipedia](http://tools.wmflabs.org/xtools/articleinfo/index.php?article=Malaysia_Airlines_Flight_370&lang=en&wiki=Wikipedia)
4. [4] <http://www.ibtimes.com/new-facebook-malware-fake-video-claimsmalaysia-airlines-missing-plane-mh370-has-been-spotted>
5. [5] <http://twittercounter.com/MAS>

# Documented Information in ISO/IEC 27001:2013 Information Security Management Systems (ISMS)

By | Noor Aida Idris

## Introduction

ISO/IEC 27001 Information Security Management Systems (hereinafter referred to as ISMS) is a management system standard for information security. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security for organisations. ISO/IEC 27001 was revised and published on 1st October 2013 as ISO/IEC 27001:2013 Information Security Management Systems (ISMS) - Requirements. Since then, organisations are exploring every resources to have better understanding of the new requirements in the revised ISO/IEC 27001.

One of the new requirements stated in the revised ISO/IEC 27001 is clause 7.5 Documented Information. Even though there are minor changes to the requirements of managing and controlling the documented information, the overall description of mandatory documented information have changed. Thus, organisations which are interested to implement ISO/IEC 27001:2013 ISMS and apply for ISO/IEC 27001:2013 ISMS certification, must have thorough understanding of the clause in order to produce the mandatory documented information for its ISMS.

As depicted in clause 7.5.1 of ISO/IEC 27001:2013 ISMS, the documented information in ISMS can be categorized as below:

- (a) documented information as required by ISO/IEC 27001:2013
- (b) documented information determined by an organisation as being necessary for the effectiveness of its ISMS.

This article focuses on documented information for category (a) which are mandatory for ISMS implementation and certification. It provides explanation on

the documented information including a list of mandatory documented information with description for each documented information. Details for category (b) will be written in an upcoming article.

## What does Documented Information Means

Documented information is defined by ISO/IEC 27000:2012 ISMS - Overview and Vocabulary as information required to be controlled and maintained by an organisation and the medium on which it is contained. Documented information can be in any format (e.g. hardcopy or softcopy) and on any medium (e.g. thumb drive, hard disk or CD) and can come from any sources.

In the previous version of ISO/IEC 27001, these documented information were known as documents and records. Examples of the documented information are documents which are created based on the ISMS requirement such as ISMS Scope, ISMS Risk Assessment Policy and ISMS Measurement Plan. As for records, they can be any evidence as a result achieved from organisational operation e.g. visitor's log book, audit reports and completed forms.

The extent of the documented information for an organisation, however, differs from one organisation to another. Factors that may influence the documented information are the size of the organisation itself including the type of processes and services it provides. In addition, the scope of ISMS and complexity of the security requirements can cause the size of documented information to vary between two organisations.

## Mandatory Documented Information

Mandatory documented information is

information that should be produced, documented and maintained by any ISMS certified organisations as proof of evidence that the ISMS has been implemented. Now, how can organisations identify which documented information is mandatory and which is not? As a clue, organisations should look for the keyword "documented information" in the clauses of ISO/IEC 27001:2013 ISMS. As an example, refer to clause 4.3 where it states "The scope shall be available as documented information". The clause 4.3 indicates that an ISMS scope is a mandatory documented information which must be produced, documented and maintained. Please take note, however, while ISMS scope must be documented, the title of the document does not necessarily have to be "ISMS scope". It is satisfactory for the ISMS scope to be documented in any document e.g. ISMS Manual or ISMS Framework.

Furthermore, some of the documented information can be combined into one single document to ensure clarity and continuity of the required information. For example, clause 6.1.2 of ISO/IEC 27001:2013 states that "The organisation shall retain documented information about the information security risk assessment process" and clause 6.1.3 of ISO/IEC 27001:2013 states that "The organisation shall retain documented information about the information security risk treatment process". An organisation may fulfil these two (2) requirements by producing a single documented information entitled "Risk Management Process" that describes both information security risk assessment and treatment process together.

There are also cases where information can exist via multiple documents or records. As an example, evidence of competence, as stated in clause 7.2 d) of ISO/IEC 27001:2013, may exist in the form of certificates of attendance for each training (e.g. ISMS Implementation Training, ISMS Internal Auditor Training and ISMS Lead Auditor Training) attended by ISMS personnel. Moreover, other competence evidence in the form of qualifications and working experience for the personnel must be produced and retained.

Documented information for ISMS are required to be maintained and kept for a certain period of time that can sufficiently verify the ISMS implementation and its effectiveness. The minimum retention period differs from one organisation to another organisation, depending on the legal and regulatory requirements, business requirements, contractual obligations or customer requirements.

The documented information such as policies and procedures need to be reviewed and approved by relevant personnel in the organisation. Evidence of the approval should be maintained by the organisation for audit purposes. Additionally, all versions of the documented information must be controlled as required by clause 7.5.3 Control of Documented Information. And finally, to ensure that the organisation continually improves the suitability, adequacy and effectiveness of its ISMS, the documented information should be reviewed regularly and updated accordingly.

For full details of documented information as required by ISO/IEC 27001:2013 ISMS, please refer to Table 1: Mandatory Documented Information in ISMS. The order of which the mandatory documented information is listed based on its appearance in the ISO/IEC 27001:2013 ISMS does not denote the importance or magnitude of the documented information.

Information required to be documented	Description	Reference in ISO/IEC 27001:2013
1. ISMS Scope	Information on organisational ISMS scope and boundaries should be documented. When determining the ISMS scope, the organisation should consider external and internal issues, requirements of interested parties relevant to information security, and interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations. Any changes to the current ISMS scope and boundaries should be reflected in the documented information.	Clause 4.3
2. Information Security Policy	Information Security Policy is the highest-level policy, which overarches other supporting policies for ISMS implementation. Guidance on the content of an information security policy document is provided in ISO/IEC 27002. The policy should be documented and reviewed regularly. The policy should be made available to the relevant people within the organisation as well as external party.	Clause 5.2 e)
3. Information security risk assessment process	Information about information security risk assessment process covers the end-to-end process of information security risk assessment activities for the organisation. This include information security risk criteria, risk identification, analysis and evaluation activities.	Clause 6.1.2
4. Information security risk treatment process	Information security risk treatment is the process of determining and implementing information security controls to modify information security risk. Information about information security risk treatment process should be documented that include the process for selecting information security risk treatment options, formulating information security risk treatment plan (RTP) and obtaining approval of the RTP from risk owners.	Clause 6.1.3
5. Statement of Applicability (SOA)	Statement of Applicability (SOA) contains the necessary information security controls and justifications for inclusions, whether they have been implemented or not; and the justifications for exclusions of information security controls from Annex A of ISO/IEC 27001:2013.	Clause 6.1.3 d)



6. Information security risk treatment plan (RTP)	An information security risk treatment plan (RTP) needs to be formulated based on the outcome of a risk assessment exercise. This plan needs to be documented and monitored to ensure that the risks are being treated accordingly. Also, each RTP must be approved by the relevant risk owner.	Clause 6.1.3 e)
7. Information security objectives	Information security objectives should be established at relevant levels and functions that are consistent with the information security policy. The objectives should be measurable, communicated and updated as and when required. Also, they should be documented and reviewed regularly.	Clause 6.2
8. Evidence of competence	Organisations should determine the competencies required for the person(s) responsible to perform tasks related to ISMS and controls that may affect the ISMS. Evidence of competence should be documented in terms of provision of trainings, records of skills, experience and qualification, actions taken to acquire the necessary competence and evaluation for the effectiveness of the actions taken.	Clause 7.2
9. information to the necessary extent to meet the confidence that the processes have been carried out as planned	Operational processes and activities related to ISMS should be carried out regularly. Information on these should be documented. Any changes related to these operational processes and activities should be documented to provide evidence that the processes and activities have been carried out as planned.	Clause 8.1
10. Results of the information security risk assessments	Information security risk assessments should be conducted at planned intervals or when there are changes that may introduce new risks to the organisation. The results of these risk assessment exercises should be documented and monitored regularly.	Clause 8.2
11. Results of the information security risk treatment	The results of the risk treatment exercise needs to be documented, which includes status of treating the risks. The documented results should be presented to top management for approval.	Clause 8.3

12.Evidence of monitoring and measuring results	Monitoring and measuring is an important process in ISMS. Any evidence that exists as a result of monitoring and measuring activities should be documented. The documented information should include what is to be monitored and measured (which can include information security processes and controls), the mechanisms to perform this; and also the personnel responsible to monitor, measure, analyse and evaluate the outcome of monitoring and measuring the ISMS.	Clause 9.1
13.Evidence of the audit programme and the audit results	Internal ISMS audit is another requirement in ISMS. Evidence that exists as a result of the internal ISMS audit should be kept and documented. The documented information may include (but not limited to) the audit programme, policies and procedures related to internal ISMS audit, audit reports and audit notes.	Clause 9.2
14.Evidence of the results from management reviews	The review of ISMS may be conducted via management review. Thus any evidence that may exist as a result of management review should be documented and retained. The documented information for management review may include (but not limited to) minutes of meetings, memos, approval sheets and related emails.	Clause 9.3
15.Evidence of nonconformities and any subsequent actions taken; and results of any corrective action	Information on the nature of the nonconformities and any subsequent actions taken should be documented and retained. Also, corrective actions that have been taken to rectify nonconformities should be documented and retained. The documented information may include (but not limited to) details of the corrective actions taken to resolve the nonconformities, status of the corrective actions and duration for the nonconformities to be resolved.	Clause 10.1

Table 1: Mandatory Documented Information in ISMS

## Conclusion

Clause 7.5 Documented Information is one of the new requirements in ISO/IEC 27001:2013 ISMS. The clause specifies requirements for all ISMS certified organisations in producing documented information. As described in this article, mandatory documented information are information that must be documented as evidence of ISMS implementation. Examples of the mandatory documented information are ISMS Scope, Information Security Policy and Statement of Applicability. Details of all mandatory document information are described in Table 1: Mandatory

Documented Information in ISMS. The documented information must be controlled in accordance to the ISMS requirement. Lastly, organisations must conduct regular review of the documented information; to ensure the ISMS remains relevant and effective.

## References:

1. ISO/IEC 27001:2013 Information Security Management Systems (ISMS) - Requirements
2. ISO/IEC 27000:2014 Information Security Management Systems (ISMS) - Overview and Vocabulary

# 2015 Cyber Security Training Schedule

2015 Cyber Security Training Schedule														
Fundamental/Introduction	Program Duration	Standard Fees (RM)	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
1 Critical Infrastructure Protection	2 days	1,650.00		9 - 10					29 - 30					
2 Digital Forensics Essential	2 days	1,950.00	6 - 7		10 - 11		20 - 21					12 - 13		
3 Malaysia Common Criteria 1.0 (MyCC) - Understanding Security Target, Protection Profile & Supporting Evaluation	1 day	1,200.00				2						20		
4 Introduction to ISO 27001 - Information Security Management System (ISMS)	1 day	1,000.00	8		3			9		4	2		4	
5 Data Encryption for Beginners	1 day	1,200.00		12										
6 Cryptography for Beginners	1 day	1,200.00			5						2			
7 Cyber CSM Security Essential	2 days	1,800.00		4 - 5			18 - 19	8 - 9			29 - 30			9 - 10
8 Google-Fu Power Search Technique	2 days	1,600.00						1 - 2						
9 Wireless Security	2 days	1,800.00											18	7 - 8
10 Forensics on Internet Application	1 day	1,200.00	13											
11 ISO/IEC 27001:2005 Migration to ISO/IEC 27001/2013 (*new)	2 days	1,600.00		24-25			5-6							
12 Cyber Terrorism (*new)	1 day	1,800.00			10									7
13 Introduction to Business Continuity Management (*new)	1 day	1,000.00				1				18				
Intermediate	Program Duration	Standard Fees (RM)	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
1 Malaysia Common Criteria (MyCC 2.0) - Foundation Evaluator Training	3 days	3,400.00				7 - 9						19 - 21		
2 Cryptography for Information Security Professional	3 days	3,600.00			24 - 26						8 - 10			
3 ISO 27001 Implementation	3 Days	3,500.00			17-19					11 - 13		6 - 8		1 - 3
4 Incident Handling and Network Security Training (IHNS)	3 days	3,650.00				21 - 23			27 - 29				23 - 25	
5 Network Security Assessment Training	3 days	2,400.00	12 - 14				12 - 14						17 - 19	14 - 16
6 Server and Desktop Security Assessment Training	3 days	2,400.00	20 - 22											
7 Web Application Security Assessment Training	3 days	2,400.00	26 - 28									5 - 7		
8 Digital Forensic for First Responder	4 days	3,400.00				13 - 16						26 - 29		
Specialization / Specific Domains	Program Duration	Standard Fees (RM)	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
1 Digital Forensics for Law Practitioner	3 days	2,400.00					5 - 7				7 - 9			
2 Security Posture Compliance, Assessment and Penetration Testing	5 days	4,000.00			2 - 6								2 - 6	
3 ISMS Internal Auditor Course (ISO 27001)	2 days	2,950.00			23 - 25				29 - 30				25 - 26	
Professional Certification	Program Duration	Standard Fees (RM)	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
1 Business Continuity Management Professional Certification (BCLE2000)	5 days	8,900.00			9 - 13		11 - 15			24 - 28		5 - 9	30 - 4	
2 ISO/IEC 27001 Lead Auditor (External Auditors)	5 days	5,499.00	19 - 23		16 - 20	20 - 24	11 - 15	8 - 12	6 - 10	3 - 7	28 - 2		23 - 27	14 - 18

Corporate Office:

**CyberSecurity Malaysia**

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

Tel: +603 8992 6888

Fax: +603 8992 6841

Email: [info@cybersecurity.my](mailto:info@cybersecurity.my)

Customer Service Hotline: 1300 88 2999

**[www.cybersecurity.my](http://www.cybersecurity.my)**

©CyberSecurity Malaysia 2014 -All Rights Reserved

