CyberSecurity
MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 38 - (1/2015)

Panduan Ibu Bapa: Keselamatan Rangkaian Sosial untuk anak-anak

Intrusion Attempt: Who’s knocking your door

6 Simple tips to stay safe on instagram

> *“People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems. ”*
>
> *Bruce Schneier, Secrets and Lies*

ISSN 1985-1995

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

Securing Our Cyberspace

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

www.cybersecurity.my

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

CyberSecurity MALAYSIA

CyberSecurity Malaysia
(726630-U)

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

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

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

An agency under
MOSTI
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

Best Brand
Internet Security
2008 & 2009

ISMS SIRIM | UKAS INFORMATION SECURITY MANAGEMENT 074
CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

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

MSC MALAYSIA
Status Company

Best Child Online
Protection Website

WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA

Today we are looking at the 38th edition of eSecurity Bulletin, which is rich with information and knowledge packed within the 34 bi-lingual articles written by our employees. The articles are a good mix of virtual and physical security issues, presented from the legal, technical, organisational and social perspectives. Through the articles, readers would gain valuable knowledge and insights that only our employees with so many years of working experience in this niche and unique field could come up with.

> “It has been famously argued that information is power and, therefore, should never be shared. The Sept. 11 attacks showed the fatal flaws in that logic. Our nation is becoming safer every day because we are aware that information increases in power only when it is shared.”
>
> (Dennis C. Blair, the former United States Director of National Intelligence).

If you agree with Blair that information is power and that power increases when shared, kindly share this e-Security Bulletin freely. With the increase in the power of information, we hope to also increase the number of people benefiting from the e-Security Bulletin. Insya-Allah.

Thank you,

Dr. Amirudin Abdul Wahab
Chief Executive Officer, CyberSecurity Malaysia

EDITORIAL BOARD

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

Steganography Series: Colour Palettes

By | Abdul Alif Bin Zakaria, Nor Azeala Mohd Yusof, Liyana Chew Binti Nizam Chew

Introduction

Steganography comes from the Greek word “Steganos,” which means covered or secret and “graphy” that means writing or drawing [1]. Therefore, steganography literally means covered writing. In other words, steganography is the hiding of secret messages within ordinary messages and their extraction at the destination. Basic steganography models contain three elements, namely the cover object, message and stego key. The object is also known as a carrier, in which a message is embedded and serves to hide the existence of the message. The object can be in the form of an image, text, audio or video. A message is the data whose secrecy a sender wishes to maintain. It can be in the same form as a cover object. A stego key functions as a password that ensures only a receiver who knows the key will be able to read the message from the cover object. A cover object with a secretly embedded message is thus called a stego object. Colour is one of the basic building blocks of image creation, which is the most common cover object used to hide messages. Therefore, this article addresses the colour palette, which is an important steganography element used to hide information in images.

Hiding Information in Images

The decrease in the price of image manipulation devices has led to an increasing number of high quality images presented in digital form. Current workstation monitor technology has an average resolution of 100 dpi (dots per inch), fax quality ranging from 200 to 400 dpi, low-cost laser and inkjet printers producing between 300 and 720 dpi or even 1200 dpi as well as scanners [2].

Audio, video and images are stored in computers as files. These files may be in different formats. However, a general image is an array of numbers that represent the intensity level of each pixel comprising the image. A colour image is represented by arrays for each of the three primary colours, which are red, green and blue. By superimposing the three arrays, each pixel, being a sum of those three colours, will produce a coloured image.

Digital images are typically stored in either 24-bit (true colour) or 8-bit files (colour palette).

24-bit pictures have better resolution; thus, the file size would be larger and there would be more space available to hide information. 3 bytes are used to represent each pixel (1 byte for each colour) in 24-bit images. These 3 bytes can be represented as hexadecimal, decimal or binary values. An FFFFFF sequence represents a combination of 100% green, 100% red and 100% blue that will produce white. This combining method is applied to each pixel in order to create an image. Information can be hidden by embedding secret messages into image pixels depending on the method implemented by users.

Colour Palettes

In computer graphics, a palette is either a given finite set of colours for the management of digital images (a colour palette), or a small on-screen graphical element for choosing from a limited set of choices. Table 1 and Table 2 are examples of a Standard Line Colour Palette and Named Colour Palette [3] for reference. Further explanations of colour palettes are given herein.

1. The total number of colours that a given system is able to generate or manage (though, due to video memory limitations, it may not be able to display them all simultaneously):
   - Full palette: For example, high-colour displays are said to have a 16-bit RGB palette.
2. The limited selection of colours that can be displayed simultaneously:

   a) On the whole screen:

   - Fixed palette selection: A given display adapter offers a fixed colour selection when its hardware registers are appropriately set. For example, the Colour Graphics Adapter (CGA) in one of the standard graphics modes can be set to show the so-called palette #1 or palette #2: two combinations of 3 fixed colours and one user-defined background colour each.

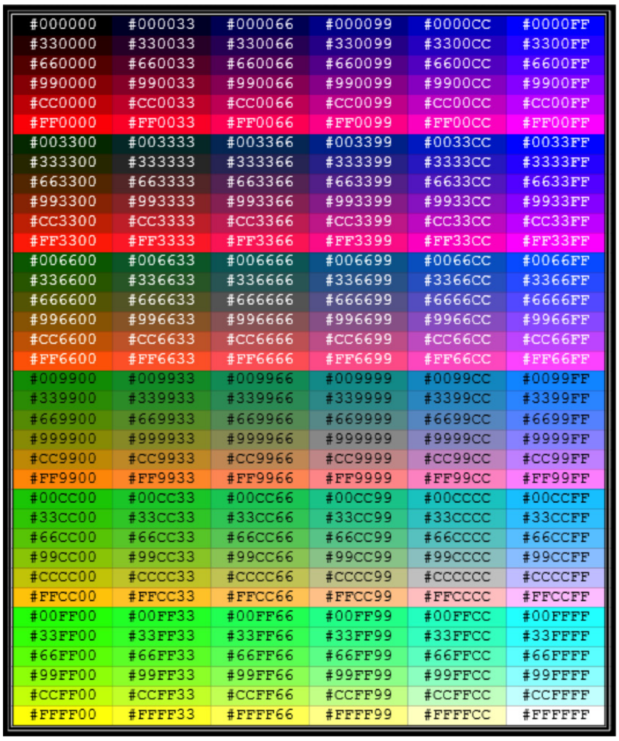
- Selected colours: In this case, the colour selection, generally from a wider, explicitly available full palette, is always chosen by software, user or program. For example, the standard VGA display adapter is known to provide a palette of 256 simultaneous colours from a total of 262,144 (2^{18}) different colours.
- Default palette or system palette: The given selected colours have been officially standardized by a body or corporation, for example the well-known Web-safe colours (216 colours) for use with Internet browsers, or the Microsoft Windows default palette.

b) On an individual image:

- Colour map or colour table: A limited colour selection is stored inside a given indexed colour image file, e.g. GIF.
- Image palette or image colours: A limited colour selection is assumed to be the full list of colours the given digital image has, even when the image file does not employ indexed colour pixel encoding.

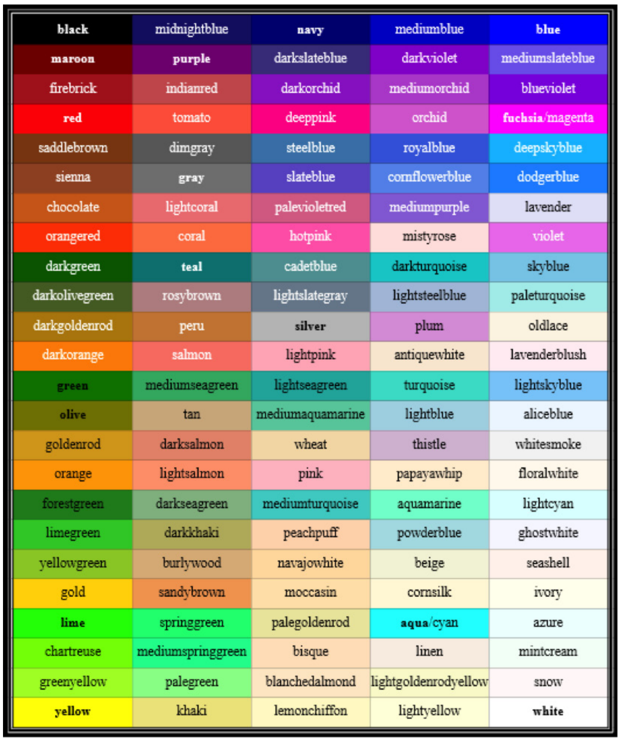
3. The underlying hardware that may be used to hold simultaneous colours:

a) Hardware palette or Colour Look-Up Table (CLUT): In order to display colours, the selected colours' values must be loaded in the colour hardware registers of the display subsystem. For example, the hardware registers of the Commodore Amiga are known both as the colour palette and the CLUT, depending on the sources.



#000000	#000033	#000066	#000099	#0000CC	#0000FF
#330000	#330033	#330066	#330099	#3300CC	#3300FF
#660000	#660033	#660066	#660099	#6600CC	#6600FF
#990000	#990033	#990066	#990099	#9900CC	#9900FF
#CC0000	#CC0033	#CC0066	#CC0099	#CC00CC	#CC00FF
#FF0000	#FF0033	#FF0066	#FF0099	#FF00CC	#FF00FF
#003300	#003333	#003366	#003399	#0033CC	#0033FF
#333300	#333333	#333366	#333399	#3333CC	#3333FF
#663300	#663333	#663366	#663399	#6633CC	#6633FF
#993300	#993333	#993366	#993399	#9933CC	#9933FF
#CC3300	#CC3333	#CC3366	#CC3399	#CC33CC	#CC33FF
#FF3300	#FF3333	#FF3366	#FF3399	#FF33CC	#FF33FF
#006600	#006633	#006666	#006699	#0066CC	#0066FF
#336600	#336633	#336666	#336699	#3366CC	#3366FF
#666600	#666633	#666666	#666699	#6666CC	#6666FF
#996600	#996633	#996666	#996699	#9966CC	#9966FF
#CC6600	#CC6633	#CC6666	#CC6699	#CC66CC	#CC66FF
#FF6600	#FF6633	#FF6666	#FF6699	#FF66CC	#FF66FF
#009900	#009933	#009966	#009999	#0099CC	#0099FF
#339900	#339933	#339966	#339999	#3399CC	#3399FF
#669900	#669933	#669966	#669999	#6699CC	#6699FF
#999900	#999933	#999966	#999999	#9999CC	#9999FF
#CC9900	#CC9933	#CC9966	#CC9999	#CC99CC	#CC99FF
#FF9900	#FF9933	#FF9966	#FF9999	#FF99CC	#FF99FF
#00CC00	#00CC33	#00CC66	#00CC99	#00CCCC	#00CCFF
#33CC00	#33CC33	#33CC66	#33CC99	#33CCCC	#33CCFF
#66CC00	#66CC33	#66CC66	#66CC99	#66CCCC	#66CCFF
#99CC00	#99CC33	#99CC66	#99CC99	#99CCCC	#99CCFF
#CCCC00	#CCCC33	#CCCC66	#CCCC99	#CCCCCC	#CCCCFF
#FFCC00	#FFCC33	#FFCC66	#FFCC99	#FFCCCC	#FFCCFF
#00FF00	#00FF33	#00FF66	#00FF99	#00FFCC	#00FFFF
#33FF00	#33FF33	#33FF66	#33FF99	#33FFCC	#33FFFF
#66FF00	#66FF33	#66FF66	#66FF99	#66FFCC	#66FFFF
#99FF00	#99FF33	#99FF66	#99FF99	#99FFCC	#99FFFF
#CCFF00	#CCFF33	#CCFF66	#CCFF99	#CCFFCC	#CCFFFF
#FFFF00	#FFFF33	#FFFF66	#FFFF99	#FFFFCC	#FFFFFF

Table 1: Standard Line Colour Palette



black	midnightblue	**navy**	mediumblue	**blue**
maroon	**purple**	darkslateblue	darkviolet	mediumslateblue
firebrick	indianred	darkorchid	mediumorchid	blueviolet
red	tomato	deeppink	orchid	**fuchsia**/magenta
saddlebrown	dimgray	steelblue	royalblue	deepskyblue
sienna	**gray**	slateblue	cornflowerblue	dodgerblue
chocolate	lightcoral	palevioletred	mediumpurple	lavender
orangered	coral	hotpink	mistyrose	violet
darkgreen	**teal**	cadetblue	darkturquoise	skyblue
darkolivegreen	rosybrown	lightslategray	lightsteelblue	paleturquoise
darkgoldenrod	peru	**silver**	plum	oldlace
darkorange	salmon	lightpink	antiquewhite	lavenderblush
green	mediumseagreen	lightseagreen	turquoise	lightskyblue
olive	tan	mediumaquamarine	lightblue	aliceblue
goldenrod	darksalmon	wheat	thistle	whitesmoke
orange	lightsalmon	pink	papayawhip	floralwhite
forestgreen	darkseagreen	mediumturquoise	aquamarine	lightcyan
limegreen	darkkhaki	peachpuff	powderblue	ghostwhite
yellowgreen	burlywood	navajowhite	beige	seashell
gold	sandybrown	moccasin	cornsilk	ivory
lime	springgreen	palegoldenrod	**aqua**/cyan	azure
chartreuse	mediumspringgreen	bisque	linen	mintcream
greenyellow	palegreen	blanchedalmond	lightgoldenrodyellow	snow
yellow	khaki	lemonchiffon	lightyellow	**white**

Table 2: Named Colour Palette

RGB Colour Space

The red, green and blue (RGB) colour space is widely used throughout computer graphics. Red, green and blue are the three primary additive colours (individual components are added together to form a desired colour) and are represented by a three-dimensional, Cartesian coordinate system as shown in Figure 1 [4]. The indicated diagonal of the cube with equal amounts of each primary component represents various grey levels. Table 3 contains the RGB values for 100% saturated colour bars -- a common video test signal.

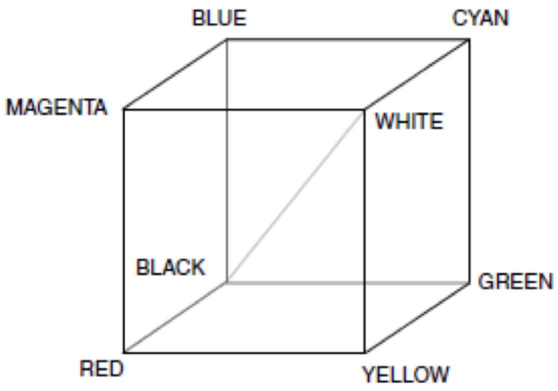


Figure 1: RGB Colour Cube

The RGB colour space is the most extensive choice for computer graphics, because the colour displays use red, green and blue to create the desired colours. Therefore, choosing the RGB colour space simplifies system architecture and design. A system that is designed using the RGB colour space can benefit from a large number of existing software routines, since this colour space has been around for a number of years.

However, RGB is not very efficient when dealing with "real-world" images. Each of the three RGB components needs to be of equal bandwidth to generate any colour within the RGB colour cube. The result of this is a frame buffer with the same pixel depth and display resolution for each RGB component. Processing an image in the RGB colour space is usually not the most efficient method. To modify the intensity or colour of a given pixel, the three RGB values must be read from the frame buffer, the intensity or colour calculated, the desired modifications performed, and the new RGB values calculated and written back to the frame buffer. A system that has access to an image stored directly in the intensity and colour format would make some processing steps faster.

Indexed Colour

Indexed colour is a technique to manage image colours in a limited manner, in order to save RAM and video memory buffer space, file storage space, telecom bandwidth and to speed up display refresh and telecom transfers. Instead of storing and managing every primary colour component of every pixel, the most representative colours, or the fixed hardware colours, are grouped into a limited size palette. This palette is an array of colour elements, in which each element (a colour) is indexed by its position. Pixels do not contain full colour components but only their index in the palette, which is sometimes referred to as pseudo-colour (Figure 2) [5].

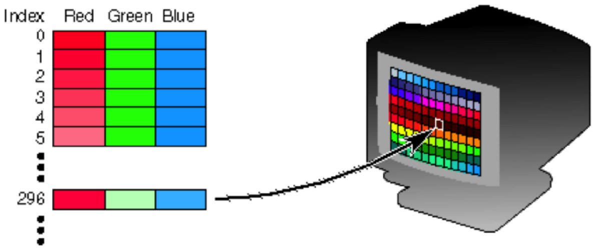


Figure 2: Colour Map

This technique saves a lot of storage space and transmission time. A true colour of the RGB colour palette has 16,777,216 (2^{24}) different possible colours and each pixel needs 24 bits, or 3 bytes. A typical 640×480 VGA resolution true-colour uncompressed image needs 640×480×3 = 921,600 bytes (900 KiB). By limiting the image colours to 256, every pixel needs only 8 bits or 1 byte, so the example image now needs only 640×480×1 = 307,200 bytes (300 KiB) plus 256×3 = 768 additional bytes to store the palette map (assuming 24-bit RGB), approximately one-third of the original size. Smaller palettes such as 4-bit (16 colours) and 2-bit (4 colours) can pack the pixels even more (to 1/6 or 1/12), obviously at the cost of colour accuracy. For little images such as icons or very simple graphics, to reproduce real-life images this loss of colour availability becomes more of a problem. Some clever tricks like combining colour quantization, anti-aliasing and dithering can approximate indexed 256-color images to the original images.

Indexed colour has been widely used in early personal computers and display adapters' hardware to reduce cost. Notable computer graphics systems that extensively use pseudo-colour palettes include EGA and VGA (for IBM PC compatibles), the Atari ST and Amiga's OCS and AGA.

Similarly, image file formats used to encapsulate images are for instance PCX and GIF along with a header. Raw image data stored in palette colour maps also emerged in the 1980s. Current image file formats, such as BMP, TIFF and PNG allow indexed colour modes, generally up to 16 or 256 (four or eight bits per pixel). These file formats commonly support some compression scheme, enhancing their ability to store the indexed colour images in smaller file sizes. Table 4 shows the general structure of an index-colour image. Basic image properties (such as image type, image size, palette offset) are stored in 'Image Header'. The colours that comprise the image are in 'Palette'. Table 5 [6] shows a common palette entry structure of a grey-level image. Each palette entry consists of an index and a colour. The number of palette items is related to the NOC of an image, for instance a 256 colour (8-bit) BMP image holds 256 palette entries. The 'Image Data' part holds all image indices.

	Normal Range	White	Yellow	Cyan	Green	Magenta	Red	Blue	Black
R	0 to 255	255	255	0	0	255	255	0	0
G	0 to 255	255	255	255	255	0	0	0	0
B	0 to 255	255	0	255	0	255	0	255	0

Table 3: 100% RGB Colour Bars

Image Header	Palette	Image Data (Index)

Table 4: Structure of an Index-colour Image

Index	Colour
00	(00, 00, 00)
01	(01, 01, 01)
.	
.	
.	.
.	
.	
FE	(FE, FE, FE)
FF	(FF, FF, FF)

Table 5: Palette Entry

Colour Look-up Table (CLUT)

CLUT is a hardware resource of the display subsystem that serves different purposes. One of the purposes is to hold the colour values for a given palette in some indexed colour graphic mode (let's say 320×200 with 256 colours, often used for computer videogames). Today, CLUTs are used mainly to perform gamma and colour temperature calibrations by hardware. Although the term 'colour look-up table' was coined in the display hardware design field (as machines always came first), it has been imported to the software jargon as a near synonym of palette too; but in these cases, it can mean not only the colour map of an indexed colour image but also any intermediary look-up table that maps one colour onto another, regardless of the indexed or true colour used. In order to avoid confusion, the term CLUT is preferred for the colour hardware registers and palettes for software colour maps when both are employed in the same study.

Grayscale images

Grayscale images do not usually need palettes. The pixel values can be stored directly in the grey level in a given range (0 to 15, 0 to 255), so image files that deal with greyscale images usually do not store a palette colour map for this purpose. But when displayed with colour devices, it is often necessary to synthesize a greyscale colour map to manage the image properly (either by loading the colour hardware registers/CLUT or by converting the image to RGB in RGB video memory). Some image file formats, such as BMP, implement greyscale by storing a greyscale palette made with full RGB values.

Colour Depth

Colour depth denotes how many bits are employed to store colour information in the image pixels: the more colours managed, the more bits that are employed. The pixel's bit patterns can be interpreted as whole integer numbers (which is the case for colour image indices) or by assigning some bits for colour-related management, such as relative intensities for every primary red-green-blue in RGB true colour images. Indexed colour palette sizes often have up to 2 raised to some power entries, which easily match pixel depth bit patterns: $2^2 = 4$, $2^4 = 16$ or $2^8 = 256$ as the most common choices. High colour uses RGB full palettes with either 15-bit or 16-bit depth, while true colour uses RGB full palettes of 24-bit depth or greater.

Conclusion

Colour palettes are vital components in the formation of image files. It is important for users to understand the structure of colour palettes if they were to build steganography applications to hide information in image files. Good colour palette management will reduce cost and increase the efficiency of steganography implementation in computer systems. In the next steganography series, another steganography component will be presented to help readers gain a better understanding of steganography overall.

References

[1] Zakaria A.A. 2010. Steganography: Secure Information Hiding. E-Security. 24: 26-28. http://www.cybersecurity.my/data/content_files/12/781.pdf

[2] Popa R. 1998. An Analysis of Steganographic Techniques. The "Politehnica" University of Timisoara. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.88.9413&rep=rep1&type=pdf

[3] Brettschneider G.D. Color Palettes. http://www.gerolf.org/doc/color/color.pdf

[4] Color Spaces. http://www.compression.ru/download/articles/color_space/ch03.pdf

[5] Color. OpenGL Programming Guide. http://www.glprogramming.com/red/chapter04.html

[6] Kim S.M., Cheng Z., and Yoo K.Y. A New Steganography Scheme based on an Index-color Image. 2009. Sixth International Conference on Information Technology: New Generations. 376-381. http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/rucha2.pdf

Online Fraud: A review on Current Trend and Mitigation to Reduce the Threat

By | Kilausuria binti Abdullah, Faiszatulnasro Mohd Maksom, Md Sahrom Abu

Introduction

In today's world, it is common to use Internet technology in handling business services and payment transactions. The swift rate of information technology usage has improved the accessibility of information and more people are involved in online transactions, regardless of age, gender and status. Almost everyone has accepted the rapidness of online commercial business, particularly in Malaysia. However, in dealing with commercial business various parties are also involved, such as clients, suppliers, banks, third-party payments, etc. In the real scenarios of today, fraudsters could be either of the parties involved, including the business owner. Fraudsters normally create fake identities for business process arrangements.

Fraud Definition

Fraud is defined as an act that is deceptive, or of trickery, or an act perpetrated to gain unfair profit from a victim. This includes any transaction activities that are planned not to be paid such as misappropriation of assets [1]. Perpetrators take money by cheating clients, suppliers, or partners through demanding certain amounts of money. As a result, victims will proceed to pay, even though the goods or services have not yet been delivered. Fraudsters may commit such fraud by involving intelligence gathering and identity theft. Further, stolen identities are used to commit fraud like buying goods and services, applying for credit cards and loans, or taking over someone's valid accounts [2]. On the other hand, general online fraud offences may include phishing, unauthorized transactions, illegal investments, impersonation and spoofing activities [3].

Fraud Triangle

Based on the fraud triangle, three factors contribute to people committing fraud: pressure, opportunities and rationalization [4].

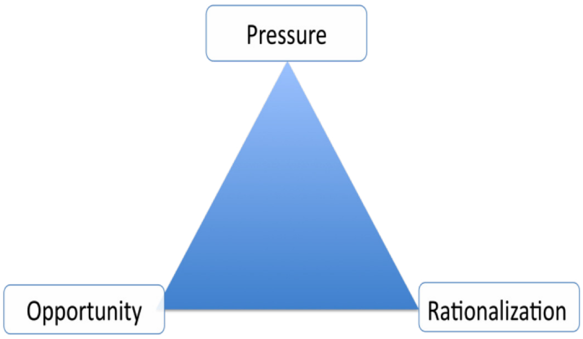


Figure 1: The Fraud Triangle

These three elements exist in an organization and influence each individual differently. The fraud triangle provides a valuable framework to analyze individual fraudulent behavior and has been adopted in auditing standards.

Fraud Categories

Internet fraud mirror fraud perpetrated over the phone or through mail. This fraud scheme uses one or more Internet components such as chat rooms, e-mail, message boards and websites to present fraudulent solicitation to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or others connected with the scheme. All of these tools are relatively cheap and available at fraudsters' fingertips.

Numerous fraud activities are carried out by fraudsters. This section reviews the most common types of fraud on the Internet nowadays. These types of fraud occur in daily business for the regular Internet and e-mail user.

1. Job scam

The job scam comes in the form of emails purportedly sent by the Recruitment Department of well-known companies in Malaysia, such as oil and gas companies (e.g. Petronas or SapuraCrest) luring job seekers with attractive job packages. However, it requires the job seekers to pay money in advance, usually under the guise of work visas, travel expenses, and out-of-pocket expenses.

2. Online scam

The scammer uses online services to present fraudulent solicitation to prospective victims, conduct fraudulent transactions, or transmit the proceeds of fraud to financial institutions or others connected with the scheme. Online scams can occur in chat rooms, via e-mail, message boards or websites.

3. 419 scam

The Nigerian, or 419 scam is one of the most common types of fraudulent e-mails currently hitting inboxes. Nigerian scam messages can also arrive via fax or letters. The messages generally claim that your help is needed to access a large sum of money, usually many millions of dollars. In fact, this money does not exist. The messages are an opening gambit designed to draw potential victims deeper into the scam. Those who initiate a dialogue with the scammers by replying to a Nigerian scam message will eventually be asked for advance fees supposedly required to allow the deal to procede.

4. Phishing

The perpetrators attempt to steal confidential personal data such as usernames, passwords and credit card details by using Phishing techniques. Perpetrators usually use spoofed e-mail messages in combination with fake websites to deceive people. Phishing perpetrators can hijack trusted and well-known brand names of banks, credit card companies, online retailers and so on [3].

5. Fraud Purchase

Fraud purchase occurs when a perpetrator approaches a merchant and proposes a business transaction. The perpetrator will perhaps use a stolen or fake credit card for the payment. As a result, merchants do not get paid for the sale. Merchants who accept credit cards may receive a chargeback for the transaction and lose money as a result.

Fraud Statistics

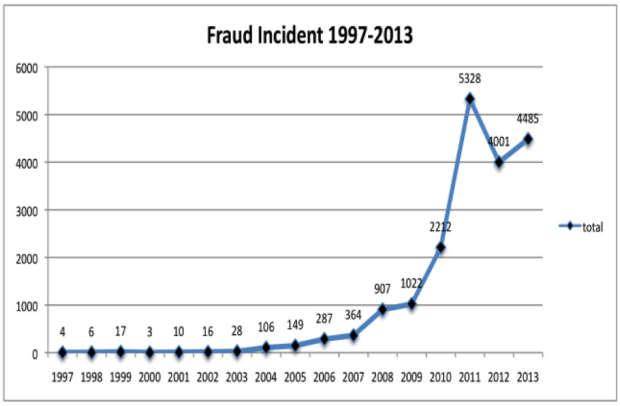


Figure 2: MyCERT Fraud Incidence Statistics (1997-2013)

Figure 2 shows the total fraud incidents recorded by MyCERT from 1997 to 2013. In general, the total incidents are increasing almost every year.

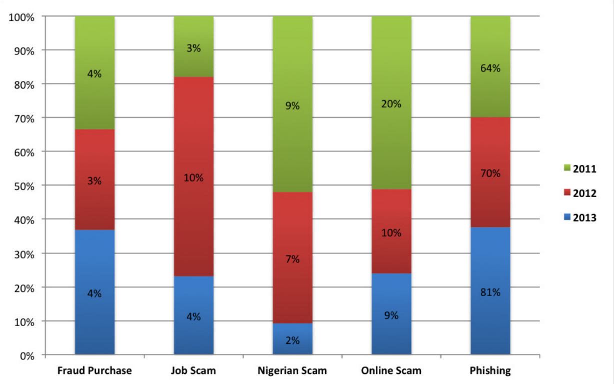


Figure 3: MyCERT statistics of the most reported fraud cases

Figure 3 shows five of the most common fraud incidents reported to MyCERT. Fraud Phishing was the most frequently reported for three consecutive years and the online scam was the second most common. The steady numbers indicate the overall view that perpetrators are still easily carrying out unlawful activities, most of which are disseminated through e-mail because it is easy and costless.

However, the Nigerian and Online scams show a gradual decrease by up to five and ten percent respectively. The figure above additionally shows that the Job scam, Fraud Purchase and Nigerian scam are the lowest incidence frauds. Hence, this indicates that the trends are different yearly and cannot be predicted. This does not, however, mean these particular incidents were less important in a certain year, but is rather indication of how the complainants could handle such instances. The Job scam is more likely to change the fraud landscape if more complainants make reports, most of whom are foreigners with knowledge of where to report such cases.

Current Trends

There are various methods of online fraud employed by perpetrators to commit such computer crime. Perpetrators would use one or a combination of methods in order to proceed with fraud agendas.

1. Manipulating third-party payment transactions

Based on a case study, one of the methods used by perpetrators is manipulating third-party payment transactions. This method is mostly used in the online scam and fraud purchase category. The perpetrator could manipulate third-party payment transactions in different ways. Some of the techniques are:

a. **Email the victim with a third-party payment selected by the perpetrator.**

   The content of the email will provide information about the payment and an attached receipt as proof that payment has been made. Perpetrators will use similar email addresses or the same email address, which contains the particular third-party payment name to assure the victim.

b. **Email the victim a receipt as proof of payment made**

   Perpetrators notify victims that payment has been made via the respective bank/wire transfer using a fake receipt.

2. Impersonation of victim identity

Perpetrators can gather much information about the victim and possibly involve either internal or external employees. Identity theft is the act of using others' personal information [5]. This method is mostly used in fraud purchases and job scams. The perpetrator will impersonate the victim and use their identity to communicate with the victim's client. The client will receive an email from the perpetrator who is now claiming to be the legit individual. The client victim will proceed to do business with the perpetrator without knowing the truth. For job scams specifically, the perpetrator will impersonate the one responsible for recruiting new staff in order to gain the victim's trust to apply for that job.

3. Email spoofing to instruct or direct payment to the perpetrator's account

Some perpetrators will spoof victims' emails in order to communicate with the victims' clients. Other than spoofing, the perpetrator will create a similar email account that is supposedly used by the victim in order to communicate with the victims' clients. After communication is established, the victim's client needs to proceed with the payment. Usually, the perpetrator will send another email consisting of a new bank account, claiming that the previous account is under maintenance or giving any other logical pretext.

4. Fake business identity

One of the methods applied by perpetrators to hide or conceal themselves from being easily traced is to use fake business identities. The information about the company itself is fake, including the company's website, address and contact person. Some perpetrators will create fake websites to make the victim's clients believe the company exists and is real.

5. Falsification of business documents

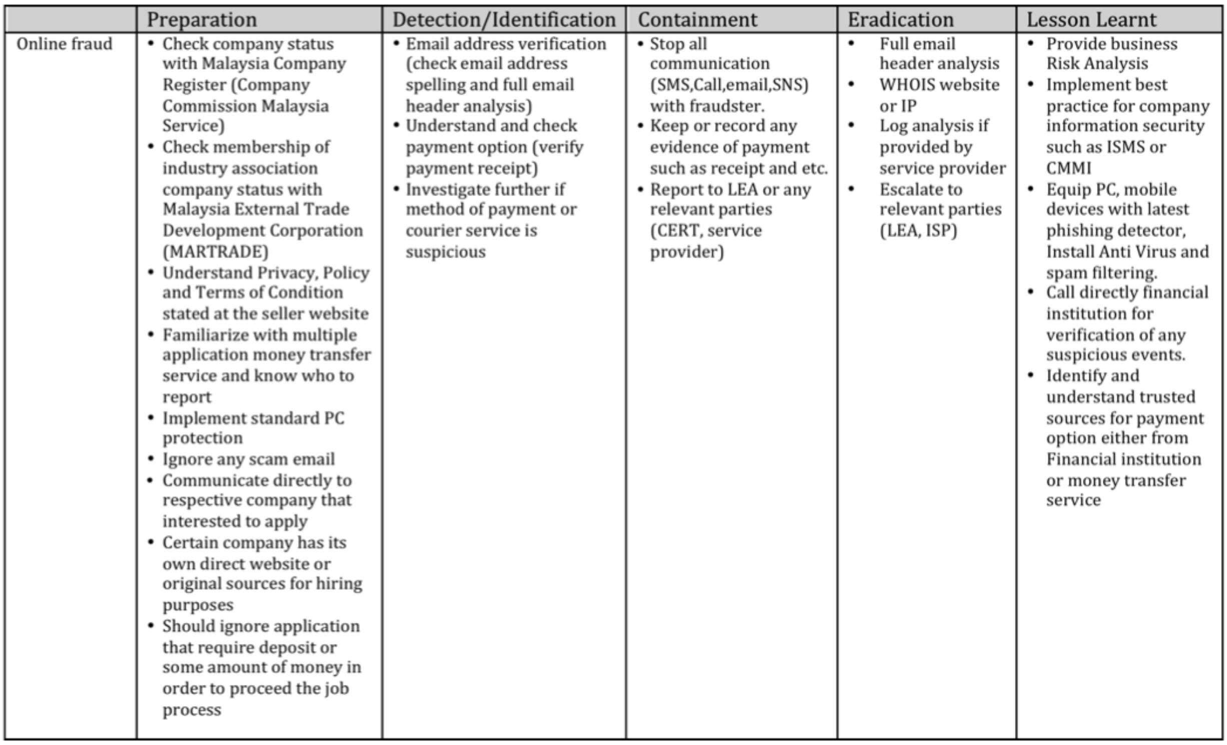
Information is an important resource for governments and industries [6]. Alteration or destruction of confidential data is a common objective for perpetrators when committing online fraud. Perpetrators falsify relevant documents in order to gain the trust of victim clients, by using fake invoices, receipts, company information, etc. However, perpetrators will use real information regarding the contact person in the document.

6. Geolocation

The majority of fraud incidents involve different geolocation strategies, for example if a victim is in Malaysia the perpetrator's information is outside Malaysia. If the victim is outside of Malaysia, the perpetrator will use a payment method that is available in Malaysia. Furthermore, there are incidents involving geolocations between East and West Malaysia. One of the ways to prevent online fraud is to use a geolocation tool [7]. Geolocation tools allow the identification of connections from IP addresses that are different from the ones habitually used by clients, IP addresses that occur at unusual times and anonymized IP addresses.

Mitigation

Several tools and services on the market were created to detect and prevent fraud incidents and are either commercial products or open source products. Despite applying technical tools to reduce fraud, the following methods



	Preparation	Detection/Identification	Containment	Eradication	Lesson Learnt
Online fraud	• Check company status with Malaysia Company Register (Company Commission Malaysia Service) • Check membership of industry association company status with Malaysia External Trade Development Corporation (MARTRADE) • Understand Privacy, Policy and Terms of Condition stated at the seller website • Familiarize with multiple application money transfer service and know who to report • Implement standard PC protection • Ignore any scam email • Communicate directly to respective company that interested to apply • Certain company has its own direct website or original sources for hiring purposes • Should ignore application that require deposit or some amount of money in order to proceed the job process	• Email address verification (check email address spelling and full email header analysis) • Understand and check payment option (verify payment receipt) • Investigate further if method of payment or courier service is suspicious	• Stop all communication (SMS,Call,email,SNS) with fraudster. • Keep or record any evidence of payment such as receipt and etc. • Report to LEA or any relevant parties (CERT, service provider)	• Full email header analysis • WHOIS website or IP • Log analysis if provided by service provider • Escalate to relevant parties (LEA, ISP)	• Provide business Risk Analysis • Implement best practice for company information security such as ISMS or CMMI • Equip PC, mobile devices with latest phishing detector, Install Anti Virus and spam filtering. • Call directly financial institution for verification of any suspicious events. • Identify and understand trusted sources for payment option either from Financial institution or money transfer service

Table 2: Online fraud best practices and incident handling

are suggested to prevent fraudulent activities based on fraud incidence case studies:

A. Control weaknesses

The approach of controlling weakness requires looking into potential for fraud by examining the key controls, which can be taken advantage of as control weaknesses, and analyzing how fraudsters manipulate a control that may not work properly [8]. Besides, organizations should implement and enforce policies and standard operating procedures to avoid any information breaches of organizational assets, personal privacy of employees and misconduct of employees based on the organization's code of ethics. An organization must adhere to its specific checks or audits of the entire assets in order to achieve its business goals. [9]. Individuals must understand and have security awareness and concern regarding information security, including personal data protection.

B. Information security policies

Information security policies should be implemented and monitored in each organization to prevent and reduce information security breaches and identity theft. In conjunction with enforcing information security policies, the confidentiality, integrity and availability of information can also be preserved.

C. Classification of information

All information assets within the organization along with personnel information should be classified prior to publishing or storing. Besides policies, the classification of information would prevent misuse of information and access by unauthorized parties or individuals.

D. Protecting electronic data and infrastructure

ICT information, including digital data should be protected against intrusion by hackers. Technology tools, such as biometrics and encryption can be used to protect digital data. Business owners need to ensure that infrastructure is protected against security breaches [10].

E. Risk Assessment Analysis

An organization and individuals must perform risk assessment analysis to understand business threats and how to prevent threats in order to achieve the business goals or objectives.

F. Best practices

There are a number of best practices or guidelines that users ought to know and implement regarding online fraud incidence. The details of best practices and handling of each incident are described in Table 2.

Summary

Fraud incidence is becoming increasingly sophisticated along with new technology and multiple methods deployed every day. Aside from using new technology, the easiest way to commit fraud is by attacking humans via social engineering techniques. Fraudsters will manipulate human trust for profit from fraudulent activities. Besides the current trends employed by perpetrators, profound research should be done on particularly targeted victims, such as buyers, sellers, suppliers, third-party payment services and business market players in order to prevent more victims from being subject to fraud. Other than implementing fraud detection and prevention systems, it is extremely important to educate users about fraud activities. Users should understand and increase their knowledge to protect themselves from being victimized. By using online technology to do online activities such as chatting on social sites, shopping, uploading and downloading photos, etc. end users must familiarize themselves and manage each application's setting to secure their activities. Apart from end users, buyers or suppliers of e-commerce products should follow best practices, such as implementing and enforcing information security policies in their companies to prevent information leakage, improper information handling and so on.

References

1. *Ghosh, M. (2010). Telecoms fraud. Computer Fraud & Security, 2010(7), 14–17. doi:10.1016/S1361-3723(10)70082-8*

2. *http://www.actionfraud.police.uk/fraud_protection/identity_fraud*

3. *http://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/799/index.html*

4. *Dellaportas, S. (2013), Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. Accounting Forum 37 (2013) 29-39*

5. *Tryfonas, B. T., Ph, D., Thomas, P., & Owen, P. (2006). ID Theft : Fraudster Techniques for Personal Data Collection, the Related Digital Evidence and Figures and Examples.*

6. *Thomas C. Richards, A historical prospective of computer related fraud, ACM SIGSAC Review, v.4 n.3, p.15-25, Summer 1986 [doi>10.1145/1058414.1058418]*

7. *Forte, D. V. (2008). Using geolocation to prevent online fraud. Computer Fraud & Security, 2008(11), 19–20. doi:10.1016/S1361-3723(08)70165-9*

8. *Coderre, D. G. (2009). Computer-aided fraud prevention and detection: A step-by-step guide. Hoboken, N.J: John Wiley & Sons*

9. *Whitman M.E. , Mattord H.J., Principles of Incident Response and Disaster Recovery, Course Technology Press, Boston, MA, 2007*

10. *Adams, R. (2010). Prevent, protect, pursue – a paradigm for preventing fraud. Computer Fraud & Security, 2010(7), 5–11. doi:10.1016/S1361-3723(10)70080-4*

Intrusion Attempt – Who's Knocking Your Door

By | Kilausuria binti Abdullah

Introduction:

An intrusion attempt is a potential for a deliberate unauthorized attempt to enter either a computer, system or network to access information and manipulate information or render a system unreliable or unusable. Even though security parameters are built around a home that is equipped with the current or latest security tools, one must also monitor the possibility of someone trying to knock the door down. Despite this, a successful attempt may have hazardous impact not only on a system but also the organization's reputation.

Types of Intrusion Attempts:

In general, intrusion attempts refer to any activity of someone trying to, or successfully breaching an individual's, entity's or nation's computers. In this report, intrusion attempts are categorized into three forms as follows:

1) Port scanning

the act of systematically scanning a computer's communication ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks but can also be malicious in nature if someone is looking for a weakened access point to break into a computer.

2) Login brute force

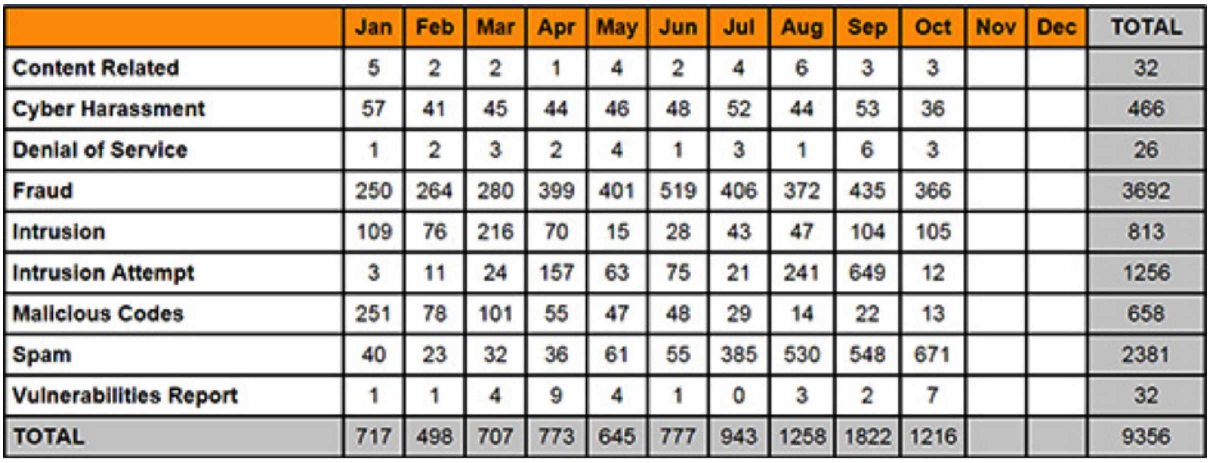
the systematic, exhaustive testing of all possible methods that can be used to break a security system. For example, in cryptanalysis, this entails trying all possible keys in the key space to decrypt a ciphered text, or trying to automate an SSH login (username and password attack).

3) Vulnerability probes

the automated process of proactively identifying possible vulnerabilities of the computing systems in a network in order to determine if and where a system can be exploited and/or threatened.

Intrusion attempts are basically received by victims, servers, networks, systems and computers. Such incidents are usually captured in the logfile of the victim's infected machine. For example, the host has performed a complete network scan and is trying to connect to SSH (Secure Shell, TCP port 22) through a user account login service. The incident handler will verify the intrusion attempt log. Once the intrusion attempt log is validated, the incident handler will inform the IP domain/owner and ISP provider of that particular IP address. The IP domain/owner and ISP provider will subsequently need to verify the intrusion attempt logfiles for further investigation and action.

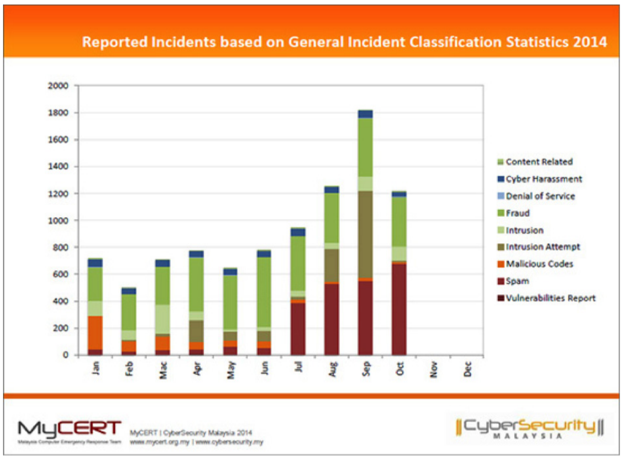
Intrusion Attempt Statistics for Q3 2014



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Content Related	5	2	2	1	4	2	4	6	3	3			32
Cyber Harassment	57	41	45	44	46	48	52	44	53	36			466
Denial of Service	1	2	3	2	4	1	3	1	6	3			26
Fraud	250	264	280	399	401	519	406	372	435	366			3692
Intrusion	109	76	216	70	15	28	43	47	104	105			813
Intrusion Attempt	3	11	24	157	63	75	21	241	649	12			1256
Malicious Codes	251	78	101	55	47	48	29	14	22	13			658
Spam	40	23	32	36	61	55	385	530	548	671			2381
Vulnerabilities Report	1	1	4	9	4	1	0	3	2	7			32
TOTAL	717	498	707	773	645	777	943	1258	1822	1216			9356

Table 1: Intrusion Attempts in Q3 (Jul-Sept) 2014

In the 3rd quarter of 2014, a total of 902 incidents were reported to CyberSecurity Malaysia under the Intrusion Attempt category as shown in Table 1 and Graph 1.



Graph 1: Intrusion Attempts in Q3 (Jul-Sept) 2014

Comparison of Intrusion Attempt Analysis

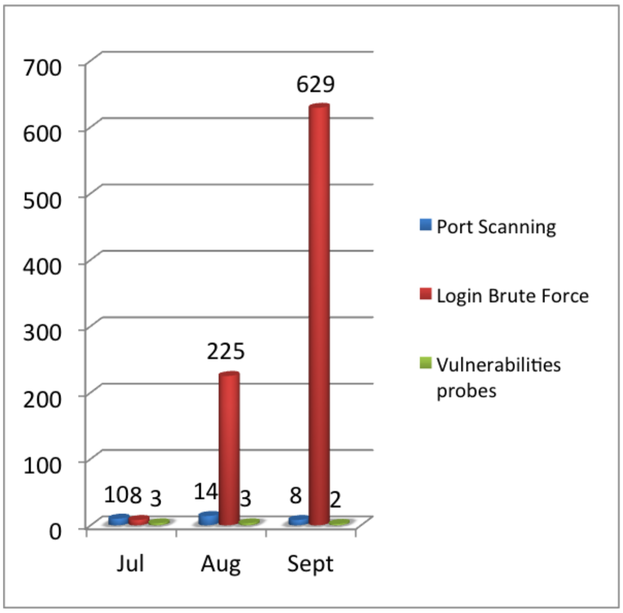
In Quarter 3 2014, a total of 902 incidents were received in the Intrusion Attempt Report as shown in Table 2 and Graph 2.

Intrusion Attempt Report Q3 (Jul-Sept) 2014

	Jul	Aug	Sept	TOTAL
Port Scanning	10	14	8	32
Login brute force	8	225	629	862
Vulnerability probes	3	3	2	8
TOTAL	21	242	639	902

Table 2: Intrusion Attempts in Q3 (Jul-Sept) 2014

Note: The statistics reflect the number of incident tickets.

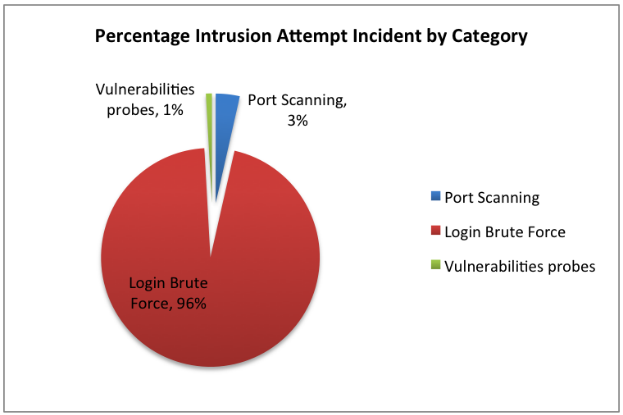


Graph 2: Intrusion Attempts in Q3 (Jul- Sept) 2014

Most intrusion attempt incidents in Q3 2014 were login brute force, as shown in Table 3 and Graph 3.

Type of Intrusion Attempt	Total
Port Scanning	32
Login brute force	862
Vulnerability probes	8

Table 3: Total Intrusion Attempt Incidents by Category



Graph 3: Percentage of Intrusion Attempt Incidents by Category

From the above graph it can be seen that the majority of intrusion attempt incidents involved are login brute force, representing 96% compared to other intrusion attempt categories. The remaining intrusion attempt categories are port scanning (3%) and vulnerability probes (1%).

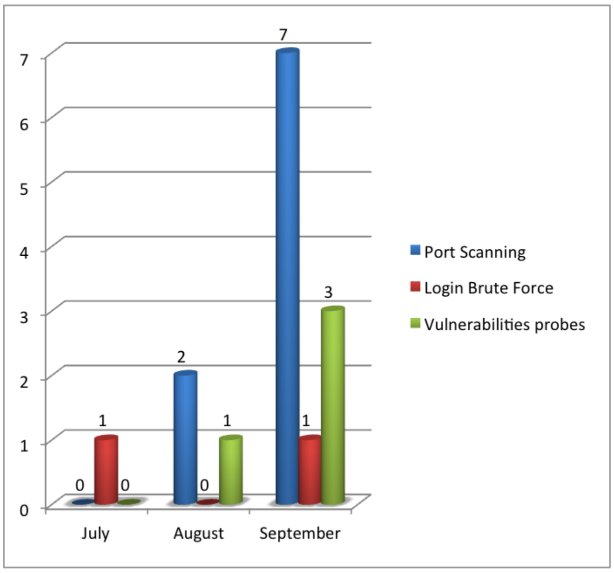
In the 3rd quarter of 2013, a total of 15 incidents were recorded as Intrusion Attempt Incidents as shown in Table 4 and Graph 4.

Intrusion Attempt Report Q3 (Jul-Sept) 2013

Intrusion Attempt Categories	July	Aug	Sept	TOTAL
Port Scanning	0	2	7	9
Login brute force	1	0	1	2
Vulnerability probes	0	1	3	4
TOTAL	1	3	11	15

Table 4: Intrusion Attempts for Q3 (July-Sept) 2013

Note: The statistics reflect the number of incident tickets.

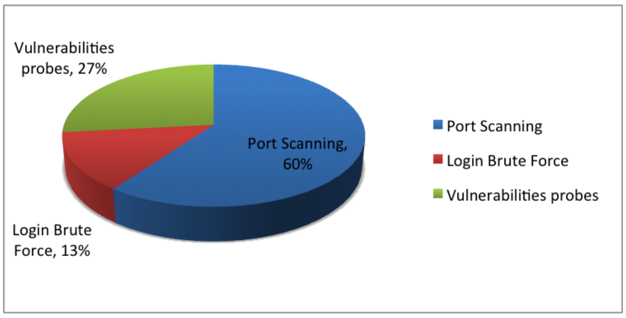


Graph 4: Intrusion Attempts for Q3 (July-Sept) 2013

Most of the intrusion attempt incidents for Quarter 3 2013 involved port scanning, as shown in Table 5 and Graph 5.

Type of Intrusion Attempt	Total
Port Scanning	9
Login brute force	2
Vulnerability probes	4

Table 5: Total Incidents of Intrusion Attempts for Q3 2013 by Category



Graph 5: Percentage of Intrusion Attempt Incidents for Q3 2013 by Category

The above graph indicates that the majority of intrusion attempt incidents involved port scanning, which represents 60% compared to other categories. The remaining categories are vulnerability probes (27%) and login brute force (13%).

According to the statistics above, intrusion attempt incidents from the 3rd quarter 2013 to the 3rd quarter 2014 increased from 15 to 902 cases.

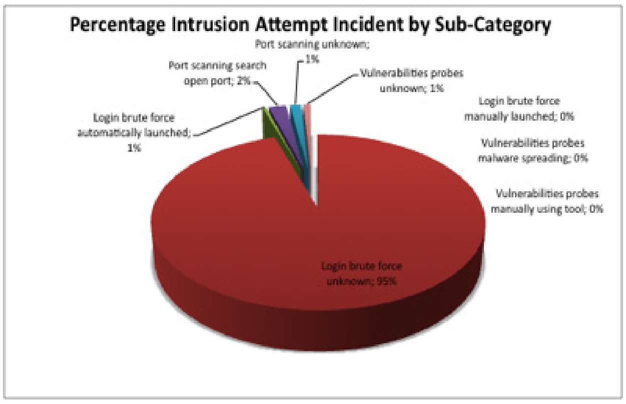
In-depth Analysis of Intrusion Attempts in Q3 2014

In the 3rd quarter of 2014, the major type of intrusion attempts discovered based on the incidents reported is login brute force. The number of intrusion attempts discovered in this quarter are listed in Table 6 and Graph 6 below.

Intrusion Attempt Sub-categories	July	Aug	Sept	TOTAL
Login brute force -- manually launched	0	0	0	0
Login brute force -- unknown	7	223	626	856
Login brute force -- automatically launched	1	2	1	4
Port scanning -- search open port	5	9	5	19
Port scanning -- unknown	5	5	2	12
Vulnerability probes -- malware spreading	0	0	0	0
Vulnerability probes -- manually using tools	0	0	0	0
Vulnerability probes -- unknown	3	3	2	8

Table 6: Percentage of Intrusion Attempt Incidents by Sub-category

Based on analysis for Q3 2014, intrusion attempt incidents under login brute force -- unknown, vulnerability probes -- unknown, had the highest reported number, or 95% of the total reported incidents. This was followed by intrusion attempts on port scanning -- open ports (2%). Intrusion attempts by login brute force -- automatically launched, port scanning -- unknown and vulnerability probes -- unknown, contributed 1% each.

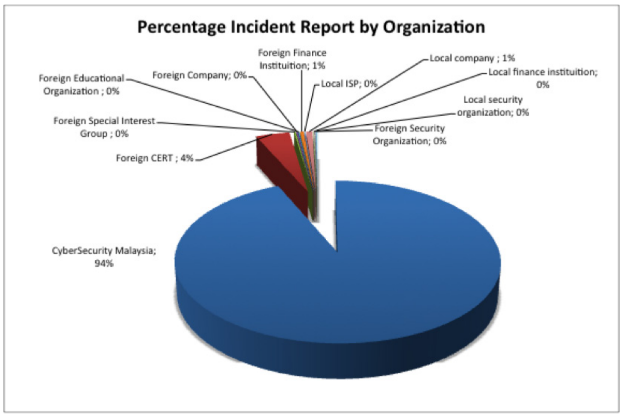


Graph 6: Percentage of Intrusion Attempt Incidents by Sub-category

A total of 902 incidents were reported in the Intrusion Attempt Report for Q3 2014. These were reported from various organizations and categorized under various intrusion attempt sub-categories. The most frequently reported incidents were from CyberSecurity Malaysia, followed by other Computer Emergency Response Teams (foreign CERT) and other organizations as shown in Table 7 and Graph 7.

Reports From	TOTAL
CyberSecurity Malaysia	843
Foreign Computer Emergency Response Teams	37
Foreign Special Interest Groups	2
Foreign Companies	2
Foreign Educational Organizations	1
Foreign Finance Institutions	4
Local ISP	1
Local Companies	7
Local Finance Institutions	1
Local Security Organizations	1
Foreign Security Organizations	2

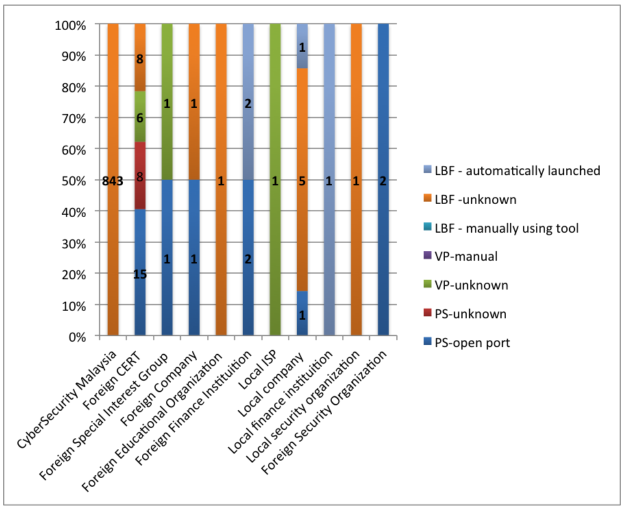
Table 7: Figures on Intrusion Attempts Based on Organization Reports



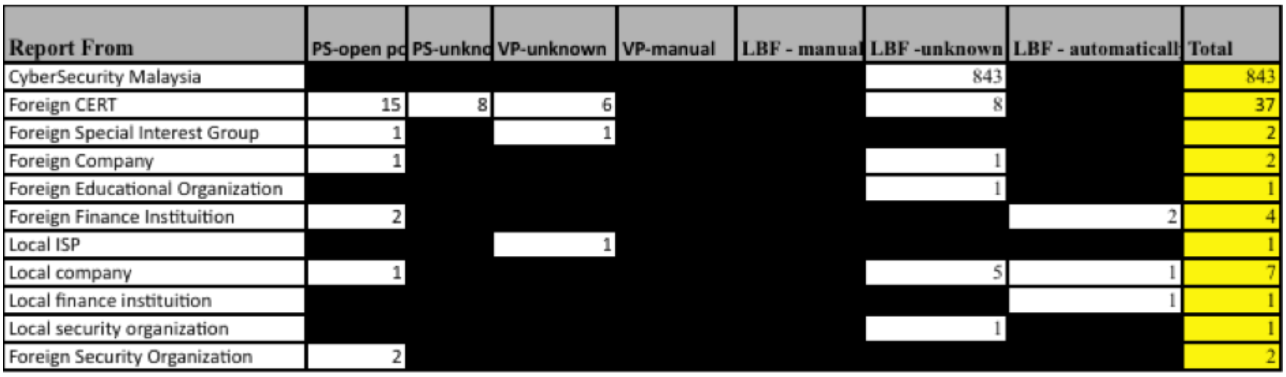
Graph 7: Percentage of Intrusion Attempts Based on Organization Reports

Most incidents of intrusion attempts reported were by CyberSecurity Malaysia, comprising 94% of the total reported incidents. Foreign Computer Emergency Response Teams (foreign CERT) contributed about 4% while local companies and foreign finance institutions both represented 1% respectively.

For Quarter 3 2014, most intrusion attempt incidents were reported by CyberSecurity Malaysia and were login brute force -- unknown, and port scanning -- unknown.



Graph 8: Sub-categories of Intrusion Attempts Based on Organization Reports



Report From	PS-open po	PS-unkno	VP-unknown	VP-manual	LBF - manual	LBF -unknown	LBF - automaticall	Total
CyberSecurity Malaysia						843		843
Foreign CERT	15	8	6			8		37
Foreign Special Interest Group	1		1					2
Foreign Company	1					1		2
Foreign Educational Organization						1		1
Foreign Finance Instituition	2						2	4
Local ISP			1					1
Local company	1					5	1	7
Local finance instituition							1	1
Local security organization						1		1
Foreign Security Organization	2							2

Table 8: Sub-categories of Intrusion Attempts Based on Organization Reports

Login Brute Force Description:

Login brute force is a password-guessing type of attack of the unauthorized access attempt kind. A brute force attack can be recognized by reviewing the operating system's security log. If such attack happens when an attacker attempts to log in to the system at any time and fails to do so, an event message is written in the operating system's security log. This attempt is generally meant to discover a password by systematically trying every possible combination of letters, numbers, and symbols until the one correct combination that works is discovered. A good target of brute force attacks is a website that requires user authentication. Brute force attacks can put user accounts at risk and also flood sites with unnecessary traffic. These attacks are easy to detect but not so easy to prevent. For example, HTTP brute force tools can relay requests through a list of open proxies. Although each request appears to come from a different IP address, this attack cannot be simply prevented by blocking the IP address. Some tools will try a different username and password on each attempt, therefore a single account cannot be simply locked out for failed password attempts.

Impact of Discovered Intrusion Attempts

The impact of reported intrusion attempts that can affect systems includes:

1. An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers and symbols until they discover the one correct combination that works.
2. By using port scan tools, attackers could determine a system's weaknesses and the best method for an attack. The negative impact of port scans are numerous and range from wasting resources, to network congestion, and enabling future, more serious attacks.

Best Practices/Recommendations for Prevention:

There are several techniques to consider for defeating a brute force login attack:

- Advanced users who want to protect their accounts from attack should be given the option to be allowed to login only from certain IP addresses.
- Assign unique login URLs to blocks of users, so that not all users can access the site from the same URL.
- Use a CAPTCHA to prevent automated attacks.
- Instead of completely locking out an account, place it in lockdown mode with limited capabilities.
- Well-chosen passwords are effective at defeating brute force login attacks. It is prudent to implement a security policy that requires users to change their passwords on a regular basis.

Therefore, it is useful for system administrators and other network defenders to detect login brute force attacks in order to recognize precursors for serious attacks.

Conclusion

In conclusion, the number of incidents categorized under intrusion attempts during the 3rd Quarter 2014 was 902 tickets. The total incident number increased by 887 from Quarter 3 the previous year. System administrators, Internet service providers (ISPs), Web hosts or regular users must be aware and concerned with intrusion attempt activities that may be present in their systems logs. The repercussions from such intrusion attempts can have high impact on the affected organization, even if few log activities are detected. Attackers will continue repeating the same activities if no additional preventive measures are in place. The kind of response received from login brute force activities could indicate whether the attacker was able to gain access to the system or whether they probed for further weaknesses such as gaining access to account data and obtaining personal information for potentially malicious purposes. System administrators and users for example, must always make sure their computers, systems and servers are regularly having the best security policies implemented, especially for defeating brute force login attacks.

References

1. http://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/799/index.html

2. https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

3. http://www.iss.net/security_center/reference/vuln/Brute_force_login_attack.htm

4. http://cseweb.ucsd.edu/~clbailey/PortScans.pdf

The Selfie Phenomenon

By | Yang Kalsum Bt Ibrahim, Rozila Ramli

Introduction

"Selfie" is a new buzzword being used today.It is one of the most popular ways of taking self-portraits with a hand-held smartphone camera [1]. Since the advent of smartphones equipped with quality cameras and preview screens, a large number of individuals have all been taking pictures of themselves for various purposes [1]. In the early days, selfies or photographic self-portraits started as taking pictures in front of a mirror or with the camera placed on a nearby object or tripod. Using current technologies, selfies are easily taken with a digital camera or a front-facing smartphone, tablet or webcam.

As painted in social media, selfies are increasingly attracting media attention and sociological scrutiny. Selfies are also becoming a useful tool to post self-portraits to social media such as Instagram and Facebook, whereby the tendency is to engage in adding and receiving Likes and comments on photos from others.

Both the good and bad sides of selfies are mentioned below.

The Good Side of Selfies

1. Capturing good angles

   Selfies are usually flattering and made to appear casual. Holding the camera a bit higher than the head makes one's eyes look bigger [2], nose appear sharper and the best features are highlighted, such as chest and cleavage.

2. "The cult of the selfie celebrates regular people"

   According to Pamela Rutledge, faculty director of the media psychology program at the Massachusetts School of Professional Psychology, "There are many more photographs available now of real people than models." [3]

3. It allows control of your image online

   People who like having the power to choose how they look enjoy taking selfies as their appearance online can be controlled.

4. Mini boost of confidence

   With cute pictures and positive comments received on appearance, selfies have a way of making us feel great about ourselves.

5. Capturing Memorable Moments

   Selfies can be taken anytime, anywhere without assistance from anyone.

The Bad Side of Selfies

1. Reveal Locations

   Selfies show locations of where people are and when they are there. Location is key, as often people only take selfies when they are at a place where they want to be seen. The intention is to impress others or to share, especially joy, with absent friends or loved ones, so the viewers might in future go to the same places and do the same things. However, such posting allows unscrupulous people to learn more about one's whereabouts and use that advantage to stalk and cause mischief.

2. Show Information about Friends

   People typically take selfies with friends [4]. Inadvertently, information about friends is also revealed, further widening the circle of people placed at risk.

3. Inform of Routine Activities

   Selfies inform viewers of a person's habits or routine activities and the sort of pursuits they enjoy. For example, people often post selfies of themselves shopping and trying on new outfits for the benefit of receiving feedback from friends. Sometimes, they are at a gym to show friends they are enjoying a workout. In doing so, they are actually providing information on the places they frequent and the regular activities they do. This information can be used to track down the people who had posted the selfies and used to cause harm in many ways.

4. Are People at Home?

   A further risk is disclosing information on when people are not usually home. Criminals often store information about people's comings or goings so that they can predict the times and for how long people leave their homes; then they use these times to burglarize homes.

5. What People Look Like

   Another danger selfies pose is regarding what people look like. The common practice of strict adherence to the protection or privacy of personal details is compromised when selfies are posted for the 'world' to see. These photos posted for the sole purpose of fun [5] can be used against the people whose selfies have been displayed.

6. Names of People on Display

   When a selfie is taken with co-workers and at a place of work, some photos may display not only the name of the company these people work for, but also the names of the co-workers, sometimes solely from the name tags that many, today, have to wear on their clothing. This could subject the people in the selfies to becoming victims of a wide range of offences against them. They can include crimes such as identity theft and blackmail to steal trade secrets.

7. 'Unflattering Details of Family Members'

   Selfies that include family members can become a bone of contention between the person who has posted them and the reluctant family members. This is especially true when family members are being shown at their best. It becomes particularly more sensitive when selfies are posted without the permission of those in the photos.

Points to Ponder

To summarize, the selfie is one of the indispensable tools for human development and progress. However, people need be aware of the dangers of selfies as they are posting personal information on social media sites. Posting selfies may lead to cyber harassment or cyber bullying. Cyber bullying, cyber stalking, and sexual, religious and racial harassment are done through social media. However, much of the harassment is often the result of people disclosing their real identity and personal details, mainly pictures, either voluntarily or unwittingly.

With selfies, it has become common for people to not think twice before taking pictures and posting them online. Some precautions to be taken are avoiding photos that reveal locations and that are immodest or potentially offensive [6].

References

[1]Bruno, Nicola, et al. "'Selfies' Reveal Systematic Deviations from Known Principles of Photographic Composition." Art & Perception 2.1-2 (2014): 45-58.

[2]"How to Take Good Selfies". http://www.wikihow.com/Take-Good-Selfies.

[3]Melissa Walker. "The Good, the Bad, and the Unexpected Consequences of Selfie Obsession". http://www.teenvogue.com/advice/2013-08/selfie-obsession.

[4]"Taking a Selfie: The Psychological Experience". http://nobullying.com/ eight-selfie-danger-signs-everyone-should-be-aware-of/.

[5]Elise Moreau. "What is a Selfie?". http://webtrends.about.com/od/Mobile-Web-Beginner/a/What-Is-A-Selfie.htm.

[6]Qustodio Team. "Selfie Safe Tips for Teens". https://www.qustodio.com/en/blog/2013/12/selfie-safety-tips-for-teens/.

6 Simple Tips to Stay Safe on Instagram

By | Norazlila Binti Mat Nor

Introduction

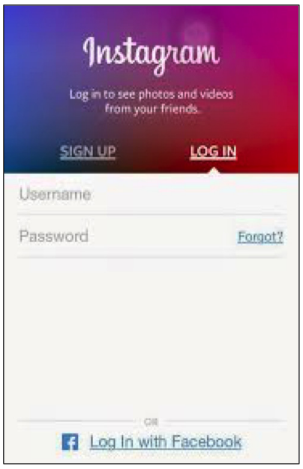
In the digital era and technology of today, social media is one of the many ways to connect people in the virtual world. Social media has exploded in recent years, connecting people in both personal and professional contexts. No doubt it makes communicating with others even easier. Remarkably, it is FREE! Simply connect to the Internet, then a variety of social media is ready to accommodate fresh ideas.

Among the current popular social media is the Instagram application. Based on Wikipedia, Instagram is a portmanteau of Instant Telegram, an online mobile photo-sharing, video-sharing and social networking service that enables users to take pictures and videos, and share them on a variety of social networking platforms, such as Facebook, Twitter, Tumblr and Flickr. Instagram was launched in October 2010. This application has rapidly gained popularity with over 100 million active users as of April 2012 and over 300 million as of December 2014.

Although there is nothing inherently dangerous about Instagram, things that may be worrying are typical issues as with all social media, such as unpleasant behavior among peers and inappropriate photos or videos that could harm reputation or attract the wrong kind of attention.

If you are Instagram users, let's take a look at the best ways to stay safe and secure on Instagram.

1. Keep your account safe

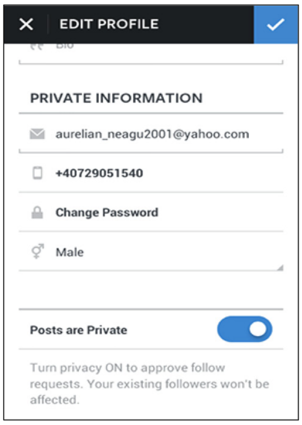


Log in to see photos and videos from your friends.

Passwords are the first layer of defence against cyber criminals. If you do not want to expose your account to the biggest risks, ensure strong passwords and do not use the same password for all your online accounts. It is also a good practice to change your password regularly. It may be uncomfortable, but it will make you less worried and your account more secure.
Since the Instagram account uses your e-mail address as a username, you must also ensure your e-mail account is safe. Anyone who can access your e-mail can probably also access your Instagram account.

If you are using other phones or computers to access Instagram, make sure to log out of the account once finished. Observe for any changes or unusual activities with your account. In case your account has been hacked and you are no longer able to log in, please immediately make a report to the Instagram Help Center.

2. Change the privacy settings for your photo feed



PRIVATE INFORMATION

aurelian_neagu2001@yahoo.com

+40729051540

Change Password

Male

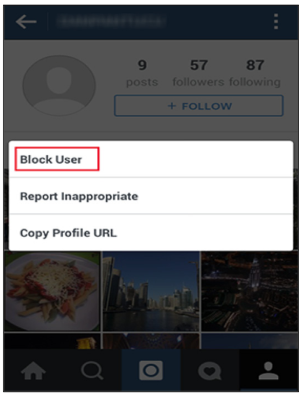
Posts are Private

Turn privacy ON to approve follow requests. Your existing followers won't be affected.

If you want to share your photos and videos only with friends or family and do not want them to be seen by everyone, edit your Instagram profile. Make sure the 'Posts are Private' option is turned on. This will ensure that only approved friends/followers will see your photos and videos. However, if you decide to share your Instagram shots on Facebook or Twitter, double-check which social services are selected on the final confirmation page before clicking the "Share" button.

Please bear in mind that it is common for people to take pictures from other accounts and use them as their own. Photos or videos posted online may be copied, altered, and shared with many people without your knowledge or consent.

3. Block followers you do not know



Block User

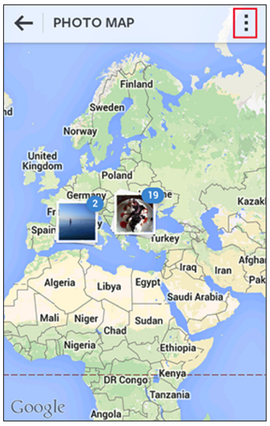
Report Inappropriate

Copy Profile URL

In case you want to remove or block any followers, choose the 'Block User' option. When applying the blocking feature, the blocked person cannot view your posts or search for your Instagram account.

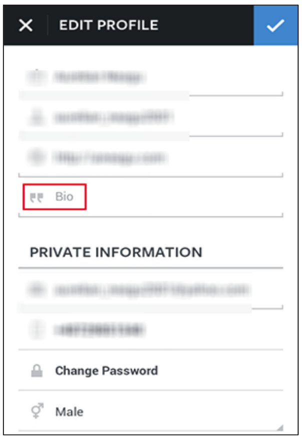
A rule of thumb is if you do not know a person in real life, then you probably should not accept them as a follower.

4. Do not expose your location



Instagram offers an additional nice feature which allows pinning any photo you choose to "map images" and it can be viewed from your profile. This feature can show your friends where you are on vacation, but you may want to think twice before sharing your home address or the location of your friend's house, for instance. Before sharing photos or videos on Instagram, avoid mentioning the exact location where you took a certain photo or video. However, if you already posted your location in a previous post, remove the location you added to your photos by wiping off your photo map. In the 'Photo Map' option, make the necessary changes in order to remove the added location from your photos.

5. Keep your profile information private



Bio

PRIVATE INFORMATION

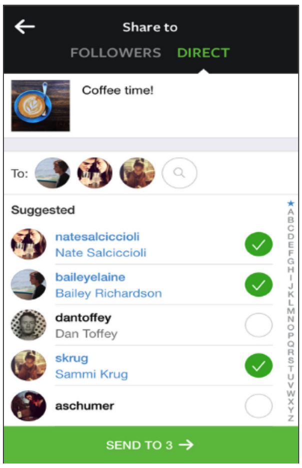
Change Password

Male

Another important step you can take to keep safe from identity theft is to hide your identity or reveal less of your Instagram profile.

Do not expose too much personal information, especially your profile information in the Instagram bio. The only detail that needs to be exposed in your profile is your Instagram username. This also applies when adding hashtags to photos or videos posted online. For example, do not mention your real name or children's real names in the hashtag, as the personal information could be used against you.

6. Share photos only with specific Instagram followers



A new feature in Instagram called "Instagram Direct" lets you pick and choose Instagram friends or followers who can see your latest photos or videos posted in Instagram. The post would not appear in the feed, search or your profile. The people you have sent the post to will get a notification. If someone you are not following sends you a photo or video on Instagram, it will go to your requests so you can decide if you want to view it.

This private photo or video sharing feature helps to only share certain photos or videos with specific followers. This is an additional layer in staying safe on Instagram.

Conclusion

Besides the 6 simple tips mentioned above, there are additional general guidelines to follow before posting on Instagram. Among of them are:

- Do not post sensitive information next to your photos.
- Do not post provocative or violent photos or videos
- Do not post photos or videos of other people without their permission
- Do not engage in online bullying

As an Instagram user, you have the option to be private. Although not many security options are available in Instagram, there are a few to be aware of in order to avoid cyber criminals. Instagram is a fun way to share your life through photos and videos. The important thing to know is how to stay safe in the community.

References

1. Wikipedia. http://en.wikipedia.org/wiki/Instagram

2. Instagram Help Center. https://help.instagram.com

3. The Essential 5 Step Guide to Secure Your Instagram Account. https://heimdalsecurity.com/blog/essential-guide-instagram/

4. Increasing Your Instagram Protection + Securing Your Instagram Account. http://www.swayamdas.com/how-to-secure-your-instagram-account.html

5. Instagram and Kids: A parent's guide to privacy and safety. http://sociallyactive.com/instagram-and-kids-a-parents-guide/

Essential Ingredients for Successful Information Security Management System (ISMS) Implementation – Not a 'One Solution Fits All'.

By | Rafidah Abdul Hamid

Introduction

There are numerous reasons for the high interest in information security. The need for standardization, demand for regulators and market demand are among the reasons. While interest is on the rise, experience shows that managing information security is not an easy task. Information security can be achieved by implementing a suitable set of controls including policies, processes, procedures, organizational structures and software and hardware security mechanisms. The process of establishing, implementing, monitoring, reviewing and improving controls requires an organization to continuously identify and maintain all changes in the business environment, security threats, industry best practices and legal requirements.

The Information Security Management System (ISMS) has been widely accepted as a systematic approach to managing information security and is implemented in many countries. Statistics by the Department of Standards Malaysia [1] reports that 201 organizations in Malaysia are ISMS-certified by its two accredited certification bodies as of January 2015. With the growing importance of ISMS, organizations are always seeking for the best ways to effectively implement ISMS. While critical success factors of ISMS implementation vary, this article emphasizes the leadership aspect and competency of the personnel involved in ISMS as two critical factors that can effectively contribute to ISMS effectiveness.

Main Ingredients in Successful ISMS Implementation

As ISMS involves comprehensive processes in managing security, there is no one immediate solution, or one solution fits all, that can be deployed to achieve successful implementation, even if hiring consultants for ISMS implementation or using audit tools to assess the organization's compliance. This section discusses two main factors or aspects that an organization should prioritize when establishing, implementing, maintaining and planning to continually improve their ISMS.

ISMS implementation in Malaysia has been a national concern since the start of adopting BS7799-2:2002 as an international standard. A pilot program was jointly conducted by SIRIM QAS International Sdn. Bhd. and CyberSecurity Malaysia in 2013. The program aimed to provide assistance to organizations with an ISMS audit to gauge the levels of ISMS compliance in the participating organizations. The audit came at the heel of a pilot project with 10 organizations participating to have their selected services/operations certified based on the BS 7799-2:2002 standard. An article titled "ISMS Pilot Program Experiences: Benefits, Challenges & Recommendations" published in CyberSecurity Malaysia's E-Security bulletin in 2003 [2] provides details of this program and discusses the various benefits and challenges faced by these organizations during their ISMS implementation. The article also includes some recommendations to smoothen the ISMS implementation process.

Apart from the recommendations for the successful implementation of ISMS during its initial implementation in Malaysia as stated in the article, CyberSecurity Malaysia provides an additional guideline on ISMS implementation. The guideline was produced in 2013 under the title "ISMS Implementation Guideline: A practical approach' [3]. It states some of the critical success factors that an organization should be aware of when implementing ISMS as follows:

a. Commitment and support from the top management should be obtained prior to implementation and continuously throughout the implementation.

b. ISMS implementation should be aligned to the organization's strategy and business objectives and requirements, and is an integral part of the overall management of the organization related to, and reflecting the organization's approach to information security risk management.

c. Information security policies and procedures are communicated promptly to all levels of personnel, from management to the front desk to ensure no misunderstandings or lack of information amongst personnel.

d. Activities designed for ISMS are supported with various creative mechanisms and approaches so that 'willingness to change' is visible and accepted by all levels of personnel.

e. Personnel involved in ISMS implementation should be equipped with relevant competencies and skills.

f. Awareness programs to all relevant personnel and entities are held consistently and continuously to create a security culture where all fully understand their security roles and responsibilities.

g. Active monitoring and continuous improvements are crucial to ensuring that risks and/or incidents are dealt with promptly, as well as ensuring that all necessary tasks are performed without delay.

All the factors mentioned above are definitely important and very much inter-related in driving successful ISMS implementation in any organization. The following section elaborates on the leadership aspects and competency of the personnel involved in ISMS implementation.

Leadership in ISMS Implementation

The guideline mentions that commitment and support from the top management should be obtained prior to implementation and continuously throughout implementation. This is very true as management usually has specific goals for the organization, which should be communicated clearly to the ISMS implementer to ensure that ISMS implementation is aligned with the organization's strategy and business objectives and requirements. Support from management is crucial as it will lead to other important factors, such as allocation of resources like manpower and financial needs for ISMS implementation.

In Malaysia, some initiatives from government agencies have fortunately provided the 'push factors' for organizations to embark on ISMS implementation. The most significant initiative was the cabinet directive issued on 24th February 2010 for ISMS to be implemented in Critical National Information Infrastructure (CNII) agencies. The directive states that CNII entities should be certified in three years with certification scope covers the information security management in the operating areas that deliver the critical services and products to the nation. This directive is observed as one of the factors that motivates and encourages management support and commitment for ISMS implementation in many organizations in Malaysia, at least for first-time certification. However, while it is always challenging to address this issue for continuous implementation in particular, setting up a firm Information Security Management Committee in the early stages of ISMS implementation is one of the mechanisms to address the leadership issue in ISMS. This committee is able to ensure continuous support and commitment by defining roles and responsibilities of those involved in ISMS implementation.

Competency of Personnel

Another important factor that should be prioritized is the competency of personnel involved in ISMS implementation. As there is increasing need for organizations to protect their information, the need for personnel with the right competency to protect information has also elevated.

A survey conducted by the Information Security Magazine in 2012 shows the increasing importance of information security professionals' roles in an organization. The survey mentioned that changes in regulations, such as SOX, PCI DSS and Data Protection, and increased threats from online criminals have raised the profile of information security. Only 7% of information security professionals were unemployed at any point during 2011, with nearly 70% reporting a salary increase and 55% expecting to receive an increase in 2012, according to a survey by a non-profit IT security trade group $(ISC)^2$. Of the 2,250 security professionals who responded to the survey, 72% said that in 2011 their organization hired individuals specifically for information security roles, and 62% said they were looking to hire additional permanent or contract information security employees that year (Information Security Magazine, 2012) [4]. The survey results indicate the increasing importance of information security professionals' roles in an organization. The survey results also reflect the importance of identifying what criteria should be taken into consideration when specifying staff to manage information security in an organization. As organizations are facing numerous regulatory requirements as well as the need to manage risk, it is crucial for them to have information security personnel with the appropriate skills and competency to ensure that information assets are protected from unauthorized use, systems are available, and the continued integrity of information and processes is assured. It is also imperative that security professionals in leadership positions have the practical security and business experience to be able to address the changing protection needs of organizations [5].

Following top management approval of initiating ISMS implementation, specific roles and responsibilities should be established for personnel who are involved in ISMS. Personnel should be aware of their responsibilities and the authority they possess within the scope of the responsibility. Therefore, it is important for organizations to equip their personnel with appropriate knowledge and skills in information security areas and also to be able to measure their competency. This definitely emphasizes the need for personnel competency plans and continuous measurement of personnel competency.

Conclusion

Critical success factors for ISMS implementation definitely vary and very much depend on other factors, such as an organization's size, core operations, financial resources, etc. However, similar concerns arise with respect to managing an organization's information security. Nonetheless, certain mechanisms exist to ensure the successful implementation of ISMS in organizations. This article emphasized leadership issues and competency of personnel involved in ISMS implementation as key aspects that can drive successful ISMS implementation in an organization.

References

1. *Department of Standard Malaysia 'Statistic on ISMS Certified Organizations', Retrieved April 2015 from http://www.jsm.gov.my/statistics#.VSH8vdyUffI*

2. *CyberSecurity Malaysia, ISMS Implementation Guideline: A practical Approach, 2013*

3. *CyberSecurity Malaysia, 'ISMS Pilot Program Experiences: Benefits, Challenges & Recommendation', 2003*

4. *'Information Security Magazine', Retrieved March 2013 from http://www.infosecurity-magazine.com/view/23928/demand-for-information-security-professionals-remains-strong-says-isc/*

5. *ISACA, 'Defining Information Security Management Position Requirements: Guidance for Executives and Managers', Retrieved March 2013 from www.isaca.org*

Mobile Devices vs Malware

By | Kamarul Baharin Khalid

As mobile devices become smarter, malware is also becoming increasingly sophisticated. Today, malware not only attacks computers but also targets mobile devices. Most people have mobile devices and the majority tend to store personal information there, like contact numbers, schedules, reminders, notes, etc., and even passwords and credit card information. Such private information is attractive to criminals, hence making mobile devices the next best target for malware attacks.

Malware, short for MALicious softWARE, is any software used to disrupt computer system operation, gather sensitive information, or gain access to private computer systems. Malware can be designed to steal information or spy on computers for an extended period without the users' knowledge, or it may be designed to cause harm, sabotage, or extort payment (ransom).

Mobile malware first emerged in 2004 on Symbian OS smartphones. The first mobile malware was called Cabir, which used the common communication method of mobile devices for sending files using Bluetooth connection. When a device was infected, it would continuously search for all other Bluetooth devices with open Bluetooth connection and try to send a ".SIS" malware installer file to the other mobile devices. If the user was unaware of this malware and was trying to receive such files and install them on their Symbian OS mobile device, the device would then become infected. Initially, Cabir was quite harmless and only displayed the word "Caribe" while spreading via Bluetooth connection. Later, other hackers modified it to steal contact information from users' mobile devices. Such modified malware even sent premium SMS messages to certain numbers and charged users on their SMS bill. This mutation essentially harmed mobile device users.

Mobile device sales boomed in 2010 with two major mobile device OSs, namely Apple iOS and Google Android OS. Apple iOS is just another mobile device Operating System, which is based on Mac OS. Android OS is another mobile device OS based on the Linux kernel. Hackers saw more potential on these new platforms, particularly Google Android OS, causing mobile malware to explode in 2011 when Android OS mobile devices were being sold and used by almost 50% of mobile device users.

Mobile malware often disguises as a legitimate application to deceive users to install it. It is distributed through the Internet via mobile browsers, social network programs, messaging applications and also app stores. Mobile malware can either install itself without user consent or it can be installed by mobile users themselves without being aware. Installed mobile malware then performs its main function without users' knowledge or permission. Mobile malware objectives are almost the same as those of computer malware, ranging from spying to key logging, test messaging, phishing, unwanted marketing (adware) and fraud. The types of mobile malware that are quite similar to computer malware are as follows:

1. Spyware and Adware: This type of malware secretly gathers private information about mobile device users. Information collected might include contact numbers, locations, messaging habits, browser history, user preferences and downloads. This information is then sent to a third party or probably the owner of the spyware itself. Sending the information uses up the mobile device user's personal data connection, either a mobile data plan (3G/4G) or Wireless network (WiFi).
2. Trojans and Viruses: These types of malware attach themselves to harmless or legitimate applications and get installed together. Once installed, these malware carry out their malicious actions. They will try to hijack the browser and cause the device to automatically send unauthorized premium rate SMS or capture the users' login credential information from other applications like social networks, online banking, app stores, etc. They may also affect smartphones by simply annoying users, to causing smartphones to become highly destructive to not repairable at all. Some may try to root the devices and gain access to users and system files in the mobile devices or memory cards.
3. Phishing Apps: Fraudsters create phishing sites that appear to have legitimate services but are actually trying to steal user credentials (phishing). Accessing the Internet through mobile devices is growing as smartphones and tablets are becoming

common. Mobile device users can access the Internet anywhere, anytime. They are not meant to replace desktop computers but are just more convenient. Fraudsters are also targeting mobile device users like desktop computer or notebook users. The smaller screens on mobile devices make the malicious phishing technique much easier to hide and be overlooked by the victims. Phishing schemes are not limited to websites but are expanding by using rogue mobile apps, programs that contain Trojans to disguise their true nature. Legitimate apps can also be infected with malware, which is only discovered when users install them.

4. Bot Processes: By introducing multitasking on mobile devices, hackers have been able to create more sophisticated mobile malware that can operate in the background of mobile devices and conceal their existence. Mobile malware is lying there without user knowledge, waiting for certain behaviors like online banking sessions to activate before striking. With multitasking, hidden processes can be executed completely invisible to the users who run executable files, or are waiting for contact from their botmasters for instructions. This will render the next wave of mobile malware more advanced, with higher botnet tendencies to actually hijack and control infected mobile devices.

How to know when a mobile device is infected with mobile malware? The symptoms are the same as for computer systems, with mobile devices exhibiting signs like unwanted behaviors and slow device performance. Common symptoms are frozen apps, mobile device freezes, failure to reboot, difficulty connecting to the network or entirely broken down devices. Mobile malware may cause lower battery life because it requires extra processing power for its actions. Knowing about mobile malware is the first step in trying to prevent mobile devices from being infected. There are several best practices that mobile users could follow to increase protection against mobile malware infections. Some are as follows:

1. Installing protection apps like antivirus or antispyware on mobile devices can help reduce infections by detecting installers, which contain rogue apps. By enabling auto scanning, protection apps will try to detect any rogue apps installed in mobile devices.
2. Download and install only apps from official app stores provided by the mobile device OS. Official app store moderators frequently monitor and maintain the app stores and try their best to remove any rogue apps published in their app stores.
3. If required to install third-party apps from websites or alternative app stores that are not official, try to do some research regarding the app, like the developer's rating and reputation. Read users' feedback and ratings on websites or forums. Look out for any disgruntled users and read their reviews too. Provide your feedback after using the app to help others in deciding whether to use it.
4. When installing any app, read and double read the permissions requested before installing. Hackers are counting on user carelessness to sneak mobile malware into mobile devices. Read the end user agreement and try to understand it before installing the app.
5. Rooting and jailbreaking mobile devices can significantly increase security vulnerabilities and does not help slow mobile malware infection. By not rooting or jailbreaking the mobile device, restrictions from the mobile device manufacturer are not removed, hence making it difficult for mobile malware to be installed without user consent. Prevention is much better then curing an infected mobile device of mobile malware. Mobile user awareness greatly helps prevent mobile malware infection. Remember, it is better to be safe than sorry.

References

1. 5 Smartphone Tips to Protect Against New Malware Attacks - http://www.entrepreneur.com/article/224691

2. A brief history of mobile malware - http://www.mobilecommercedaily.com/a-brief-history-of-mobile-malware

3. A Brief History of Mobile Malware - http://countermeasures.trendmicro.eu/wp-content/uploads/2012/02/History-of-Mobile-Malware.pdf

4. Mobile Malware: 10 Tips for Prevention - http://mobileenterprise.edgl.com/tech-spotlight/Mobile-Malware--10-Tips-for-Prevention83191

5. Ten Ways to Prevent Viruses and Malware - http://anti-virus-software-review.toptenreviews.com/ten-ways-to-prevent-viruses-and-malware.html

6. Preventing Mobile Malware Attacks - http://www.slideshare.net/patsyrivera/preventing-mobile-malware-attacks

7. Common Mobile Malware Types: Cybersecurity 101 - https://www.veracode.com/blog/2013/10/common-mobile-malware-types-cybersecurity-101

8. Top BYOD security threat: Mobile malware - http://blog.trendmicro.com/top-byod-security-threat-mobile-malware/

9. Six Tips to Prevent Mobile Malware Attacks - http://www.easetech.com/blog/six-tips-to-prevent-mobile-malware-attacks.aspx

10. 10 ways to combat the threat of mobile malware - http://www.techrepublic.com/blog/10-things/10-ways-to-combat-the-threat-of-mobile-malware/

11. When Malware Goes Mobile - http://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/10-tips-to-prevent-mobile-malware.aspx

Basic Mathematics in Cryptography

By | Liyana Chew Nizam Chew & Norul Hidayah Bt Lot@Ahmad Zawawi

Introduction

This article introduces the basic mathematics in cryptography required to understand encryption systems. Cryptography is the process of writing using ciphers to keep messages secret. Cryptanalysis is the science of attacking ciphers, finding weaknesses, or even proving that a cipher is secure. Cryptology covers both cryptography and cryptanalysis; it is a complete science of secure communication. The science of cryptology is at least 2,000 years old, having existed long before the invention of complex mechanical and electromechanical machines. Modern computing has made it possible to encipher huge amounts of data securely in a reasonable time, while also making it easier for cryptanalyst to break cryptographic systems. With the increase of cryptology researchers worldwide, cryptology is a rapidly growing subject. The fast growth of technology also provides more sophisticated and efficient means of encryption.

Even though cryptology and technology are both developing fast, it does not mean the underlying mathematics are moving equally fast. Modular arithmetic was developed by Gauss in his book published in the 18th century. Prime numbers and factorization have been studied for thousands of years, which has led to the development of public-key cryptography by Fermat in the 17th century and Euler in the 18th. Fermat and Pascal provided the foundations of the probability theory in the 17th century.

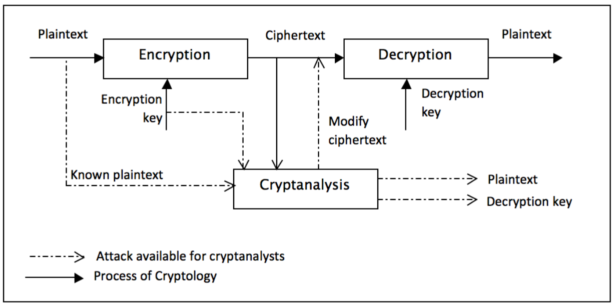


Figure 1: Cryptography and cryptanalysis

Modular Arithmetic

Modular arithmetic has been around at least as long as since calenders first existed. When calculating days in a week, we are actually performing modulo-7 addition and subtraction. The duration from Monday to Sunday is 7 days, and it turns back from Sunday to Monday. To do modular arithmetic, simply do normal arithmetic, divide the result by the chosen modulus number and take the remainder.

$$\frac{A}{B} = Q\ remaider\ R$$

$A =$ divider, $B =$ divisor, $Q=$ quotient, $R =$ remainder

Alternatively, to do arithmetic in a traditional way if necessary, keep subtracting or adding the modulus until the result is positive and is less than the modulus number. Note that in both cases the result is between 0 and less than the modulus number. For example, calculate 17 Modulo-7. Divide 17 by 7 and get 3 as a remainder. Or subtract 7 from 17 to get 10, and subtract 7 again to get 3. Either way, the answer is 3.

Modular addition and subtraction

Caesar Cipher was an early use of modular arithmetic in encryption, in which each letter of a message was encrypted by replacing it with the letter three places further along in the alphabet. For example, letter A is replaced by letter D. To view the process in a mathematical function, each alphabet letter can be represented by a number between 0 and 25 (0 represents A, 1 represents B ... and 25 represents Z). The encryption key would be denoted by +3, and the operation of encrypting a letter is then to add the key to the letter's corresponding number. For example, to encrypt E=4, we add 3 to get 7=H. The decryption key would be denoted by -3, and the operation of decrypting a letter is then to subtract the key from the letter's corresponding number. For example, to decrypt H=7, we subtract 3 to get 4=E.

Where is the use of the modular according to Ceaser Cipher? Encrypted X, Y and Z will be A, B and C respectively. In a mathematical calculation, X= 23 added with encryption key +3 would become 26, for which we have no letter. The same case applies to Y and Z. Thus, we need a kind of arithmetic whereby 26, 27 and 28 become 0, 1 and 2. This is modulo-26 arithmetic. To perform it, we can use the rules like in normal arithmetic but need to subtract 26 whenever the result is equal to, or greater than 26.

Modular exponentiation

Modular exponentiation ($A^B \ mod \ C$) entails taking a number to a power, which is done by repeated multiplication just as in normal arithmetic. Modular exponentiation is important in encryption because it is fairly easy to do but very hard to undo. This is the property of a oneway function. $A^B \ mod \ C$ is an exponential property. Often in cryptography, we will calculate large values of B, and unfortunately, A^B becomes very large even for modest sized B values. For example, $2^{40} \ mod \ 7 = 4294967296 \ mod \ 7$.

There are tricks that make modular exponentiation easier and are best described with an example. We wish to calculate $7^{18} \ mod \ 31$. The normal approach would be to start with 1 and multiply it by 7, 18 times. The answer in normal arithmetic would be 1628413597910449 and when it is divided by 31, the remainder is 2. In this way, we need to deal with large numbers and many multiplications. It is very complicated!

A better solution to approach this problem is to remove the need to handle a large number and the multiplication function. Thus, we are going to use a simple divide and conquer strategy. It is recognized that $7^{18} = 7^{16+2} = 7^{16} \times 7^2$. Now, the power number is already reduced to 16 and 2, which can be calculated easily by squaring, and we can obtain the remainder. 7^2 =49 has a remainder of 18. Calculating 7^{16} is done as follows:

$$7^{16} = 7^{(2\times2\times2\times2)}$$

So,

$$7^2 = 49 \ mod \ 31, \ remainder = 18$$
$$18^2 = 324 \ mod \ 31, \ remainder = 10$$
$$10^2 = 100 \ mod \ 31, \ remainder = 7$$

Finally, we solve $7^{16} \times 7^2$ by multiplying the two power numbers' remainders together: $18 \times 7 = 126 \ mod \ 31, \ remainder = 2$.

Linear feedback shift register

Linear feedback shift register uses a polynomial function of tapping/delays and an exclusive-OR process to produce a long pseudo-random sequence of bits. The choice of polynomial will ensure that the machine generates a maximal-length sequence; in case the power degree of the polynomial is 7, the maximal-length sequence is 127 bits (2^7-1 =127 bits). In the example in Figure 2, the equivalent generator polynomial is $1+ x^2 + x^3+ x^4+ x^7$, and the shift register is actually doing exclusive-OR for bit(b) at tapping with polynomials of power degree 7, known as GF(2^7). It turns out that if the generator polynomial is irreducible (prime polynomial), the resulting sequence will be maximal-length.

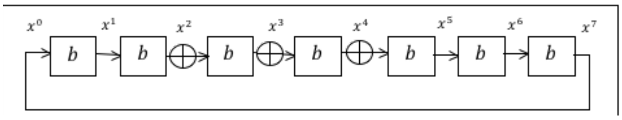


Figure 2: 1+ x^2 + x^3+ x^4+ x^7 represents a linear feedback shift register

Prime numbers

Prime numbers are defined as positive integers greater than 1 with the only divisors being 1 and itself. For such a simple definition it is actually difficult to determine whether a number is prime, especially if the given number is very large. Nobody knows a simple formula that will generate all the prime numbers. All numbers (except prime numbers) have exactly one prime factorization – that is to say, every number can be reached by multiplying some prime numbers together. If we do the calculation backwards, such as generating two prime numbers and then multiply both, 19 ×31, the result is 589. As an easy and quick example, we know that 19 and 31 are prime factorizations for 589. However, if given a larger number, to find the factoring numbers is computationally difficult to solve. It is easy for smaller numbers, but in dealing with very large numbers, it can take a computer days, months, years, even centuries to solve. There is no easy shortcut for factoring numbers – it is a trial and error process. For example, given the number 18702793917923601630399172085487309806239690904217430897009854360839512072469, try to find the prime factorization. How long will you take to find the prime factorization?

Where do we use prime numbers in cryptography? Prime numbers are used in public-key encryption systems. The goal of a public-key system is to find a pair of functions represented by numerical keys, which are the inverses of each other and where the second function (decryption) cannot easily be deduced from the first function. The most practically useful public-key encryption system so far developed is the RSA algorithm, named after its inventors Rivest, Shamir and Adelman. Diffie-Hellman is another approach to public-key encryption.

Probability Theory

The probability theory is commonly used in cryptology, particularly in cryptanalysis. A few classical ciphers have been broken using the probability theory. One important point about probability with regard to encryption is that it is really all about counting how many times things happen. For example, with a fair dice we should find that $\frac{1}{6}$ of the throws will produce a 5, so we say that the probability of throwing a 5 is $\frac{1}{6}$. As we increase the number of throws, the measured fraction should approach $\frac{1}{6}$ more closely.

Letter distributions in English text show that the letter 'e' occurs often and the letter 'z' occurs less often. Figure 3 shows the approximate probabilities of the 26 letters of the alphabet. For a message that has been encrypted using a substitution cipher, in which every same letter has been replaced by another same letter (one-to-one mapping of substitution), an attacker could make an ordered histogram of the letters in the ciphertext. The most frequently occurring letter can be guessed to be letter 'e'. The attacker should be able to match the letters one by one according to their relative frequency of occurrence, and break the cipher.

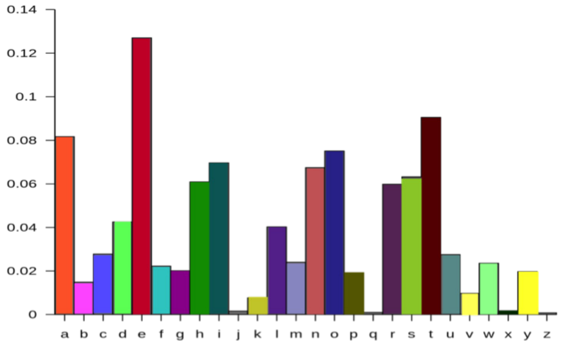


Figure 3: Frequency of English letters in text

Conclusion

Modular arithmetic is the basis of many older encryption algorithms as well as modern public-key systems. The special case of modulo-2 arithmetic is important in pseudo-random number generation as well as authentication. Theorems about prime numbers are the foundation for public-key systems. Finally, the probability theory is an important contributor in cryptanalysis and consequently, in improving the security of cryptographic systems.

References

1. Learning series – Journey into Cryptography https://www.khanacademy.org/computing/computer-science/cryptography

2. Keijo Ruohonen, 2014. Mathematical Cryptography. http://math.tut.fi/~ruohonen/MC.pdf

3. R. Vijay Shankar and Prof. C. Pandu Rangan, 1997. Shannon's Theory of Cryptography. CS702: Seminar.

4. Marsha Lynn Moreno, 2005. Frequency Analysis in Light of Language Innovation: Exploring letter frequencies across time, from the days of Old English to the days of now.

5. Jerry Crow, 2003. Prime Numbers in Public Key Cryptography An Introduction. SANS Training & GIAC Certification.

Famous Cryptologists Around The World

By | Nik Azura binti Nik Abdullah, Nor Azeala binti Mohd Yusof and Isma Norshahila binti Mohammad Shah

Cryptographers : AES Inventors

Advanced Encryption Standard (AES) is a symmetric-key algorithm used worldwide to protect classified information.

Vincent Rijmen

Vincent Rijmen, a Belgian cryptographer, was born in 1970. He obtained a degree in Electronics Engineering from Katholieke Universiteit Leuven in 1993 and finished his PhD at the same university in 1997. He became a postdoctoral researcher at the COSIC lab.

Rijmen has had several collaboration projects with Joan Daemen, who is also a Belgian cryptographer. One of their most popular joint projects is the Rjindael algorithm, with Vincent Rijmen being the main designer of the Rjindael block cipher. In October 2000, the algorithm was selected by the National Institute for Standards and Technology (NIST) to become the Advanced Encryption Standard (AES).

Rijmen's favourite research topic has always been the design and cryptanalysis of block ciphers. He also studies other symmetric cryptographic primitives, such as MAC algorithms and hash functions. His knowledge allows him to evaluate numerous industrial computer security systems like e-banking and file encryption systems.

The innovation brought by Vincent Rijmen has qualified him to be selected as one of the top 100 innovators in the world under the age of 35 in the MIT Technology Review TR100 in 2002.

Joan Daemen

Joan Daemen was born in 1965. He graduated in Electro-mechanical Engineering from the Katholieke Universiteit Leuven. He joined the COSIC research group and has worked on the design and cryptanalysis of block ciphers, stream ciphers and cryptographic hash functions.

Joan Daemen was the co-designer of the Rjindael cipher with Vincent Rijmen, which was selected as the Advanced Encryption Standard (AES) in 2001.

Daemen is primarily active in the design of cryptographic protocols for smart cards, the architecture of multi-application smart card management and personalization systems. Recently, he has concentrated on the analysis and design of mechanisms and cipher features to protect against attacks that exploit implementation weaknesses.

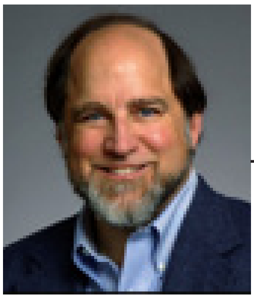
Cryptographers : RSA Inventors

RSA (Rivest-Shamir-Adleman) is a public-key encryption system. It is widely used for secure data transmission.

Adi Shamir

Adi Shamir is an Israeli cryptographer born in 1952 in Tel Aviv. He received his tertiary education from Tel Aviv University and Weizmann Institute and obtained his PhD degree in Computer Science in 1977.

Shamir is well-known in the cryptography society for being a co-inventor of the RSA algorithm, co-inventor of the Feige-Fiat-Shamir identification scheme and one of the inventors of differential cryptanalysis, a method of attacking block ciphers. His other inventions include the Shamir secret sharing scheme, breaking of the Merkle-Hallman knapsack cryptosystem, visual cryptography and the TWIRL and TWINKLE factoring devices.



Ron Rivest

Ron Rivest was born in 1947 and grew up in New York. He graduated from Yale University in 1969 with B.A in Mathematics and from Stanford University in 1973 with a PhD in Computer Science.

Rivest's contributions in cryptography include being a co-inventor of the RSA algorithm, co-founder of RSA Data Security, Versign and Peppercoin and also co-author of the text Introduction to Algorithms. He is also the inventor of the symmetric key encryption algorithms RC2, RC4 and RC5, and co-inventor of RC6. "RC" stands for Rivest Cipher. He also authored the MD2, MD4, MD5 and MD6 cryptographic hash functions. Rivest's interests in security are not limited to encryption. In 2006 he invented the Three Ballot voting system to protect voters' privacy.

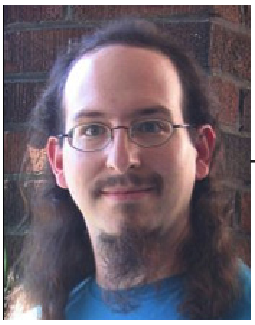
Len Adlemen

Len Adleman, an American computer scientist, was born in 1945 in California. He received his B.S. in Mathematics in 1968 and PhD in Computer Science in 1976 from University of California, Berkeley.

Adleman was involved in the invention of the RSA algorithm. He was the one who kept testing the system and trying to break it. He was able to break 42 different coding systems for RSA but failed during the 43rd attempt. This attempt, based on a difficult factoring problem, was finally selected to be used in this public crypto key system. In the early 90s he redirected his interest towards the field of DNA computing, where he made a discovery in AIDS research, which eventually led to his discovering DNA computing.

Cryptanalysts

Experts in analysing and breaking codes and ciphers.



Ian Goldberg

Ian Avrum Goldberg is an associate professor at the School of Computer Science, University of Waterloo. He was born on March 31, 1973. He received his Bachelor of Mathematics from the University of Waterloo in Pure Mathematics and Computer Science. He obtained his Ph.D. from the University of California, Berkeley, in December 2000.

Goldberg is best known for breaking Netscape's implementation of SSL with David Wagner in 1995. Goldberg with Nikita Borisov and David Wagner conducted one of the first cryptanalyses on the WEP wireless encryption protocol and revealed serious flaws in the design. Goldberg was a co-author of the Off-the-Record (OTR) instant messaging encryption protocol. He was also the author of the Perl script included in the novel Cryptonomicon by Neal Stephenson.

Eli Biham

Israeli cryptographer and cryptanalyst, Eli Biham is currently a professor at the Technion Israeli Institute of Technology, Computer Science Department. Biham received his Ph.D for publicly inventing differential cryptanalysis while working under Adi Shamir.

Biham's contributions in cryptography include being a co-inventor of related-key attacks, publicly inventing differential cryptanalysis during his Ph.D under Adi Shamir, attacking all triple modes of operation, impossible differential cryptanalysis (with Adi Shamir and Alex Biryukov), breaking the ANSI X9.52 CBCM mode (with Lars Knudsen), breaking the GSM security mechanisms (with Elad Barkan and Nathan Keller) and differential Fault Analysis (with Adi Shamir).

Lars Knudsen

Lars Ramkilde Knudsen is a Danish researcher in cryptography. He was born on 21 February 1962. Knudsen enrolled at Aarthus University in 1984 to study mathematics and computer science, and gained an MSc in 1992 and a PhD in 1994. He is currently a professor in the Department of Mathematics at the Technical University of Denmark.

Knudsen is interested in the design and analysis of block ciphers, hash functions and message authentication codes (MACs). He introduced the technique of impossible differential cryptanalysis and integral cryptanalysis. Knudsen has published analyses of a variety of cryptographic designs, including the R-MAC scheme, the SHA-1 and MD2 hash functions and at least a dozen block ciphers: DES, DFC, IDEA, etc. He has also designed ciphers including AES candidates DEAL and Serpent.

Designing a Secured Office Premise from a Physical Security Perspective

By | Syahran Abdul Halim

Introduction

To meet the challenges of today's globalized economy, an organization must be able to analyse its systems' vulnerabilities, identify the real threats and potential risks its business is being exposed to. The various threats that might come in the forms of natural disasters or people, such as criminals, hacktivists, terrorists, business competitors, their own employees and/or contractors who are targeting the business with certain motives must be considered.

According to WhatIs.com, physical security is defined as the protection of personnel, hardware, programs, networks and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. Wikipedia describes physical security as security measures designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems, which include CCTV surveillance, security guards, protective barriers, locks, access control protocols and many other techniques.

Objective of Having a Secured Office

The main objective of having secured office premises, amongst others, is to protect company assets and sensitive information from fire, natural disasters, burglary, theft, vandalism and terrorism on the office premises. Assets can be people, the facility in which they work and the data, equipment, support systems, media and supplies they utilize.

Risk Assessment

To create and design secure office premises, it is necessary to know the main elements involved and the potential threats faced by the company, which is done by conducting risk assessment. The Business Dictionary defines Risk Assessment as the identification, evaluation and estimation of the levels of risks involved in a situation, comparisons against benchmarks or standards and determination of an acceptable level of risk.

In conducting a risk assessment, several issues should be addressed, namely:

- Are secure areas controlled?
- Are review and maintenance of access controls taking place?
- Have the business requirements for access control been defined and documented?
- Are there any non-standard entry points to the secure areas?
- Are these non-standard entry points secured and/or monitored?
- Are visitors required to have supervision on the premises?
- Are visitors allowed within secure areas?
- If your organization shares access to your facility, does it have proper controls to segregate access?
- Do guards at entrances and exits randomly check briefcases, boxes or portable PCs to prevent unauthorized items from coming in or leaving?
- Do guards allow visitors to bring laptop computers into the institution without proper signoff or authorization?
- Are fire detectors and an automatic extinguishing system installed on the ceiling, below the raised flooring and above dropped ceilings in labs / computer rooms and libraries?
- Are data center and server center activities monitored and recorded on closed-circuit TV, and are they displayed on a bank of real-time monitors?
- Does access to a controlled area prevent "tail-gating" by unauthorized people who

attempt to follow authorized personnel into the area?

- Is there any possibility of events that could cause interruptions to the business process in the surrounding area?

Risk Assessment is a method to assist a company identify the potential risks, threats and vulnerabilities, thus enabling it to plan for appropriate control measures to manage the identified risks.

Examples of Control Measures for Office Physical Security

In designing secured office premises, the following controls should be considered for implementation based on risk assessment.

a. Security Guards

Large scale companies or companies with their own buildings, warehouse or factory would prefer to employ their own security personnel, whereas others might prefer outsourcing from security firms. Guards can be used in two ways: to monitor the front desk of a company or building (the access control point) and to patrol the grounds of a larger company or office complex. Depending on the risks, armed guards can be deployed for high security offices such as in the finance sector.

Today's guards, especially those who monitor building access, should possess good communication skills and should be able to handle several tasks. Guards often act as concierges and goodwill ambassadors, greeting the company's guests as they come in, answering questions and providing directions. Ideally, they should present a positive public image for the company and/or building that employs them.

b. Physical Locks

Basically, we use locks to prevent unauthorized access to our offices, cabinets, desks, servers, store, etc., in order to protect our information assets. Locks are just one more barrier to slow the advance of intruders into our premises. However, locks—even those considered “high security”—are easily bypassed with the right tools, time and training. Depending on risk levels and budget, the more barriers in place, the better security could be provided. There are a few types of locks from traditional to modern technology on the market that are widely used, such as door knob locks, deadbolts, keys, rotary/push-button combination locks, etc.

c. Biometric Access System

A Biometric System is for the automated recognition of individuals based on their behavioural and biological characteristics. The system serves as an additional tier of security and provides one of the greatest benefits to company security. In addition, biometric system users cannot be socially engineered, and data cannot be shared or used by others. There is no requirement to remember passwords or PINs, thus eliminating overhead costs. Furthermore, biometric data comes with the individual, hence it is unique.

Access control systems start with establishing "point of control" access over an office. That means that all tenants and guests are routed through a control area before admittance is authorized. A database is available to track and check all transactions made by tenants.

d. CCTV Surveillance Systems

Locking the door itself only at best delays intruders or unauthorized persons from accessing the premises. Someone could break in, or a person with authorization could misuse their authority. For this situation, CCTV surveillance is often used to continuously monitor designated areas, with motion detection technology to record only when someone is moving about. It can even be set up to send e-mail or cell phone notifications when certain prohibited motions are detected (such as after hours).

Cameras are normally placed at vulnerable points on the premises, which need to be monitored. Such cameras are normally placed at a main entrance or any other restricted areas on the office premises. Depending on the organizational needs, all recorded videos can be stored on a hard disk and kept for a certain approved period of time for future retrieval and reference. CCTV can also be used in common areas on the office premises to monitor vandals, as well as to prevent criminal activities or misconduct.

e. Fire Protection Systems

In order to protect and secure company assets and information within offices, it is crucial to protect the offices from fire. This is done by installing an effective fire protection system. The system should be able to integrate the operational characteristics and abilities of different types of systems and equipment used during fire department operations, namely access to a water source, applying a suppression agent to control a particular type of fire, providing information concerning the location of a fire and more.

Fire Services Act 341: 1988

"Mandatory article section 27-36 of the Fire Services Act 341, 1988 (Fire Certificate) - The owners and managers of designated premises are required to apply for a Fire Certificate which certifies that the premises "complies with the life safety, fire prevention, fire protection and firefighting requirements of the Fire Services Act 1988". Subsequently, it has to be renewed annually and issued by BOMBA "on condition that the said facilities remain in good order at all times."

During the design phase, passive fire protection with the installation of firewalls and fire rated floor assemblies may be considered. This would form fire compartments intended to limit the spread of fire, high temperatures and smoke, and have active fire protection with manual and automatic detection and suppression of fires, such as fire sprinkler and fire alarm systems.

f. Power Supply

Most security facilities and equipment (Biometric, CCTV and Fire Protection System) are powered by electric supply. Power supply failure can lead to the malfunction of all electrical equipment, hence exposing the company to various threats during downtime. A continuous supply of electricity is to assure the availability of security facilities and equipment on office premises. Therefore, the need for power backup like Uninterruptible Power Supply (UPS) is crucial to ensure its availability for a certain duration of time depending on the required capacity.

Conclusion

To design secure office premises, all the risks need to be identified and understood, something that is achievable by conducting risk assessment. Depending on the types of risks and their possible impacts, suitable control measures need to be put in place to reduce the risks to acceptable levels. Continuous monitoring and reviewing of security systems should be done from time to time to ensure all control measures are efficient and meet the business objectives.

References

1. *http://www.burnsmcd.com/Services/Detail/Physical-Security#sthash.DydfvBmZ.dpuf*

2. *http://www.techrepublic.com/blog/10-things/10-physical-security-measures-every-organization-should-take/*

3. *http://www.techrepublic.com/blog/it-security/physical-security-with-locks-biometrics-and-other-fallacies/*

4. *http://www.questbiometrics.com/advantages-of-biometrics.html*

5. *http://www.slideshare.net/prabhjeet946/biometric-security-advantages-and-disadvantages*

6. *http://www.referenceforbusiness.com/small/Mail-Op/Office-Security.html*

7. *http://www.kpkt.gov.my/kpkt_2013/akta/Act341y1988bi.pdf*

8. *http://www.businessdictionary.com/definition/risk-assessment.html*

9. *http://www.bankinfosecurity.com/checklist-for-physical-security-risk-assessments-a-695*

ISO/IEC 27001: Have you Chosen the Correct Measurements?

By | Wan Nasra bt Wan Firuz

Introduction

How does an organisation gauge their Information Security Management System (ISMS) performance? Will the parameters selected benefit the organisation financially and operationally? According to Gaffri Johnson [1], the common challenge for most organisations is streamlining their ISMS and operational requirements. Choosing what to measure, setting targets and deciding how to operationalise the measurements also pose a challenge for many organisations. Therefore, this article attempts to provide direction as to what constitutes meaningful measurement. The ISO/IEC 27001 requirements are highlighted and linked in order to emphasize the potential sources of measurement. Subsequently, the importance of objective measurement is emphasised.

ISO/IEC 27001 Measurement Requirements

The measurement-related requirements according to ISO/IEC 27001:2013 standard are depicted in Figure 1 below:

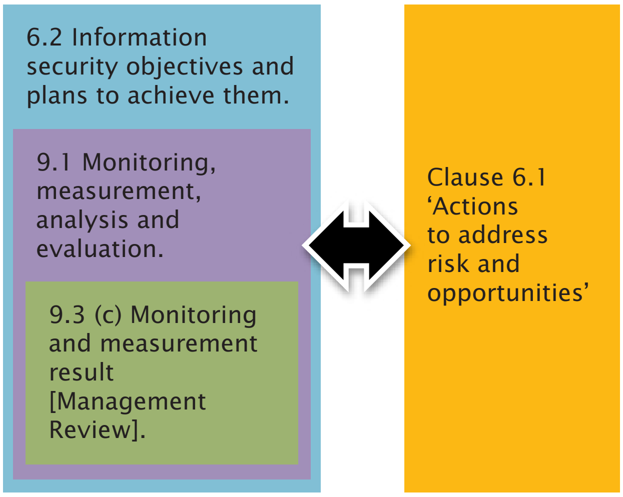

6.2 Information security objectives and plans to achieve them.
9.1 Monitoring, measurement, analysis and evaluation.
9.3 (c) Monitoring and measurement result [Management Review].
Clause 6.1 'Actions to address risk and opportunities'

Figure 1: Relationship between measurement and information security objectives

Ultimately, an organisation endeavours to know whether their ISMS meets the objectives defined under Clause 6.2. In order to set the information security objectives, it is crucial for an organisation to first identify what their core services are and note information security-related issues revolving around these services. The issues can be divided into internal and external matters. Identifying the issues will eventually lead to identifying the interested parties, who are associated with the ISMS scope. According to ISO/TC 223 [2], interested parties can be the stakeholders, the media, vendors, competitors, insurers, and even family members of employees. Their requirements, if taken into account, will provide the organisation with a reasonable notion of what their information security objectives will be.

Clause 9.1 provides organisations with a high level guidance regarding the parameters required to perform objective measurement. According to Chew et al. [3], the three measurable aspects of information security are business impact, efficiency and implementation. If an organisation has performed risk assessment, they can reasonably obtain these three measurement aspects from the assessment. This warrants reference to the organisation's established risk acceptance criteria and the approved risk treatment action (additional reference to Clause 6.1 is necessary, 'Actions to address risk and opportunities'). The selected measurement can then be compared to the information security objectives.

Finally, since the measurement implementation process itself is iterative by nature, care should be taken so that appropriate aspects of information security are measured for a specific time period. At the agreed time, the measurement results should be reported in the management review (Clause 9.3). The importance of doing this is further emphasized in the next section.

Objective Measurement Selection

Rostyslav Barabanov [4] introduced several common potential scenarios in an organisation, which require objective answers. One common query arises when the management wishes to obtain information about investment returns. Another typical query is whether the operations are fulfilling the intended outcome. These queries would most likely arise during management review, while answers to the queries can be obtained from having measurements that meet the information security objectives.

To do this, data collection is required. Data that may be useful as security measures may include, for example, the output of various logs and scans; statistics on training or implementation; security assessment results; statistics from network monitoring devices; incident statistics; internal audits; and business continuity exercises (ISO/IEC JTC 1 SC27 [5]).

In producing each security measure, organisations might be dealing with big data, which, if not presented objectively, will not provide the desired answers. An example is useful to elucidate this concept. Consider a measurement related to the implementation statistics, e.g. percentage of computers already installed with current antivirus definitions. If the percentage is presented versus the number of months (Figure 2), it may be interesting for the Chief Information Security Officer (CISO) but not actionable in any way. If instead, the percentage is presented versus the number of departments or regional offices (Figure 3), the CISO would have an indication of which business line is struggling with this activity. Action can consequently be taken to improve performance. These types of objective and actionable measurements are important for driving operational and financial performance (Dan Rathbun [6]).

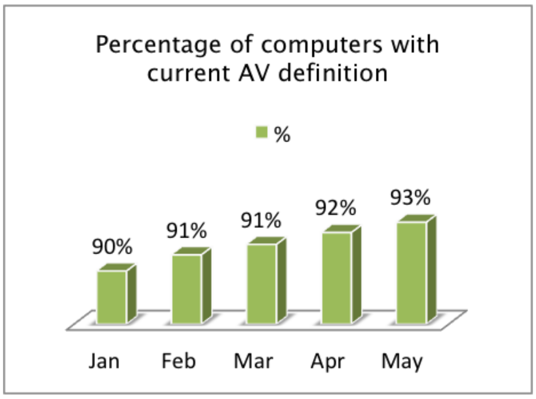


Figure 2: Data visualisation based on months (baseline value is 85%)

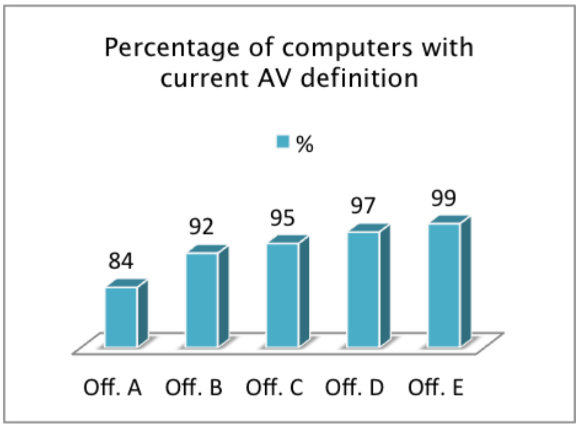


Figure 3: Data visualisation based on regional offices (baseline value is 85%)

Conclusion

The selection of objective measurements and the ability to link them to the information security objectives, are important to ensure that organisations are capable of monitoring their performance, financially and operationally. Not only would the organisation be able to achieve its intended outcome, but the safety of family members working in that particular organisation would also, to a certain extent, be guaranteed.

References

1. Gaffri Johnson. 2014. Measuring ISO 27001 ISMS Processes. Neupart Infromation Security Management.

2. ISO/TC 223. 2012. ISO 22313: Societal security - Business continuity management systems – Guidance. International Organisation for Standardization.

3. Chew et al. 2008. Performance Meaurement Guide for Information Security. National Institute of Infromation Security and Technology.

4. Rostyslav Barabanov. 2011. Information Security Metrics. DSV Report.

5. ISO/IEC JTC 1 SC 27. 2009. ISO/IEC 27004: Information technology - Security Techniques - Information Security Management - Monitoring, Measurement, Analysis And Evaluation. International Organisation for Standardization.

6. Dan Rathbun. 2009. Gathering Security Metrics and Reaping the Rewards. SANS Institute.

7. ISO/IEC JTC 1 SC 27. 2013. ISO/IEC 27001: Information technology - Security Techniques - Information Security Management System - Requirements. International Organisation for Standardization.

The Importance of Job Analysis in Certification Examination

By | Razana Md Salleh

Introduction

According to Standard ISO/IEC 17024 - *General requirements for bodies* operating certification of persons, certification examination is one means of providing assurance to the public that the certified individuals who work in a job or profession are at least minimally competent.

But how is the competency level required for a job set? How do we fairly assess and certify individuals as sufficiently competent? Standard ISO/IEC 17024 defines competence in clause 3.6 as the "ability to apply knowledge and skills to achieve intended results". Job Analysis is a systematic approach defined in the Standard to identify the job and task description, followed by required competence and abilities to perform the job and task. By performing Job Analysis in developing a certification examination, we can ensure the competence of individuals is correctly identified and fairly assessed.

Job Analysis

Job Analysis is one of the requirements in Standard ISO/IEC 17024, clause 8.4(e), which requires for a certification body or organization to prove that a job or practice analysis is conducted and updated to demonstrate the development and maintenance of its certification examination.

One of the goals of job analysis is to identify the important tasks of a job or profession. A good certification examination should emphasize such tasks and reliably asses the Knowledge, Skill and Ability statements (KSAs) of the examination candidates.

How is job analysis conducted? There are various methods available to carry out job analysis, but the most common approach is by following the five (5) steps below:

1. Develop the task statements. Subject matter experts (SMEs) in the profession are selected to identify the job tasks or other activities performed by professionals in the domain in question. Define possible KSAs for the tasks. (The phases of developing a list of tasks and linking KSA to various tasks can be separate sessions or combined).
2. Develop a survey questionnaire using the results from the first step.
3. Select a representative sample of practitioners in the profession to respond to the survey.
4. Ask the survey respondents to rate each task-oriented item according to frequency and importance of being a competent professional in the domain.
5. Analyze the survey data to determine the relative importance of each task and define the examination specifications.

Output of Job Analysis #1: Task Statements

As mentioned in Step 1 above, the first activity in job analysis is to list the job tasks or activities. Data about the job can be obtained from direct observation, interviews with practitioners or SMEs, and analyzing job-related documented materials. Task statements must use descriptors that are both accurate and have a common meaning to those who will use the results of a job analysis to develop the examination questions (items). Table 1 below is an example of task statements. These are general tasks in a Service Analyst's job.

Services Analyst (General) Task Statements	
1	Work in an environment which routinely requires a calm, courteous and tactful approach while handling problems or complaints.
2	Communicate verbally in stressful situations (e.g., dealing with angry or hostile individuals, handling multiple requests for information simultaneously, defending a conflicting opinion or approach).
3	Prepare memos, letters and correspondence documents to communicate with peers, supervisors, outside agency personnel and the public.

4	Interpret complex or technical information and materials (e.g., trade journals, academic journals, technical reports, scientific literature and work procedures).
5	Perform basic statistical analyses to summarize numerical data (e.g., calculating means and standard deviations).
6	Verbally summarize data and information in an impromptu manner (e.g., reporting the outcome of a meeting or debate, responding to questions following a presentation).
7	Deliver formal presentations to large groups of people (e.g., presenting a paper at a conference, addressing a city council).
8	Work as an academic instructor or teaching assistant in an academic institution (e.g., grade school teacher, teaching assistant for a college history class).

Table 1: Sample task statements

Besides task statements, KSAs are developed that may be required to successfully perform the job. An example of KSA statements for a Service Analyst's job is shown in Table 2.

Services Analyst (General) Knowledge, Skill and Ability (KSA) Statements	
1	Knowledge of proper spelling, grammar, punctuation and sentence structure in the English language to ensure that prepared and/or reviewed written materials are complete, succinct and free of writing errors.
2	Knowledge of algebraic theory and concepts to calculate a variety of values related to work project budgets, resources and cost/benefit analyses.
3	Knowledge of basic statistics (e.g., mean, standard deviation, variance) to calculate and interpret data and conduct statistical analyses.
4	Skill to clearly and concisely explain, in writing, the contents of technical materials, such as trade journals, policies or procedures, to audiences with varying levels of expertise.
5	Skill to verbally summarize a variety of facts, statistics and/or data clearly and concisely in an impromptu manner, and adjusting the level and tone of the message appropriately to be understood by the respective audience.
6	Skill to establish and maintain cooperative relations with a variety of individuals, including departmental employees, personnel from other state agencies/departments, consultants, vendors and/or the public.
7	Ability to communicate verbally in stressful situations, such as when dealing with angry or hostile individuals or in emergency conditions.
8	Ability to recognize the sensitive nature and/or political ramifications of a situation.

Table 2: Example of KSA statements

Output of Job Analysis #2: Task Rating

Once the inventory of tasks and KSA statements is developed, the tasks are formatted into a survey questionnaire and rated by practitioners or subject matter experts (SMEs) in terms of certain characteristics, such as frequency, importance, time spent criticality or difficulty learning. An example of task rating is given below, in which the tasks are rated by using two scales: (1) the frequency of performing each task and (2) the importance of each task to the job. The two scales are illustrated below:

FREQUENCY SCALE	IMPORTANCE SCALE
Daily	Very Important
Weekly	
Monthly	Important
Yearly	
Never	Not Important

Besides task rating, KSA rating can be combined into a survey questionnaire to gather more reliable data. An example of the KSA rating can be seen below in which the KSA is rated by using three scales: (1) the importance of KSA to performing the job, (2) the expected level of KSA for professionals at the entry level of the job, and (3) whether possessing more of these KSAs beyond the minimum requirements leads to better job performance. The three scales are illustrated below:

IMPORTANCE SCALE	EXPECTED AT JOB ENTRY	RELATIONSHIP TO JOB PERFORMANCE
Very Important	All	No Observable Relationship

Important	Most	Observable Relationship
Not Important	Some	(possessing beyond the minimal level required of these KSAs does result in better job performance)

An example of KSA statements mapped to the KSA rating scale is given in Table 3. If the survey questionnaire produced reliable data, the results are basically a complete set of requirements for individuals to successfully complete a task or job.

Output of Job Analysis #3: Examination Specification

Once the survey data are gathered, one of the challenges in developing good certification examination is to translate the survey data results into examination specifications. This process requires extensive input from SMEs to define the important examination characteristics, such as:

- Total number of items (questions) in the examination
- Number of items for each domain (particular group of questions)
- Examination format
- Cognitive level of test items
- Weighting of items

	KSA Statement Importance Scale	Importance Scale	Expected Entry to the Job	Relationship to Job Performance
1.	Ability to communicate verbally in stressful situations, such as when dealing with angry or hostile individuals, or in emergency conditions. communicate verbally in stressful situations, such as when dealing with angry or hostile individuals, or in emergency conditions.	Very Important	Most	Observable Relationship
2.	Skill to establish and maintain cooperative relations with a variety of individuals, including departmental employees, personnel from other state agencies/departments, consultants, vendors and/or the public.	Important	Some	Observable Relationship

Table 3: Example of KSA statement mapped to the KSA rating for a Service Analyst's job

For an organization that develops certification schemes based on Standard ISO/IEC 17024, the examination specifications serve as legal documentation supporting the validity of examination and act as evidence of the job analysis activities.

Conclusion

Basically, job analysis has an important role in protecting examinees from unfair examination. A thorough job analysis will serve the public well, while examinees, for the most part, are assured of relevant certification examination through the job analysis effort. Job analysis is not only critical for the validity of the examination, but organizations that develop their own certification schemes must conduct job analysis as it is among the requirements of Standard ISO/IEC 17024 to be fulfilled.

References

1. Conformity Assessment – General Requirements for Bodies Operating Certification of Persons (ISO/IEC 17024:2003)

2. Raymond, Mark R. "Job Analysis and the Development of Test Specifications for Licensure and Certification Examinations." (1995).

3. California State Personnel Board. "Sample Job Analysis Report" (2003).

Generation Y (Gen Y) Online Behavior

By | Marinah Syazwani Mokhtar

Introduction

Generations can be categorized according to birth dates as follows: the Silent Generation (1925-45), the Baby Boomers (1946-60), Generation X (1961-81) and Generation Y, which is the generation of people born during the 1980s and early 1990s. Individuals from Generation Y are sometimes referred to as Gen Y, the Millennial Generation, echo boomers, the Internet generation, iGen and the Net generation. They grew up with new technology and are therefore tech-savvy. Generation Y is active online and is connected to the Internet 24/7, 365 days a year. They prefer to spend their entire lives in a digital environment and equip themselves with the latest gadgets and technology, such as tablets, laptops and smart phones. Generation Y actively search, share and contribute to social media platforms such as Facebook, Twitter and Instagram.

Social media usage

Social media is defined as the collection of online communications channels dedicated to community-based input, interaction, content sharing and collaboration. In other words, users can generate and share a variety of content through online services. Social media has started to become widely used after 2003, despite having existed since the birth of the Millennial Generation. It consists of social networking sites, virtual games, blogs, online review/rating sites and video sharing sites. Social networks and blogs are the top online destinations of any country, accounting for the majority of time online and reaching 60% or more active Internet users. A 2013 Industry Performance Report published by an Internet regulator, the Malaysian Communications and Multimedia Commission (MCMC), states that Malaysia has 19.2 million Internet users, of which 15.6 million are active on Facebook. A 2010 survey conducted by the international firm TNS identified Malaysians to have the highest numbers of friends on social networking websites like Facebook. The Media Insight Project, comprising the American Press Institute and the Associated Press-NORC Centre for Public Affairs Research, has recently carried out a survey of 1,046 American adults aged 18 to 34. It was found that the three most favored online activities were reading and sending emails (72%), keeping up-to-speed with what peers are doing (71%) and streaming TV, music or films (68%).

Gen Y Social Media Use

The main reason Gen Y use social media is because they need to interact with others. The majority of social media users are around 18 to 34 years old and mostly use social media platforms to interact with friends, family and acquaintances. For example on Facebook, users feel the need to post and reply to comments, providing feedback or suggestions about products or brands used. Nowadays, the Millennial Generation uses Instagram to share pictures or moments with followers. Gen Y also employ this platform to generate income and as medium to start online businesses. Social media also serves to obtain information and for entertainment.

Antecedents of Gen Y's Social Media Use

Gen Y's increased social media use can be attributed to technical infrastructure and individual factors.

In terms of technical infrastructure, investments in technological infrastructures can significantly affect Internet and social media use. For instance, Telekom Malaysia (TM), Malaysia's broadband champion and leading integrated information and communication group, offers a comprehensive range of communication services and solutions for broadband, data and fixed-line. They provide UniFi service via fiber optics to deliver high speed Internet to customers' homes. Moreover, TM facilitates a fast-moving world of broadband.

Individual factors, such as socioeconomic status, personal values/preferences and age/lifecycle stage additionally play an important role in shaping Gen Y's social media use. Several of these factors interact with, or result from pertinent environmental factors; hence, they are relatively stable, as is their impact on social media use. In particular, Gen Y's socioeconomic status (as reflected by education, income and other markers of societal standing) in a geographic region will be strongly influenced by the economic and technological environment. For example, low education may lead to low skill levels and usage with emphasis on entertainment rather than information.

Impact of Gen Y's Social Media Use

The use of social media among Gen Y impacts individuals, companies and society in specific ways.

For individuals, the main reason Gen Y are always connected to social media is to keep in touch with others because it is how they interact with the community and socialize. For example, Facebook can increase social capital because people like to share about themselves, and see what others share and say about them. This is the way users shape their own identity. In addition, it helps provide an emotional and psychological boost as the relationships between family, friends and acquaintances become tighter.

For companies, social media serves as a potential source of market intelligence. Social networking sites and blogs are used and monitored to collect information in order to market services and goods. Through social media, firms can strengthen relationships with customers by encouraging them to engage with their brands by interacting with each other. Gen Y's use of social media also has effects on customer-employee interactions as well as how companies hire, manage and motivate employees. These implications are especially significant because increasing numbers of Gen Y members are entering the workforce. Nowadays, several companies check prospective employees' social networking sites prior to hiring and sometimes even terminate existing employees based on what is found.

For society, Gen Y's use of social media may be leading to changes in social norms and behavior at the societal level in domains such as civic and political engagement, privacy and public safety. Gen Y's social media use also has positive effects on political engagements. For example, some ministers create or have their own social network accounts, such as Facebook and Twitter, to become closer to people. As such, it can help encourage and approach the Millennial Generation to share ideas that may contribute towards the country's development.

Conclusion

Gen Y's use of social media is already changing the marketplace, the workplace and society in general. There will be direct influence on individuals, companies and society in different ways. It is evident that Gen Y's use of social media has positive impact on improving self-esteem, getting closer to the community and also sharing ideas regarding the country's leaders.

References

1. *http://www.djsresearch.co.uk/InformationTechnologyMarketResearchInsightsAndFindings/article/Survey-examines-Generation-Ys-online-behaviour-02074*

2. *http://www.talentedheads.com/2013/04/09/generation-confused/*

3. *http://www.themalaysianinsider.com/malaysia/article/malaysians-spend-five-hours-online-daily-and-it-is-mostly-on-social-media-s*

4. *Understanding Generation Y and their use of social media: a review and research agenda, Emerald Group Publishing Ltd*

What Organizations Need to Know About Distributed Denial-of-Service (DDOS) Attacks

By | Sharifah Roziah Mohd Kassim

Introduction

DDoS entails unauthorized activity to prevent legitimate users from accessing information they need, such as web and e-mail services. DDOS attacks simultaneously compromise the availability of information. The most common type of attack happens when an attacker "floods" a network with excessive unauthorized requests. Normally, servers can only process a certain number of requests at a time, so if an attacker overloads the server with an exceeding number of requests, the server will become unable to process legitimate requests from Internet users. Attackers may use spam e-mail messages to launch similar attacks on someone's e-mail account, which is also known as mailbombing. E-mail account holders are assigned a specific quota that limits the amount of data they can have in their account at any given time. By sending illegitimate large e-mail messages to the account, an attacker can consume the quota, preventing one from receiving legitimate messages.

Basically, there are two types of DDOS attacks. One includes network-centric attacks, which overload a service by using up bandwidth causing network congestion. The other type is the application layer attack, which overloads a service or database with application calls, resulting in service unavailability.

The Difference between DOS and DDOS

The differences between DOS and DDOS is that DOS is an older trend and less complex compared to DDOS. The impact is low as it is a one-to-one attack, or attacker to victim. Botnets are not used in DOS and mostly Layer 3 (Network) is targeted. Mitigating DOS attacks is less difficult compared to DDOS attacks.

DDOS has become a trend now and is getting larger, more complex and evolving. The impact of DDOS attacks is much more severe than DOS attacks, as many DDOS agents launch an attack on one victim. An attacker uses multiple compromised computers known as botnets to attack a victim's computer.

How a DDOS Attack can Bring Down a Site or Service

A DDOS attack can bring down a site or service by making it unaccesible to users. This is achieved by overwhelming a website or server with large data or mutiple unauthorised requests, to which the target system either responds very slowly or crashes completely. The traffic or requests required to do this are typically done by using botnets, which are compromised computers also known as zombies.

Who Can be a Victims of a DDOS Attack?

Anybody who runs Internet services or applications is very likely to become a victim. Victims can be financial institutions, media portals, Internet Service Providers, Industries and E-commerce companies. However, adequate DDOS mitigation practices in place will assist to mitigate attacks and minimize the impact on organizations.

The Current DDOS Trend

The current observed trend of DDOS attacks is a tremendous increase in the volume of Layer 7 (Application) attacks compared to Layer 3 (Network) and Layer 4 (Transport) attacks. The trend now is to use more DNS and UDP attacks and use less SYN and ICMP floods. Attack size has also increased, with many attacks exceeding 100 Gbps and the largest reaching 179 Gbps.

The reflected amplification (DrDoS) attack is emerging as a popular attack method
that amplifies the attack volume with even more severe impact. Asian countries appear to be the main source of DDoS attacks. Many Malaysian IPs have been found to be participating in NTP Amplification attacks and DNS Amplification attacks, which may indicate the high possibility that IPs are already compromised and installed with malicious software to be part of DDOS Agents.

Tracing the Attacker

With any cyber attack, one of the goals is to trace the attacker(s). However, apart from technically analyzing the attack, ISPs or even LEAs are required to cooperate in tracing the attacker. The drawbacks are Time and Difficulty. Focus is usually on stopping the DDOS attacks rather than tracing the attacker, followed by having proper prevention mechanisms against DDOS in place and identifying/rectifying the source of attack for total attack eradication.

Concerns About DDOS

Due to the business needs of organizations that depend on Internet infrastructure, it is critical for services to be up and stable all the time for business growth. The impact of a DDoS attack can be serious and widespread, affecting services and business functions, perhaps for many hours or many days if suitable measures to mitigate the attack are not taken. On average, more than 7,000 distributed denial-of-service (DDoS) attacks are observed daily – a number that is growing rapidly. If a website functions primarily by just providing information to the public at no cost, then any loss of revenue caused by the attack may be minimal. However, if a website functions as an e-Commerce site that generates profit, any revenue loss due to a DDoS attack could be serious. For example, industry analyst firms estimate that a 24-hour outage in a large e-Commerce company can cost up to US$30 million.

Conclusion

Denial-of-service (DoS) attacks are on the rise and have evolved into a complex and overwhelming security challenge for large and small organizations in various sectors. Attacks have dramatically evolved from DOS to include distributed (DDoS) attacks and, more recently, distributed reflector (DRDoS) attacks. Impact can be extremely severe and affect the performance of organizations, consequently causing potentially significant financial losses. The early identifications of attacks, quick mitigation and having DDOS prevention mechanisms in place can be a best practice for organizations in defending against DDOS attacks. Without proper mitigation, stopping a DDOS attack immediately would be a challenge as time would be needed to communicate with the service providers and wait for their further action to stop the attack.

References

1. *http://www.mycert.org.my*

2. *https://devcentral.f5.com/articles/layer-4-vs-layer-7-dos-attack*

3. *http://en.wikipedia.org/wiki/Denial-of-service_attack*

4. *http://searchsecurity.techtarget.com/definition/SYN-flooding*

Security of Software Products and their Procurement Process

By | Tormizi Bin Kasim

Introduction to Procurement

Procurement is the acquisition of goods, services and works from external parties or vendors. The goods, services and works are assessed so they can be the best to meet organizational needs at competitive prices. Formal procurement activities include preparing and processing the request and end receipts for goods, services and works as well as making relevant payments. Therefore, the procurement process begins with purchase planning and ends with a contract/agreement as well as payment to external parties or vendors who provided the goods, services or works.

Part of the procurement process is to ensure that the goods, services or works to be acquired, comply with the security requirements set by the organization. Therefore, the procurement process is very important to ensure the procured goods, services or works help the organization meet its business and security objectives. On the other hand, if the procurement process is not managed properly, the security of goods, services or works will be compromised, hence exposing the organization to various security risks.

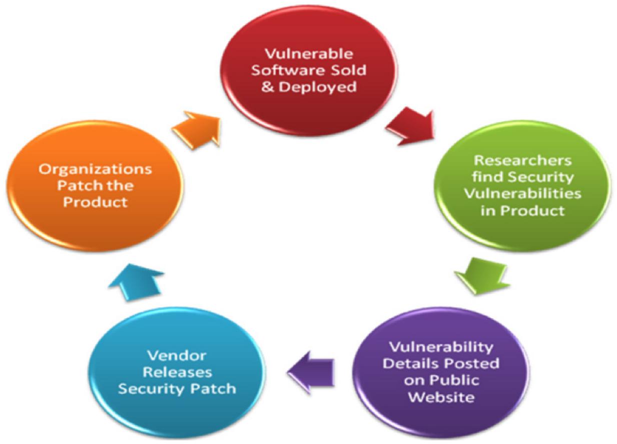
The aim of this article is to provide insight into the security procurement process and
suggest a suitable security approach for procurement, especially when the acquisition of Open Source ICT Products and Applications is involved.

Acquisition of Security Software

Most ICT products and applications used in organizations today are Commercial Off-the-Shelf (COTS) Solutions. These products and applications are not built or developed in-house, hence they need to be customized to suit the user's environment. Customization may include COTS re-configuration in order to meet organizational requirements and business expectations. In most cases, the organization does not have total control over customization processes done by third party vendors, hence such processess are often overlooked, thus not guaranteeing COTS security. The security situation is worse when there are several COTS already in place in an organization and are undergoing the same customization process. The lack of security of any products and applications, especially those provided by third party vendors, will present a weak link in the entire security chain of the organization. In this regard, adopting Common Criteria (CC) Standard ISO/IEC 15408 by an oganization and COTS compliance with CC Standards can be crucial to ensuring the acquired solutions have the necessary security features. From here, any security flaws discovered during COTS evaluation need to be mended to ensure they are not exploited to compromise the organization.

In general, most product developers adopt a Secure System Development Lifecycle (SDLC) framework to warrant the security of their products before being released on the market. However, COTS do not have perfect security! Security flaws that exist in COTS are often discovered by researchers at a later stage and will be posted on public websites, pressuring vendors to release security patches in order to protect their customers and business. All affected users will then take the necessary actions to fix the flaws using the released security patches. However, only major product developers and vendors research and release security patches in order to protect their image and reputation. In the case of Small & Medium Enterprises (SME), they may not have a mature process in place to deal with security issues due to several financial factors and the unavailability of security experts. In view of this, the organization needs to explicitly bind such vendors through procurement contracts to rectify any arising issues in the future, otherwise the organization can do little to drive them to do so.

A diagram of the current practice or trend adopted by the industry for correcting security issues with products is depicted below:


Vulnerable Software Sold & Deployed
Researchers find Security Vulnerabilities in Product
Vulnerability Details Posted on Public Website
Vendor Releases Security Patch
Organizations Patch the Product

Security in the Procurement Process

The procurement process changes from time to time. However, from a high level perspective, the following activities that comprise any procurement process are explained here. One of the practical approaches in dealing with security issues in the procurement process is the inclusion of relevant security specifications as part of the procurement requirements.

a) Clear Understanding of Business Requirements

The procurement process should be modified to mandate the inclusion of security requirements as a part of the business requirements. This step is not as easy as it sounds, though. Security requirements could be as simple as having an application that supports strong authentication, or it could push the business to key in a list of complex security requirements that might include not only security requirements from a business perspective, but also audit requirements to comply with governing standards like SOX, HIPAA, PCI, DSS, etc. Deriving security requirements is a structured process, and this step is very important because it sets the security base for the procurement process. As the organization moves forward into the next phases of the Procurement Lifecycle, it will need data accumulated up to this stage.

b) Supplier Identification and Shortlisting

In this stage, the organization shortlists potential vendors. Once done, the organization will communicate with the vendors and share a Request For Proposal (RFP) with them. The RFP contains detailed business requirements to ensure that both buyer and seller are on the same page and the seller bids after perusing all of the business requirements. This is a sweet point for the security team. The organization will have to work with the business to determine detailed security requirements, including the audit requirements that meet the governing standard requirements. For this reason, an organization needs to include security requirements into the RFP to ensure clear communication from the beginning of any procurement process.

c) Pricing and Contract Negotiations

This is another area in which organizations should consider embedding security requirements to meet their security expectations. Pricing is not a concern for the security team, therefore they will not dive into the details of how the procurement team negotiates prices and arrives at a final figure with the selected vendors. The organization might have some concerns about the contract negotiations part of this step. Contract negotiations have detailed terms and conditions that both the organization and vendors study before making a deal. There are two key points of interest to the security team here: the Service Level Agreement and Support Terms and Conditions.

The Service Level Agreement, commonly referred to as SLA, is an important document of interest to the information security team. Having the SLA terms address security concerns will ensure the organization, as the user, will bind the vendors to provide the required services. The SLA is done during a decision-making period for the smooth functioning of business. Depending on the vendors, there can be different SLA levels (e.g. Gold, Platinum, etc.). The point for the user to note is that the SLA is a significant point not to be overlooked by the Security Team. A comprehensive discussion with the management should take place before finalizing the SLA with the vendors concerned.

d) Finalization and Product Shipping

This step deals with finalizing the procurement deal and formally closing the entire procurement process for a particular product. It also ensures that a product shipped by a vendor is successfully received by an organization. The security team does not have a big role in this step. They deal more with formalizing and signing final contracts, which are tracked by the procurement team until the procurement process concludes.

Conclusion

By adopting a systematic approach to the security procurement process and by including security requirements, organizations are able to protect the acquisition of products, i.e. goods, services or works from external parties such as vendors selected to provide the products. An organization cannot do much to rectify a situation at a later stage if there are gaps in the procurement contract. Therefore, it is also important for the organization to prepare inventories of all products and their histories from the start until the end of the contract. When the contract is due for renewal, the organization can refer to the inventories to evaluate the products' performance and use them to enhance security requirements and negotiate the terms and conditions for better future handling of security matters. The security team should track all products throughout the contract and evaluate the effectiveness of the products' performance as well as the vendors' after-sale service support. An organization can improve the situation in future, as all renewed contracts and new, updated procurement processes will have to address more accurate security requirements. Expired contracts may not be considered for renewal if the relevant vendors have failed to deliver the required products in accordance with the terms and conditions.

References

1. http://en.wikipedia.org/wiki/Request_for proposal

2. http://www.purchasing.tas.gov.au/buyingforgovernment/

3. http://www.veracode.com/solutions/cots-security-audits-best-practices

4. http://www.purchasing.tas.gov.au/buyingforgovernment/

Security Vetting

By | Sharifah Sajidah bt Syed Noor Mohammad

Introduction -- What is Security Vetting?

According to the Collins English Dictionary, Security Vetting is the process of investigating somebody to establish their trustworthiness. Wikipedia says Vetting is the process of performing a background check on someone before offering them employment, conferring an award, etc. A prospective person or project may be vetted before making a hiring decision.

In CyberSecurity Malaysia, all employees must also undergo this process of Security Vetting by completing the *"Borang Soalan Keselamatan Unit Tapisan Keselamatan"*. Employment with CyberSecurity Malaysia is additionally subject to a Security Vetting report, which is done by the Chief Government Security Office (CGSO), Prime Minister's Department *(Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, Jabatan Perdana Menteri)*. It is a process through which individuals are screened for their suitability to carry out work within the organisation. A suitable person possesses integrity and reliability and is not vulnerable to improper influence.

Vetting Dimensions

The breadth of vetting checks increases in proportion to the sensitivity of the role. Hence, CyberSecurity Malaysia adopts the following security forms: ***Borang Tapisan Keselamatan Kasar and Borang Tapisan Keselamatan Halus.***

However, dynamic technology changes have taken over manual security vetting forms and replaced them with an online system. The CGSO has successfully developed an online security vetting system known as e-Vetting. The online system is part of the continuous improvement effort to reinforce the structured and accountable process of vetting.

Information required for vetting is subject to the role of the employees. Employees may have direct or indirect access to classified/ confidential documents and/or have direct or indirect access to secret or top secret documents, such as secretaries, assistants in the technical department, system administrators, Human Resource personnel, managers, specialists and top management.

The information required on e-Vetting forms is as follows:

a. Applicant's profile including current position, address, identification number, etc.
b. Education background
c. Spouse details
d. Information on parents/guardians
e. Previous employment
f. Siblings and their jobs
g. Involvement in committees/associations
h. Criminal history details (if any)
i. Activities and purpose abroad
j. Latihan Ala Ketenteraaan di Dalam/Luar Negara
k. References
l. Declaration by applicant
m. Verification by Head of Department/Superior

Rationale of Having Security Vetting in the Organisation

a. To align with our manifesto, which is securing cyberspace, and in parallel with our presence as a national cybersecurity specialist agency under the Ministry of Science, Technology and Innovation (MOSTI), we provide specialized cybersecurity services contributing immensely towards a bigger national objective of preventing and minimizing disruptions to critical information infrastructure in order to protect the public, economy and government services.

   Failure to comply with procedures, rules and regulations for protecting security, classified or sensitive information, which is not limited to transmitting, processing, manipulating and storing, and which results in incremental doubt of a clearance subject's trustworthiness, judgment, reliability, or willingness and ability to safeguard, is a serious security concern.

b. To comply with the ISO 27001:2005 standard, a holistic, coordinated view of the organization's information security risks is necessary in order to implement a comprehensive suite of information security controls. Effective information security reduces risk by protecting the organization from threats and vulnerabilities to ensure business continuity. The standard has a specific clause on Human Resource Security, which comprises prior employment, during employment and termination of employment. Thus, as part of the safety measure in hiring new employees, pre-employment checks or background checks are imposed prior to making an offer of employment to an individual. The biggest concerns are the need to protect all assets inclusive of human resources against threats from hostile intelligence services and information from unauthorized disclosure, theft fraud or malfeasance, and unsubstantiated or false claims of experience on resumes.

c. In terms of security, it is necessary for all levels of employees to be free of undesirable elements. They shall have attributes, such as reliability, free of immorality and not easily influenced by anti-national elements, espionage sabotage and subversive behavior. Security Vetting can be used to confirm and verify employees' following aspects:

- Identity,
- Involvement in illegal activities,
- Criminal convictions relevant to the role, particularly if not volunteered by the applicant and are only revealed through other checks,
- False or unsubstantiated claims on the resume or application form,
- Unsubstantiated qualifications,
- Employment history.

Vetting Process

a. All employees who are subject to security vetting are required to complete the E-Vetting form online by accessing the CGSO website www.evetting.cgso.gov.my. Prior to that, employees are informed they are to be vetted and briefed on the process. It is important for employees to provide full and accurate information, as any omissions may cause a delay in their application. The candidates must declare that the information given is true and complete, and acknowledge that any false statement or deliberate omission may be grounds to deny employment. All applications for security vetting must be treated impartially irrespective of gender, marital status, age, race and religion.

b. Applicants can obtain the e-Vetting form by using their identity card number as the user ID.

c. To ensure a smooth e-Vetting process, government agencies should appoint two (2) Human Resource officers to be responsible as System Administrator/Verifier (Pegawai Pengesah) for all e-Vetting applications. The roles of the system administrator/verifier are to review and verify the application. They will then submit the new e-Vetting application to the CGSO's office. Furthermore, the CGSO will execute the verification process with an appointed investigation panel. All personal information gathered during the vetting process is handled in the strictest of confidence by the vetting agencies.

d. The depth of checks will vary according to the level of regular access to sensitive information that the job or task will entail. With the online system, the processing period has been shortened from three (3) months, to one (1) -- one month and a half (1 ½).

e. The system also enables applicants to check their e-Vetting application status at any point in time until the results are made available by the CGSO. Apart from that, the system also enables e-Vetting certificate printing either by the system administrator/verifier or the applicant.

f. Upon obtaining approval, the CGSO will notify the system administrator/verifier and the applicant of no crime records found. However, should there be any misleading information or crime record, the CGSO will notify the system administrator/verifier through a letter advising on the way forward, such as an interview session with the applicant, etc.

Conclusion

The primary objective of having Security Vetting is to protect intelligence, operations and assets and to preserve safety by providing an acceptable level of assurance of employee integrity at CyberSecurity Malaysia. Owing to the sensitivity of our work, submitting misleading and/or false information during the vetting process would be regarded as evidence of untrustworthiness. In such circumstance, the applicant's security vetting clearance may be declined.

References

1. http://en.wikipedia.org/wiki/Background_check

2. http://www.dorset.police.uk/pdf/P27-2009Vetting_Policy_V1_1.pdf

3. http://www.thamesvalley.police.uk/pub-policiesandprocedures-vetting.pdf

4. http://www.cgso.gov.my/portal/#e-vetting

5. http://www.cybersecurity.my

6. ISO/IEC 27001:2005

7. Pekeliling Perkhidmatan Bilangan 6 Tahun 2011, bertajuk Pindaan Pelaksanaan Tapisan Keselamatan Bagi Pegawai Yang Dilantik Dalam Perkhidmatan Awam JPA.BK(S) 256/6/26 Jld.2 (18)

Open Source Intelligence: Extracting Meaningful Insight from Publicly Available Sources

By | Mohamad Nizam Kassim

Introduction

Since the inception of social media platforms, the amount of published information has experienced an unprecedented growth, earning it its own name -- Big Data (LaValle *et al*., 2013). Most of this published information comes from user-generated content through various social media platforms with several functionalities, such as content creation, content sharing and multi-party comments. This scenario is referred to as information overload or information explosion (Bergamaschi et al., 2010). User-generated content provides opportunities for interested parties to gain meaningful insight from large, open source data using a structured analysis approach called Open Source Intelligence (OSINT).

Open Source Intelligence

OSINT is defined as "actionable intelligence produced from publicly available information that is gathered, analyzed and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement" (Glassman *et al.,* 2012). OSINT is a subset of the intelligence discipline that includes signal intelligence (information analysis on intercept signals), human intelligence (information analysis on humans in person) and geospatial intelligence (information analysis on satellite, aerial photography, mapping/terrain data) (Schaurer *et al.,* 2011). It is important to remember that OSINT focuses on the analysis of open source data on the Internet or in other words, publicly available information. This article briefly explains the subject of open source intelligence, intelligence analysis and its application in cross domains, but not open source software.

Open Source Data

OSINT takes advantage of open access data that is publicly available on the Internet for everyone to use or republish without any commercial restriction (copyright, patent) or other control mechanisms. Therefore, OSINT uses online media sources (online news, online magazines and commercial websites), public data (government and educational institutions' websites), user-generated websites (social networks, wikis, blogs) and many more. The main objective of OSINT is to apply the large sets of publicly available information from open source data and process specified data or processed intelligence into tailored knowledge or meaningful insight for decision-making and actionable intelligence by specific individuals or groups. However, not all publicly available information is worth analyzing. Therefore, the intelligence analyst needs to identify the reliability of sources and information from those sources, as illustrated in Figure 1 (Willox, 2006).

Source reliability includes source authenticity, trustworthiness and competence. Sources of information are usually rated in five categories, namely completely reliable, usually reliable, fairly reliable, usually not reliable and unreliable. Sources of information that are considered reliable are those whose information is logical in common sense and supported by independent or third-party reliable sources. Similar to source reliability, information is usually rated in five categories: confirmed, probably true, possibly true, doubtfully true and improbably true. Another crucial aspect of open source data is the validity of information, whereby the segregation of information, that is, past, current and future information, needs to be grouped based on a timeline in order to avoid confusion or be misleading during intelligence analysis. Thus, intelligence analysis starts with a structured approach to identify the quality of data sources and their respective information that leads to the quality of processed intelligence.

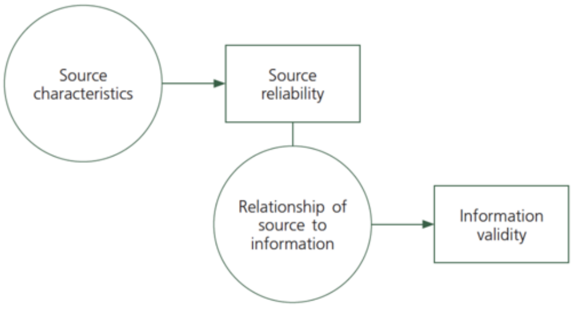


Figure 1: Sources and Information Reliability Evaluation

Open Source Intelligence Tools

There are many open source and commercial tools that can be used to conduct open source intelligence activities. These tools can be categorized based on their generic features for specific functions such as people reconnaissance (pipl.com, knowem.com, tineye.com), organization reconnaissance (Search Diggity and Google Hacking Database) and infrastructure reconnaissance (shodanhq.com, dnsstuff.com). People reconnaissance focuses on building profiles on individuals based on their online presence on the Internet from various open source data. Profiles include names, pictures, online accounts, professional and academic qualifications, known associates and many more. In general, people are somehow associated with certain specified organizations. Therefore, organization reconnaissance focuses on building profiles on institution or corporate information such as financial reports, corporate news/press releases, products/services and so on. Such profile is crucial to understanding the background history of an organization and its future activities based on information about its business, competitors or customers from various open source data. On the other hand, infrastructure reconnaissance focuses on the organization's infrastructure in great detail with an overview of the organization's infrastructure, and its network relationship with other networks can be viewed. People, organization and infrastructure reconnaissance is often performed simultaneously and usually takes some time to gather more information and validate source and information reliability. In short, open source intelligence tools are used to collect specified information from the Internet while further intelligence analysis needs to be done in search of consistent patterns and/or systematic relationships between variables, for example people, organizations and infrastructure. Then the findings are validated by applying appropriate intelligence analysis.

Intelligence Analysis

There are four types of intelligence analysis of data collected from open sources, namely inference, conclusion, prediction and estimation, as illustrated in Figure 2 (Willox, 2006).

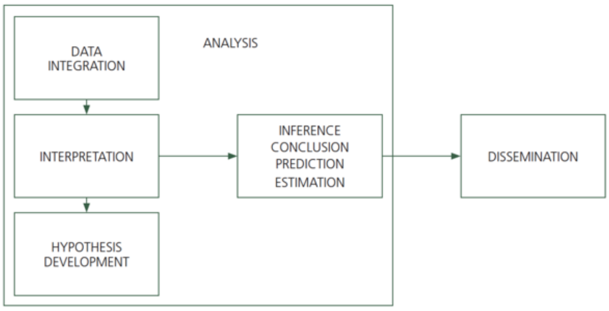


Figure 2: Intelligence Analysis Process

Intelligence analysis starts with compiling all collected data, which is a step also known as data integration. Then, exploratory data analysis or integration is performed in order to find the relationships among variables (people, entities, issues, events, places). The most common techniques used are charting: link charting to show relationships among entities featuring in the analysis, event charting to show chronological relationships among entities or sequences of events, frequency charting to organize, summarize and interpret quantitative information and data correlation to illustrate relationships between different variables (Benes, 2013). From pattern consistency in charting techniques, meaningful insight can be extracted to form a hypothesis, a tentative explanation or a theory that requires additional information for confirmation or rejection. It can also help make an inference -- a process of deriving logical conclusions from premises known or assumed to be true, or a conclusion -- an explanation that is well supported. Alternatively, insight can help form a prediction, an inference about something that will happen in the future, or an estimation (an inference made about the whole of a sample, typically quantitative in nature) (Schaurer *et al.,* 2011; Glassman *et al.,* 2012). Therefore, the output of intelligence analysis is processed knowledge, which is supported by a structured analysis approach and not by analysts' opinions and intuition. Finally, the actionable intelligence or processed knowledge is disseminated to the intended individuals or groups.

Open Source Intelligence Applications

The application of OSINT activities varies in nature depending on industry verticals. Among the OSINT applications in business are business intelligence, commercial intelligence and competitive intelligence. Other applications are defense intelligence for defense, strategic intelligence for the government, etc. These applications are often in the form of visualization dashboards with specified parameters that describe meaningful insight for intended individuals or groups.

Conclusion

OSINT is essentially a field of extracting meaningful insight from open source data. It provides intelligence analysts with opportunities to gather, filter and make sense of data in a structured manner that leads to quality, yet reliable, actionable intelligence or processed knowledge. OSINT is therefore a crucial capability for organizations to remain relevant and competitive in today's reality by making sense of data. Remember, Excellent Actionable Intelligence is Power!

References

1. Benes, L. (2013). OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. Journal of Strategic Security, 6(5), 5.

2. Bergamaschi, S., Guerra, F., & Leiba, B. (2010). Guest editors' introduction: information overload. Internet Computing, IEEE, 14(6), 10-13.

3. Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior, 28(2), 673-682.

4. LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S., & Kruschwitz, N. (2013). Big data, analytics and the path from insights to value. MIT Sloan Management Review, 21.

5. Schaurer, F., & Störger, J. (2011). Guide to the Study of Intelligence. The Evolution of the Open Source Intelligence (OSINT). The Intelligencer, Association of Former Intelligence Officers, 2.

6. Willox, N. (2006). Transforming data into decisions: A framework for addressing the open source intelligence (OSINT) challenge. Homeland Defense Journal,4(7), 42-47.

The Knowledge and Skills Supporting the Role and Responsibilities of an Information Security Analyst

By | Sharifah Norwahidah Syed Norman, Razana Md Salleh, Nahzatulshima Zainuddin

Introduction

Nowadays, technology and information play an important role in the organizational environment. Due to the changing nature of technology, most organizations are facing challenges in implementing security over data and information. The majority of organizations agree that the implementation of effective IT can provide advantages and improve business performance. However, the rapid growth of technology additionally provides criminals with the means to cause loss and harm to organizations. With the duty to reduce such risks, an information security analyst is one of the individuals responsible for protecting the organizations' information and data.

An information security analyst is an important team member, who helps an organization take measures to protect sensitive and critical data. The analyst will help develop, implement and ensure policy compliance to protect the organization's data from improper access or use. Currently, among information security analysts' essential roles are planning and carrying out security measures to protect organizations' computer networks and systems. Their responsibilities are continually expanding as the number of cyberattacks increase. Goodall, Lutters & Komlodi (2004) agree that information security analysts are responsible for defending their organization's network infrastructure from intruders. Finally, good understanding of the organization's business will help analysts perform more effectively, as they recognize which information is most critical to the organization.

Skills of the Information Security Analyst

As mentioned by Nord and Nord (1997), an analyst is an individual who studies the special needs and problems of an organization. To perform system studies, the experienced analyst requires sufficient skills and knowledge. An information security analyst needs several skills to help them resolve problem regarding security in an organization. Technical skills are critical to the information security analyst to be able to determine and take measures to prevent attacks, which may come from inside or outside the organization. The analyst may be included in planning for other threats to the organization's data, such as maintaining power to servers in case of a local outage, and planning for operations continuity at alternate sites in the event of main site closure.

Another skill is the ability to communicate with audiences of different levels. When communicating security issues to non-technical staff, the analyst must be able to make technical concepts understood by a general audience. As cited by Nord & Nord (1997), the most important skills of a security analyst are maintaining customer affairs, maintaining communications, assessing customer needs, providing recommendations and conducting presentations. Wilkins & Noll (2000) agree that the ability to work collaboratively, work with users and clients, communicate with users and manage projects will continue to be a significant skill of all information security staff groups. These skills should be conveyed through various information security training courses, such as system and database analysis.

In a research by McMurtrey et al. (2008), it was found that another vital set of skills for new IT professionals includes soft skills, such as problem-solving, critical thinking and teamwork skills. Critical thinking entails using logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems. Critical thinking is the ability to think clearly and rationally, and includes the ability to engage in reflective and independent thinking. Someone with critical thinking skills is able to understand logical connections between ideas.

Last but not least, as mentioned by Lee, C.K. & Han 2008, technical skills related to development, software, social skills and business are equally important for an information security analyst. Information security analysts must continually adapt to current cyber threats and be alert to the latest methods used by hackers to attack or hack computer systems. Analysts need to research new security technology that can effectively protect their organization. They need to have the skills to monitor security operations related to people, processes and technologies.

The knowledge of the Information Security Analyst

Knowledge can refer to theoretical or practical understanding of a subject. It can be in implicit form (practical skills or expertise) or explicit form (theoretical understanding of a subject). Information security analysts need to have sufficient knowledge to successfully perform tasks. Examples of knowledge for an information security analysts are tabulated in Table 1.

Knowledge	**Description**
Security Procedures	Knowledge of information technology trends and impact on related security procedures and processes as well as the current and developing information technology service requirements.
Communication	Possess strong interpersonal skills and the ability to effectively communicate with a wide range of individuals and constituencies in a diverse community.
Operating Systems	Knowledge of Windows and/or Linux operating systems, IP data networks, testing, monitoring and management.
Telecommunications	Knowledge of transmission, broadcasting, switching, control, and operation of telecommunications systems.
Administration and Management	Knowledge of business and management principles involved in strategic planning, resource allocation, human resource modeling, leadership techniques, production methods, and coordination of people and resources.
Public Safety and Security	Knowledge of relevant equipment, policies, procedures and strategies to promote effective local, state or national security operations for the protection of people, data, property and institutions.
Communications and Media	Knowledge of media production, communication, and dissemination techniques and methods. This includes alternative ways to inform and entertain via written, oral and visual media.
Customer and Personal Services	Knowledge of principles and processes for providing customer and personal services. This includes customer needs assessment, meeting quality standards for services and customer satisfaction evaluation.
Production and Processing	Knowledge of raw materials, production processes, quality control, costs and other techniques for maximizing effective manufacturing and distribution of goods.
Design	Knowledge of design techniques, tools and principles involved in the development of precision technical plans, blueprints, drawings and models.

Table 1 Knowledge of the Information Security Analyst

The roles and responsibilities of the Information Security Analyst

Information security analysts have important parts and responsibilities in organizations. Information security analysts are responsible for maintaining the security and integrity of data. They must have knowledge in every aspect of information security within the company. Their main job is to analyze the company's security measures and determine whether they are effective. Information security analysts are accountable for implementing any information security-related training, for instance proper security measures for webmail. Security analysts must work with business administrators as well as IT professionals to communicate security system flaws. They should recommend changes that can improve every aspect of company security.

Furthermore, information security analysts' responsibilities are creating, testing and implementing network disaster recovery plans. A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Information security analysts should be heavily involved in developing the organization's disaster recovery plan for employees to follow in case of emergency.

The plan should include preventive measures, such as regular backup and transfer of data to offsite locations, as well as plans to restore IT operations after a disaster. Analysts should continually test the steps in their recovery plans. Organizations cannot always avoid disasters, but with careful planning the effects of a disaster can be minimized. The objective of a disaster recovery plan is to minimize downtime and data loss.

In addition, information security analysts are required to conduct risk assessments, which involve the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. The objective of performing risk management is to enable the organization to accomplish its mission by improving the security of the IT systems that store, process or transmit organizational information, by enabling management to make well-informed risk management decisions to justify the value as part of an IT budget.

Last but not least, information security analysts are responsible for training new staff on network and information security procedures. Wilkins & Noll (2000) stated that for end-user staff, specific courses that address these skills and other "soft skills" ought to be developed through training and awareness. Too many people are still knowingly or unknowingly careless with information security while risk professionals are trying their best to train, inform and inspire their employees about the importance of protecting information security. Most employees remain largely unaware of the substantial consequences of a data breach. For training to be effective, it needs to be embedded in the roles of employees, and many organizations need to review both the nature and frequency of their training. Reporting security breaches is one good way to help improve awareness.

Conclusion

In conclusion, the information security analyst is an important member of an organization. An information security analyst is required to have a combination of problem-solving skills, analytical abilities and a thorough understanding of information security. They need to be able to communicate effectively both verbally and in writing. Information security analysts must be well-versed in security rules, regulations and standards. They must have knowledge in different areas, including electronics/ computer science, telecommunications, engineering technology, public safety and more. Understanding the skills and roles required of an information security analyst is critical, as this issue could impact the way organizations hire and train employees.

References

1. Goodall, J., Lutters, W., & Komlodi, A. (2004). The work of intrusion detection: rethinking the role of security analysts.

2. Lee, C.K., & Han, H. (2008). Analysis of skills requirement for entry-level programmer/ analysts in Fortune 500 corporations. Journal of Information Systems Education, 19(1), 17.

3. McMurtrey, M., Downey, J., Zeltmann, S., & Friedman, W. (2008). Critical skill sets of entry-level IT professionals: An empirical examination of perceptions from field personnel. Journal of Information Technology Education: Research, 7(1), 101-120.

4. Nord, G. D., & Nord, J. H. (1997). Information systems project development: knowledge and domain requirements for the systems analyst. Industrial Management & Data Systems, 97(1), 17-24.

5. Wilkins, M. L., & Noll, C. L. (2000). Critical skills of IS professionals: Developing a curriculum for the future. Journal of Information Systems Education, 11(3-4), 105-110.

6. What is an Information Security Analyst?. Retrieved April 1, 2015, from http://www.computersciencedegreehub.com/information-security-analyst/

7. What skills are required for Information Security Analysts?. Retrieved April 1, 2015, from https://www.mymajors.com/career/information-security-analysts/skills/

Social Engineering in Malaysia

By | Adlil Ammal B Mohd Kharul Apendi

Introduction

Intruders and hackers are on the lookout for ways to gain access to valuable resources, such as computer systems or corporate and personal information that can be used maliciously or for personal gain. Sometimes invaders get a chance when there are genuine gaps in security that can be breached. Basically, they can also get through on account of human behaviour, such as trust, which people sometimes ignore in terms of the consequences of being careless with information. In the past, people who always used confidence and took advantage to cheat others were called con artists, but today these kinds of people are known as social engineers [1].

Definition of Social Engineering

Social Engineering is the term associated by the hacker community with the process of using social interactions to obtain information about a "victim's" computer system [2]. The term Social Engineering also reflects confidence tricks or simple fraud aimed to obtain information or computing system access. Additionally, many social engineering attacks are made possible with help from insiders within an organization. These threats are commonly referred to as “Insider Threats” [3]. The attacker does not usually show or expose themselves to the victims while they gather information. Social Engineering occurs in many forms, but generally through various natural facets of human behavior. A social engineer uses a victim’s weakness based on behavior patterns to get information. Several common human behaviors often exploited by social engineers are presented below.

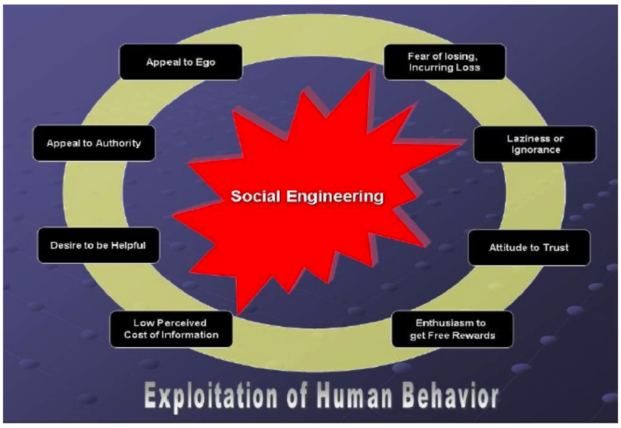
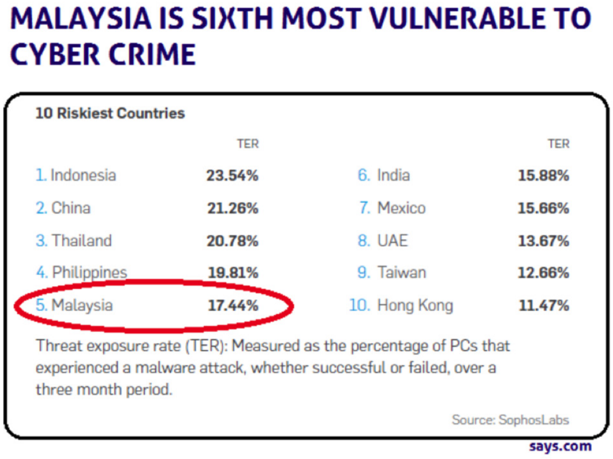

Appeal to Ego
Fear of losing, Incurring Loss
Appeal to Authority
Laziness or Ignorance
Social Engineering
Desire to be Helpful
Attitude to Trust
Low Perceived Cost of Information
Enthusiasm to get Free Rewards
Exploitation of Human Behavior

Figure 1: Common exploitation of human behavior

Social engineering is still the most effective and probably the easiest method of attaining secret information. Some social engineers are hard to detect because they are trained to get information without being suspicious to the victim.

Social Engineering Cases in Malaysia

Based on a SophosLabs report, Malaysia is the sixth most vulnerable country in the world for cybercrime [4] (Figure 2), which includes several types of attacks and fraud that are most often caused by social engineering. Other cybercrimes reported are cyber invasion attempts, spam, denial-of-service, content-related offences, malicious codes and cyber defamation. All these cases of social engineering particularly happen due to the carelessness of victims themselves and unethical persons that aim at something regardless of how to achieve it. Besides, Malaysians are among the highest social networking users worldwide, with the number of social engineers having also increased simultaneously. Digital News Asia has reported the case of a victim who was cheated by a telephone operator claiming to be a bank officer. This victim lost about RM 3600, which was all the money in her savings account [5]. Furthermore, police have also received many reports regarding social engineering cases.



MALAYSIA IS SIXTH MOST VULNERABLE TO CYBER CRIME

10 Riskiest Countries

	TER		TER
1. Indonesia	23.54%	6. India	15.88%
2. China	21.26%	7. Mexico	15.66%
3. Thailand	20.78%	8. UAE	13.67%
4. Philippines	19.81%	9. Taiwan	12.66%
5. Malaysia	17.44%	10. Hong Kong	11.47%

Threat exposure rate (TER): Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over a three month period.

Source: SophosLabs

says.com

Figure 2: Sophos Security Threat Report 2013

Social Engineering Categories

Social engineering is divided into two categories, namely technology-based approaches and non-technical approaches. The first, technology-based approach category contains social engineering meant to deceive a victim who is interacting with an authentic website or system and to lead the victim to provide private and confidential information. As an example, popup windows will alert users that an application or system has a problem, and the user needs to revalidate in order to proceed. The innocent user will enter personal or private information without checking, and once they have entered the information, unethical hackers gain access to the system with the user's credentials. Sometimes the victim does not notice information is being stolen until something happens. On the other hand, in the non-technical approach category of fraud, innocent people are attacked only by deception through taking advantage of human behavior weaknesses. This situation occurs when a hacker impersonates or acts as a person of authority, such as a bank operator, manager or many others. Usually, the hacker will ask the representative person whether he or she has forgotten their password and would like to request for a new one. After resetting the new password, the user conveys it to the hacker who now has access to the account or system.

Technical Attack types

i. Phishing

Occurs through email that appears to come from legitimate businesses, requesting for verification of information and giving a warning if the request is not followed. Such phishing emails usually contain fake links that request confidential information from the user.

ii. Vishing

Vishing is the practice of leveraging Voice over Internet Protocol (VoIP) technology to deceive the public of private, personal and financial information for the purpose of financial reward. Vishing exploits public trust through the landline telephone provider TM in Malaysia.

iii. Interesting Software

In this situation, a victim becomes convinced to download and install a useful program or application that may infect their computer and cause the hacker to steal information.

Non-technical Attack Types

i. Direct Approach

This method occurs when someone hands over their ID and password to someone else without a proper channel. The person who conveyed their password may not think about the consequences. The person receiving the password may use the ID and password to access the database and do anything they want. Another approach is tailgating. Tailgating entails gaining unauthorized entry to a secured area by closely following someone with authority to enter the premise. If something happens, it may affect the wrong person.

ii. Dumpster Diving

In this act of information gathering, someone in an organization throws away mail or documents without shredding them first. Identity theft potentially results when dumpster divers find identification information and sell it to others. Other risky information that is always targeted by hackers includes company phone books, employee details and paperwork. Besides, hackers can retrieve confidential information from a computer hard disk. There are numerous ways to retrieve information from disks, even if the user thinks the data has been 'deleted' from the disk.

iii. Spying and eavesdropping

A clever spy can determine an ID and password by observing a user typing these in. All that is required is to be present, behind the user, and be able to see their fingers on the keyboard. If the policy is for the helpdesk to communicate passwords to users by phone, then if a hacker can eavesdrop or listen in on the conversation, passwords are compromised. An infrequent computer user may even be in the habit of writing their IDs and passwords down, thereby providing spies with an additional avenue to get the information.

iv. Acting as Technical Experts

This is the case where an intruder pretends to be a support technician working on a network problem and requests the user to allow access to the workstation and fix the problem. The unsuspecting user, especially if not tech-savvy, will probably not ask any questions or may even watch while the computer is taken over by the so called 'technician'. Here, the user is trying to be helpful and do their part in fixing a problem with the company's network.

Countermeasures and Safeguarding

The key to maintaining the confidentiality, integrity and availability of an organization's information and information systems is controlling who accesses what information. This is accomplished by being able to identify the requestor, verifying they are not an impostor and ensuring the requestor has the proper level of clearance to access a given resource. Beside that, a lot of preventive action can be taken to avert social engineers from perpetrating crimes against victims. CyberSecurity Malaysia's Chief Operating Officer, Dr Zahri, has advised the public to ignore any calls from unknown callers who seem suspicious, secondly, not to reveal personal details to strangers that one has never met in person, next, to not transfer money from ATM or online to an unknown party and whose background is unfamiliar. If necessary, people should go directly to an office or authorized payment center such as post office or bank, and always keep the official receipts. Users also need to know they have a right to ask why and how another person obtained their personal information like MyKad number or mobile phone number.

Based on the Privacy Data Protection act, someone cannot distribute others' information without a notice to the owners. Otherwise, it becomes a violation of someone's privacy policy. Nevertheless, if something happens, victims must immediately inform their bank, so the bank can monitor the account for suspicious activity, block the affected account or attempt to cancel any money transfers made to scammers' accounts. Moreover, for investigation purposes, victims need to keep all evidence like call logs, SMS, emails and transaction slips issued by the bank. Lastly, individuals should not hesitate to make a police report or Cyber999 report with the evidence. In addition, to prevent social engineering from occuring, organizations need to establish frameworks of trust on employees to ensure they understand the sensitivity of information. Employees also need to identify which information is sensitive and evaluate its exposure to social engineering and breakdowns in security systems. Establishing security protocols, policies and procedures for handling sensitive information could also help thwart social engineering. The security framework ought to be regularly tested because no information integrity is perfect and waste management services that have dumpsters with locks should be utilized. The locks should be limited only to the waste management company and cleaning staff. Placing dumpsters in view of employees is another way of instilling fear of being caught or seen by others. Dumpsters could also be located behind a locked gate, where people would have to trespass before attempting to access the dumpsite. Lastly, upon employing a security policy in an organization that addresses social engineering, all employees should have to complete security awareness training while some personnel should also receive resistance training [3].

Impact of Social Engineering on the Organization

Information Security is essential for any organization 'to continue to be in business'. If information security is not given priority, especially in the current environment with threats of terrorism looming in the background every day, even a small gap in security can bring an organization down. The financial cost could be punitive to the organization and individuals, so much so that insurers are now beginning to cover losses arising from certain kinds of security breaches. There is also the cost of lost reputation and goodwill, which can affect a company's base in the long term. For example, a malicious individual may get access to credit card information that online vendors obtain from customers. Once the customer finds out their credit information has been compromised, they will no longer wish to do business with that vendor, as they would consider that site insecure. They might also initiate lawsuits against the company, which would lower the reputation of the company and turn away prospective or existing clients. In addition, successful social engineering attacks give attackers the means to bypass millions in money invested in technical and non-technical protection mechanisms and consulting, completely nullifying security investment, firewalls, secure routers, PKI, email and security guards.

Conclusion

Social engineering, by any name, has existed in many forms throughout history and will continue to exist because it relies on human nature. The social engineer attempts to exploit human weaknesses for their personal gain without having to be technical, networking or security experts. Because of this, organizations and individuals alike must arm themselves with the knowledge of what information can be used, how information spread could avoid further attacks or actually compromise their systems, how attackers develop attacks, and in what forms attacks may appear. In response to such knowledge, policies, procedures, training and response plans must be formulated to address both the general threat and specific delivery methods of attack. Good Information Security strategy is a critical component of an overall strategy to ensure the success of an organization. The impact of Social Engineering attacks can be reduced by implementing a comprehensive information security strategy. Such a strategy against security breaches would include measures ranging from publishing a well-written security policy, implementing ongoing security awareness and education programs, following through with auditing programs to monitor policy compliance, installing security devices to prevent unauthorized physical access and buying insurance. Besides, the public also needs to be aware of attackers or scammers before something bad happens to them personally.

References

1. Thornburgh, T., Social engineering: the "Dark Art", in Proceedings of the 1st annual conference on Information security curriculum development. 2004, ACM: Kennesaw, Georgia. p. 133-135.

2. Dealy, I.S.W.B., Information Security Technology? Dont Rely on It. 1995.

3. Orgill, G.L., et al., The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems, in Proceedings of the 5th conference on Information technology education. 2004, ACM: Salt Lake City, UT, USA. p. 177-181.

4. Insider, T.M., Malaysia is sixth most vulnerable country in the world cyber crime. 2013.

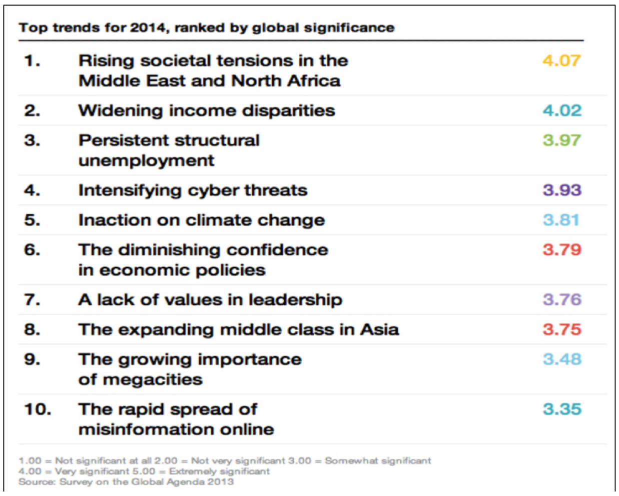
5. Goh, G., Scammers in Malaysia up their game with social engineering, in Digital News Asia. 2014.

The Rapid Spread of Misinformation Online

By | Adlil Ammal Bin Mohd Kharul Apendi, Nur Hidayah Rahim

Introduction

Nowadays, most everyone is connected to the Internet thanks to the rapid growth of technology and social networks worldwide. Any news can spread globally with just one click. This shows how fast news spreads, but the problem is how genuine the news spread is. News can simply be conveyed through the Internet, smartphones, tablets and computers -- a phenomenon that can be a serious problem and needs to be dealt with as soon as possible. Many shortcomings can be the result of false information, such as misunderstandings, chaos, the media taking action to increase news and so on. These ethical issues were listed in the top ten trending in 2014 and are ranked by significance as shown below.



Top trends for 2014, ranked by global significance

1.	Rising societal tensions in the Middle East and North Africa	4.07
2.	Widening income disparities	4.02
3.	Persistent structural unemployment	3.97
4.	Intensifying cyber threats	3.93
5.	Inaction on climate change	3.81
6.	The diminishing confidence in economic policies	3.79
7.	A lack of values in leadership	3.76
8.	The expanding middle class in Asia	3.75
9.	The growing importance of megacities	3.48
10.	The rapid spread of misinformation online	3.35

1.00 = Not significant at all 2.00 = Not very significant 3.00 = Somewhat significant
4.00 = Very significant 5.00 = Extremely significant
Source: Survey on the Global Agenda 2013

Figure 1: Top trends for 2014 ranked by global significance [1].

What is misinformation? According to the Cambridge Online Dictionary, misinformation is wrong information or facts that lead people to be misinformed [2]. Online information deals with large volumes of data stored in the cloud. Based on Figure 1, three out of ten issues are are related to social media. The team refers to this as a "semantic attack" and regards it as the "soft underbelly of the Internet [3]." It is called a semantic attack because attackers will spread the word through Twitter, Facebook, blogs, etc with the intention to attract people or with personal hidden agendas.

Misinformation prevails in many forms, such as through superimposed pictures, rumors, jokes, tweets, status updates and so on. Individuals who do this mostly have their own intentions, like bring peopled down, make fun, make jokes, get revenge or express their feelings. For any reason, this action is unethical because it will negatively impact others.

Contributing Factors and Impact of Misinformation Online

Numerous factors contribute to online misinformation and have certain impact. These are psychological factors, no control of misinformation online and lack of knowledge on how to filter information.

Psychological factors

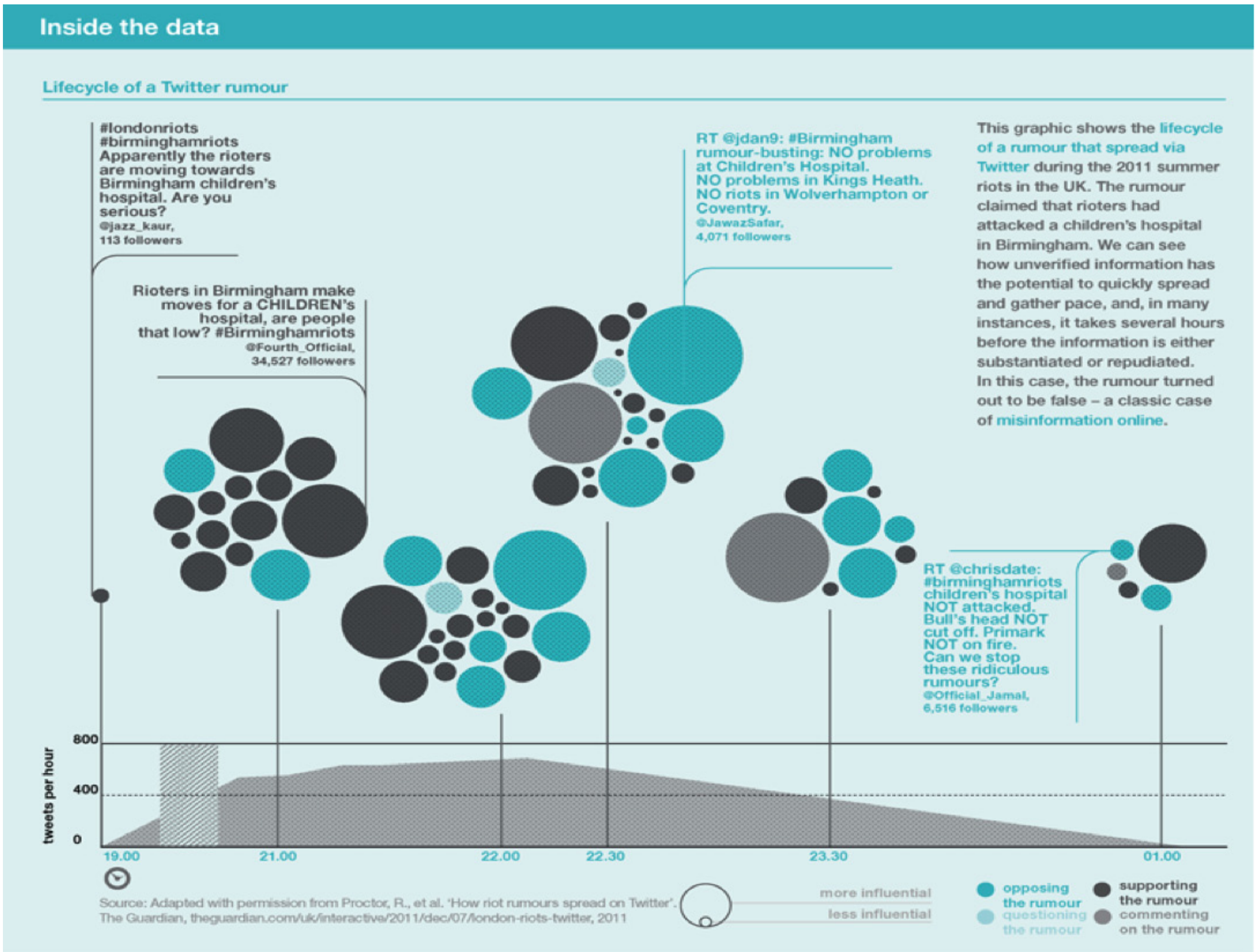
Based on research, those involved with spreading misinformation online have some psychological problem. This is supported by the fact that always want to be no one know everything and no one comments on the status without verifying wheteher it is true. This kind of attitude will bring shame because when people find out the truth, the culprit will surely feel bad once people will make a joke of them. Besides, from an Islamic view, this unethical issue is among the greatest sins. It is similar to slander, because spreading the wrong information can shame and humiliate victims.

No control of online misinformation

When large amounts of data stored in the cloud are involved, no one is able to control or detect all misinformation of data. Everything depends on the application owner or organization to filter their applications. For example, Twitter cannot control the misinformation of news because there are very many followers on this social network. Thus, it is easy to spread news by retweeting status updates, which will trend worldwide.

Lack of knowledge to filter the information received

Teenagers or children who use social networks without adult supervision mostly have a lack of knowledge of how to filter received information. Most will simply update their status based on their imagination. This group can usually attract a lot of people with misinformation. These kinds of people who easily trust any online information are excessively reliable on the Internet.



Inside the data

Lifecycle of a Twitter rumour

This graphic shows the lifecycle of a rumour that spread via Twitter during the 2011 summer riots in the UK. The rumour claimed that rioters had attacked a children's hospital in Birmingham. We can see how unverified information has the potential to quickly spread and gather pace, and, in many instances, it takes several hours before the information is either substantiated or repudiated. In this case, the rumour turned out to be false – a classic case of misinformation online.

#londonriots #birminghamriots Apparently the rioters are moving towards Birmingham children's hospital. Are you serious?
@jazz_kaur, 113 followers
Rioters in Birmingham make moves for a CHILDREN's hospital, are people that low? #Birminghamriots
@Fourth_Official, 34,527 followers
RT @jdan9: #Birmingham rumour-busting: NO problems at Children's Hospital. NO problems in Kings Heath. NO riots in Wolverhampton or Coventry.
@JawazSafar, 4,071 followers
RT @chrisdate: #birminghamriots children's hospital NOT attacked. Bull's head NOT cut off. Primark NOT on fire. Can we stop these ridiculous rumours?
@Official_Jamal, 6,516 followers
tweets per hour
800
400
0
19.00
21.00
22.00
22.30
23.30
01.00
more influential
less influential
opposing the rumour
questioning the rumour
supporting the rumour
commenting on the rumour

Source: Adapted with permission from Proctor, R., et al. 'How riot rumours spread on Twitter'. The Guardian, theguardian.com/uk/interactive/2011/dec/07/london-riots-twitter, 2011

Figure 2: Life cycle of Twitter rumors [3].

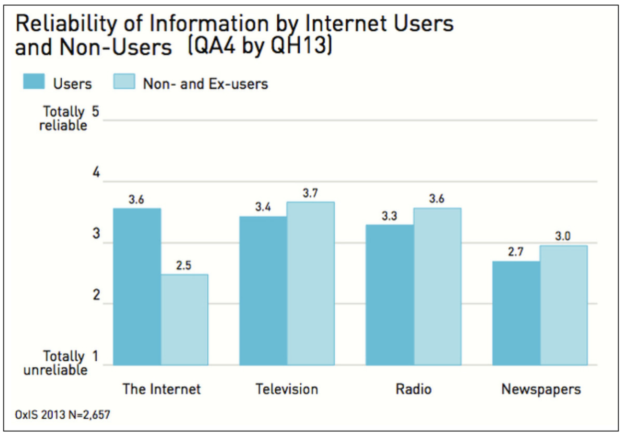


Figure 2: Reliability on information by Internet users [1].

Based on research and surveys, most people rely more on the Internet rather than television, radio and newspapers because they are addicted to the Internet. In this generation, gadgets are glued to hands. Any information becomes known through alerts on phones or gadgets. This situation is very worrying to many, because traditional media normally has more genuine information. However, traditional media reports information more slowly than the Internet. Traditional media is also neglected because it is more costly than the Internet which is more efficient but unfortunately cannot be trusted.

Ways to Prevent and Slow Down Issues

There are several ways to prevent and slow down these issues from becoming top trending. It is impossible to completely stop such ethical issues because it hard to find the victims and wrongdoers. Thus, everyone should play a role in minimizing incidence. For example, the social media community needs to partake in clearing if they discover any misinformation. There are two cases in which misinformation of a different kind occurred in the United States: the December 2012 Newtown shootings and the April 2013 Boston bombings. In the Newtown case, online and mainstream media misidentified a Facebook page as that of the shooter. After the Boston bombings, social media users engaged in online detective work, examining images taken at the scene and wrongfully claiming that a missing student was one of the bombers; but in this case, mainstream media outlets also played a part in perpetuating and validating the misinformation by publishing images of the wrong suspects [4].

The next prevention step is to restrict media policies or laws. For instance, Facebook, Twitter or any social network needs to have a policy of aprehending culprits and bringing cases to court. The application owner should take action to clarify or report any misinformation within their organization or application.

Users and the public should be educated to tackle online misinformation. They should not simply trust any information they come across but rather make sure the data is genuine before sharing with others. There is a simple way to prevent getting misinformation. Browser settings should be set to block untrusted pages or websites, thus making it much easier to filter genuine information. The public and users should also motivate and train themselves away from the "itchy finger to share everything publicly or create misinformation on their social networks".

Nowadays, not all pictures or videos can be deemed proof of any status or statement claimed because there is a lot of technology that can make or fake proof. Numerous superimposed pictures are created to defame people, including scandal videos that are spreading fast. The only way to trust videos is to recognize and identify the video footage, which can usually be evidence of information.

It has also been suggested that online social networks add an additional layer of challenges in the detection of such semantic attacks to the conventional world-wide web and other Internet services. The rate of misinformation diffusion can be very rapid as evidenced by recent events driven by panic spreading online regarding the so-called swine flu in 2009 and a mass exodus from an Asian nation also driven by unnecessary online panic [5].

Challenges in Overcoming the Issue

It is not easy to overcome misinformation. More effort will be required when it comes to the high numbers of people that need to be handled. Besides, a great challenge is to control and filter the huge amounts of data in the cloud. It has already become a habit and trend of the public to share trending or attractive information. For example, regarding the MH370 airplane tragedy with Malaysia Airlines, the keyboard warriors in Malaysia were competing with each other to spread news and rumors without waiting for information from legitimate authorities. This became a sensitive issue as it involved the whole country and victims' families.

The next challenge regards awareness of the negative impact of spreading misinformation, especially for the young generation. This Gen Y is more advanced in using new technology. Parents and teachers should emphasize educating this generation, since they are still young and hardly have the ability to differentiate between good or bad.

Conclusion

As a conclusion, online misinformation needs to be controlled and prevented before it becomes worse, as it involves the whole world. This is worrisome to all because misinformation can have a negative impact on relationships, economies, countries and so on. Unethical individuals need to be educated to prevent them from continuously doing the wrong thing. It is very important for everyone to take a fair share of responsibility and play a role to overcome this unethical matter. By spreading misinformation, some people may use it as an opportunity for personal benefits. For the young generation, do take all advice and guidance from elders, as it can prevent negative outcomes. Besides, think about the consequences first, before taking any action.

References

[1] F. Vis, "Hard Evidence: How does false information spread online ?," 2014. [Online]. Available: https://theconversation.com/hard-evidence-how-does-false-information-spread-online-25567. [Accessed: 18-Oct-2014].

[2] "Cambridge Dictionaries Online," 2014. [Online]. Available: http://dictionary.cambridge.org/dictionary/british/misinformation. [Accessed: 24-Oct-2014].

[3] S. Media, "Let's cull the trend of digital media rumors," 2014. [Online]. Available: http://www.digitalqatar.qa/en/2013/11/20/lets-cull-the-trend-of-digital-media-rumors/. [Accessed: 20-Oct-2014].

[4] G. E. Goldberg, "The Rapid Spread of Misinformation Online," 2014. [Online]. Available: http://www.huffingtonpost.com/farida-vis/the-rapid-spread-of-misinformation-online_b_4665678.html. [Accessed: 24-Oct-2014].

[5] K. P. K. Kumar and G. Geethakumari, "A taxonomy for modelling and analysis of diffusion of (mis)information in social networks," Int. J. Commun. Networks Distrib. Syst., vol. 13, no. 2, p. 119, 2014.

Product Tampering: Business Continuity and Regaining Trust

By | Mohd Syamsyul Shuib, Zeti Suhana Zainudin

Abstract

Product tampering is one of the threats encountered by product manufacturing companies. The impact of this threat entails consumers losing their trust in the company, leading to a decline in the company's financial performance and further tainting their reputation in the eyes of the public. This paper will examine some of the product tampering and product recall incidents that have recently happened in Malaysia. In addition, an attempt is made to examine business continuity plans (BCP), and particularly crisis management plans, and to determine the effectiveness and efficiency of the plan executed by the affected companies based on the said incidents. Further recommendations of how to improve the BCP are also deliberated in this paper in order to regain and ultimately maintain consumers' trust.

Keywords- Product tampering; Product recall; BCP; trust; crisis management plan; halal

Introduction

Product tampering refers to intentional modification of products after they have been manufactured, which renders them harmful to consumers. [1] It is one of the biggest nonphysical damage crises to a manufacturing organization. According to Wheeler (2006), product tampering can be classified into three categories:

> Class 1: Incidents that may include serious health consequences, threaten lives, affect a significant number of people or expose them to risk;
>
> Class 2: Incidents that may reasonably cause adverse health consequences or are often of a temporary or medically reversible danger, which may or may not cause adverse health consequences;
>
> Class 3: Incidents that are considered reversible with little or no adverse health consequences. [2]

Product tampering is often used to distress consumers or to threaten a company. Despite the fact that few fatalities have occurred due to product tampering compared to the total number of complaints, the probability of spreading fear and causing actual physical harm to the public is still high.

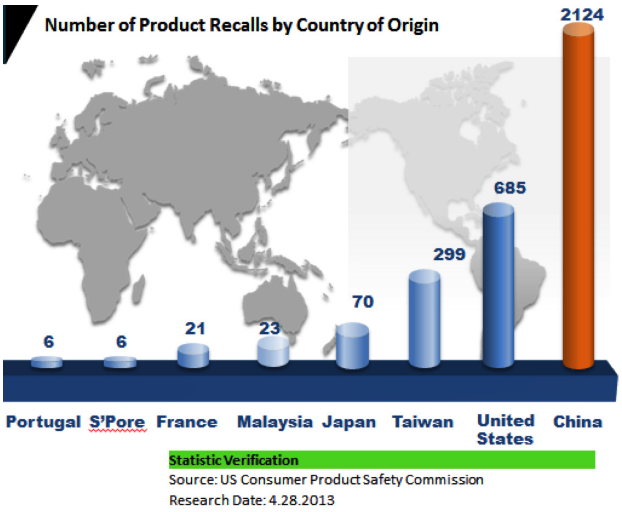
Product Recall

Product tampering is often associated with product recall. Product recall as defined by Wheeler (2006) as the immediate action taken by a company when encountering a product tampering incident, whereby the product accountability for the past 72 hours is the most crucial. [2] MyStandard Malaysian Consumer Product Safety (2014) defined product recall as "the removal from distribution, sale or consumer use of a product that does not comply with legislation in Malaysia and due to the discovery of safety issues." [3]

The foundation of the recall concept is determined by the company's food safety policies, ethical understanding, regulatory requirements and financial limitations that protect both the consumers and company itself. An efficient recall process can save the company's name and avoid further damage due to negative feedback from the public. The three main corrective actions are destroying, replacing or altering the product.
A recall plan should strive to achieve the following goals:

- Protect consumer health
- Comply with existing rules and regulations
- Minimize the cost of the recall
- Regain and improve the company's reputation [4]

Chart 1 below depicts the number of product recalls by selected country of origin.



Statistic Verification
Source: US Consumer Product Safety Commission
Research Date: 4.28.2013

CHART I : Product Recalls by Country

Among the incidents related to product tampering are accidental or intentional contamination, impairment and mislabeling; actual, alleged or threats of malicious and wrongful alteration or contamination; and falsely reporting to the media an alleged, but not actual, accidental contamination.

The objective of this paper is to examine how product manufacturing companies can optimize their business continuity plan to regain consumers' trust following product tampering threats.

Incidents in Malaysia

Cadbury Malaysia

The word "Halal" is defined as permissible by Islamic Law. Muslims are only allowed to consume products based on the Islamic Law. In the context of product tampering threats, food and beverages particularly may be at risk of being tampered in terms of non-halal ingredients or contamination. Among the main non-halal ingredients are pork and alcohol.

On Friday, 23 May 2014, posts on social media revealed that two variants of Cadbury chocolates – Cadbury Dairy Milk Hazelnut 175g (with batch number 200813M01H I2, expiry on 13 November 2014) and Cadbury Dairy Milk Roast Almond 175g (with batch number 221013N01R I1, expiry on 15 January 2015) were being analyzed by the Ministry of Health for traces of porcine DNA (or pork). Despite not having the actual laboratory test results for verification, Cadbury Malaysia proactively initiated a voluntary nationwide recall of the affected batches the following day, 24 May 2014.

On 26 May 2014, Cadbury Malaysia opened its factory in Shah Alam to the Department of Islamic Development Malaysia (JAKIM) officers, particularly from the halal enforcement team, to collect samples of the two chocolate product variants for further testing. After a week, the team shared their findings that the test results evidently indicated that the two variants in the affected batches were halal.

On 29 May 2014, the BBC online news reported that certain Muslim groups were calling for a boycott of Cadbury products in Malaysia. A Muslim retail group stated that the 800 stores it represented had been asked not to sell Cadbury products. The Head of Research with the Muslim Consumers Association Malaysia, reiterated that the action was to "teach all companies in Malaysia to maintain and protect the sensitivities of Malaysians" in a news conference in Kuala Lumpur. [5]

On 2 June 2014, Yahoo! News reported that the Muslim Consumers Association of Malaysia (PPIM) stated they would continue the consumers' boycott despite the announcement from JAKIM that the chocolate maker's products were found to be free from pork DNA. The boycott would not cease until the Ministry of Health denied its previous statement regarding the presence of porcine DNA in the food product.

On 4 June 2014, the Deputy Health Minister said in the Star online news that the Ministry was locating the officer who had leaked the preliminary report with unsanctioned results on the testing of chocolates purportedly containing porcine DNA. The minister also acknowledged that had contamination occurred and halal matters been confirmed, this would have been handled by JAKIM from then on and the Ministry would no longer have made such announcements. [6]

Danone Dumex

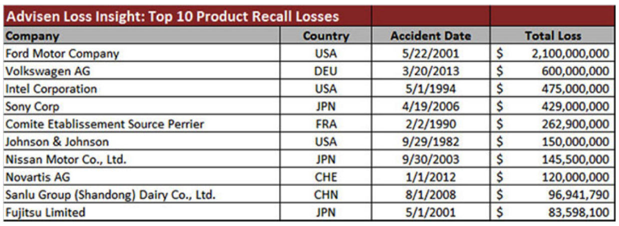
The Star Online reported on 4 August 2013 that Danone Dumex (Malaysia) Sdn Bhd had to recall certain milk products such as Dumex Dupro, Mamex Cherish, Mamex Explore and Bebelac due to possible botulism contamination and as precaution. The measure was taken in lieu of the warning by New Zealand authorities related to a whey protein concentrate (WPC) product manufactured by Fonterra. WPC was suspected to have been contaminated with Clostridium Botulinum, which can cause food poisoning or botulism. WPC is an ingredient mostly found in infant formula, growing-up milk powder and sports drinks, products that are exported to various countries including Malaysia. [7]

On 8 May 2014, Danone Dumex posted an alert on its official website: "Erroneous posting causes unnecessary anxiety and confusion" in response to Facebook users re-posting outdated news on a company's past precautionary product recall. The company reiterated on the website that "all Danone Dumex Products have always been safe, are safe and will continue to be safe". [8]

Impact

Generally, the impact of product tampering incidents can be perceived from three different angles: impact on the company both externally and internally as well as impact on the consumers. External impact on the company refers to the effects based on the consequences from actions taken by external parties, particularly consumers. Examples of actions taken by consumers include sabotage in the form of deliberate damage or destruction and boycotting, which is protesting by refusing to purchase certain brands from the related company. The consumers' actions may lead to a company's questionable reputational integrity/ trust, furthermore causing damage to the reputation and brand carried by the company. Internal impact on the company refers to the effects based on the consequences of actions taken by parties within or having direct support from the company, such as employees, creditors and shareholders. Internal impact includes brain drain, whereby the best managers and key personnel leave the company and seek safety elsewhere [9]; management become vulnerable with loss of respect for senior managers and their decisions being questioned; arguments within management, whereby previously dismissed disparities begin to surface; concerns from creditors as the product tampering incident may affect their own businesses or incomes; shareholders become anxious and subsequently ditch their stocks; massive costs from product recalls and drops in sales/business performance.

Table 1 below depicts the top 10 financial losses across the world due to product recall.



Advisen Loss Insight: Top 10 Product Recall Losses			
Company	**Country**	**Accident Date**	**Total Loss**
Ford Motor Company	USA	5/22/2001	$ 2,100,000,000
Volkswagen AG	DEU	3/20/2013	$ 600,000,000
Intel Corporation	USA	5/1/1994	$ 475,000,000
Sony Corp	JPN	4/19/2006	$ 429,000,000
Comite Etablissement Source Perrier	FRA	2/2/1990	$ 262,900,000
Johnson & Johnson	USA	9/29/1982	$ 150,000,000
Nissan Motor Co., Ltd.	JPN	9/30/2003	$ 145,500,000
Novartis AG	CHE	1/1/2012	$ 120,000,000
Sanlu Group (Shandong) Dairy Co., Ltd.	CHN	8/1/2008	$ 96,941,790
Fujitsu Limited	JPN	5/1/2001	$ 83,598,100

TABLE I : Top 10 Product Recall Losses

Source: Advisen database [10]

Consumers put their trust in manufacturing companies to provide safe foods, beverages and medicines. The impact of tampering particularly with the said products relates to safety (injury) and health (illness or death). With safety and health impact, tampering may lead to a company's image becoming heavily tarnished and its financial capability becoming unstable. In other words, a single incident and any subsequent media coverage can pose a significant threat to consumer confidence, hard-won retail space, important contracts, market shares, brand credibility, reputation and profit. [11]

Business Continuity Plan

Product manufacturing companies need to have a business continuity plan as preparation to deal with product tampering threats and furthermore regain consumers' trust. Threats could turn into a crisis that could cause other crises to emerge if companies do not manage them well in the first place. The focus of this study is on crisis management and crisis communication, which can be utilized by companies to reduce the impact on their business.

According to Whitman and Mattord (2007) the definition of crisis management is actions taken by a company in response to an emergency situation in an effort to minimize injury or loss of life. They also defined crisis communication as the public relations aspect of crisis management, communicating both internally and externally about what happened and what the company is doing to manage the crisis. In order to handle the various stages of crisis, manage perceptions and combat rumors, a crisis management plan needs to be in place and also cover crisis communication. The Crisis Management Plan (CMP) is a documented plan used as guidance or reference. It contains actions to be taken as instructed by the Executive Management in the event of a crisis striking the company. Companies should also form a crisis management team to devise a CMP based on the criticality of a product tampering crisis for them, to execute the right action at the right time. During crisis, the CMT members will cooperate and work as a team to gain control of the crisis in order to minimize the crisis impact. The said plan must be viable with the participation of the Executive Management and workable with the participation of the CMT members. The plan should be communicated via training to convey employee awareness, and it should be tested and exercised to ensure the plan works. The aim is to afford the company's management the opportunity to manage a crisis successfully with little or no damage to the company.

Whitman and Mattord (2007) also stated there are three stages of crisis, namely pre-crisis, acute-crisis and post-crisis. The pre-crisis stage is when the "critical situation" starts and the organization becomes aware of it. Acute-crisis is when the "critical situation" was not controlled during the pre-crisis stage and it becomes visible outside the organization. Post-crisis occurs when the crisis is contained and the organization is trying to recoup its reputation and/or losses. [12]

Pre-Crisis

In the pre-crisis stage, the emerging critical situation is confronted in an effort to resolve the matter before further damage arises that would lead to the acute-crisis stage. The situation is recognized and any pre-crisis warning should be heeded as part of the damage assessment. Based on the assessment result, appropriate and necessary actions should be taken to remove the threat, by seeking the support from external crisis management consultants, among other actions. In the event the critical situation cannot be handled and contained in the pre-crisis stage, the situation may advance to the acute-crisis stage.

Acute-Crisis

During the acute-crisis stage, the CMT is activated with support from the Executive Management Team (EMT) to proceed with the CMT. At this stage, damage control actions are executed to minimize the damage and avoid any further damage from happening. A crisis communication plan should also be triggered, since a critical situation in the acute-crisis stage would already appear in media headlines. The plan also requires that a well-trained spokesperson is assigned to deal with the media in communicating to the public. This is to give assurance that the critical situation is under the company's control and is being handled in an organized and timely manner. The spokesperson should be able to tell the company's version of the story with holding statements designed for use immediately after a crisis break and key messages specifically related to crisis handling.

Another criterion to consider for crisis communication is the communication methods with internal stakeholders, external stakeholders and the media (print, radio, television, Internet, etc.). [13] The most recent emerging method of communicating with the public is social media. Halsall (2014) recommended a 5-step guide to use on social media in crisis management.

1. Timing is everything

   The sooner the company can provide consumers with their presence and dedication to addressing the critical situation, i.e. product tampering incident, the sooner the company would earn the consumers' trust. One of the social media consultancy firms, Frishling, advises companies to issue a new update every ten minutes in the immediate aftermath, even if there is nothing new to report. Subsequently, more time between updates in the days and weeks could be left. However, it is important to keep the pressure turned up until the brand and its consumers are out of the danger zone.

2. Own the conversation

   Companies should not let the conversation on the product tampering incident get out of control by deciding on an appropriate hashtag in the social media, e.g. on Twitter, for the public to follow from the very beginning of the crisis. This should be used as a symbol across all platforms for all trustworthy, reliable and honest information surrounding the crisis/incident.

3. Stick to a designated source

   It is advisable that brands limit the number of sources people feel they need to look to, to find dedicated information regarding a crisis. Otherwise, information can become scattered and misinterpreted, and focus can be lost.

4. Give a call to action

   Give the consumers action to take, instructions, or advise instead of leaving them hanging with no direction, despite having no explanation yet about the crisis. Consumers would interpret that the company really cares about their welfare.

5. Do not lash out

   Social media will take any opportunity to spread rumors and false information about a crisis. However, the company is definitely not advised to provide any negative or aggressive reactions, as by doing so, it may put the company's integrity at stake. [14]

Post-Crisis

After the crisis or critical situation has been controlled, the company can shift into the post-crisis stage. At this point, the EMT need to recoup some of the losses by making a public apology and showing empathy. Internally, the EMT should revise the existing procedures/control to prevent the same incident from recurring. A post-mortem should also be conducted to evaluate the efficiency and effectiveness of the company's existing crisis management plan. Based on the evaluation, appropriate actions are to be strategized to further improvise the crisis management plan. In order to regain the consumers' trust, a broader range of potential communication initiatives should be considered. In the case of Cadbury Malaysia, the company managed to rope in JAKIM, who was invited to the factory to collect samples and perform laboratory tests on the samples. Upon having the laboratory test results, the company received its halal certification back from JAKIM. Cadbury Malaysia also invited a panel of religious leaders and scholars to their manufacturing plant. [15] As a symbol of commitment, videos of the halal certification process in manufacturing were also uploaded on the company's website.

For Danone Dumex Malaysia, the company voluntarily recalled products upon confirmation that their products indeed contained contamination that could cause food poisoning. Additionally, Danone Dumex Malaysia published a statement on the company's website of their commitment to produce safe products for the consumers.

Conclusion

Product tampering incidents cause consumers to lose trust in brands and product manufacturing companies. Companies should have an effective and efficient business continuity plan, with particular focus on crisis management and crisis communication. Dedicated spokespersons should be assigned to avoid public miscommunication and confusion of information. Time is also one of the main factors forcing companies to act fast. At additional cost, companies could obtain the involvement of professional crisis management consultants. During crisis communication, companies should always convey accurate information, as the information provided to the public might or will be used against the companies at a later time. When deciding on the actions to be taken, companies must consider the short and long-term effects of the actions on the companies as well as the public. Crisis response that is well-managed together with an effective crisis recovery program, will paint a favorable impression for the stakeholders and renew their confidence in the companies. This will ultimately lead to consumers' trust in the company being regained and further maintained in future comings.

References

[1] USLegal.com (date not available). Tampering Law & Legal Definition. Retrieved from http://definitions.uslegal.com/t/tampering/

[2] Rod Wheeler (2006). Product Tampering.

[3] MyStandard: Malaysian Consumer Product Safety (2014). Product Recall. Retrieved from: http://mystandard.kpdnkk.gov.my/mystandard_portal2014/index.php?r=column/cfive&id=67

[4] Gönül Kaletunç, Ferhan Özadali. Ohio State University Extension Fact Sheet, Understanding the Recall Concept in the Food Industry. Retrieved from http://ohioline.osu.edu/aex-fact/0251.html

[5] BBC news online (29 May 2014). Muslim groups call for boycott of Cadbury in Malaysia. Retrieved from http://www.bbc.com/news/business-27616258

[6] The Star online (4 June 2014). Health Ministry searching for officer who leaked report on porcine DNA. Retrieved from http://www.thestar.com.my/News/Nation/2014/06/04/Health-Ministry-searching-for-officer-who-leaked-report-on-porcine-DNA/

[7] The Star online (4 August 2013). Danone Dumex Malaysia recalls some of its milk products, possible botulism contamination. Retrieved from http://www.thestar.com.my/News/Nation/2013/08/04/Milk-botulism-Danone-Dumex-recall/

[8] Danone Dumex Malaysia (8 May 2014). Alert: Erroneous posting causes unnecessary anxiety and confusion. Retrieved from http://corporate.dumex.com.my/?ch=mediareleases

[9] Edward S. Devlin (2007). Crisis Management Planning and Execution.

[10] Chad Hemenway (19 June 2014). A look at

product recall cases from the Advisen database. Retrieved from http://www.advisenrisknetwork.com/2014/06/19/advisen-database-look-product-recall-cases/

[11] AIG Insurance New Zealand Limited (March 2014). Contaminated Product Insurance.

[12] Michael E.Whitman and Herbert J.Mattord (2007). Principle of Incident Response and Disaster Recovery

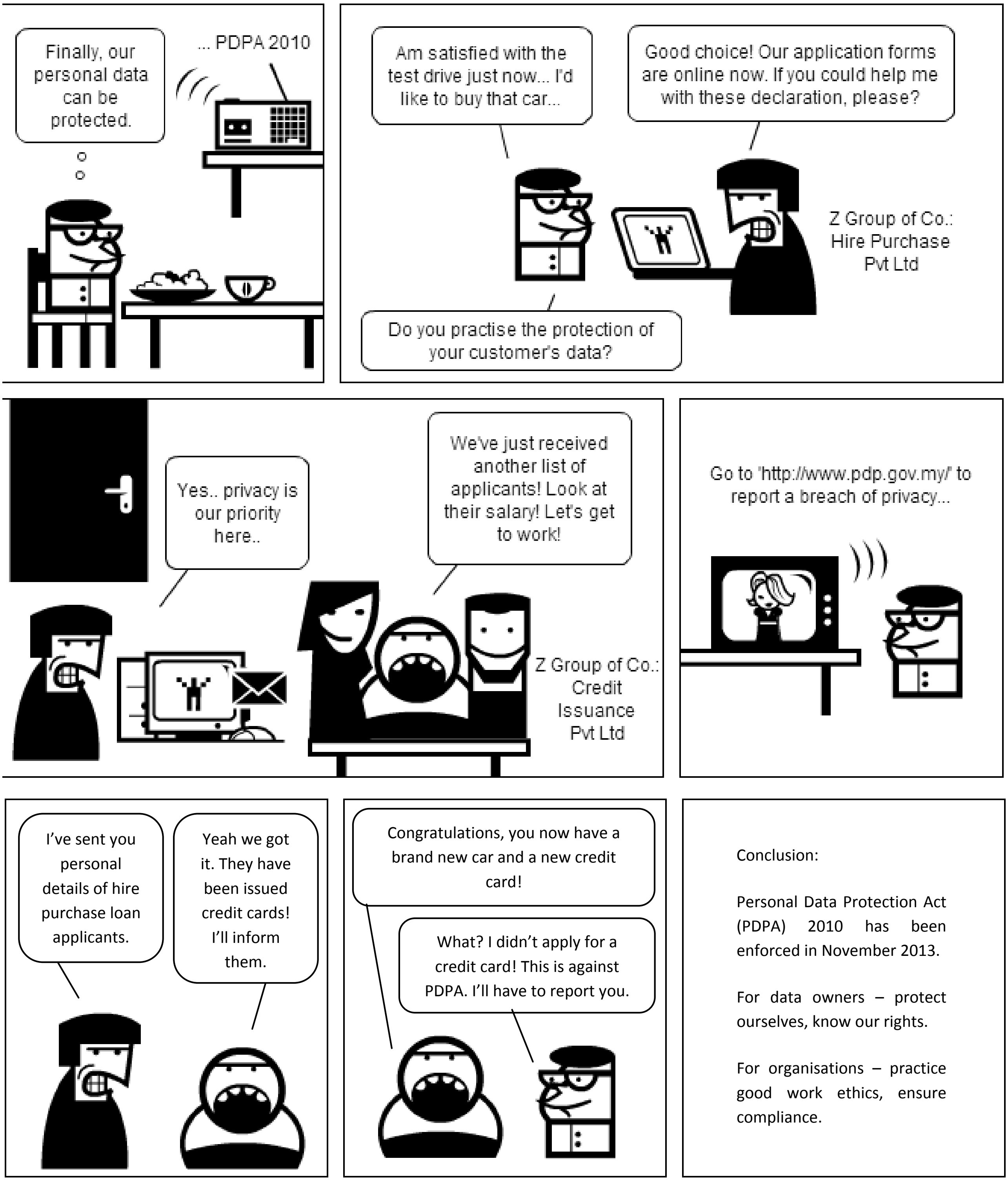
[13] Andrew Hiles (2007). The Definitive Handbook of Business Continuity Management (2nd edition).

[14] Adele Halsall (2014). The 5 Step Guide To Using Social Media in Crisis Management. Retrieved from http://www.jeffbullas.com/2014/06/26/a-5-step-guide-to-using-social-media-in-crisis-management/

[15] Rezwana Manjur (24 July 2014). Cadbury Malaysia reaches out to religious leaders. Retrieved from http://www.marketing-interactive.com/cadbury-malaysia-invites-religious-leader/

PDPA 2010: Know your rights

By | Wan Nasra bt Wan Firuz


Finally, our personal data can be protected.
... PDPA 2010
Am satisfied with the test drive just now... I'd like to buy that car...
Good choice! Our application forms are online now. If you could help me with these declaration, please?
Z Group of Co.: Hire Purchase Pvt Ltd
Do you practise the protection of your customer's data?
Yes.. privacy is our priority here..
We've just received another list of applicants! Look at their salary! Let's get to work!
Z Group of Co.: Credit Issuance Pvt Ltd
Go to 'http://www.pdp.gov.my/' to report a breach of privacy...
I've sent you personal details of hire purchase loan applicants.
Yeah we got it. They have been issued credit cards! I'll inform them.
Congratulations, you now have a brand new car and a new credit card!
What? I didn't apply for a credit card! This is against PDPA. I'll have to report you.

Conclusion:

Personal Data Protection Act (PDPA) 2010 has been enforced in November 2013.

For data owners – protect ourselves, know our rights.

For organisations – practice good work ethics, ensure compliance.

ADAB of a Digital Citizen: PART 1

By | Aaron Ikram Mokhtar

Introduction

This is the first of a two part series of articles that explain the "ADAB" methodology. This methodology has been developed by CyberSecurity Malaysia's Outreach Department for our cyber safety education and awareness programs. This first part introduces what "ADAB of a Digital Citizen" means, how it came about, and why it was developed.

The "CyberSAFE" Outreach Department

Realising the crucial need to educate the public on cyber safety, The CyberSecurity Malaysia's Outreach Department was set up in 2009 to increase public awareness and knowledge when logging on the Internet to communicate, as well as to inform and convey information and data that directly impacts Malaysia's digital citizens through our CyberSAFE™ initiative (short for Cyber Security Awareness for Everyone). Through the CyberSAFE programs, useful and practical knowledge is imparted to provide essential information and necessary resources to a wide spectrum of Internet users. This will help their online experience be secure, safe and productive.

There are many ways CyberSAFE deliver its message and content, some of which include:

- Awareness lectures
- Training workshops
- The CyberSAFE Online Portal (www.cybersafe.my)
- Content development (articles/posters/videos)
- Social media platforms like Facebook
- Awareness programs and campaigns

Cyber Safety Education and Awareness

The Outreach Department of CyberSecurity Malaysia has been given a mandate to conduct cyber safety awareness programs in order to make people aware about their own security and privacy when they are online. The challenges the Outreach Department faces when conducting cyber safety awareness programs are not technical, but human-related:

1. How do we get people to prioritise their online security and privacy?
2. How do we get people to understand and be aware that the Internet has a very long memory and we all are accountable for everything shared and posted on the Internet?

In a nutshell, how do we get people to take care of themselves online and prevent their personal data from being used and abused by cybercriminals?

Through these CyberSAFE programs, it has been very satisfying to see more and more Malaysians realise their virtual life on the Internet is not separate but rather an extension of their real-world life. Just as there are guidelines to govern our daily lives, Malaysians are understanding there are also necessary guidelines to govern our virtual existence. We have observed and learned that by establishing a connection between a person's online behavior and their real-world behaviour, it is possible to convince and show them how one can significantly impact the other. As a result, we are beginning to see people being more aware and more proactive in taking ownership of what they say and do online. Indeed, online self-governance is one of our main objectives.

To further effectively develop cyber safety content and deliver it efficiently, a set of frameworks must be in place to guide the processes and keep them on track. This methodology of getting our message across to the public is called "ADAB of a Digital Citizen".

Adab of a Digital Citizen

Etiquette in IT (information technology), or what is starting to be commonly referred to as "netiquette", has been an increasing point of discussion among Internet groups, organisations and individuals when operating online.

Wikipedia defines etiquette as *"a code of behavior that delineates expectations for social behavior according to contemporary conventional norms within a society, social class, or group."*, and *defines etiquette in technology as "conduct, or a set of social conventions that is socially acceptable in an online or digital situation"*.

The question that arises now is, whose "set of social behavior and conventional norms" should we refer to and use as a benchmark?

Do we look at western social norms? American? European? Or do we look closer to home in the east, at Japan? Singapore? Or Australia? We haven't even begun to talk about cultural and religious social norms.

Malaysia has a population of 30.3 million people (2014 estimate) of multicultural and multi-religious background. Ideally, the best solution for Malaysia would be one that has Malaysia's digital citizen in mind and that takes our multicultural background into account. Over the last 2 years we have been developing a methodology and framework -- the result of looking for a set of online social behaviour guidelines and best practices in touch and in tune with the challenges faced by Malaysia's digital citizens on a daily basis.

The result is what we, at the Outreach Department, call "ADAB of a Digital Citizen". We believe we have in place a strong foundation to build upon a national cyber safety education platform that empowers the development of strong relevant content, a structure of delivering the content clearly and a baseline for all future programs to refer to.

"THE RIGHT KNOWLEDGE USED IN THE RIGHT PLACE AND TIME"

The word adab can't be directly translatable from Arabic to English since it encompasses many aspects of human interaction and varies from culture to culture.

Wikipedia defines adab in the context of behavior as *"...prescribed Islamic etiquette: refinement, good manners, morals, decorum, decency, humaneness."* One binding similarity when talking about adab among different cultures is that adab is *"a regard for personal reputation and standing through the practice of a certain code of behavior"*. It is said that to exhibit adab would be to show proper discrimination of correct order, behavior and taste.

Though many books and experts have delved deeply into the study of adab, in the context of "ADAB of a Digital Citizen" we refer to the works of Syed Muhammad Naquib al-Attas and his vast scholarly research and study of this subject. We studied his literature, and from our understanding, we came up with adab defined as:

"the right knowledge used in the right place and time".

By defining adab as "the right knowledge used in the right place and time", adab is no longer merely focused on how we interact with one another as humans, but we can also include how we interact with our environment and the tools we use in it. Thus, for instance, there is now an adab to how we drive a car, read books, use a mobile device, a computer and the Internet.

Once a clear definition for adab was agreed upon, it was time to develop the content that would be taught to Malaysia's digital citizens.

Content Outline

In developing content that would be used under the "ADAB of a Digital Citizen" methodology, we reviewed:

- all past awareness programs
- feedback from past program participants
- The CyberSAFE in School Program survey results

It was important to ensure that the content developed was thorough and covered important components/interactions of a person's online experience. In the end, it became clear that almost all interactions between Malaysia's digital citizens with the Internet could be divided into four key categories:

1. KNOW YOUR GADGET:
   - Understanding the hardware/tools available to connect to the Internet, and their strengths and weaknesses.
2. SECURE YOUR CONNECTION:
   - Ensuring that when sending and receiving information it is safe from prying eyes.
3. MASTER YOUR PLATFORM:
   - Whether an operating system, mobile app, or cloud platform, one must do their best to know the abilities and settings of the platform used.
4. CAREFUL WHAT YOU SHARE:
   - Finally, it is very important to be careful what we say, do and share online because a blunder can have the biggest negative impact on an individual's reputation and credibility.

To be Continued

In part 2 of "ADAB of a Digital Citizen" details of the 4 key content categories will be given, further elaborating on each one's focus, subject outline and objectives.

References

1. http://en.wikipedia.org/wiki/Adab_(Islam)

2. http://en.wikipedia.org/wiki/Syed_Muhammad_Naquib_al-Attas

3. https://www.youtube.com/watch?v=L5pyXqZq4E0

4. http://www.wolframalpha.com/input/?i=malaysia

Consumer Protection in the e-transaction

By | Nurul Husna Khasim

Introduction

Electronic commerce (e-commerce) is one of the most profound business transaction trends since the birth of the Internet. E-commerce describes the buying and selling of goods and services, or the transmitting of funds or data over an electronic network, especially the Internet. This technology has gained greater popularity nowadays with many people tending to choose online transactions, which are easier and faster than conventional business transactions. Despite the convenience offered by e-commerce, this technology has some drawbacks: online transactions that are done virtually often lead to people taking advantage of the security, privacy and authenticity of business transactions. Currently, a lot of online scams are happening while online shopping continues to record a significant amount of fraud cases on the various online marketplaces. In simple words, the safety of e-commerce is arguable and sometimes violates consumer rights. This has prompted calls for more stringent regulations to be imposed on online businesses. This article discusses and explains measures to protect the rights of consumers while doing transactions in cyberspace. The importance of the acts and regulations implemented by governments, especially in Malaysia, is highlighted.

E-Commerce in Malaysia

E-commerce in Malaysia is relatively new but it is clearly expanding day by day. Numerous e-commerce sites suddenly appear and offer every single product from groceries to baby items. However, there are major concerns from the consumer side relating to many aspects of e-commerce, such as the contractual aspect. For example, in terms of the availability of payment and delivery contracts on merchants' websites, not all merchants provide a contract to preserve the consumer's rights. Other than that, consumers need to look at the privacy aspect, like the consumer's personal data (address, phone number, etc). Last but not least is the banking aspect. An example is the security of Internet banking as a payment method (e-transaction).

In Malaysia, several acts have been passed and amended to regulate online commercial transactions. The Malaysia's Consumer Act of 1999 generally protects Malaysian consumers against unfair practices. In 2007, amendments were made to the act in order to widen its scope to cover electronic transactions. In 2010, another amendment was introduced to further protect the consumer. However, e-commerce surprisingly continues to contribute an abundance of reports on fraud cases originating from various online market places, such as eBay Malaysia, Lelong.my, Mudah.my, Rakuten Malaysia and others. This indirectly shows that the current acts and regulations are still not enough to counter and prevent reported cases from recurring over and over again.

Based on DailyExpress, a report by the Companies Commission of Malaysia in February 2013, statistics show there are approximately 600 online companies and 16000 online businesses registered. The number of reported cases to the Consumer Tribunal also rose significantly, and as of 2011, the police received reports of 876 cases of fraud involving delivery parcel losses worth RM18.9 million. In 2012, such losses increased to RM34.6, even though the number of reported cases dropped to 814. In 2006, the government under the Ministry of Domestic Trade, Co-operatives and Consumerism introduced the Electronic Commerce Act 2006, and in 2011 some amendments were made to regulate online market services. Basically, the new regulation requires online business owners or merchants to disclose a significant amount of information on their website or trade space on the marketplace regarding their business. Merchants are required to disclose their business/company information, details of goods or services, methods of payment, as well as any terms or conditions applicable.

With the current trend of social media also having become one of the mediums that people use to sell and buy various things, consumers can try the following checks as a guide for shopping online. First, make sure the seller is legit. People tend to choose trusted sellers who are already established and well-known. However, some may venture and try new and unknown sellers. So starting from 1st July 2013, all online businesses and services in Malaysia have to comply with the Consumer Protection (Electronic Trade Transactions) Regulations 2012. Under the Consumer

Protection Regulations, an online marketplace operator is required, among others, to provide their full details, terms and conditions of sale, rectify errors and maintain records. The new law applies to two (2) types of persons, namely those who operate a business for the purpose of supplying goods or services through a website or online marketplace ("Online Business Owner") and persons who provide an online marketplace ("Online Marketplace Operator").

The regulations require all online business suppliers to disclose the following information:

- The business name (be it the name of the owner, company or business)
- The registration number of the business or company, if applicable
- Contact details such as email address and telephone number, or address of the online business supplier
- Description of the goods or services
- Full price of the goods or services; transportation costs, taxes and other costs
- Methods of payment
- Terms and conditions of sale
- Estimated time of delivery of the goods or services to the buyers

The merchant must also provide the appropriate means to enable buyers to rectify any errors prior to confirming any purchases. Next, an acknowledgement receipt must be issued to the buyer without undue delay. Failure to disclose this information or providing false or misleading information is an offence.

As for online marketplace owners that sell third-party goods or services, they must keep and maintain information of the third-party suppliers for at least two years, such as name, telephone number and address.

Conclusion

Malaysia has introduced various kind of consumer protection acts, such as the Consumer Protection Act 1999, Consumer Protection (Electronic Trade Transactions) Act and some limited consumer provisions incorporated into part 8 of the Communications and Multimedia Act 1998. However, laws may be in place to ultimately protect the consumer, but the greater responsibility still lies with the consumer.

References

1. Pang Tun Yau (2013). Protecting Consumers Online: All You Need To Know About The Amended Consumer Protection Regulations 2012. Retrieved from http://www.lowyat.net/2013/07/protecting-consumers-online-all-you-need-to-know-about-the-amended-consumer-protection-regulations-2012/

2. Joseph Sipalan (2013). New regulations to protect online shoppers to be implemented from July 1. Retrieved from http://www.thestar.com.my/News/Nation/2013/02/20/New-regulations-to-protect-online-shoppers-to-be-implemented-from-July-1/

3. (2013). Laws to protect online shoppers from July. Retrieved from http://www.dailyexpress.com.my/news.cfm?NewsID=84367

4. Foong Cheng Leong (2013). Attention e-commerce businesses: Fraud, the law and you. Retrieved from http://www.digitalnewsasia.com/insights/attention-ecommerce-businesses-fraud-the-law-and-you

5. CK Wong (2013). New regulations for e-commerce business: Are you ready, or risking huge fines? Retrieved from http://www.ecommercemilo.com/2013/05/consumer-protection-electronic-trade-transactions-regulations-2012.html#.VSHazfmUcSM

6. Electronic Commerce Act 2006 Retrieve from http://www.agc.gov.my/Akta/Vol.%2014/Act%20658.pdf

7. Akta Perlindungan Pengguna 1999 (Peraturan-Peraturan Perlindungan Pengguna (urus niaga Perdagangan EleKtroniK) 2012) retrieved from http://www.bnm.gov.my/documents/2013/Peraturan%20ECommerce.pdf

8. Zainal Azhar Mohamed (2014). Rakyat Malaysia Kehilangan RM1.775 Bilion Tahun Lalu Menerusi Jenayah Komersial. Retrieved from http://www.mstar.com.my/berita/berita-semasa/2014/02/17/rakyat-malaysia-kehilangan-rm1775-bilion-tahun-lalu-menerusi-jenayah-komersial/

How to Deal With Tracking Cookies

By | Muhammad Arman Bin Selamat, Mohd Fadzlan Bin Mohamed Kamal & Mohd Faizal Bin Sulong

Introduction

Definitions of cookies vary, but in simple words, a cookie is a small piece of text file that stores information in a computer when someone is visiting a website. According to Merriam-Webster, a cookie is a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a website server; it contains personal information (a user identification code, customized preferences, or records of pages visited).

What are cookies used for?

Cookies are used for a variety of reasons, such as for logging services where they store user emails or names that can be accessed by specific sites. They can also be used to recognize users every time they move from page to page without having to authenticate or reprocess each new page visited.

Cookie types

Based on Wikipedia, there are seven types of cookies:

1. Session cookies
   - Session cookies are created temporarily in a web browser's subfolder while the user is visiting a website. Once the user leaves the site, the session cookie is deleted.
2. Persistent cookies
   - Persistent cookie files remain in the web browser's subfolder and are reactivated once you visit the website that created that particular cookie. A persistent cookie remains in the browser's subfolder for the duration period set within the cookie's file.
3. Secure cookies
   - A secure cookie can only be transmitted over an encrypted connection (i.e. HTTPS). This makes the cookie less likely to be exposed to cookie theft via eavesdropping.
4. HttpOnly cookies
   - HttpOnly cookies can only be used when transmitted via HTTP (or HTTPS). They are not accessible through non-HTTP APIs such as JavaScript. This restriction mitigates, but does not eliminate, the threat of session cookie theft via cross-site scripting (XSS). HttpOnly cookies are supported by most modern browsers.
5. Third-party cookies
   - Third-party cookies belong to domains different from domains shown in the address bar. These sorts of cookies typically appear when web pages feature content such as banner advertisements from external websites. This opens up the potential for tracking the user's browsing history, and is often used by advertisers in an effort to offer relevant advertisements to each user.
6. Supercookies
   - A "supercookie" originates from a Top-Level Domain (such as .com) or a Public Suffix (such as .co.uk). Ordinary cookies, by contrast, have an origin of a specific domain name, such as example.com.
7. Zombie cookies
   - Zombie cookies are cookies that are automatically recreated after being deleted. This is accomplished with the help of a client-side script. The script starts by storing the cookie's content in multiple locations, such as Flash local storage, HTML5 storage, and other client-side storage locations. When the script detects the cookie's absence, it recreates the cookie using the data stored in these locations.

What is a tracking cookie?

It is a version of cookies that track user entries and activities on visited websites. Tracking cookies are sometimes also called third-party cookies. These can be used to build a picture of users' web surfing habits. Since users are not aware of this type of cookie by not cleaning a browser cache, these tracking cookies could be installed without one's knowledge and they could be monitoring user activities at any given time.

What does a Tracking cookie do?

A tracking cookie might hold details about an Internet Protocol (IP) address, a last viewed website, viewing preferences, or a browser type, and send these details to a remote database for analysis. Many tracking cookies are designed to use this information for marketing analysis. However, some cookies are programmed to send specific user information, such as names and addresses, to the tracker host.

Can tracking cookies harm computers?

The short answer is no. But it depends on how the cookie creators (or programmers) intend to use the tracking cookies. Tracking cookies are not viruses or malicious codes. Cookies are only text files and therefore cannot be dangerous to a computer.

The main purpose of tracking cookies is to identify users and possibly prepare customized web pages or small advertising columns depending on user interest or browsing habits. When a user enters a Web site using cookies, the user may be asked to fill in a form to provide such information as user name and interests. This information is sent to the user's web browser as a cookie file. The next time the user enters the same website, the browser will send the cookie to the web server. The server can use this information to present the user with custom web pages.

How to stop trackers

All types of cookies can be removed manually or by using browser extension add-ons. There are numerous great add-ons designed specifically to help users remove all these cookies. Some good extensions are listed below:

1. **Adblock Plus** - Adblock Plus (ABP) lets users block annoying ads, tracking, malware and other things the user may not want in the web browser. Adblock Plus is an open source project created by Wladimir Palant in 2006. It is available for Mozilla Firefox, Internet Explorer, Google Chrome, Opera, Safari and Yandex Browser web browsers. In November 2012, Adblock Plus was also released as an app for Android devices. The extension allows users to prevent page elements, such as advertisements, from being downloaded and displayed.
2. **Ghostery** - Ghostery is a proprietary freeware privacy-related browser extension for Mozilla Firefox, Google Chrome, Internet Explorer, Opera and Apple Safari, and is owned by the advertising and privacy technology company Ghostery, Inc. (formerly Evidon). It enables users to easily detect and control web bugs, which are objects embedded in a web page and are invisible to the user, and which allow the collection of the user's browsing habits.
3. **NoScript** - NoScript is a great extension, providing users with an incredible amount of information about what's happening behind the scenes on any site the user visits. The trouble with it is that the information can be overwhelming, and if users do not allow certain things, the site will simply not work until users do allow them.
4. **ScriptNo for Chrome** - ScriptNo, also known as ScriptSafe, is much like Ghostery in that any scripts running on any site a user visits will sound alarms. The difference is that while Ghostery is a bit more exclusive about the types of information it alerts to, ScriptNo will sound the alarm at just about everything, which would break a ton of websites. If you visit the site, half of it will not load or work, and you will have to selectively enable scripts until it is usable. Still, its intuitive interface helps users choose which scripts on a page they wish to allow and which to block without sacrificing the actual content on the page they would like to read.

How do we manually remove cookies?

On Chrome web browser:

1. Open the Google Chrome browser and go to Menu (1), then click on Settings (2) as shown in Figure 1.

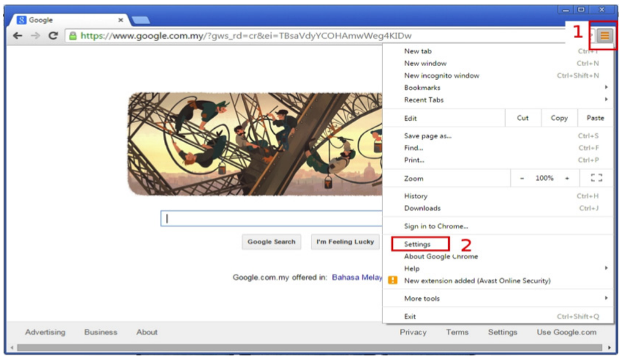
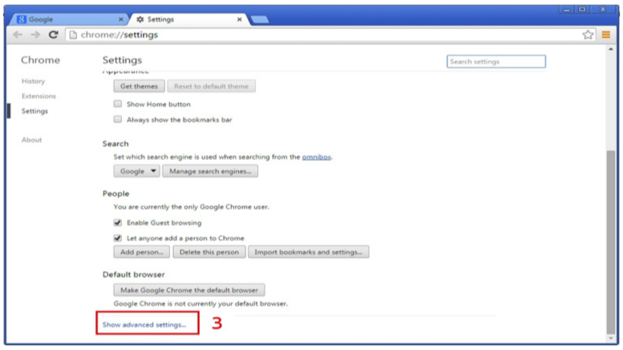


Figure 1: Google Chrome browser menu and settings.

2. Click on Show advanced settings (3) as shown in Figure 2.



□ Show Home button

□ Always show the bookmarks bar

Search

Set which search engine is used when searching from the omnibox.

Google ▾ | Manage search engines...

People

You are currently the only Google Chrome user.

☑ Enable Guest browsing

☑ Let anyone add a person to Chrome

Add person... | Delete this person | Import bookmarks and settings...

Default browser

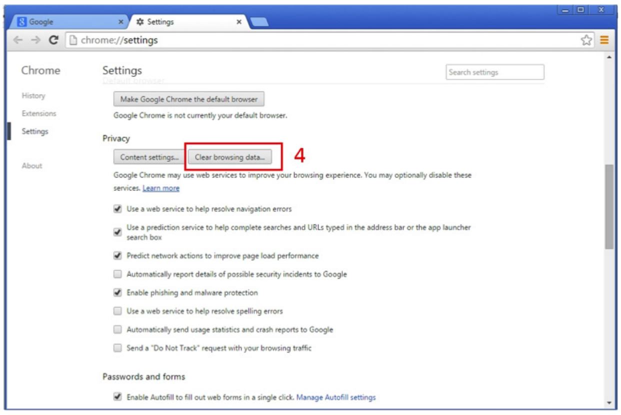
Make Google Chrome the default browser

Google Chrome is not currently your default browser.

Show advanced settings...

Figure 2: Advanced settings

3. Click on the Clear browsing data (4) button as shown in Figure 3.



Settings

Google Chrome is not currently your default browser.

Privacy

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

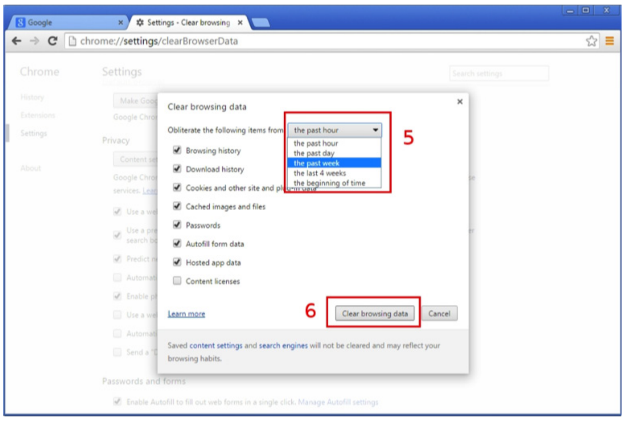
☑ Use a web service to help resolve navigation errors
☑ Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box
☑ Predict network actions to improve page load performance
☐ Automatically report details of possible security incidents to Google
☑ Enable phishing and malware protection
☐ Use a web service to help resolve spelling errors
☐ Automatically send usage statistics and crash reports to Google
☐ Send a "Do Not Track" request with your browsing traffic

Passwords and forms

☑ Enable Autofill to fill out web forms in a single click. Manage Autofill settings

Figure 3: Clear browsing data button

4. Select how far back you want to delete the data (5), and then click the Clear browsing data button (6) as shown in Figure 4.



Clear browsing data

Obliterate the following items from: the past hour

☑ Browsing history
☑ Download history
☑ Cookies and other site and plug-in data
☑ Cached images and files
☑ Passwords
☑ Autofill form data
☑ Hosted app data
☐ Content licenses

Saved content settings and search engines will not be cleared and may reflect your browsing habits.

Figure 4: Choosing from when to clear the browsing data.

For Firefox web browser:

1. Open the Firefox web browser and go to the History menu (1), then click on Clear Recent History (2) as shown in Figure 5.

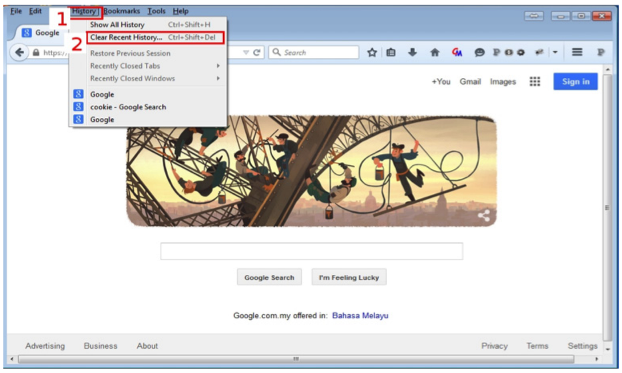
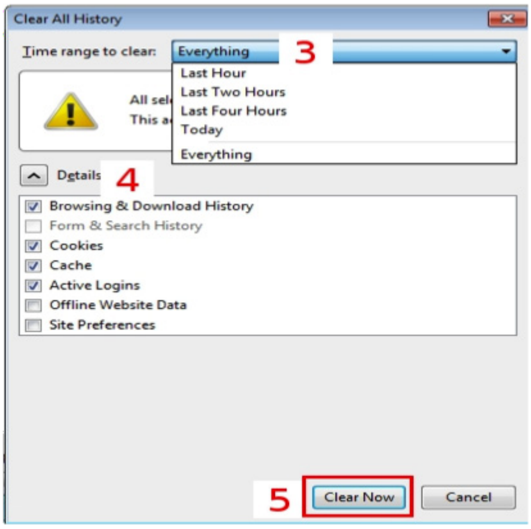


Figure 5: Firefox clear recent history settings

2. Choose the Time range to clear data (3), then click Details (4) to expand the list of items that can be chosen to remove and tick which activity is to be cleared. Once done, click on Clear Now (5) as shown in Figure 6.



Time range to clear: Everything

☑ Browsing & Download History
☐ Form & Search History
☑ Cookies
☑ Cache
☑ Active Logins
☐ Offline Website Data
☐ Site Preferences

Figure 6: Clear all history details

For Internet Explorer:

1. Open the Internet Explorer browser, then click on Safety (1), and after that select Delete Browsing History (or you can use ctrl+shift+del for shortcut hot keys).

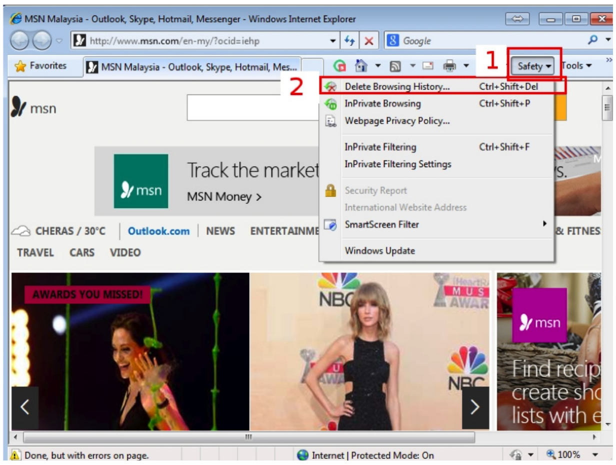

MSN Malaysia - Outlook, Skype, Hotmail, Messenger - Windows Internet Explorer
http://www.msn.com/en-my/?ocid=iehp
Google
Favorites
MSN Malaysia - Outlook, Skype, Hotmail, Mes...
1
Safety
Tools
2
Delete Browsing History... Ctrl+Shift+Del
InPrivate Browsing Ctrl+Shift+P
Webpage Privacy Policy...
InPrivate Filtering Ctrl+Shift+F
InPrivate Filtering Settings
Security Report
International Website Address
SmartScreen Filter
Windows Update
msn
Track the market
MSN Money >
CHERAS / 30°C
Outlook.com
NEWS
ENTERTAINME
& FITNES
TRAVEL
CARS
VIDEO
AWARDS YOU MISSED!
Find recip
Done, but with errors on page.
Internet | Protected Mode: On
100%

Figure 8: Delete browsing history on Internet Explorer browser

Reference

1. http://en.wikipedia.org/wiki/HTTP_cookie
2. http://www.tomsguide.com/us/-tracking-cookie-definition,news-17506.html
3. https://www.f-secure.com/sw-desc/tracking_cookie.shtml
4. http://www.avg.com/ww-en/faq.num-2334
5. http://www.wikihow.com/Delete-Tracking-Cookies
6. https://code.google.com/p/scriptno/
7. https://www.ghostery.com/en/home
8. https://noscript.net/
9. https://adblockplus.org/

What is Practical About Technical Writing?

By | Norhafizah Hashim, Zaleha Abd Rahim and Zahri Yunos

Introduction

Writing is a medium of communication that represents language through the inscription or recording of signs and symbols [1]. As a normal human being, at least once, we have written a piece of writing before, be it for official or non official purpose. This shows that the ability to write is already instilled in our self but we need to enhance the skill and polish the talent in order to write a good article. Technical writing is a style of writing that has a very different purpose and characteristics than other writing styles such as creative writing, academic writing or business writing. Technical writing is produced specifically to provide information to the end-user regarding subject matter that is scientific, educational, medical or technical in nature. Thus, some authors especially the budding writers feel that technical writing is difficult and very challenging. Below are some guidelines and useful tips that can assists the writer in their technical writing.

Where Do I Begin?

When you are required to write a technical article, the most common question that comes to your mind most probably is, 'What topic should I write?. Think about which topic or area that you are interested in and what you would like to know more about [2]. For example, if your job relates to web security, you may want to write something on web security. For example, ‘Security flaws in web application’. Or perhaps if you are working on finding web application vulnerabilities; you may want to enhance your knowledge in finding the latest tools and their effectiveness and it could be an area which you may want to look at and write about. Never write an article on a topic which you are not confident and not familiar [3] [4]. In other words, your article depends a lot on your knowledge, area and job scope.

Don't Be Afraid

Why people are so afraid of writing? Are you afraid that people might laugh at you or criticise your level of writing skills? Writing an article is not as ‘scary’ as ‘public speaking-presentation’. You don’t have to face people (well, not physically). Therefore, the most important thing is to have the courage to try. Don’t be afraid. Starts with a small steps like writing for a magazine or newspaper. Of course, nobody is perfect. Next, when you are confident, start writing for journals. You may start with a low impact factor journals and later submit to the high impact journals which are indexed by Scorpus and ISI.

Writing is Not a One Day Job

Writing a technical article is a challenging task, takes a lot of your personal time and requires you to do research on topic that you want to write. This is why you need to start early. Many of us often give excuses that we are busy with daily routines and do not have time to write. The truth is, you can always find time to write. You just have to make a strong commitment and challenge yourself to write every day, even if you only write for a little bit. The people who truly want to write will find time to do so.

How Do I Begin?

First, you need to identify and gather as much relevant and reliable resources that you can and choose which ones you could use as your references [5]. Then, identify and know your target readers. You need to understand your target reader's interest and what they can get after reading your article. After that, you must have a PROBLEM STATEMENT. The title of your paper should clearly give an idea of the problem statement. If possible, have a catchy and specific title in order to get your reader's attention.

- Once you have a question in mind, begin for sourcing information which are relevant to the topic either theoretical or empirical work – the process. Read everything you can; academic research, literature, and information in the popular press and on the Internet [5].

- When you already have a topic and framework, read all your references. Tip: While reading, if you find any relevant information which can be used in your paper, extract those information and include it in your paper (source document).

- For abstract, follow guideline provided by respective journal. Highlight introduction, problem statement, solution, contribution and result. Abstract should be prepared after your paper is completed. After all, how can you summarize something that is not yet written?

- Write a draft. An article should have 3 sections: introduction, body (problem statement, solution, contribution, result) and conclusion. A 1000 words article will approximately fills up 3-4 page, double spacing.

- Identify keywords. Keywords are very important. Assigning the right keywords will determine whether your paper will appear in search results or not.

- Cite adequate and reliable resources. Ten (10) and above references are better, preferable recent references.

- Look for associate writers. Put them as co-authors or give acknowledgement, depending on their contribution.

- Make sure the language is as simple as possible [6]. Do not use bombastic words.

- Provide reference to all articles relevant to your write-up. Give them credit

- Make sure you read your article several times, use spell-check and if possible get others to proof-read and their views. Even when writing a draft letter, do not review it immediately. You may be overlooking some flaws or miss some important points. Allow several hours (or a day) before you review it [7].

- Success factor: Commitment is very important and interest is a bonus. Usually once you start, the interest will follow later.

Summary

CyberSecurity Malaysia encourages its staff to write so that information is shared and knowledge is expanded. In addition, writing is one of the ways for staff to be recognized as an expert in their area. If you claimed to be the subject matter expert, then writing is considered as a medium to proof the claim. It could not be based solely on certifications. You need to write, so people will cite your paper as reference and later refer to you as the subject matter expert.

"The journey of a thousand miles begins with one step. Don’t be afraid.”

References

[1] Writing. Available at: http://en.wikipedia.org/wiki/Writing

[2] Get Published in Journal. Available at: http://www.writeexpress.com/writing-research-papers.html

[3] Tips for writing a good Technical Article. Available at: http://aroramohit.com/blog/tips-for-writing-a-good-technical-article

[4] 5 Tips For Writing Interesting Technical Articles. Available at: https://dzone.com/articles/5-tips-for-writing-interesting

[5] What is a Literature Review?. Available at: http://www.sagepub.com/sites/default/files/upm-binaries/55172_Coughlan.pdf

[6] Clueless About Technical Writing? Get Started With These Essential Tips. Available at: http://www.copyblogger.com/technical-writing/

[7] Top 10 Tips to Writing Excellent Articles (Technical Blogging). Available at: http://www.deepeshmd.com/musings/top-10-tips-writing-excellent-articles-technical-blogging/

Panduan Ibubapa : Keselamatan Rangkaian Sosial untuk Anak-Anak

By | Nur Haslaily Mohd Nasir

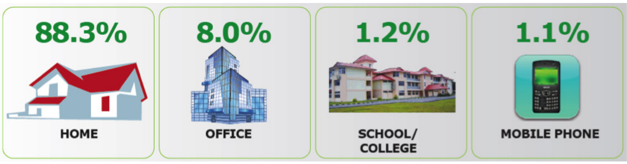
Pengenalan

Majoriti generasi Z yang berumur 7 hingga 18 tahun sekarang ini adalah generasi celik teknologi. Mereka diibaratkan makan, tidur dan bernafas dengan internet. Berdasarkan laporan Kajian Keselamatan Atas Talian Kebangsaan yang diterbitkan Digi Telecommunications Sdn Bhd (tahun ?) merumuskan mereka boleh melayari internet dengan mahir tetapi kurang pertimbangan tingkah laku baik, etika positif di alam siber dan cara melindungi diri ketika mengunakan kemudahan dalam talian. Kaji selidik ini melibatkan kira-kira 14,000 pelajar sekolah seluruh Malaysia yang menyertai bengkel *'CyberSAFE in Schools 2014'* yang telah berjalan selama sembilan bulan. Ia merupakan kajian yang dianalisa daripada beberapa dimensi berkaitan dengan tingkah laku di internet yang melibatkan keselamatan atas talian, buli siber, rangkaian sokongan dan kebimbangan peribadi.

Rangkaian sosial merupakan salah satu cabang teknologi intenet yang menjadi diet utama dalam kehidupan harian bagi orang muda yang tergolong daripada Generasi X, Y, Z dan Alpha. Ia merangkumi pelbagai perkhidmatan seperti Facebook, Google +, YouTube, Instagram, Twitter, Skype, dan lain-lain lagi. Rangkaian sosial adalah taman permainan maya yang besar dan membolehkan interaksi langsung antara individu di mana mereka boleh bermain, belajar dan bersosial. Ia sangat mudah diakses oleh sesiapa sahaja yang mempunyai komputer, telefon mudah alih dan peranti elektronik, termasuklah anak-anak kita.

Laporan Ekonomi 2013/2014 yang dikeluarkan oleh Kementerian Kewangan menunjukkan kadar penembusan rangkaian sosial sebanyak 91 peratus dengan satu daripada tiga minit yang digunakan dalam talian adalah untuk rangkaian sosial. 11.8 juta rakyat dianggarkan mempunyai akaun Facebook dengan lebih 80 peratus melayari internet untuk mengakses Facebook. Laporan itu menyebut rakyat Malaysia semakin banyak menghabiskan masa melayari internet berbanding media lain seperti televisyen, radio dan suratkhabar dengan penggunaan internet yang meluas untuk rangkaian sosial.

Merujuk kepada *'Household Use of The Internet Survey 2011'* yang dijalankan oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) sehingga 30 Jun 2011, menunjukkan komposisi terbesar sebanyak 88.3 peratus daripada keseluruhan responden adalah mereka yang mengakses internet daripada rumah. Ini termasuklah golongan kanak-kanak yang mengunakan rangkaian sosial daripada rumah masing-masing.



Rajah 1 : Statistik Tingkahlaku Pengguna Bagi Tempat Penggunaan Internet

Oleh yang demikian, ibubapa perlulah menjadi individu pertama yang bertanggungjawab memberi pendedahan awal kepada anak-anak tentang keselamatan rangkaian sosial apabila berhubung untuk menghantar maklumat peribadi, berinteraksi dengan kawan-kawan mahupun bermain permainan maya.

Berikut adalah tips 2B 3D 2P untuk ibubapa mendidik anak-anak mereka mengenai keselamatan dalam rangkaian sosial:

Tips Pertama : BELAJAR DAN BANTU (2B)

- Sentiasa terlibat dan terokai jenis-jenis rangkaian sosial yang anak-anak anda gunakan. Belajarlah bagaimana untuk menggunakan Facebook, Twitter, Intagram, Snapchat, dan lain-lain aplikasi rangkaian sosial yang berkenaan.

- Wujudkan akaun anda sendiri dan fahami tentang privasi tetapan supaya anda boleh mengetahui bagaimana anda boleh melindungi anak-anak anda.

- Periksa had umur bagi setiap perkhidmatan rangkaian sosial atau permainan yang digunakan oleh anak anda. Laman web seperti Facebook dan Instagram menetapkan had umur bermula daripada 13 tahun dan ke atas.

- Bantulah anak-anak memilih nama log masuk yang sesuai dan bimbing mereka untuk menetapkan konfigurasi keselamatan seperti melupuskan lokasi semasa juga nombor telefon supaya mengelakkan mereka menyiarkan maklumat penting dalam rangkaian sosial dengan sengaja.

- Ibubapa perlu juga belajar bagaimana untuk menyimpan salinan perbualan atas talian dan tahu bagaimana untuk memeriksa sejarah pengunaan akses internet anak-anak anda.

- Fahami juga cara dan saluran yang betul untuk membantu anak-anak melaporkan sebarang penyalahgunaan rangkaian sosial melalui Cyber999 Help Centre menggunakan email cyber999@cybersecurity.my atau hubungi talian hotline 1-300-88-2999. CyberSecurity Malaysia mencatatkan kira-kira 324 insiden siber yang berkaitan dengan Laman Rangkaian sosial sehingga berakhir 2011. Pada suku pertama tahun 2011 sahaja, terdapat kira-kira 177 insiden yang dilaporkan kepada Malaysia Computer Emergency Response Team (MyCERT).

Tips Kedua : DENGAR, DORONG, DIDIK (3D)

- Galakkan anak-anak anda untuk berkongsi pengalaman mereka menggunakan rangkaian sosial dengan anda. Dengar dan beri ruang untuk mereka memberitahu anda apa yang mereka rasa tidak selesa ketika mengunakan rangkaian sosial.

- Menegaskan bahawa anak-anak anda tidak boleh memberikan sebarang maklumat peribadi dalam talian. Ini termasuklah nombor telefon bimbit, maklumat ahli keluarga, alamat rumah, kampung halaman, nama sekolah, tempat permainan, dan apa-apa maklumat peribadi yang boleh dimanipulasi oleh orang yang tidak dikenali untuk mengesan mereka. Jangan biarkan mereka menghantar gambar diri sendiri mahupun ahli keluarga ke ....

- Jelaskan bahawa maklumat dan imej dalam talian boleh hidup selama-lamanya dan sesiapa sahaja di dunia boleh mengakses apa yang mereka paparkan di laman rangkaian sosial. Ia boleh menjadi sangat sukar dan kadang-kadang mustahil untuk memadamkan semula maklumat mahupun gambar yang telah dihantar yang mungkin telah disalin dan dipaparkan di tempat lain.

- Didik anak-anak bagaimana untuk menghormati orang lain di dalam rangkaian sosial. Pastikan mereka tahu etika dan peraturan tingkah laku yang baik tidak pernah berubah di dalam talian mahupun dalam kehidupan sebenar. Mengajar anak-anak anda bahawa perbezaan antara yang benar dengan yang salah adalah sama di dalam rangkaian sosial kerana ia adalah seperti kehidupan sebenar.

- Beritahu anak-anak bahawa mereka tidak boleh bertemu rakan-rakan dalam rangkaian sosial secara peribadi. Jelaskan bahawa rakan-rakan dalam rangkaian sosial mungkin bukan seperti yang mereka fikirkan. Anak-anak perlu diterangkan bahawa di laman rangkaian sosial, ramai orang tidak mendedahkan identiti sebenar mereka dan mungkin juga berpura-pura menjadi orang lain.

- Mengajar anak-anak anda bahawa tidak semua yang mereka baca atau lihat dalam rangkaian sosial adalah benar. Galakkan mereka bertanya kepada anda sekiranya mereka tidak pasti.

- Didik mereka untuk tidak sekali-kali memberi kata laluan kepada sesiapa sahaja walaupun rakan karib mereka. Jelaskan bahawa jika orang lain mempunyai kata laluan mereka, mereka boleh membuat penipuan menggunakan identiti anak-anak anda.

- Anak-anak juga perlu diingatkan supaya jangan sekali-kali terpedaya dengan iklan banner, tawaran hadiah atau menerima jemputan ke rumah anda.

Tips Ketiga : PERATURAN DAN PANTAUAN (2P)

- Sertai rangkaian sosial anak anda sebagai *‘follower’* atau *‘friend’* mereka supaya anda boleh memantau aktiviti mereka.

- Baca apa yang mereka tulis di rangkaian sosial dan respon-respon yang mereka terima. Lihatlah gambar yang mereka telah pilih untuk dikongsi. Kenali juga siapa rakan-rakan mereka di rangkaian sosial dan nilai apa jenis maklumat yang mereka kongsi.

- Hadkan dan pantau aktiviti dalam talian anak-anak anda dengan memasang perisian pemantauan internet pada komputer mahupun gadjet yang mereka gunakan. Kawalan ibubapa boleh membantu anda menapis kandungan berbahaya, memantau tapak lawatan anak anda, dan mengetahui apa yang mereka lakukan di dalam talian.

- Jika keluarga anda mempunyai beberapa komputer berkongsi sambungan internet melalui 'router', anda mungkin boleh mempertimbangkan menghadkan masa penggunaan internet. Menyekat akses kepada waktu yang munasabah membantu memastikan bahawa mereka tidak menghabiskan sepanjang malam dalam talian.

- Jika anda mempunyai komputer keluarga, cuba untuk meletakkan ia di kawasan terbuka di mana anda boleh melihat aktiviti dalam talian anak-anak anda. Jangan biarkan anak anda mempunyai komputer atau gadjet yang boleh mengakses internet di dalam bilik mereka tanpa pantauan ibubapa.

Kesimpulan

Teknologi komunikasi mempunyai manafaat yang sangat besar kepada masyarakat. Adalah penting bagi ibubapa untuk mengiktiraf peranannya dalam kehidupan kanak-kanak. Mereka telah dilahirkan dalam zaman teknologi dan ia akan menjadi masa depan mereka. Mereka sangat mudah menyesuaikan diri dan mengunakannya dengan penuh yakin. Walau bagaimanapun, ini tidak bermakna mereka tahu bagaimana untuk menggunakannya dengan selamat.

Tugas ibubapa adalah untuk menjaga mereka daripada bahaya sepanjang penerokaan maya mereka. Anda tidak perlu menjadi seorang pakar teknologi. Ilmu, pemantauan dan bimbingan adalah perlindungan terbaik bagi anak-anak. Manakala peraturan pengunaan internet di rumah dan di luar rumah adalah wajar untuk memupuk disiplin bagi mengelakkan ketagihan internet mahupun rangkaian sosial di kalangan kanak-kanak. Ibubapa juga berperanan penting untuk menonjolkan contoh tauladan yang baik ketika melayari internet.

Rujukan

1. "Teach Your Kids Online Safety" : http://www.cybersafe.my/

2. "Parents' Guide to Online Safety" : www.cybersmart.gov.au/

3. "A Parents' Guide to Facebook" : www.connectsafely.org/

4. "Bajet 2014: Pengguna Internet Malaysia cecah 25 juta orang pada 2015" : Berita Harian (25 Oktober 2013)

5. "Pelajar kurang arif aspek keselamatan berinternet" : Utusan Malaysia (3 November 2014)

6. "Household Use of The Internet Survey 2011" Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM)

7. "Best Practises On Social Networking Sites (SNS)" - CyberSecurity Malaysia (2011)

Keganasan Siber di Malaysia : Analisis Liberalisme Institusionalisme

By | Nurfarhana Nasrulhaq binti Mohd Zulkifli

Pengenalan

Teknologi siber telah membuka ruang kemajuan ekonomi dan sosial negara namun dalam masa yang sama memungkinkan penyalahgunaan yang akan mencetuskan keganasan siber. Walaupun Malaysia belum mengalami situasi sebenar keganasan siber, namun pihak kerajaan Malaysia telah mengambil inisiatif awal untuk membendung masalah ini melalui kerjasama dengan negara-negara lain. Ini adalah kerana Malaysia tidak akan dapat menangani masalah keganasan siber secara sendirian memandangkan pengaruh dan kesan internet adalah meluas dan merentasi sempadan, Oleh itu, kerjasama bersepadu di antara negara-negara serantau dan antarabangsa amat penting bagi memantapkan lagi usaha-usaha untuk menjamin keselamatan siber di peringkat global. Di sebalik pentingnya kerjasama ini, wujudnya jurang dan kekangan kerana penyalahgunaan alam maya merupakan perkara baru bagi sesetengah negara yang kekurangan pakar-pakar berkemahiran untuk mengatasi gejala ini dan ianya menyentuh pelbagai isu sensitif negara.

Teori Liberalisme Institusionalisme

Teori liberalisme institusionalisme telah diaplikasikan oleh kebanyakan negara dalam usaha untuk mengurangkan ancaman yang boleh menggugat keselamatan sesebuah negara. Pendekatan teori ini adalah berdasarkan kepada kepercayaan bahawa keamanan boleh diwujudkan di dalam anarki antarabangsa. Kerajaan yang mengamalkan teori ini mempercayai bahawa hubungan pelbagai hala dapat membantu dalam mewujudkan kerjasama dan interaksi di antara negara-negara yang berbeza. Mereka berpendapat bahawa penekanan harus diberikan kepada tadbir urus global dan penubuhan organisasi antarabangsa sebagai satu cara bagi menjelaskan hubungan antarabangsa. Tambahan lagi, liberal institusionalisme berpendapat bahawa untuk mencapai keamanan dalam hal ehwal antarabangsa, negara mesti bekerjasama dan menggunakan kedaulatan mereka untuk membina 'masyarakat bersepadu' bagi menggalakkan pertumbuhan ekonomi dan bertindak balas terhadap isu-isu keselamatan serantau dan antarabangsa.

Dalam mengamalkan liberal institusionalisme, setiap negara berusaha untuk memaksimumkan keuntungan mutlak melalui kerjasama antara negara dan kurang memberi fokus kepada kelebihan yang dicapai oleh negara-negara lain dalam pelaksanaan kerjasama ini. Dengan memberi tumpuan kepada organisasi-organisasi antarabangsa seperti Pertubuhan Bangsa-bangsa Bersatu (PBB), Kesatuan Eropah, dan ASEAN, pengamal liberal institusionalisme berpendapat ini boleh memberi penekanan terhadap 'soft power' dan kerjasama melalui prosedur undang-undang antarabangsa, diplomasi dan organisasi antarabangsa yang dikenali secara umum dapat dilaksanakan.

Liberalisme Institusionalisme : Pelaksanaan oleh Malaysia

Terdapat tiga ciri tertentu bagi penglibatan aktor sosial mempunyai pengaruh langsung ke atas bentuk institusi dan pematuhan dalam institusi berdasarkan teori liberalisme institusionalisme. Pertamanya, aktor tertentu mempengaruhi keputusan sesebuah institusi. Contohnya, Amerika Syarikat (AS), sebuah negara kuasa besar dan merupakan anggota utama dalam institusi seperti PBB, memainkan peranan dalam mengkategorikan sebarang insiden yang berkaitan dengan keganasan sebagai satu aktiviti jenayah dan perlu memeranginya. Ini termasuklah keganasan siber. Menerusi PBB, AS memainkan peranan utama dalam menentukan keputusan PBB termasuklah dalam mengeluarkan resolusi PBB. Resolusi-resolusi yang dikeluarkan yang berkaitan dengan keganasan adalah Resolusi 66/178 (Bantuan teknikal untuk melaksanakan konvensyen antarabangsa dan protokol yang berkaitan dengan memerangi keganasan), Resolusi 1373 (Menubuhkan Jawatankuasa untuk memantau pelaksanaan anti-keganasan menerusi kewangan dan kerjasama antarabangsa) dan Resolusi 1540 (Percambahan nuklear, kimia dan biologi dalam maksud penghantaran, merupakan ancaman kepada keamanan dan keselamatan). Resolusi-resolusi ini dikeluarkan berdasarkan pengalaman yang dialami oleh

AS selepas berlakunya insiden 11 September 2001 untuk memerangi keganasan termasuklah keganasan siber.

Berdasarkan Resolusi yang dikemukakan, Malaysia sebagai negara anggota PBB merupakan negara yang perlu memainkan peranan dalam menangani keganasan dengan menyokong Resolusi ini melalui penyertaan konvensyen-konvensyen dan protokol di peringkat antarabangsa. Sekiranya Malaysia tidak melaksanakan resolusi-resolusi ini dengan tidak menggubal undang-undang domestik, AS akan mendakwa Malaysia tidak mengambil inisiatif untuk memerangi keganasan. Senario terburuk yang mungkin berlaku ialah Malaysia akan diserang oleh kuasa-kuasa besar seperti yang terjadi di Afghanistan, di mana AS telah menyerang Afghanistan kerana tidak bertindak secara proaktif dalam saranan dan dokongan yang dibuat di peringkat antarabangsa. Ketika resolusi anti-keganasan diperkenalkan, Malaysia berada dalam keadaan dilema bagi menyatakan sokongan. Ini adalah kerana kumpulan-kumpulan pengganas telah menggunakan Islam sebagai asas perjuangan untuk mendapatkan sokongan Malaysia. Namun, Malaysia tidak mahu dianggap sebagai the *missing link* dalam menangani pengganas. Lantas mengambil langkah proaktif dengan menggubal beberapa akta perundangan berkaitan keganasan dan keselamatan negara. Selepas 11 September 2001, Malaysia dilihat sebagai antara negara yang menjadi sasaran pengganas seperti al-Qaeda dan Jemaah Islamiyah (JI). Walaupun fokus serangan tidak ditujukan kepada Malaysia, namun didapati gerakan kumpulan pengganas adalah merentasi sempadan. Oleh yang demikian, kerjasama antara negara-negara serantau dan antarabangsa diperlukan bagi menangani masalah keganasan terutamanya keganasan siber.

Keduanya, peraturan, norma dan prinsip-prinsip yang dikeluarkan oleh organisasi antarabangsa akan mempengaruhi interaksi dan tindakan aktor negara dan aktor bukan negara. Resolusi yang dikeluarkan oleh PBB memperlihatkan saranan organisasi antarabangsa dan juga perjanjian antarabangsa dalam teori liberalisme institusionalisme kepada Malaysia untuk mengambil langkah-langkah tertentu bagi menangani masalah keganasan siber. Pematuhan Malaysia terhadap perjanjian antarabangsa dan saranan organisasi antarabangsa jelas menunjukkan Malaysia komited untuk membendung keganasan siber sekali gus menyangkalkan tanggapan AS bahawa Malaysia tidak berbuat apa-apa untuk menangani isu ini. Sebagai contoh, Akta Perdagangan Strategik 2010 digubal sebagai respons kepada resolusi yang dikeluarkan oleh PBB untuk menghalang tindakan aktor bukan negara menghantar sebarang senjata pemusnahan besar-besaran (WMD) dan perkara yang berkaitan dengannya termasuklah penghantaran secara siber iaitu penghantaran sebarang teknologi atau dokumen yang berkaitan dengan keganasan ke destinasi di dalam atau luar Malaysia secara siber.

Ciri ketiga liberalisme institusionalisme ialah sistem penguatkuasa dipengaruhi oleh norma-norma antarabangsa, institusi domestik dan keadaan politik sesebuah negara. Pada tahun 2011, satu Gerak Kumpulan, iaitu *Countering the Use of Internet for Terrorist Purposes of the Counter-Terrorism Implementation Task Force* telah ditubuhkan untuk menyediakan rangka kerja memerangi keganasan yang selari, jelas dan fokus untuk entiti sistem PBB. Rangka kerja ini telah menerbitkan garis panduan aspek perundangan dan teknikal dalam menangani penggunaan Internet oleh pengganas untuk tujuan keganasan *(Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects)*. Rangka kerja ini telah mengenal pasti tiga pendekatan strategik yang boleh digunakan untuk menangani aktiviti pengganas terhadap Internet iaitu:

a. Undang-undang jenayah siber yang telah digubal oleh sesebuah negara;

b. (b) Undang-undang anti-keganasan atau untuk menangani keganasan secara umum (tidak khusus kepada Internet); dan

c. (c) Undang-undang khusus terhadap penggunaan Internet dalam menangani keganasan.

Malaysia telah mengaplikasikan dua pendekatan, iaitu pendekatan (a) dan (b). Pendekatan (a) merujuk kepada Akta Jenayah Komputer 1997 secara domestik. Manakala, di peringkat antarabangsa, Malaysia boleh merujuk dan menyertai Konvensyen Budapest terhadap Jenayah Siber dalam melakukan kerjasama antarabangsa yang lebih jitu untuk menangani masalah ini. Bagi Konvensyen Budapest terhadap Jenayah Siber, Malaysia dalam proses penelitian untuk menyertai konvensyen tersebut. Pendekatan (b) merujuk kepada undang-undang seperti Kanun Keseksaan (Akta 574) Bab VIA yang menerangkan mengenai kesalahan dan hukuman ke atas mereka yang melakukan keganasan. Pendekatan ini juga memberi perbicaraan bagi mana-mana undang-undang yang dikatakan relevan dalam menangani masalah keganasan. Bagi pendekatan (c), Malaysia masih tidak ada perundangan yang khusus untuk menangani aktiviti keganasan siber. Ini adalah kerana perundangan sedia ada dilihat memadai untuk melakukan pendakwaan dan menjatuhkan hukuman bagi di atas kesalahan jenayah siber. Walaupun Malaysia tidak mempunyai peruntukan undang-undang yang spesifik dalam menangani keganasan siber, namun Malaysia merupakan negara yang bebas untuk mengaplikasikan mana-mana undang-undang yang dirasakan sesuai bagi mencegah dan menangani sesuatu masalah yang boleh menggugat dan memudaratkan negara. Tambahan lagi, Perkara 149 (1) Perlembagaan Persekutuan memperuntukkan keistimewaan yang membolehkan penggunaan semua akta yang dirasakan relevan untuk diaplikasikan bagi membendung permasalahan ini.

Penglibatan Malaysia Bagi Menangani Keganasan Siber

Malaysia telah mengambil langkah awal bagi menangani keganasan siber dengan melibatkan diri di dalam institusi antarabangsa dan serantau. Melalui penglibatan aktif ini, Malaysia dapat berkongsi maklumat, pengetahuan, pengalaman dan bantuan teknikal serta dapat merapatkan jurang yang wujud dalam menangani keganasan siber dan instrumen perundangan yang digunakan di antara negara anggota. Di peringkat antarabangsa, menerusi PBB, Malaysia bertindak dengan memberi sokongan terhadap resolusi keganasan yang telah dikeluarkan seperti yang diterangkan di atas. Penglibatan Malaysia di peringkat serantau pula adalah menerusi *ASEAN Regionl Forum (ARF)*. Malaysia merupakan antara negara yang aktif dalam membincangkan isu-isu keganasan siber di ARF.

Peranan ARF dalam menangani penggunaan Internet oleh pengganas adalah, pertamanya, meneroka penggunaan pusat-pusat latihan yang sedia ada untuk latihan menangani penggunaan Internet oleh pengganas dengan memberikan tumpuan kepada teknik-teknik penyiasatan bagi menangani jenayah siber dan forensik digital. Kedua, mengambil bahagian dalam rangka kerja undang-undang untuk menangani masalah tersebut. Sebagai respon kepada peranan ini, Malaysia sedang dalam proses untuk menyertai Konvensyen Budapest terhadap jenayah siber. ARF juga terlibat dalam pembangunan kapasiti dan latihan bersama serta program-program penyelidikan dan pembangunan dan perkongsian teknologi.

Selain daripada ARF, Malaysia juga turut terlibat di dalam gerak kumpulan *Council for Security Cooperation in the Asia Pacific (CSCAP)* yang mengumpulkan kajian dan kepakaran dalam menangani permasalahan keselamatan negara dengan memberikan cadangan dan panduan dalam membuat dasar. CSCAP, dengan kerjasama di antara negara-negara di Asia Pasifik termasuk Malaysia, telah membincangkan mengenai keselamatan siber di peringkat serantau. Maka, memorandum keselamatan siber, iaitu Memorandum.20, *Ensuring a Safer Cyber Security Environment* telah diterbitkan. Memorandum ini menjelaskan mengenai penemuan dan cadangan mengenai langkah-langkah bagi melaksanakan keselamatan siber untuk kebaikan rantau Asia Pasifik.

Kesimpulan

Penglibatan kerjasama antara negara-negara adalah penting bagi memastikan keselamatan negara dan masyarakat sejagat terjamin. Ini adalah kerana tindakan keganasan siber adalah sesuatu yang tiada sempadan. Pengganas siber kini tidak menumpukan hanya pada satu sasaran sahaja dan pergerakan mereka juga bukannya statik walaupun tidak begitu meluas. Justeru, kerjasama dan kolaborasi serantau dan antarabangsa yang erat dan mampan perlu terjalin agar perkongsian maklumat dan kepakaran untuk menangani keganasan siber dapat dilaksanakan. Setiap negara perlu mematuhi dan menghormati undang-undang negara masing-masing dan juga undang-undang antarabangsa.

Rujukan

1. *Anon. e-International Relations,: http://www.e-ir.info/2011/09/01/ liberal-institutionalism-an-alternative-ir-theory-or-just-maintaining-the-status-quo/*

2. *CSCAP Memorandum No.20, Ensuring A Safer Cyber Security Environment. 2012.http://www.cscap.org/uploads/docs/Memorandums/CSCAP%20 Memorandum%20No%2020%20%20Ensuring%20 a%20Safer%20Cyber%2 0Security%20Environment.pdf*

3. *Malaysia. 2012. Perlembagaan Persekutuan Malaysia 1957.*

4. *Council of Europe. 2004. Convention on Cybercrime (Budapest). Budapest :Council of Europe.*

5. *United Nations, General Assembly. Resolution 66/178. 30 Mac 2012 http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ-ECOSOC/CCPCJ- ECOSOC-00/CCPCJ-ECOSOC-11/GA_res_66-178.pdf*

6. *United Nations Global Counter-Terrorism Strategy (Background Note), March 2009. http://www.un.org/terrorism/pdfs/CT_Background_ March_2009_terrorism2.pdf*

7. *United Nations Office on Drugs Crime. 2012. The Use of the Internet for Terrorist Purposes. New York: United Nations.*

Makmal Forensik Digital Bertaraf Dunia

By | Mohd Zabri Adil Talib, Mohamad Firham Efendy Md Senan, Fauzi Mohd Darus

Latar Belakang

Tahukah anda bahawa negara Malaysia memiliki kemampuan bertaraf dunia dalam bidang forensik digital?

CyberSecurity Malaysia (dahulu dikenali sebagai NISER),agensi di bawah Kementerian Sains Teknologi dan Innovasi (MOSTI) telah diamanahkan untuk merintis teknologi forensik digital ini selaras dengan perkembangan pesat teknologi digital terkini di dunia.

Justeru, pada 27 April 2002, MOSTI telah meluluskan cadangan CyberSecurity Malaysia (CSM) untuk menubuhkan satu Jabatan Forensik Digital di bawah projek RMK 9 MOSTI. Objektif penubuhan jabatan ini adalah untuk _ menyediakan bantuan pakar terutamanya kepada agensi-agensi penguatkuasaan undang-undang, perundangan serta institusi-institusi akademik.

Foto 01: Ruang penerimaan eksibit Makmal Forensik Digital CyberSecurity Malaysia

Dalam usaha untuk menjadikan CyberSecurity Malaysia (CSM) sebagai sebuah agensi rujukan kebangsaan dalam bidang forensik digital dan keselamatan siber, sejumlah pelaburan telah di buat dan beberapa teknologi terkini dari pelbagai negara di seluruh dunia telah di bawa masuk. Hasilnya, Makmal Forensik Digital CyberSecurity Malaysia merupakan satu-satunya makmal forensik yang terunggul di Malaysia.

Foto 02: CSM telah mewujudkan jenama ekslusif 'CyberCSI'

Untuk memastikan proses pemindahan masuk teknologi dan pengetahuan forensik digital ini menjadi rujukan generasi akan datang, pendokumentasian telah dilakukan sebaik mungkin dan telah diklasifikasikan sebagai khazanah negara. Disamping itu pelbagai latihan kepakaran forensik digital dan program kesedaran keselamatan siber turut dilaksanakan agar pengetahuan yang diperolehi dikongsi bersama rakyat Malaysia.

Keperluan Teknologi Forensik Digital

a) Gaya hidup masa kini - Jejak kehidupan dalam talian Internet.

Sains adalah sebahagian daripada kehidupan rakyat Malaysia. Negara Malaysia pula telah dirancang untuk mencapai status negara maju pada tahun 2020. Oleh yang demikian, dapat dijangka peningkatan berterusan kadar celik IT dan tahap intelektual rakyat Malaysia akan meningkat dan perbincangan berkenaan teknologi di kalangan orang awam akan menjadi satu kebiasaan.

Di zaman sosial media ini, hampir setiap rakyat Malaysia mempunyai jejak kehidupan dalam talian Internet. Setiap aktiviti komunikasi atau aktiviti perpindahan data yang berlaku, di mana akan meninggalkan kesan hasil daripada aktiviti tersebut. Rekod berkaitan aktiviti-aktiviti sebegini adalah penting dan boleh digunakan untuk siasatan dan pembuktian kes di mahkamah.

Jika diberikan pendedahan dan kesedaran awam secara meluas berkenaan sains forensik, rakyat Malaysia boleh menggunakan rekod-rekod digital sebagai alibi untuk menyokong atau menyangkal sesuatu pembuktian keterangan di mahkamah. Ini kerana jika proses pemeliharaan data digital tersebut dijalankan mengikut kaedah saintifik yang betul, maka ia sah untuk digunapakai di mahkamah.

Cyber crime
Malaysia landscape
Parcel scam hits widow hard
Phishing sharks
RM861,000 lost in cyber scam
Trio claim trial to charge of illegal deposit-taking
BNM can hold on to Geneva's gold pending appeal
Manipulasi Internet
ayuan gadis manja
world
8,000 fall for get-rich scam in Malaysia
Malaysia: Facebook 'used to recruit female drug mules'
BEWARE of PHONE SCAMS!
BORNEO POST online
Cyber crime a ticking bomb in Malaysia
RM5,000 lesap bahana e-mel
Ex-Silver Bird directors plead not guilty

Foto 03: Penjenayah semakin mahir menggunakan teknologi untuk tujuan jenayah mereka

Rakyat Malaysia yang faham tentang teknologi, pastinya akan lebih peka dengan corak ancaman, tahap risiko dan potensi untuk menjadi mangsa kepada ancaman penjenayah siber. Masyarakat boleh menggunakan pengetahuan mereka dalam bidang sains ini, bukan sahaja dalam usaha untuk mencegah daripada menjadi mangsa malah mungkin dapat membantu agensi penguatkuasa undang-udang dalam usaha membanteras jenayah.

b) Penjenayah juga menggunakan platform teknologi yang sama.

Hingga tahun 2015 ini, kita sudah diperkenalkan dengan pelbagai platform teknologi baru yang bukan sahaja efisien dalam kehidupan harian malah majoritinya, ditawarkan secara percuma. Pengguna hanya perlu mendaftar sahaja. Semua teknologi baru yang diperkenalkan ini bertujuan untuk meningkatkan tahap kualiti hidup kita, terutama di era teknologi IPV6 dan Internet of Things (IoT) ketika ini.
Namun begitu, harus diingati bahawa platform teknologi yang sama juga digunakan oleh penjenayah untuk menjayakan matlamat jenayah mereka.

Oleh itu, agensi penguatkuasa wajib meningkatkan tahap dan piawaian kualiti siasatan mereka agar jenayah sebegini dapat dicegah. Ini dapat dilakukan dengan mengambilkira faktor platform teknologi seperti platform media sosial dan aplikasi telefon pintar, yang digunakan oleh penjenayah dalam jenayah tersebut. Kaedah terbaik harus difikirkan untuk membuktikan fakta kes di mahkamah nanti. Seharusnya setiap kes siasatan jenayah dijalankan sebaik mungkin, seperti ia akan berakhir dengan pembuktian di mahkamah.

Kepentingan Teknologi Forensik Digital

Forensik digital adalah satu cabang sains. Ia digunakan dalam membantu sesuatu pembuktian fakta dengan mengambil kira elemen saintifik dan perundangan sebelum dibentangkan di mahkamah.

Dengan kata lain, , keterangan yang dibuktikan melalui kaedah forensik akan mempunyai nilai keistimewaan tersendiri (privilege) dan sukar untuk disangkal melalui hujah balas.

Hujah balas untuk mencabar atau menyangkal keterangan forensik digital, hanya boleh dilakukan dengan mengemukakan hujah balas bersandarkan keterangan saintifik sahaja.

Hanya hakim mahkamah tersebut sahaja yang berhak untuk menentukan keputusan sama ada hujah balas keterangan forensik digital tersebut diterima atau tidak dalam proses penghakiman. Pembuktian menggunakan keterangan forensik digital adalah strategi pilihan yang popular dalam perundangan terutama dalam kes perundangan berprofil tinggi atau kes perundangan yang melibatkan jumlah nilai tuntutan yang besar .

Statistik Kes Forensik Digital Yang Dilaporkan

Pada tahun 2014 sahaja, CSM telah menerima sebanyak 341 kes forensik digital yang terdiri daripada 217 kes analisa forensik digital, 11 kes khidmat pemulihan data (data recovery) dan 113 kes untuk khidmat bantuan teknikal di lokasi tempat kejadian.

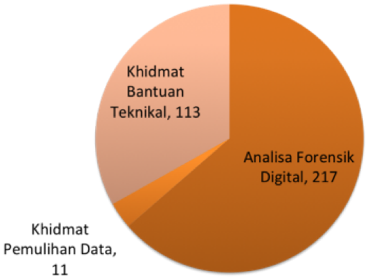


Foto 04: Pecahan jenis kes yang dirujuk kepada Makmal Forensik Digital CSM.

Di antara agensi penguatkuasaan yang mendapatkan khidmat forensik digital CSM adalah seperti Polis Diraja Malaysia (PDRM), Suruhanjaya Pencegahan Rasuah Malaysia (SPRM), Kementerian Perdagangan Dalam Negeri, Koperasi Dan Kepenggunaan (KPDNKK), Jabatan Kastam Diraja Malaysia (JKDM) dan Cawangan Penguatkuasaan Farmasi, Jabatan Kesihatan Malaysia.

Daripada 341 kes yang diterima pada tahun 2014, sejumlah besar kes adalah melibatkan Akta Suruhanjaya Pencegahan Rasuah Malaysia 2009, Kanun Keseksaan Malaysia, Akta Hakcipta 1987, dan Akta Dadah Berbahaya 1952.

CSM mempunyai juruanalisa forensik digital yang bertauliah dan mempunyai pensijilan professional dalam bidang forensik digital seperti *GIAC Certified Forensics Analyst (GCFA), EnCase Certified Examiner (EnCE),* dan *Computer Hacking Forensic Investigator (CHFI).* Dan pada tahun 2014, juruanalisa forensik digital CSM telah terlibat dalam pelbagai operasi penguatkuasaan yang dijalankan oleh agensi-agensi penguatkuasaan undang-undang Malaysia.

Pegawai-pegawai Forensik Digital CSM pernah terlibat di dalam operasi berskala besar seperti Ops SOGA yang djalankan oleh PDRM untuk membanteras kegiatan pertaruhan dan perjudian bola sepak sepanjang musim perlawanan bola sepak Piala Dunia 2014.

Dalam operasi ini, PDRM telah berjaya menumpaskan sindiket perjudian yang melibatkan pertaruhan sebanyak RM7.5 juta sehari[1]. CSM berperanan dalam membuat analisa forensik ke atas 12 unit pelayan komputer yang disyaki mempunyai laman web perjudian yang merangkumi rangkaian perjudian di rantau Asia Pasifik.
Unit Forensik Digital CSM juga terlibat dalam operasi Ops Diesel 2 North (OD2N) dan Ops Diesel 1 East (OP1E), di mana unit ini telah membantu pihak KPDNKK dan Jabatan Peguam Negara dalam menganalisa eksibit komputer dan telefon bimbit yang dirampas untuk menangani sindiket penyeludupan diesel dan petrol di Malaysia.

Dalam OD2N, KPDNKK telah berjaya merampas sebanyak 140,000 liter diesel dan 46,350 liter petrol bernilai RM1 juta selain wang tunai berjumlah RM320,483. Manakala untuk OP1E, KPDNKK telah berjaya membekukan 15 akaun perbankan pemilik ahli sindiket penyeludupan diesel yang berjumlah RM2.9 juta[2].

Bukan itu sahaja, CSM juga turut terlibat dalam membantu pihak PDRM bagi operasi misi mencari dan menyelamat (SAR) MH370. CSM dipertanggungjawabkan untuk menganalisa sistem simulator kapal terbang milik juruterbang MH370, Kapten Zaharie Ahmad Shah, bagi mencari maklumat yang berkaitan dengan kehilangan pesawat MH370 yang berlaku pada bulan Mac 2014 yang lalu[3].

Dengan penglibatan CSM di dalam operasi-operasi dan kes-kes seperti di atas jelas menunjukkan bahawa juruanalisa forensik digital CSM adalah kompeten dan berkebolehan untuk membantu pihak penguakuasaan undang-undang membanteras jenayah khususnya jenayah siber.

Sistem Pengurusan Kualiti

Setelah beroperasi lebih daripada 5 tahun, CyberSecurity Malaysia telah memulakan usaha untuk mendapatkan akreditasi untuk makmal forensik digital. Ini dilakukan demi memastikan keterangan digital dari pemeriksaan dan analisa yang telah dijalankan, adalah berkualiti tinggi.

Makmal Forensik Digital CSM adalah yang pertama di rantau Asia Pasifik yang mendapat pentauliahan akreditasi *American Society of Crime Lab Director / Laboratory Accreditation Board (ASCLD/LAB)* untuk disipllin *'Digital & Multimedia Evidence'.*

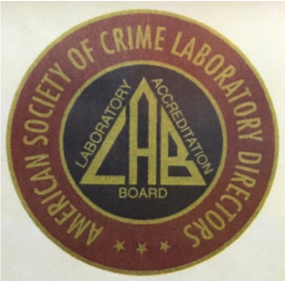

AMERICAN SOCIETY OF CRIME LABORATORY DIRECTORS
LABORATORY ACCREDITATION BOARD
LAB

Foto 05: ASCLD/LAB adalah gabungan kumpulan pakar tidak berasaskan keuntungan yang berdedikasi untuk menyediakan kecemerlangan dalam bidang sains forensik melalui kepimpinan dan inovasi.

Akreditasi ini adalah berdasarkan ISO/ IEC 17025: 2005 dan ASCLD/LAB - International 2011 iaitu keperluan tambahan spesifik untuk makmal forensik digital.

Skim akreditasi yang telah diimplementasi telah terbukti berkesan dengan memperkenalkan cara bekerja yg sistematik dan efisien, sekaligus telah meminimakan risiko kesilapan manusia dalam proses pemeriksaan dan analisa forensik digital.

Skim Latihan Forensik Digital

Demi untuk memastikan pengetahuan mengenai forensik digital ini berkembang luas di Malaysia, Jabatan Forensik Digital CSM telah membangunkan modul-modul latihan berkaitan subjek forensik digital dengan menggunakan pendekatan latihan praktikal khas untuk golongan professional dan pengamal undang-undang.

Antara latihan-latihan yang ditawarkan adalah berperingkat seperti berikut:

1. Peringkat permulaan:
   a. Kursus Digital Forensics Essential
   b. Kursus Forensics on Internet Application

2. Peringkat pertengahan:
   a. Kursus Digital Forensics For First Responder
   b. Kursus Forensics For Law Practioners

Untuk maklumat lanjut, anda boleh merujuk kepada laman web Cyberguru di https://www.cyberguru.my/cybersec/training

Selain daripada itu, CSM juga telah menjalinkan kerjasama dengan pihak institusi pengajian tinggi tempatan dimana pegawai-pegawai forensik digital CSM telah dilantik menjadi pensyarah jemputan bagi kursus peringkat Sarjana seperti Program Sarjana Keselamatan Siber Universiti Kebangsaan Malaysia.

CSM juga menyokong mana-mana pelajar peringkat kedoktoran atau institusi penyelidikan lain yang berminat untuk menjalankan penyelidikan berkaitan forensik digital.

Bagi agensi penguatkuasa undang-undang pula, CSM terlibat dalam memberikan latihan teknikal berkaitan forensik digital yang diadakan di akademi atau pusat latihan yang terpilih.

Sebagai contoh, kerjasama dengan Institut Latihan Kehakiman dan Perundangan Bangi sudah terjalin sejak dari tahun 2008. Melalui kerjasama ini, telah membantu menyebarkan pengetahuan tentang forensik digital dan kesedaran tentang kepentingan keterangan elektronik dalam pembuktian kes mahkamah. Kursus ini bukan sahaja dihadiri oleh pegawai penyiasat, timbalan pendakwaraya atau peguam malah ia disertai juga oleh pegawai mahkamah, majistret dan hakim.

CSM berharap dengan menawarkan kursus latihan praktikal digital forensik ini, ia akan meningkatkan tahap intelektual rakyat Malaysia dalam bidang forensik digital.

Penambahbaikan Dan Penyelidikan Yang Berterusan

Bidang forensik digital memerlukan penambahbaikan yang berterusan baik dari segi peralatan forensik digital dan juga pengetahuan kepakaran para juruanalisa forensik digital. Ini adalah kerana setiap kes yang diterima adalah unik dan tidak semua peralatan forensik digital sedia ada mampu untuk menyelesaikan masalah tersebut. Justeru, Makmal Forensik Digital CSM telah menambah satu lagi makmal penyelidikan forensik siber yang diberi nama 'Makmal X Forensik Siber'. Kelulusan geran Technofund yang diperolehi daripada MOSTI telah membolehkan makmal ini memulakan projek penyelidikan yang pertama iaitu *"GPU Enhanced Robust Multi-Dimensional Facial Identification System For CCTV Evidence In Video Forensics Analysis"*.

Tercetusnya idea projek ini adalah dari pengumpulan masalah dan cabaran yang dihadapi oleh juruanalisa forensik digital terhadap kes analisa CCTV yang melibatkan pengecaman wajah. Masalah yang dihadapi adalah kualiti video CCTV yang sedia ada di negara ini kebanyakannya tidak membantu dalam penganalisaan pengecaman wajah. Diharap hasil penyelidikan projek ini akan dapat membantu juruanalisa dalam melakukan penganalisaan pengecaman wajah tersebut.

Penyelidikan yang terterusan dalam bidang forensik digital juga adalah satu aspek yang penting agar hasil keputusan analisa forensik digital dapat diperincikan dan dijelaskan secara saintifik. Penjelasan secara saintifik dapat dilakukan oleh seorang juruanalisa dengan lebih yakin menerusi penghasilan kajian yang berterusan dalam bidang forensik digital.

Melalui penyelidikan yang berterusan juga secara tidak langsung akan menghasilkan harta intelek yang lebih berkualiti. Seterusnya, juga dapat memupuk minat penyelidik tempatan untuk menjadi lebih inovatif dalam bidang forensik digital. Walau bagaimana pun kolaborasi di antara pihak perundangan, pihak berkuasa, industri, dan juga para akademik amat diperlukan untuk menjadikan penyelidikan forensik digital di negara ini mampu berdaya saing di peringkat antarabangsa.

Kesimpulan

Penubuhan Makmal Forensik Digital CyberSecurity Malaysia yang dilengkapi dengan peralatan-peralatan canggih setanding dengan makmal forensik digital bertaraf dunia merupakan satu pelaburan yang berjaya oleh MOSTI. Ini terbukti di mana CSM telah berjaya membantu proses perundangan dalam pembuktian bahan bukti digital di mahkamah.
Nama CSM juga telah terpahat diperingkat antarabangsa sebagai sebuah Pusat Rujukan Nasional bertaraf dunia.

Rujukan

1. Polis tumpas sindiket judi bola sepak bertaruh RM7.5 juta sehari (Kosmo, 26 Jun 2014)

2. KPDNKK, Jabatan Peguam Negara rampas diesel nilai RM8.4j (Harian Metro, 6 April 2014)

3. MH370: Kebanyakan maklumat simulator telah dipadamkan (Utusan Malaysia, 19 Mac 2014)

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
Customer Service Hotline: 1300 88 2999
www.cybersecurity.my

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

Best Brand
Internet Security
2008 & 2009

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

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

Status Company

Best Child Online
Protection Website