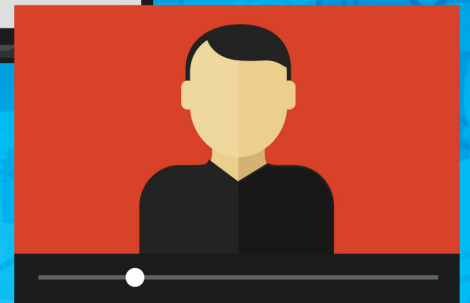


eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 49 - (2/2020)



Business Continuity And Covid-19

Remote Audit As A Continuity Tool During Covid-19

Covid-19: Landskap Keselamatan Siber Di Malaysia Semasa PKP

"Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they will do wonderful things with them"

Steve Jobs

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



Securing Our Cyberspace

CyberSecurity Malaysia is the national cybersecurity specialist and technical agency committed to provide a broad range of cybersecurity innovation-led services, programmes and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace. Among specialised cyber security services provided are Cyber Security Responsive Services; Cyber Security Proactive Services; Outreach and Capacity Building; Strategic Study and Engagement, and Industry and Research Development.

For more information, please visit
www.cybersecurity.my

For general inquiry, please email to
info@cybersecurity.my

Stay connected with us on
www.facebook.com/CyberSecurityMalaysia and
www.twitter.com/cybersecuritymy



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA



CyberSecurity Malaysia

(726630-U)

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

T: +603 - 8800 7999
F: +603 - 8008 7000
E: info@cybersecurity.my

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



WELCOME MESSAGE FROM THE CEO OF CYBERSECURITY MALAYSIA



Dear Readers,

Prior to the pandemic Covid-19, many saw technology as simple complementary tools, not as essential elements to the functionality that has been integrated in our lifestyles. With most of the world in forms of lockdown due to Covid-19, we are relying on technological devices to stay connected with one another more than we used to.

The Internet is enabling vital services to provide information, to communicate and manage emergencies. At the same time cyber ethical challenges are emerging, including threats to cybersecurity, increase in cybercrime, governments collecting more personal data and information than before, voluntary or compulsory tracing and the deepening of inequalities in education and in work for those without Internet access.

Towards the new normal of hybrid workplaces, organisations are now taking counts of their business continuity measures and addressing the needs that can restore productivity to high level. A big part of this effort is ensuring that they have the right technological infrastructure and tools for their employees.

In Malaysia, during the recent *Movement Control Order (MCO)* and *Restricted Movement Control Order (RMCO)* period from 18 March to 20 May 2020, Cyber999 received a total of 2,726 cyber incidents reports among Malaysians compared to 1,380 reports which increased 97.53% during the same period in 2019.

Cybercriminals have been taking advantage of today's global pandemic by adapting and updating their attack methods to capitalize on peoples' fears. Nonetheless, this sudden rush of technology development and adoption have resulted in vulnerabilities being exposed, highlighting risks

concerning inequality, privacy, and security. The risks to society, the economy, and to our children, have multiplied enormously. Hence, the global health crisis also has had a significant impact on the education landscape of the country, accelerating the digitisation of higher education.

Parents, guardians, and educators have had to adapt to new creative ways of keeping them engaged. Often, this means encouraging our children/students to go online more to use various resources and to help them focus on their learning during the day. It is likely to increase the amount of screen time and giving them a big chance to be a victim of cyber threats. As a parent/guardian, it may cause concern to see how much time they are spending online, and you may be worried about their health, and their safety. It is our duty to ensure their safety is more important than ever.

Moving forward past this pandemic, we need to anticipate the change in the technology landscape and think hard on what policies ought to be put in place. Technology adoption is no longer optional, it is now the needed solution to cushion the devastating impact of the pandemic. Cautious steps are vital as technological emergency measures could also expose citizens to vulnerabilities that violate human rights and privacy.

The Global Financial Crisis 2007-2009 and the 2004 Tsunami in Asia are clear examples of how human behaviour reacts to crisis that has shaken the world. Whenever a new crisis emerges, different criminal actors are the first to jump on the occasion to exploit unsuspecting victims in times of fear, uncertainty, and doubt. These exploits take multiple forms, from the physical to the digital world. History has taught us that the most efficient method to initially counter these threats is through prevention and awareness towards all levels of corporate and personal life.

With that, I am pleased to present 40 interesting and informative articles in this second publication of e-Security Bulletin year 2020 to reflect current issues in cybersecurity and technological landscape. I would like to convey my utmost appreciation to all contributors for their nobility of sharing invaluable knowledge and for continuous support towards our goal of enhancing online safety.

Thank you and warmest regards.

Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab FASc
Chief Executive Officer, CyberSecurity Malaysia

EDITORIAL BOARD

Chief Editor

Ts. Dr. Zahri bin Yunos

Editor

Lt Col Mustaffa bin Ahmad (Retired) C|CISO

Internal Reviewers

1. Mohd Shamil bin Mohd Yusoff
2. Ramona Susanty binti Ab Hamid
3. Nur Arafah binti Atan
4. Jazannul Azriq bin Aripin

Designer & Illustrator

1. Edwan bin Mohammad Aidid
2. Zaihasrul bin Ariffin

READERS' ENQUIRY

Outreach and Corporate Communications, Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia.

PUBLISHED AND DESIGNED BY
CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

TABLE OF CONTENTS

1.	Securing Your Android Application Before Going Into Production	1
2.	Basic Approach For Onion Web Server Basic Configuration And Proof Of Concept	5
3.	Eradicating Fake News In Malaysia	14
4.	SSL Certificate	17
5.	The Critical Role Of Security And Authorization In SAP System	20
6.	Quick Response (QR) Codes	23
7.	Implementation Of Cyber Range For Cyber Defence Strategy	26
8.	A Study On CCTV Installation and Recommendation From Developed Nations Perspective	29
9.	Windows Artifact Analysis : The Importance In E-Discovery Analysis	33
10.	Application of OBD-II Standard In Vehicle Diagnostics	38
11.	OIC-CERT Contribution To The OIC-2025 Strategic Agenda	41
12.	Secure Your Zoom To Prevent Any Cyber-Attack Gloom	45
13.	Coping In The Workplace with Covid-19	48
14.	Crime Prevention Through Environmental Design: Elements And Illustration	49
15.	Data Sanitization – Definition, Importance, Methods And Advantages	52
16.	DeepFake: Fake Videos – Generated By AI	55
17.	Business Continuity and COVID-19	58
18.	Remote Audit As A Continuity Tool During Covid-19	61
19.	Crossword Puzzle: Understanding ISO 22301:2019	66
20.	Cyber Security Marketing Strategy – What Hiking Can Teach Us	68
21.	How To Reduce Gadget Addiction For Kids	71
22.	Can WPA3 Be The Game Changer In Wi-Fi Security?	73
23.	Book Review – Interesting Read On Big Tech: Yahoo, Amazon & Netflix!	76
24.	Global ACE Certification	79
25.	Drones – Models Of UAV And The Evolution Of The Future	82
26.	Crypto-Ransomware Behaviour On Infected Machine	85
27.	Courses Of Action Matrix: The Cyber Kill Chain Complement For Incident Handlers	87
28.	Understanding Human Elements In Inculcating Information Security Culture In An Organization ...	90
29.	Cyber Security: Putting Resilience Before Insurance	95
30.	A Brief Review of Authenticated Encryption	99
31.	Effective Communication In Digital Age	102
32.	Damn Vulnerability Web Application: Command Injection	105
33.	Security Concerns On Online Meeting Applications	111
34.	Covid-19: Landskap Keselamatan Siber Di Malaysia Semasa PKP	114
35.	Mengenali Ancaman Dalam Siber Ke Atas Sistem Pembuatan Pintar	120
36.	Insiden Keselamatan Siber – Ini Yang Anda Perlu Tahu Dan Lakukan!	122
37.	Kenali Jenis-Jenis Perisian Hasad (<i>Malware</i>).....	124
38.	Cara Mendidik Anak-Anak Agar Berintegriti Semasa Menggunakan Internet	126
39.	Buli Siber Di Media Sosial	128
40.	Integriti Dalam Dunia Siber, Tanggungjawab Bersama	131

Securing Your Android Application Before Going Into Production

By | Muhammad Azizi Bin Jamadi

Building an Android application today is a lot easier than ever before. With the right tools, research and skills, you can easily code your own Android application. Since Android is an open source platform, it affords flexibility to create and build your app with features and functionality tailored for your users.

By making your app more secure, it not only maintains integrity but also builds superior trust with your users. Here are some important tips to consider before releasing your app into production environment.

Implement Secure Communication

Most applications need to establish backend communication to exchange information and data. Should the developer be concerned about security under this scope, use HTTPS (Hyper Text Protocol Secure) from a trusted certificate authority (CA) certificate to encrypt any data transfer between client and back-end server to mask text communication and protect the information exchange.

During development phases, developers usually overlook this matter in favour of troubleshooting and debugging. Hence, make sure HTTPS is built in during coding.

Implement SSL Pinning

SSL Pinning must be built into the app to avoid Man-In-The-Middle (MITM) attack by embedding a list of trusted certificate information into the app code and using this information to verify against the server certificate during runtime. If there is any discrepancy on trusted certificate information between the app and server, the connection is automatically terminated and no data exchange will occur.

This implementation ensures that the app is communicating only to the dedicated and trusted server. However, app developers need to take note that implementing this mechanism will add

operational complexity and limit the ability to migrate or update certificate authorities without making changes to the app.

Shrink, Obfuscate And Optimize Your Android App Code

Obfuscation helps improve your application build release version by removing unused codes and resources, reducing the size of application and making it harder to decipher.

Obfuscation process will also shorten your app's classes name and members. App developers using Android Studio can use features offered by ProGuard. ProGuard is a Java class file shrinker, optimizer, obfuscator and preverifier. It makes app codes smaller, increases its efficiency and obfuscates your code, making it harder for reverse-engineers. This mechanism offered by ProGuard can be implemented by adding additional code in your project level build.gradle (Module:app) file.

```
buildTypes {
    release {
        minifyEnabled true
        shrinkResources true
        proguardFiles getDefaultProguardFile('proguard-android-optimize.txt'),
            'proguard-rules.pro'
    }
    debug {
        minifyEnabled false
        shrinkResources false
        proguardFiles getDefaultProguardFile('proguard-android.txt'),
            'proguard-rules.pro'
    }
}
```

Proguard rule snippet for Android Studio project

Most Android malware applications utilize this mechanism to hide its malicious functionality and evade reverse-engineering. Some use off-the-shelf obfuscation plugins, while others via their own obfuscation method by combining encoding and encryption on their string, Java class name and function.

2

Developers can now use obfuscation to further secure and protect your code and minimize attack surface in your application.

Disable Debugging, Emulator And Root Detection

To ensure your app is deployed securely and functions normally, it must undergo checks before allowing the user to access its functionality and features. This can enhance security especially when the app is handling highly sensitive financial data, which require extra protection. This feature will prevent your app from being manipulated or hacked by dynamic instrumentation toolkits such as Frida that can inject payload to alter behaviour, value or functionality.

First and foremost, check on the environment which the app is running. Is the app running on an emulator or physical device? Whenever attack happens whether to reverse the code, attach debugging tools or using dynamic instrumentation toolkit, it is usually done using an emulator.

Most Android emulators share some common system and hardware identifiers which you can check such as brand, hardware, manufacturer, user, model, board or anything related that match the checking parameter or variables that indicate that it is running in an emulator.

Secondly, check that Developer Option settings has been turned on. Developer Option allows user of the device to perform debugging process to interact and manipulate application and enable advanced features for development or configuring Android device.

Next, check its path if the device has been rooted by verifying if su binary has been installed or BusyBox and root manager app such as Magisk Manager, Superuser etc. You may also use su command to check whether higher privilege command can be executed.

```
public void Checking() {  
    //check for developer option  
    int DeveloperOption = Settings.Global  
        .getInt(this.getContentResolver(),  
            Settings.Global.DEVELOPMENT_SETTINGS_  
ENABLED, 0);  
    int USBDebug = Settings.Global  
        .getInt(this.getContentResolver(),  
            Settings.Global.ADB_ENABLED, 0);  
  
    if (DeveloperOption > 0) {  
        Log.i(TAG, "Debugging Check: " + "Developer enable");  
        if (USBDebug > 0)
```

```
        Log.i(TAG, "Debugging Check: " + "USB  
Debugging enable");  
    }
```

```
    //Check if application running in emulator  
    int kill = 0;  
    if (Build.BRAND.contentEquals("Android"))  
        kill = kill + 1;  
    if (Build.HARDWARE.contentEquals("vbox86"))  
        kill = kill + 1;  
    if (Build.MANUFACTURER.contentEquals("unknown"))  
        kill = kill + 1;  
    if (Build.USER.equals("genymotion"))  
        kill = kill + 1;  
    if (kill > 0)  
        Log.i(TAG, "Checking: " + "This is Emulator");
```

```
    //Root detection by checking su binary  
    //there is more path you can check or add  
    String[] paths = {"sbin/su", "/system/bin/su"};  
    for (String path : paths) {  
        if (new File(path).exists()) {  
            Log.i(TAG, "Checking: " + "SU binary found");  
        }  
    }
```

```
    //set return value if require  
}
```

Code snippet to check for emulator, root, developer mode and USB debugging.

```
//Logcat Output  
I/MainActivity: Debugging Check: Developer enable  
I/MainActivity: Debugging Check: USB Debugging enable  
I/MainActivity: Checking: This is Emulator  
I/MainActivity: Checking: SU binary found
```

Logcat output during runtime.

Disabling debugging for your app is the final step before releasing your application. This simple line of code can be added into your project level build.gradle (Module:app) file under buildTypes.

```
buildTypes {  
    release {  
        ...  
        debuggable false  
        ...  
    }  
    debug {  
        ...  
        debuggable true  
        ...  
    }  
}
```

Additional rules to disabling app debug mode.

Protecting App Privacy And Content Of Your Application

Once Android application is put into background, the system will take the snapshot of current application activity which will appear on the Recent Screen.

If you are concerned about user privacy, dealing with sensitive information and security, you can prevent it from appearing in screenshots or from being viewed on non-secure display by adding this snippet of code in your activity. Results of the implementation of this code can be referred in the screenshot shown below:

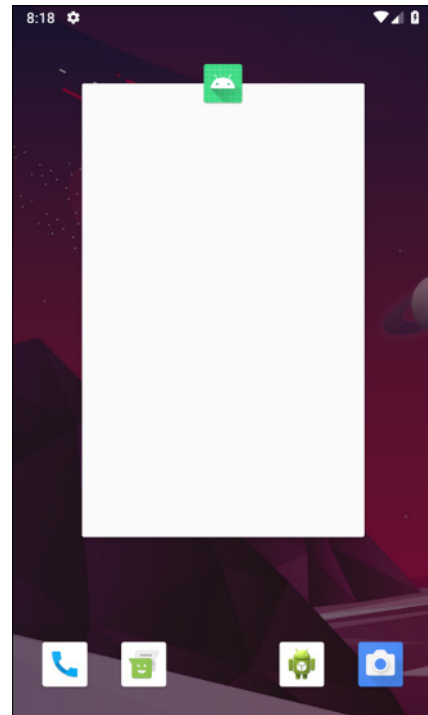
```
public class MainActivity extends AppCompatActivity {

    private static final String TAG = "MainActivity";

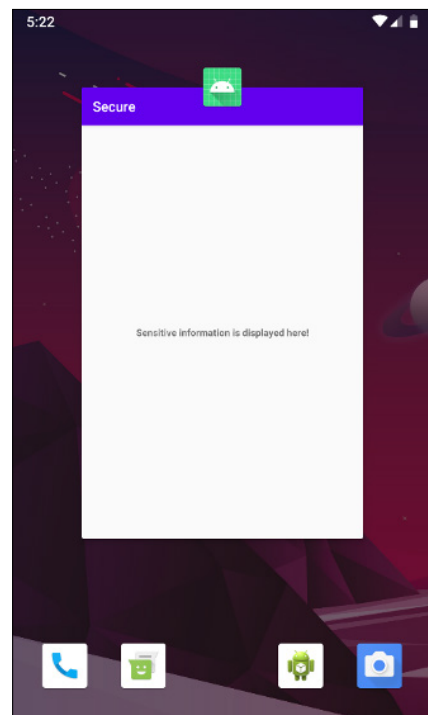
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        //blank the screenshot viewed in Overview Screen
        getWindow().setFlags(WindowManager.LayoutParams.FLAG_SECURE,
            WindowManager.LayoutParams.FLAG_SECURE);
    }
}
```

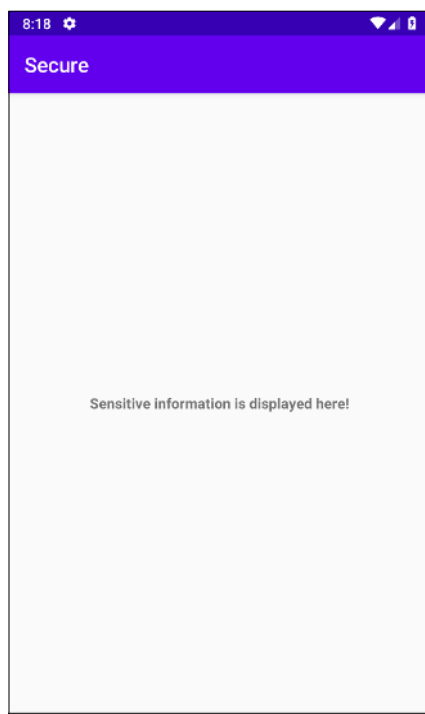
Java code snippet that blank the app screenshot Activity displayed in Recent Screen.



App screenshot displayed in Recent Screen



Without using secure flag



Current application activity that display sensitive information

Inspecting Device Integrity By Implementing SafetyNet Attestation Test

SafetyNet provides a set of features and APIs that help protect your app against security threats. SafetyNet Attestation Test is implemented in services such as Google Pay as a software standard whereby every device that uses this service is required to pass this test. SafetyNet Attestation Test API determines whether a device running your app satisfies Android compatibility tests. The API provides granular details about the device and system modification and returns Boolean values that express different levels of system integrity checking. It checks if the app is executed in a compromised, rooted, tampered or genuine device. You can explore this mechanism to further secure your app.

Checking Installer Of Your App Whether Installed From Official Store Or Sideloaded

Normally, Android device users need to install their apps from Google Play Store. For some developers, they allow their users to download their app from other sources known as sideloading or through Android Debug Bridge (ADB) command.

You can check your apps has been installed from the official store or sideloading by implementing this code snippet in your app.

```
public Boolean checkInstaller(){
    boolean result = true;
    String package_installer = getApplicationContext()
        .getPackageManager()
        .getInstallerPackageName(getApplicationContext()
        .getPackageName());

    //package name for Google Play Store is
    com.android.vending
    package_installer = getApplicationContext()
        .getPackageManager()
        .getInstallerPackageName(getApplicationContext()
        .getPackageName());

    if (package_installer != null) {
        if (package_installer.contentEquals("com.
        android.vending"))
            rtn = true;
        } else
            rtn = false;
        return rtn;
    }
}
```

Java code snippet that checks for app package installer

Installing unverified apps from unknown sources can compromise security of Android devices. Malware authors sometimes use legitimate app icon to dupe unsuspecting users to install their apps. Thus, this mechanism protects your app and user from app piracy and minimize attack vectors to your application infrastructure.

Conclusion

The above are just some of the important methods to strengthen security of your app and implement counter measures to reduce attack surfaces and its infrastructure. Even though, an average user may not be aware of these security implementation, they can be rest assured that the developer has fulfilled his or her duties to protect their app infrastructure.

References

1. *Android Developer SafetyNet Attestation API:* <https://ly.my/of7g>
2. *ProGuard Manual Introduction:* <https://ly.my/of7h>
3. *Android Developer App security best practices:* <https://ly.my/of7i>
4. *Android Developer Protect against security threats with SafetyNet:* <https://ly.my/of7j>
5. *FRIDA: Dynamic instrumentation toolkit:* <https://frida.re>
6. *CertificatePinner - OkHttp:* <https://ly.my/of7v>

Basic Approach For Onion Web Server Basic Configuration And Proof Of Concept

By | Engku Azlan Bin Engku Habib

There is really not much difference hosting on the Dark Web or Surface Web. The Dark Web is content not accessible to conventional search engines. It is not indexed and users must know the exact .onion website intended to visit, as the .onion sites do not have DNS services that resolve URL to IP addresses^[1], which also serves the purpose for anonymity.

Basically any computer that runs Tor software can host a hidden (e.g., web) service. Tor software operating on a Tor host will create a local file directory, assign a port number for the service, and generate a public-private key pair when it configures a hidden service. Tor software creates a 16-character hostname by first computing a hash of the public key of that key pair and then

converting the first 80 bits of this hash from a binary value to ASCII to make the resulting 16 characters conform to the "letter digit hyphen" requirement for the System () protocol^[1].

For the purpose of this Proof of Concept, Kali Linux was used as the Operating System of choice and nginx as the Web Server (specific server hardening was not implemented as it is meant as PoC only) and configured as virtual machine on Parallels Desktop.

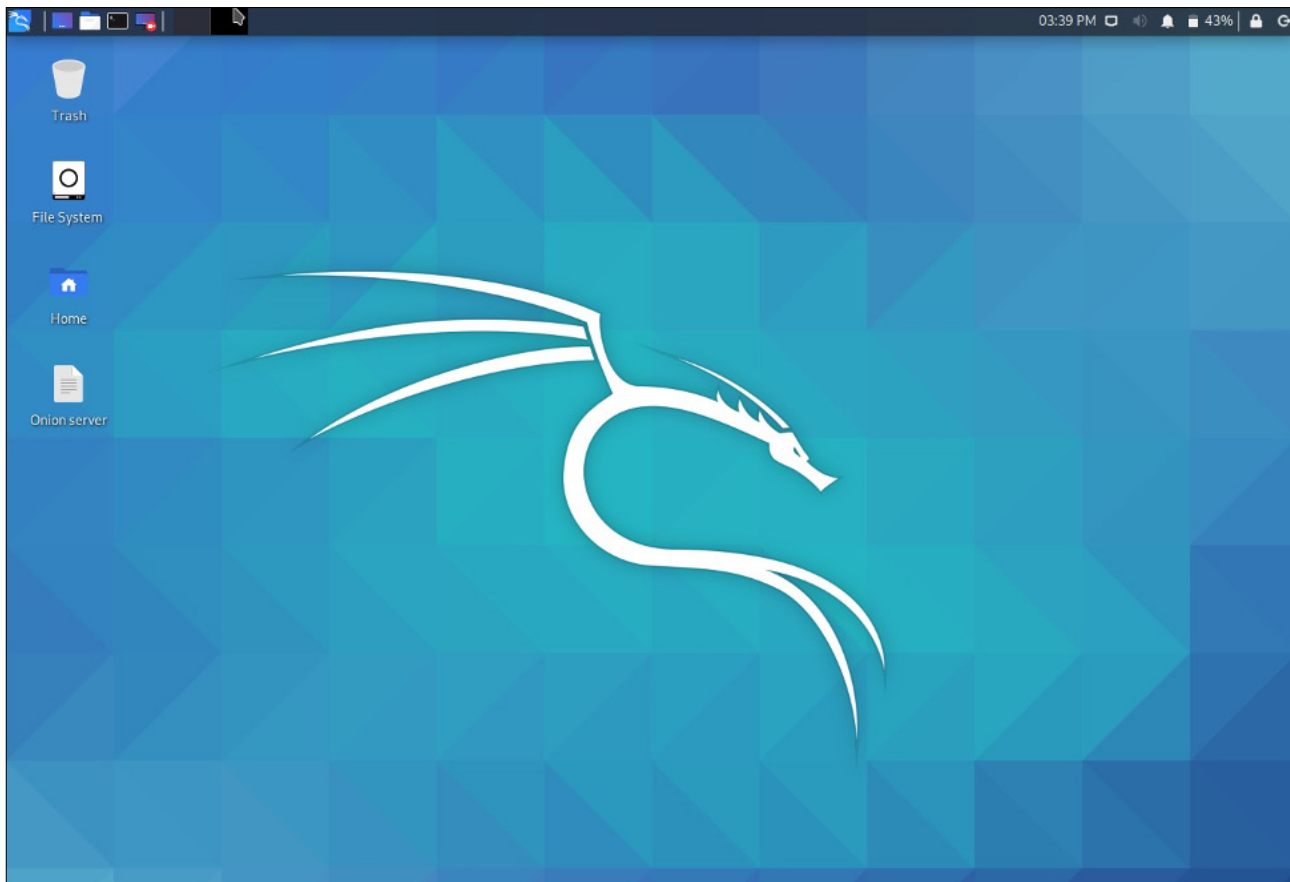
Steps Taken For Onion Web Server Installation And Configuration

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at <http://cdimage.kali.org/kali-weekly/>. Downloads are **rate limited to 5 concurrent connections**.

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit (Installer)	Torrent	2020.2	3.6G	ae9a3b6a1e016cd464ca31ef5055506cecf55a10f61b1f1ac8313eddb12ad7
Kali Linux 64-Bit (Live)	Torrent	2020.2	2.9G	e90e0cfb4bc8fc640219dba66c9fe4308c9502164e432c47a30af50ce9cb3ba2
Kali Linux 64-Bit (NetInstaller)	Torrent	2020.2	420M	def160159e12ff52fb5f4991240bd760500d7cd5ee38601a8bf35809a20f9450

STEP 1: Download the kali-linux-2020.2-installer-amd64.iso file from <https://www.kali.org/downloads/>^[2]



STEP 2: A parallel desktop was used to virtualize the Kali Linux on a MacOS Catalina with default installation options

```
john@Linux:~/Desktop$ sudo apt-get install nginx

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for john:
Reading package lists... Done
Building dependency tree
Reading state information... Done
nginx is already the newest version (1.18.0-1).
nginx set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

STEP 3: Download and install NGINX

```

john@Linux:~/Desktop$ sudo apt-get install ntpget tor
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package ntpget
john@Linux:~/Desktop$ sudo apt-get install ntpdate tor
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  tor-geoipdb torsocks
Suggested packages:
  mixmaster torbrowser-launcher tor-arm apparmor-utils obfs4proxy
The following NEW packages will be installed:
  ntpdate tor tor-geoipdb torsocks
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,661 kB of archives.
After this operation, 14.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 ntpdate amd64
  1:4.2.8p14+dfsg-2 [156 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 tor amd64 0.4
  .3.5-1 [1,943 kB]
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 tor-geoipdb a
  ll 0.4.3.5-1 [1,486 kB]
Get:4 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 torsocks amd6
  4 2.3.0-2+b1 [76.3 kB]
Fetched 3,661 kB in 3s (1,336 kB/s)
Selecting previously unselected package ntpdate.
(Reading database ... 349043 files and directories currently installed.)
Preparing to unpack .../ntpdate_1%3a4.2.8p14+dfsg-2_amd64.deb ...
Unpacking ntpdate (1:4.2.8p14+dfsg-2) ...
Selecting previously unselected package tor.
Preparing to unpack .../tor_0.4.3.5-1_amd64.deb ...
Unpacking tor (0.4.3.5-1) ...
Selecting previously unselected package tor-geoipdb.
Preparing to unpack .../tor-geoipdb_0.4.3.5-1_all.deb ...
Unpacking tor-geoipdb (0.4.3.5-1) ...

```

```

Get:4 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 torsocks amd6
  4 2.3.0-2+b1 [76.3 kB]
Fetched 3,661 kB in 3s (1,336 kB/s)
Selecting previously unselected package ntpdate.
(Reading database ... 349043 files and directories currently installed.)
Preparing to unpack .../ntpdate_1%3a4.2.8p14+dfsg-2_amd64.deb ...
Unpacking ntpdate (1:4.2.8p14+dfsg-2) ...
Selecting previously unselected package tor.
Preparing to unpack .../tor_0.4.3.5-1_amd64.deb ...
Unpacking tor (0.4.3.5-1) ...
Selecting previously unselected package tor-geoipdb.
Preparing to unpack .../tor-geoipdb_0.4.3.5-1_all.deb ...
Unpacking tor-geoipdb (0.4.3.5-1) ...
Selecting previously unselected package torsocks.
Preparing to unpack .../torsocks_2.3.0-2+b1_amd64.deb ...
Unpacking torsocks (2.3.0-2+b1) ...
Setting up ntpdate (1:4.2.8p14+dfsg-2) ...
Setting up tor (0.4.3.5-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
Something or somebody made /var/log/tor disappear.
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up torsocks (2.3.0-2+b1) ...
Setting up tor-geoipdb (0.4.3.5-1) ...
Processing triggers for systemd (245.5-3) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for kali-menu (2020.2.2) ...

```

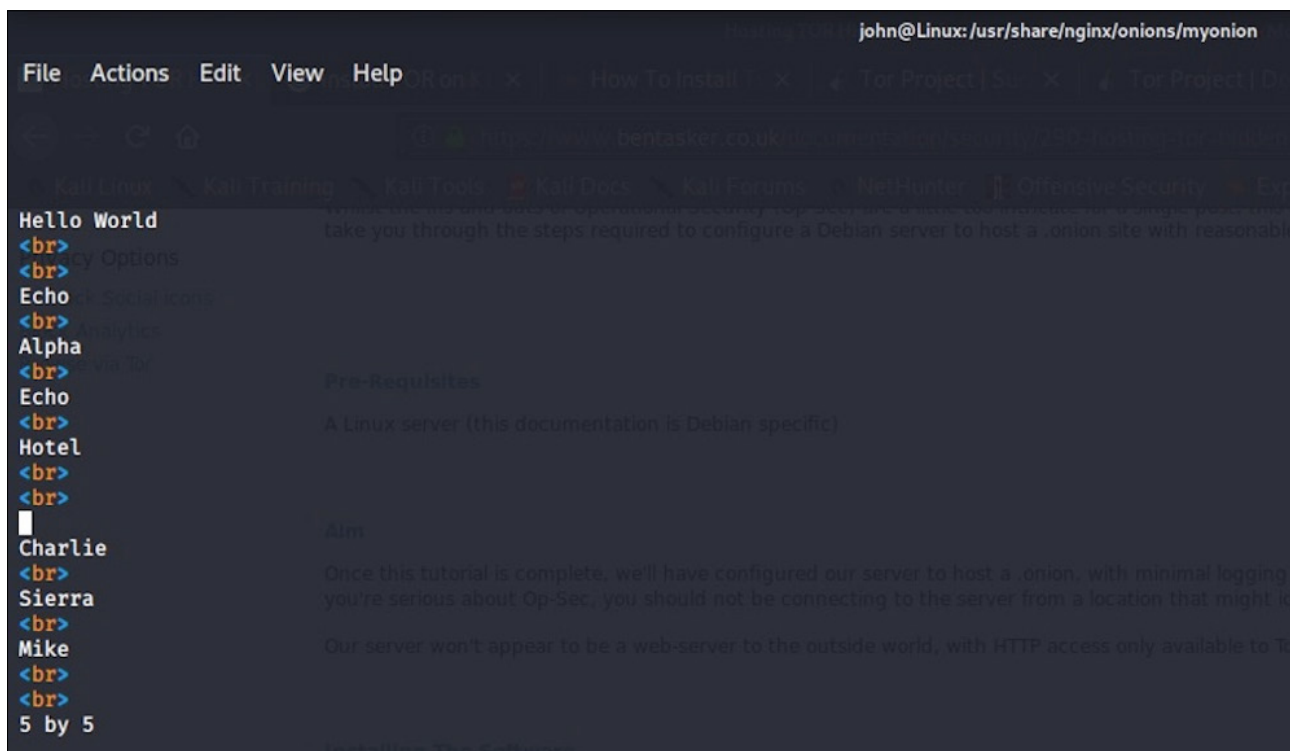
STEP 4: Download and install Tor and ntpdate, because Tor requires an accurate clock

```
john@Linux:~/Desktop$ service tor stop
bash: service: command not found
john@Linux:~/Desktop$ sudo service tor stop
john@Linux:~/Desktop$
```

STEP 5: Stop Tor service

```
john@Linux:~/Desktop$ sudo mkdir -p /usr/share/nginx/onions/myonion
john@Linux:~$ sudo chown -R debian-tor:debian-tor /usr/share/nginx/onions/myonion
john@Linux:~$ cd /usr/share/nginx/onions/myonion/
john@Linux:/usr/share/nginx/onions/myonion$ vi index.html
```

STEP 6: Create a hosting area for .onion domain



The screenshot shows a web browser window with the address bar displaying "john@Linux: /usr/share/nginx/onions/myonion". The browser has tabs for "Tor Project (10)". The page content is as follows:

```

Hello World
<br>
by Options
<br>
Echo
<br>
Alpha
<br>
Echo
<br>
Hotel
<br>
Charlie
<br>
Sierra
<br>
Mike
<br>
5 by 5
  
```

STEP 7: Edit the index.html with some sample text to indicate that it is not the default web page and as a proof when it is viewed using a Tor network


```
john@Linux:/usr/share/nginx/onions$ sudo chmod 777 myonion
john@Linux:/usr/share/nginx/onions$ ls -al
total 12
drwxr-xr-x 3 root      root      4096 Jun  6 10:52 .
drwxr-xr-x 5 root      root      4096 Jun  6 10:52 ..
drwxrwxrwx 2 debian-tor debian-tor 4096 Jun  6 10:52 myonion
```

STEP 8: Change the Read permission in the directory to allow any users to access the index.html file

```
john@Linux:~$ cd /etc/nginx/sites-available/
john@Linux:/etc/nginx/sites-available$ vi default
```

```
server{
    listen 127.0.0.1:9070;
    root /usr/share/nginx/onions/myonion;
    index index.html index.html;

    # server_name foo.bar; # We'll amend this later

server_name acbstizvngo5qcgxy375bymgqrea7t6ayw6ysz7uykmpqd7sucfd22yd.onion;

    location / {
        autoindex on;
    }
}
```

STEP 9: Configure the correct document root in the file etc/nginx/sites-available/default

```

user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf

events {
    worker_connections 768;
    # multi_accept on;
}

http {

    ##
    # Basic Settings
    ##

    server_tokens off;
    sendfile on;
    tcp_nopush on;
    tcp_nodelay on;
    keepalive_timeout 65;
    types_hash_max_size 2048;

```

STEP 10: Locate the http block and add the highlighted line at etc/nginx/nginx.conf

```

john@Linux:/etc/nginx$ sudo service nginx start
john@Linux:/etc/nginx$ sudo wget --header="Host: foo.bar" http://127.0.0.1:9070/
--2020-06-06 11:13:31-- http://127.0.0.1:9070/
Connecting to 127.0.0.1:9070... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16 [text/html]
Saving to:

index.html
100%[=====]
16 --.-KB/s in 0s

2020-06-06 11:13:31 (1.42 MB/s) - saved [16/16]

```

STEP 11: Restart the NGINX service and the WGET command

```
john@Linux:/etc/nginx$ cd /etc/tor
john@Linux:/etc/tor$ vi torrc
```

```
SocksPort 0 # what port to open for local application connections
SockslistenAddress 127.0.0.1 # accept connections only from localhost

RunAsDaemon 1
DataDirectory /var/lib/tor

HiddenServiceDir /var/lib/tor/myonion/
HiddenServicePort 80 127.0.0.1:9070
```

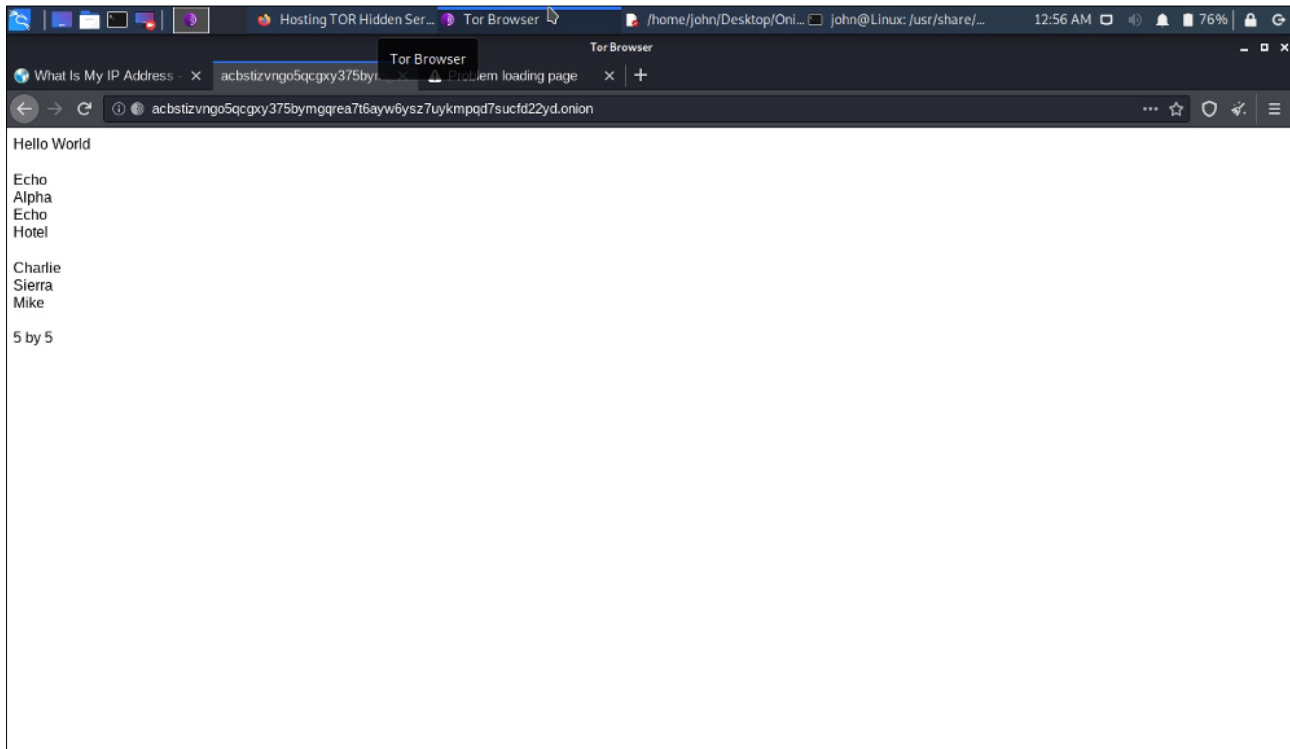
STEP 12: The next step is to configure the Tor client and inform it to provide a hidden service at etc/tor/torrc

```
john@Linux:/etc/tor$ sudo service tor start
john@Linux:/etc/tor$ sudo cat /var/lib/tor/myonion/hostname
acbstizvngo5qcgxy375bymgqrea7t6ayw6ysz7uykmpqd7sucfd22yd.onion
```

STEP 13: : Launch the Tor service and verify if the directory /var/lib/tor/myonion has been created. The procedure should work and display the .onion URL

```
john@Linux:~$ cd Downloads/
john@Linux:~/Downloads$ ls
tor-browser_en-US  tor-browser-linux64-9.5_en-US.tar.xz
john@Linux:~/Downloads$
john@Linux:~/Downloads$ cd tor-browser_en-US/
john@Linux:~/Downloads/tor-browser_en-US$ ./start-tor-
browser.desktop
Launching './Browser/start-tor-browser --detach'...
john@Linux:~/Downloads/tor-browser_en-US$ cd
john@Linux:~$ sudo service tor start
[sudo] password for john:
john@Linux:~$
```

STEP 14: Download Tor Browser^[3] from <https://www.torproject.org/> and install it on the server for final verification.



STEP 15: From the Tor browser, try to access “acbstizvngo5qcgxy375bymgqrea7t6ayw6ysz7uykmpqd7sucfd22yd.onion” (without quote).and as a proof when it is viewed using a Tor network

The site was able to be viewed from the Tor network and verified the Tor site configuration was successful.

From the Proof of Concept shown, one can conclude that setting up an .onion website does not require extra effort compared to creating and running a basic website. Therefore, any tech savvy person could set it up for whatever purpose— whether it’s good or bad. Given the nature of a Tor network, it takes a lot of time, effort and technical expertise to find the culprit behind any malicious activity conducted over such network.

As for the .onion URL, one might argue that some sites also resemble the Surface Web URL. Did you know Facebook has a site accessible via the dark web? facebookcorewwi.onion allows access to Facebook through the Tor protocol, using its .onion top-level domain. It took Facebook extra effort and technical expertise to create this URL^[4], whereby it involved hashing method to achieve the objective.

Due to the way that the URLs for .onion are

configured, using the 16-character hash generated when a public key is created as the URL, has led to allegations that Facebook was able to brute-force its way into selecting the public key it desired.

According to Tor project leader, Roger Dingledine,^[5] Facebook perform vanity name for the first half of the .onion URL (“facebook”), which is only 40 bits so it was possible to generate keys over and over until the user got some keys whose first 40 bits of the hash matches the string he or she wanted.

Facebook had some keys whose name started with “facebook”. As such, Facebook looked at the second half of each of them to decide which one would be most memorable for the second half of the name as well. “corewwi” was concluded as the best addition to first half of the .onion URL (“facebook”).

Facebook’s Tor network address – facebookcorewwi.onion – is actually a backronym that stands for *Facebook’s Core WWW Infrastructure*^[6]

References

1. <https://www.icann.org/news/blog/the-dark-web-the-land-of-hidden-services>
2. <https://www.kali.org/downloads/>
3. <https://www.torproject.org/thank-you/>
4. <https://www.zdnet.com/article/facebook-sets-up-hidden-service-for-tor-users/>
5. <https://lists.torproject.org/pipermail/tor-talk/2014-October/035412.html>
6. <https://en.wikipedia.org/wiki/Facebookcorewwwi.onion>

Eradicating Fake News In Malaysia

By | Mohamad Hafiz Bin Rahman

Introduction

Fake news is described as misinformation or disinformation to manipulate news content to deceive readers. Such content is usually created to either skew people's opinions, push a political agenda or cause uncertainty. Fake news has become a nightmare for everyone including the Government, law enforcement authorities, politicians and the public but can be lucrative to media outlets.

The spread of fake news is cause of great concern for all. Social media makes it easy to spread fake news. Most people are less inclined to verify news shared by friends within their social network. As a result, fake news has become the biggest problem not only in Malaysia but around the world.

This article will discuss the strategies and methods to combat fake news. It is important to

recognize fake news and stop its dissemination by not spreading them to your family and friends.

1.0 How Does Fake News Spread

Fake news can spread through social media channels such as Facebook, Instagram, Twitter, and WhatsApp because these platforms allow almost anyone to publish their thoughts or share stories in online communities without any editorial approval. Most people do not check the source of news before they share it. As such, this can lead to fake news spreading quickly or even going viral. Sometimes an individual's opinions and beliefs are influenced by what they read and who they interact with. As a result, readers end up being divided into groups according to their orientation and beliefs.

At the same time, it has become harder to identify the original source of any news story, and this

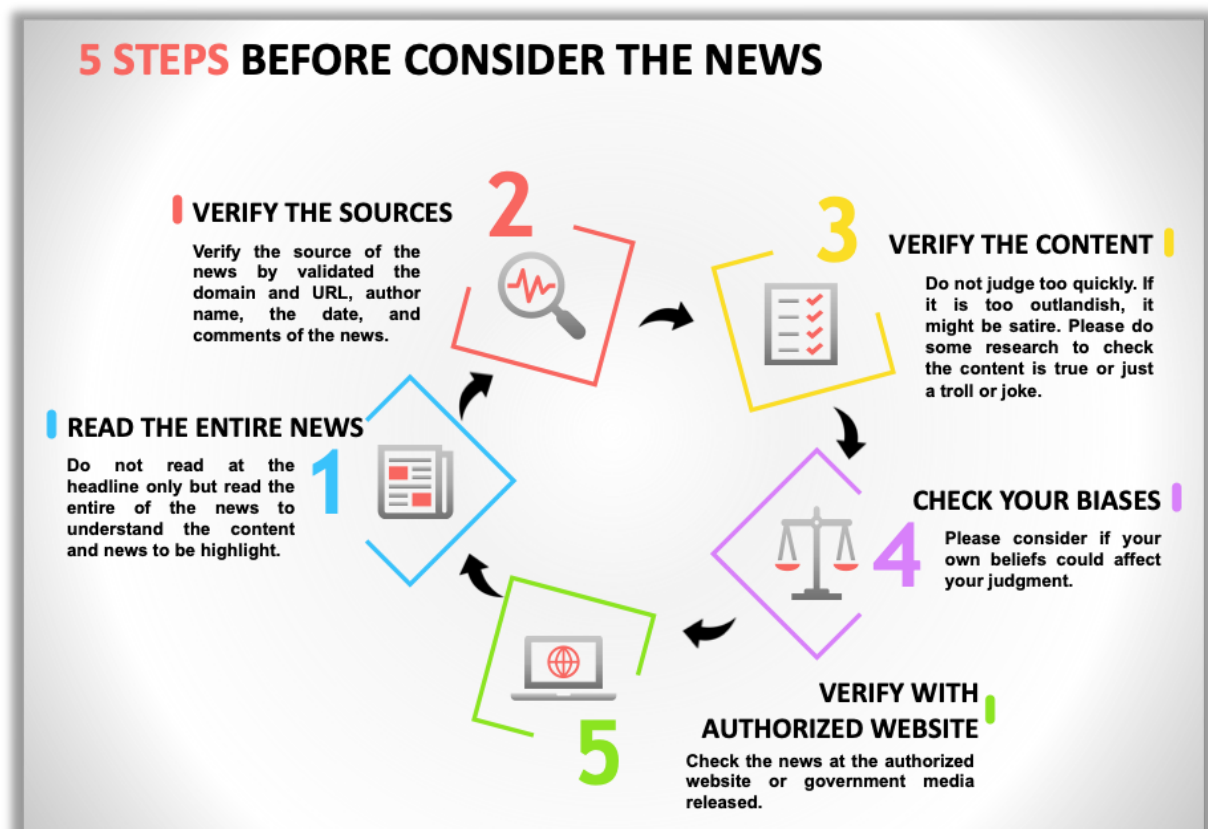


Figure 1: How To Evaluate The News

can make it difficult to assess the accuracy of the news. Fake news is not just pervasive on social media, but it can also spread through traditional word of mouth among the community.

The Edelman Trust Barometer 2019 report revealed that 82% of Internet users in Malaysia were concerned about the false information and fake news being weaponised, but at the same time, 48% of them trust the social media platform.

2.0 Check The News Quality

While there are many resources available to check news quality, one of the simplest steps you can perform a check as shown in **Figure 1**.

2.1 Read The Entire News

Read beyond the headline. If your attention was drawn to a sensational headline, read a little further before deciding to pass along the new information. Even in legitimate news stories, the headline does not always tell the whole story. But fake news may include many revealing signs in the text, especially attempts to be satirical.

2.2 Verify The Source

Check and validate the sources of the news:

1. Validate the domain and URL to make sure the content comes from authorized sources or websites.
2. Check the author's name and do some research about the author's background to ensure the identity of the author is real.
3. Check the author's previous articles on the topic to make sure he / she is credible.
4. Check published date of the news article. Not all news is fake, but rather distortion of real events over different periods of time. This irresponsible act takes a legitimate news story and manipulates the content or claim to make it a current event although it happened a long time ago.
5. Use Google reverse image or

TinEye to find where a potential image appears online if you are not sure.

6. Check the supporting sources and validate them as well.

2.3 Verify The Content

Check the entire news article and ensure it's supported by facts or statistics. It must make sense and sound logical. Sometimes fake news is created just as a joke or to troll someone.

2.4 Check Your Biases

This is difficult to address but prejudice and biasness could affect your stand on an issue. Try to be objective when you read the news to understand the real facts.

2.5 Verify With Authorized Website

Refer to an authorized websites that will enable you to verify the facts of the news or viral news. For example, Sebenarnya.my was launched for the public to check and report unauthenticated news items. It was developed by Malaysian Communications and Multimedia Commission (MCMC) to combat the spread of false news. This is a one-stop centre and online portal for Malaysians to verify news which is spreading through the social media platforms, blogs, websites, and online news.

Through this portal, it is hoped that online fake news that affect our community and nation will be addressed effectively.

3.0 Take Action And Combat Fake News

We have to work together to mitigate the spread of the fake news in our society by reporting them to the authorities. Always remind ourselves that spreading fake news will not yield good results but complicate the situation even more.

Here are some tips to combat fake news:

3.1 Develop a critical mindset

Critical thinking is a key competency in media and information literacy, and we need to advocate its importance. Evaluate the news that you read and if it sounds too good or sometimes too bad to be true, it probably is. Keeping your emotional reaction to these stories in check is also important. Instead, take a logical and analytical approach to what you see and hear.

Ask yourself, "Why was this story written? Is it to convince me of a certain point of view? Is it selling me a particular product? Or is it trying to get me to click on different websites? Am I being triggered? Or this is just a trick or a joke?"

3.2 Think before you share

Read the entire article or news before deciding whether or not to share it. Think about the impact if you do.

3.3 Examine the evidence

A reliable news report should contain plenty of information – such as expert interviews, survey results, official statistics as well as accurate, reliable, and corroborated eye-witness accounts of on-scene people. If these are missing, then question it.

3.4 Do not share if not sure

You can do your part in stopping the spread of fake news by not spreading it further on social media through email or online conversation. Use your common sense. Bear in mind that fake news is meant to manipulate your hopes and fears. Consider if your own beliefs could affect your judgment.

question is whether the people care enough to use those tools or not.

Editors should play a critical role by producing trustworthy and high-quality information to the public. Content consumers must be well educated about how news information propagates in today's world so that they are better able to distinguish credible sources and stories from their social circle.

Under Section 233 of the Communications and Multimedia Act (CMA) 1998, anyone convicted of spreading fake news liable to legal action that carries a fine of not more than RM50, 000 or imprisonment of not more than one year or both. This act shows that Malaysia is seriously committed to fighting fake news that adversely affects our society.

References

1. *Edelman Trust Barometer Malaysia Results (Rep.).* (2019). Retrieved from https://www.edelman.my/sites/g/files/aatuss366/files/2019-05/2019_Edelman_Trust_Barometer_Malaysia_Results.pdf
2. *Keepin' It Real: Tips & Strategies for Evaluating Fake News: Home.* (n.d.). Retrieved August 26, 2020, from <https://libguides.lmu.edu/c.php?g=595781>
3. *Lu, D.* (2019). *Fighting fake news.* *New Scientist*, 244(3255), 9. doi:10.1016/s0262-4079(19)32089-5
4. *Malaysia, Attorney General's Chambers of Malaysia.* (n.d.). *LAW OF MALAYSIA ACT 855 COMMUNICATIONS AND MULTIMEDIA ACT 1998.* Retrieved from <http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20589.pdf>
5. *Robertson, E.* (2020, May 11). *How to Spot Fake News.* Retrieved August 26, 2020, from <https://www.factcheck.org/2016/11/how-to-spot-fake-news/>

Conclusion

As a responsible Internet user, we must look at every aspect of the news before simply sharing it with our family and friends. There are so many tools which can be used for verification. The

SSL Certificate

By | Mohd Nor A'kashah Bin Mohd Kamal, Nur Fazila Binti Selamat, Nurul 'Ain Binti Zakariah & Mohd Faisal Bin Abdullah

What Is An SSL Certificate?

Secure Socket Layer (SSL) certificate is also known as digital certificate. It creates a secure link between a website and visitor's browser to reduce the risk of sensitive information being viewed by others such as passwords, financial information, user's personal data, medical records and proprietary information. It authenticates the identity of a website to guarantee visitors that they are on a genuine site.^[1] Normally, SSL certificates are used for credit card transactions, data transfer and logins as well as securing social media sites.^[2]

How to identify if a website has SSL certificate? ^[1]

1. Padlock symbol to the left of the URL
2. URL starts with https instead of http
3. A trust seals
4. A green address bar (if the website uses Extended Validation (EV) SSL certificate)

How Does SSL Certificate Work?

This Presumes That SSL Has Already Been Issued By SSL Issuing Authority.



Types Of SSL Certificate

There are three types of SSL certificate which are:

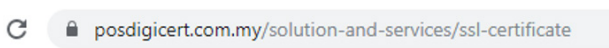
1. Extended Validation (EV SSL) Certificate

- This certificate is the most trusted and secure solution used by world's leading online businesses. To obtain this certificate, the certified authority (CA) will verify details such as company's business registration, checking the information with a third-party database, and verifying the applicant's identity. If the browser's URL bar turns green and has a padlock, user will know that the company is listed under EV SSL certificate.

- Examples of websites:

Organization	URL
Maybank Malaysia	https://www.maybank2u.com.my/home/m2u/common/login.do
Malaysian Communications and Multimedia Commission (MCMC)	https://www.mcmc.gov.my/
Apple	https://www.apple.com/my/
Hong Leong Bank	https://www.hlb.com.my/

- Example for EV SSL certificate from browsers :



EV SSL certificate in Chrome browser.



EV SSL certificate in Internet Explorer browser.

2. Domain Validated (DV SSL) Certificate

- DV SSL certificate is the lowest level of authentication used to validate SSL certificates. This certificate is commonly used by cybercriminals because it is so easy to obtain. They can also make a website look more secure than it actually is.^[3] Even though the information is encrypted, the receiver on the other end is still a question mark.^[4] DV certificate is most suitable for blogs or simple websites.
- Examples of websites:

Organization	URL
Shopee	https://shopee.com.my/
Mudah.com	https://mudah.com/
Digi	https://www.digi.com.my/
redone	https://www.redone.com.my/

- Example for DV SSL^[4] certificate from browsers:



DV SSL in Chrome



DV SSL in IE

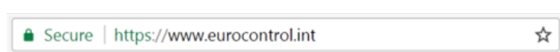
3. Organization Validated (OV SSL) Certificate

- OV SSL certificate is a certificate that confirms the existence of organization. It has a moderate level of trust. An OV certificate tells a customer that the website they are browsing belongs to a business. It is suitable for websites that do not deal with sensitive transactions. This certificate can be obtained within minutes only.

a. Examples of websites:

Organization	URL
Lazada	https://www.lazada.com.my
Trivago	https://www.trivago.com.my/
Malaysiakini	https://www.malaysiakini.com
Lowyat.net	https://www.lowyat.net/
Maxis	https://www.maxis.com.my

b. Example of OV SSL^[4] certificate from browsers:



OV SSL in Chrome



OV SSL in IE

How To Differentiate OV, DV And EV Certificates?

Users can differentiate these SSL certificates by clicking on the padlock symbol on the URL bar, then click on the certificate policy. The information of the certificate of the website will be given.^[6]

Type	Policy Identifier
Domain Validated	2.23.140.1.2.1
Organization Validated	2.23.140.1.2.2
Extended Validated	2.23.140.1.1

Conclusion

A SSL certificate is no longer luxury, but a necessity for every website. With the rise of cybercriminal activities, the validity of a website is important to customers. It is also compulsory for a website to install SSL certificate to receive payments as compliance to payment card industry (PCI) to ensure the transactions are safe and to prevent any loss of data.

References

1. Everything You Need to Know About SSL Certificates. Retrieved from https://www.verisign.com/en_US/website-presence/online/ssl-certificates/index.xhtml
2. What is an SSL Certificate? Retrieved from <https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/>
3. What is an SSL Certificate? Retrieved from <https://us.norton.com/internetsecurity-how-to-ssl-certificates-what-consumers-need-to-know.html>
4. What Are The Different Types of SSL Certificates? Retrieved from <https://www.globalsign.com/en/ssl-information-center/types-of-ssl-certificate/>
5. What is the difference between Secure and Not Secure? Retrieved from <https://www.exabytes.my/web-security/ssl>
6. Domain Validated vs. Organization Validated SSL. Retrieved from <https://www.globalsign.com/en/ssl-information-center/telling-dv-and-ov-certificates-apart/>

The Critical Role of Security And Authorization In SAP System

By | Muhammad Nazmie Bin Mat Nasir

Introduction

System Application Products in Data Processing (SAP) is a global provider of enterprise-class information system with proven success supporting large global manufacturing and distribution enterprises. SAP utilizes ERP software applications to improve the performance of organizations' resource planning, internal control and operational control. This multi-module application software integrates activities across functional departments, from product planning, parts purchasing, internal control, product sales and distribution, plant maintenance, quality control, human resource also as finance and controlling (Atul R. Junnarkar¹, 2017).

The control and reduction of risks will be an important focus in Information Technology in the coming years. Having powerful control over security and authorization means new requirements are needed to secure processes, systems, and users of an organization. Security and Authorization is part of SAP's methods in controlling and protecting its system, transactions and programs from unauthorized access. Security and Authorization are defined as an authorization security mechanism to determine access levels or user privileges associated with system resources including files, services, computer programs, data and application features (Seneviratne, 2018). This is often the default method of granting or denying access to a network resource which allows the user access to various resources based on the user's identity. It helps to manage the users within SAP system such as role's creation, profile creation, role and profile assignment, and authorization assignment.

Types Of Standards Administration Security And Authorization Roles

There are several types of standard administration roles to ensure that security

and authorization of the SAP system is secure. Through the delegation and distribution of tasks, it will be more effective in managing the roles whereby only an authorized individual can make changes in the system. The types of standard administration roles include the following:

Super administrator –

The super administrator role has full access to the system which includes all rights for all subjects in the portal's content directory. It also provides full access to all tools of the content, system and user administrators. The account password of super users must be kept in a safe place by a security administrator and must be changed each time after use. This role should be strictly controlled and monitored to ensure access is only confined to its proper purpose.

Content administrator –

The content administrator role allows for maintenance of portal content, including the option to define portal roles, work sets, pages and iViews. This role includes responsibilities in editing the portal content such as maintenance of authorization and object properties.

System administrator –

System administrator is responsible for maintaining ongoing reliability, performance and support of the SAP application such as system configuration, transports, authorizations, monitoring and portal display. The system administrator will perform troubleshooting for hardware, software and system problems when an error occurs.

User administrator –

User administrator is responsible for assigning and managing user access to the system such as creating new users, assigning roles to the users, mapping the portal user name to potentially deviating user IDs in backend applications, user replication with external directories, group administration, and others. The selection of right role will ensure that the access and actions allowed for transactions in the system are accurate and meet the work requirements. For example, a new user that needs to use the system must request the role that is related to his/her job functions and responsibilities. The

access given is limited based on the position of the user. This will ensure that the system is secure from unauthorized users.

Approach In SAP Security Design

The following are the approach taken in SAP security design:

1. Define Segregation of Duties, Policies and Ruleset Design

Segregation of Duties (SoD) is a first step in implementing SAP application security. It will identify the problems and corrective actions to be taken in identifying necessary business processes to ensure the risk of errors can be prevented. SoD policies classify several risk levels which are critical, high, medium, and low. Critical risk means the risk cannot be mitigated and requires remediation to avoid impact to business operation or company value. High risk means that there is financial risk impact including its profit and loss and image of the organization. Medium risk warrants financial statement reclassification and non-compliance with internal policies. Low risk costs more to mitigate than the cost of the risk to the business.

2. Initial Role and User Design

The initial role and user design is designed to analyse individual tasks and functions that may be used on the SAP transaction system once the system goes live. The SAP security team will group all the transactions into the start stages of SAP roles according to their functions and tasks of every department. At this stage, the role templates are documented, detailing the role technical names and underlining transaction codes. Each department will have their own authorization to access the system in doing a transaction.

3. Role Build and User Assignment

The roles can be built on SAP after getting approval and directly assigned to the end users. There are two phases to start the technical design which is needed to build “master roles” or “template roles” including group transactions. When building master roles, close coordination is required between the system integrator and BPOs so that all standard and custom SAP transactions and objects will be used as part of the role

design. Apart from that, one needs to create “child” roles as the security restrictions are applied for example company code and cost centre limitations. This can ensure more restrictive access and increased transparency regarding the authorization is given to a user. Role assignment is a critical part in designing SAP application security due to the different restrictions applied to the users. For example, some users may need the access to one, multiple or all company codes or cost centres, in case of shared services departments.

4. Role and User Access Risk Analysis

This stage requires SAP security monitoring solution to perform periodic role and user analyses to see if the newly designed SAP roles are following with SoD policies. Risk analyses should be run on a periodic basis, especially after unit and integration testing, which is when the SAP system design are going to be updated to accommodate process improvements. To make sure there's no error hits when go live, the SAP security provisioning process must be designed and implemented. This needs SAP security teams to do a risk simulation in SAP access control to granting user access or modifying a task.

5. Security Testing and Go-Live Preparation

This is the most critical part which is needed to conduct a User Acceptance Testing (UAT) for all transactions to minimize any potential issues when the system goes ‘live’. All the roles will be executed by the SAP security testing to ensure transactions can be accessed with all the requirement and authorization objects completed for example display, update and post financial transaction. This process of testing should be done from end to end before moving and assigning any new roles in the production environment. In addition, the final UAT process must be done in the quality assurance environment with the new SAP roles to be used in the production environment. This will ensure that all errors are fixed and can be accessed by the users when it goes live.

6. Move to Production and Support

The new SAP roles can be moved to the production environment once testing is completed. While moving new roles to production, it is essential to monitor how well UAT perform as it could still encounter some issues during live stage. Thus, not only do security and authorization team needs to resolve the problems on a timely basis, but they also need to run access risk reports to see if security changes will lead to SoD or other access risk. During live stage, the power users will be temporarily used to stabilize the system and ensure users able to perform their job functions during and after live. It is important to get rid of the temporary access that has been used once the system stabilises to adapt a new role that has been deployed.

References

1. https://www.protiviti.com/sites/default/files/united_states/insights/designing-sap-application-security-protiviti.pdf
2. <https://www.guru99.com/what-is-sap-definition-of-sap-erp-software.html>
3. <https://www.irjet.net/archives/V4/i2/IRJET-V4I2413.pdf>
4. <https://medium.com/@senuseneviratneit/oauth-2-0-framework-5cc1c15dec08>

Conclusion

The SAP system's security and authorization plays an important role in protecting and controlling SAP system transactions. SAP security may be a balancing act that involves all the tools, processes, and controls set as to limit what users can access within an SAP environment. This helps to make sure the users can get the access that they require which is only related to their job scope and beyond that. This method will ensure the business process is more effective and efficient as the role's creation to access the system is assigned appropriately to the respective users. The risk to the organization can be minimized and therefore the data will be highly protected from theft and unauthorized access.

Quick Response (QR) Codes

By | Mohammad Zailani Bin Shato, Mu'az Bin Ahmad, Ahmad Amieruddin Afiq Bin Rahmat, Mohd Masri Bin Abd Kamad & Mohd Azlan Bin Mohd Nor

Introduction

Today, millions of people are utilizing QR codes as an attendance management solution. In Malaysia, the MySejahtera app adopts QR Code features. This application was developed by the government to control the movement of Malaysians while reducing the COVID-19 infection. Most of the latest smartphone models have an integrated QR code reader in the phone camera such as Samsung's Bixby Vision and Apple's iOS 11 operating system. For smartphones which do not have a QR Code reader, there are plenty of alternatives available in the app stores for download with just the touch of a button.

What Is A QR Codes?

Before we learn how to generate it, let's make sure what is a QR Code. QR Code stands for Quick-Response codes, a type of bar code that consists of a printed square pattern of small black and white squares that encode data which can be quickly readable by a smartphone and computer system. The black and white squares represent numbers from 0 to 9, letters from A to Z, or characters in non-Latin contents, for example, Japanese kanji.

The QR Code is a two-dimensional version of a barcode containing data, which is able to convey specific information with the scan of a mobile device.



Example of a QR Code

How Do QR Codes work?

The structure of a QR Code

The present day QR Code consists of seven parts. Each part makes such a pixel design that seems to be like a crossword puzzle. It passes on certain data through the Code. For example, the print course, timing, blunder resistance, and empty spaces to separate the code from what surrounds it.



1. Positioning Detection Markers

Located at three corners of each code, it allows a scanner to accurately recognize the Code and read it at high speed, while indicating the direction in which the Code is printed. They essentially help quickly identify the presence of a QR Code in an image and its orientation.



2. Alignment markings

Smaller than the position detection markers, they help straighten out QR Codes drawn on a curved surface. And the more information a Code stores, the larger it is and the more alignment patterns it requires.



3. Timing Pattern

Alternating black/white modules on the QR Code with the idea of accurately helping configure the data grid. Using these lines, the scanner determines how large the data matrix is.



4. Version Information

With currently 40 different QR Code versions, these markers specify the one that is being used. The most common ones are versions 1 to 7.



5. Format Information

With currently 40 different QR Code versions, The format patterns contain information about the error tolerance and the data mask pattern and make it easier to scan the Code.



6. Data and Error Correction Keys

The error correction mechanism inherent in the QR Code structure is where all your data is contained, also sharing the space with the error correction blocks that allow up to 30% of the Code to be damaged.



7. Data and Error Correction Keys

The error correction mechanism inherent in the QR Code structure is where all your data is contained, also sharing the space with the error correction blocks that allow up to 30% of the Code to be damaged.

Type Of QR Codes

In generating the QR Codes, there are two types of codes which can be created:

i. Static QR Code

The destination site URL is placed directly into the QR code and cannot be modified.



Static

Direct to URL
<https://www.cybersecurity.my>



<https://www.cybersecurity.my>

ii. Dynamic QR codes

Use a short URL for the QR code which then re-directs users to the destination site URL. This short URL works like an intermediary that connects the code with the data. After the QR code has been generated, it still can change the URL.



Dynamic

Short URL - able to change
<https://qr.go.page.link/vSwXz>

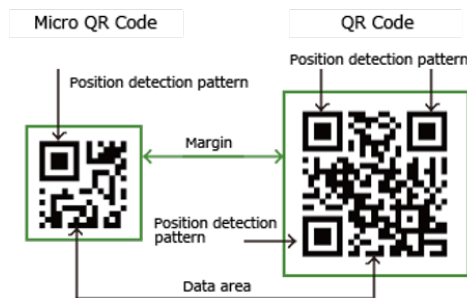


<https://www.cybersecurity.my>

Others Custom Of QR Codes

1. Micro QR Codes

Micro QR code is a smaller version of the QR code standard for application where symbol size is a limitation. It requires a smaller space and uses smaller amounts of data.



Comparison of Micro QR Codes and Normal size QR Code.

2. iQR Codes

In contrast to the square shape of a typical QR Code, iQR Codes use a rectangular shape. iQR Codes can hold both smaller and larger data amounts than traditional and micro QR Codes due to this shape.

iQR Code



iQR Code
(Rectangular type)



Example of iQR Code

Advantages And Disadvantages Of QR code

Advantages

QR codes can be utilized for almost everything. Often, they help both consumers and businesses. For example, a start-up company can save money and advertisement costs by directing a QR code to its website or URL. A customer can search this QR code and this allows the information to be saved for future reference. Another important advantage is that QR Codes can cater for multiple types of marketing sources. QR codes acts as

the link and it also introduces consumers to other types of ads that the QR code has done for company or service. This maximizes exposure and can potentially generate revenue.

Disadvantages

Many people are still not aware of QR codes. Although QR codes are found everywhere from plant specimen labels to library catalogues, there is still a large demographic across the society who still do not know what it is.

This poses a problem as companies and businesses use the QR code to advertise information that a potential customer might be interested in, but if the customer doesn't know how to find the information, then they may not buy the product or service and that could lose thousands of dollars in business. One way of addressing this problem is knowledge of the products. Not only should businesses be using QR codes for its obvious benefits and advantages, but they should also be directing customers on where and how to get the information.

The most obvious disadvantage is that a QR code must be scanned with a mobile device or smartphone. Without a smartphone, users will not be able to scan the code and thus, unable to get information. QR codes also require an Internet connection.

References

1. *QR Codes 101: A Beginner's Guide*, <https://www.qr-code-generator.com/qr-code-marketing/qr-codes-basics/>
2. *What Is A QR Code And Why Do You Need One?* <https://searchengineland.com/what-is-a-qr-code-and-why-do-you-need-one-27588>
3. *How QR Codes Work and Their History*, <https://www.qr-code-generator.com/blog/how-qr-codes-work-and-their-history/>
4. *What is a QR Code?* <https://www.camcode.com/asset-tags/what-is-a-qr-code/>
5. *Advantages and Disadvantages of QR code* <http://www.estateqrcodes.com/advantages-disadvantages.html>

Implementation Of Cyber Range For Cyber Defence Strategy

By | Mohamad Firham Efendy Bin Md Senan, Hafizah Binti Che Hasan & Muhammad Fadzlan Bin Zainal

Introduction

Cyber defense comprises activities that measure the effectiveness of mitigating a cyber-attack. A good cyber defense strategy is to understand a cyber-attack from multiple points of view. The complexity in cyber security threats has also been increasing over time. Cyber attackers are always one step ahead because they are equipped with advanced technology and a variation of techniques, which makes them much more organized and lethal. Cyber security awareness is therefore required at all levels ready to defend against these cyber-attacks. Rigorous cyber security training is required in order to gain a thorough understanding on how a cyber-attack works.

A cyber range allows companies to simulate real-world cyber-attack scenarios. It is mostly used for cyber warfare training and cyber technology development ^[1]. However, it can also be used for digital forensic analysis. A simulation is conducted to understand how an incident occur without resorting to a real environment platform. Cyber range can be used to understand the tactics, techniques, and procedures to be implemented in a complex networking system environment. Cyber range also helps to define the respective functions and roles of cyber security experts in various scenarios.

2. How Does Cyber Range Works?

Cyber ranges are used to train and strengthen the skills of cyber security engineers. These virtual environments simulate new and complex challenges to improve the protection and efficiency of cyber infrastructures and IT systems in the real world. While Cyber ranges may operate in either a physical or virtual environment, they can mimic even the most complicated networks used by government, commercial organizations or the military. In order to provide a realistic training environment and to utilize the entire gamut of cyber defense, a Network Traffic Generator within a Cyber

Range can generate legitimate and malicious traffic which are realistic and varied. ^[2].

Cyber ranges that are used for training and practice mostly operate on a dueling team basis, i.e. red versus blue team environment. With the red team targeting the virtual network; while the blue team securing the infrastructure. In general, a white team will be required to ensure that some elements of the cyber range operate as planned for training purposes as they will be used to teach how to attack and defend.

3. Implementing Cyber Defense

Cyber Defense is a computer network defense mechanism which responds to actions, protects critical infrastructure and provides information assurance for organizations, government entities and related networks^[3]. A Cyber Defense team will help strengthen and defend their organization. With the necessary resources and skills in place, steps and measures can be taken to remediate and eradicate threats.

Cyber Range is an ideal platform that helps develop the capabilities of cyber defense professionals. It enables a team to work together, discuss and make decisions that affect the entire cyber defense chain ^[4]. In an exercise, security teams are given 21 different types of attack with various real-world scenarios. This is designed to prepare and sharpen their skills in hyper-realistic cyber-attacks while running massive performance tests without suffering any adverse effects.

Table 1 shows the type of attacks provided.

Type	Attack
01	Denial of Service (DoS)
02	Distributed Denial of Service (DDoS)
03	Reflective Denial of Service (RDoS)
04	Distributed Reflective Denial of Service (DRDoS)
05	Permanent Denial of Service (PDoS)
06	Network Reconnaissance
07	Application Reconnaissance
08	Brute Force
09	Data Leakage
10	Server-Side Vulnerabilities and Exploit
11	Web Applications
12	Web Shells
13	Client-Side Vulnerabilities
14	Web Exploit Kits
15	Malicious Domains
16	Spams
17	Malicious Websites
18	Phishing Websites
19	Newly Emerging and Known Malwares
20	MalSpams
21	Botnet Communications

Table 1. Type of attacks

3.1 Roles in Cyber Range Exercises

During cyber range exercises, the participants are divided into several teams such as white team, blue team, red team, purple team, etc. For example, a typical cyber range exercise can be divided into two teams:

White Team –

exercise managers, referees, instructors and organizers. They provide the scenario, set out rules and framework for the team's exercises. The White team assign tasks to the participants. They also act as instructors and provide basic information to participants if needed and also control and generate the noise that comes from Traffic Generator.

Blue team –

participants are responsible to secure networks and deal with attacks. They have to follow the exercise's rules and respond to a given scenario. Participants in Blue teams need to manage and assign each role based on incident detection, incident handling, and incident response. Figure 1 shows the interactions between the teams ^[5].

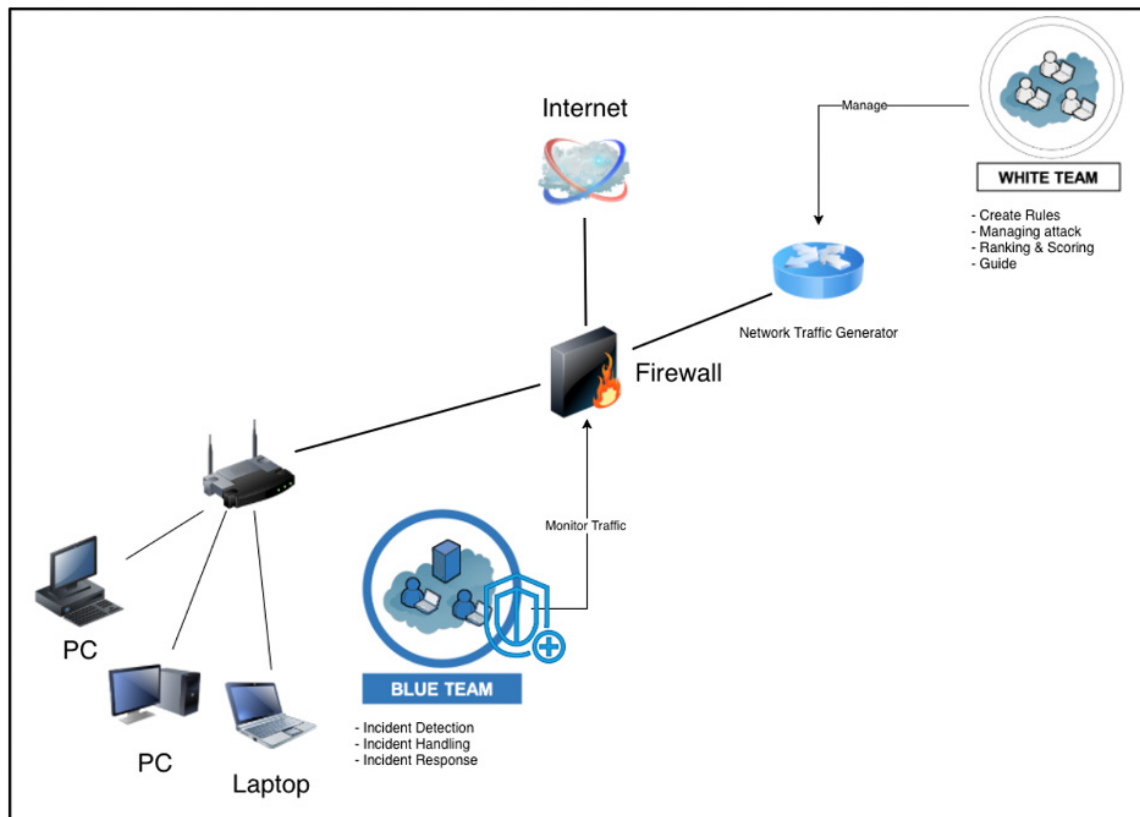


Figure 1. Basic Roles in Cyber Range

4. Challenges

While there are some advantages in using the Cyber Range platform to train personnel as part of Cyber Defensive strategy, there are also some disadvantages. Cyber Ranges are not real operational environments. In a Cyber Range platform, a person from White Team will try to reflect all or part of the possibilities which adversaries could use, including all possible vulnerabilities that could be exploited. Designing, developing and deploying the systems for a Cyber Range requires a lot of time and effort.

As a Cyber Range is an ephemeral environment that is used for training purposes, the training environments need to be scaled to realistically mirror enterprise infrastructure.

Among the major challenges with cyber ranges is that they often need to be manually configured from the ground up, which could introduce an error and does not always represent the target operating environment and thus produces a questionable result.^[6] Additionally, the white team is required to set up the learning objectives. Thus, it needs to have all information about the participants or learners' skills and capabilities before the commencing the actual exercise. [8]. Besides learning objectives, there is also a need to make sure that this exercise or training has a balanced team to build a sense of teamwork.

Conclusion

An example of successful Cyber Range is Cyber Defence Exercise (CDX), which is organised by the NSA for military academy cadets from the US and Canada. Other examples of Cyber Range initiatives include those developed by Estonian Defence Forces. This effort was observed and used during the NATO Cyber Coalition exercise. And it is proven that Cyber Range could be used as a platform for cyber warfare training and simulation.

Besides building a cyber defence strategy, Cyber Ranges could also create an important terrain for cyber red teams. However, the success rate depends entirely on the design and deployment elements during preparation ^[7].

Cyber Range could also be used as a copy of a range, which means once it has been tested, a new threat emerges that may affect the physical

network can be tested against the virtual cyber range to see what adverse effects it has on the system ^[8]. Cyber Range can also be used to penetrate a specific hardware or software.

References

1. T. Debatty, W. Mees, "Building a Cyber Range for training CyberDefense Situation Awareness" ICMCS 2019
2. S. Braidley, "Extending Our Cyber-Range CYRAN with Social Engineering Capabilities," *Researchgate*, 2016.
3. Technopedia, 2019. <https://www.technopedia.com/definition/6705/cyber-defense>
4. Cyber Test Systems, 2018. <https://www.cybertestsystems.com/#!/cyber-range>
5. Tajul Azhar, Tajul Ariffin., Syarifah, Shahidan., "Cyber Defense Competition and Information Security: The Red Teaming Exercise Implementation to Resolve Skills and Techniques with Cyber Range Concept," *e-Journal LIS Liga Ilmu Serantau*, 2018.
6. B. Ferguson, "National Cyber Range Overview", *IEEE Military Communications Conference*, 2014.
7. E. Ç. H. R. Pascal Brangetto, "Cyber Red Teaming," *NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDC)*, 2015.
8. J. V. e. al, "Lessons Learned From Complex Hands-on Defence Exercises in a Cyber Range," *IEEE*, 2017.

A Study on CCTV Installation And Recommendation From Developed Nations Perspective

By | Sharifah Nurul Asyikin Binti Syed Abdullah, Ts. Tajul Josalmin Bin Tajul Ariffin, Mohd Izuan Effenddy Bin Yusof, Akmal Suriani Binti Mohamed Rakof & Fakhrol Afiq Bin Abd Aziz

Introduction

Emerging technologies and the 4th Industrial Revolution (IR 4.0) has brought about significant changes to almost all aspects of humanity. The world is fast moving towards digitalization and people are now more connected than ever. With the advancements in technologies and high speed access of data being stored in the cloud, information protection has become one of the rising concerns amongst public.

Of late, there has been a spike in interest in creating safe environments through the introduction of Cyber-Physical Systems (CPS), a sub-component of IR 4.0. This has led to the proliferation of closed-circuit television (CCTV) systems in the public as well as private spaces. This article intends to describe and compare guidelines from developed nations on the installation and usage of CCTV systems for users and vendors. The countries under review are United States of America, United Kingdom, Australia and New Zealand. This comparative overview of guidelines could assist practitioners and scholars who are interested in CCTV or for civil servants when applying such guidelines in Malaysia.

2. Comparative Overview Of The Guidelines

The guidelines of the four (4) countries used in this comparative study are publicly accessible via the countries' official website. This article focuses on certain aspects of the guidelines i.e. the specifications of the CCTV, the proposed recommendations on camera placement and also management and monitoring of the CCTV.

2.1 CCTV Management and Monitoring

SURVEILLANCE GUIDELINES	
Australia and New Zealand	<ul style="list-style-type: none"> • Ensure at least one trained operator available to assist • Protect data by restricting the ability to delete information from system • To export recording, password is required • Keep the CCTV Operator's manual with the system • Ensure software required is ready for playback recording • Simple maintenance schedule to ensure system remains operational
United Kingdom	<ul style="list-style-type: none"> • Must have specific purpose and legitimate aim • Regular views to ensure its use remains justified • Transparency on the use of surveillance from published contact point to information and complaints • Clear responsibility and accountability of the camera systems activities • Clear rules, policies and procedures before system is used • Policies in place on need for information. Information deleted when not needed • Restricted access. Clearly defined rules. Specified law enforcement • Operators should consider using approved operational and technical standards. • Security measure against unauthorized access • Effective review and audit mechanism to ensure legal compliance • Evidential value to support public safety and law enforcement • Supporting information must be accurate and relevant
United States of America	<ul style="list-style-type: none"> • Video surveillance only for law enforcement purpose • Video surveillance only to address serious threats to public safety • Able and effective achieve the purpose. • Ensure the decision.

Table 1.0: Different aspects of management and monitoring of CCTV.

From Table 1.0 above, United States of America (USA) has clearly specified that CCTVs should be used for law enforcement purposes only. United Kingdom (UK) also emphasize the importance of CCTV recordings as evidential value to support public safety and law enforcement. However, Australia and New Zealand do not consider this aspect of CCTV recordings in their guideline.

2.2 CCTV Specifications

SPECIFICATIONS	
Australia and New Zealand	<ul style="list-style-type: none"> Resolution- Face identification 120% resolution Camera exposure – night mode, infrared, illumination, sensor light Motion detection – if no motion is sensed, set at 1fps. Avoid areas with high movement. If pre-roll is available, minimum should be 10 second Frame rate 8fps Less compression quality, better recorded detail Time/Date on screen – On Screen Display should not cover the view Overwrite period – store recording for minimum 31 days Power Loss Recovery
United Kingdom	<ul style="list-style-type: none"> Resolution – based on objectives Playback – metadata included Export – able to export video at the same quality Storage – access control: password/encryption, capacity for 31 days
United States of America	<ul style="list-style-type: none"> Image quality- if the purpose is to capture evidence of a crime, choose more frames per second Zoom and rotation- cannot-public identify people and object in private areas. Fixed or portable – based on location. Wired or wireless – wired connections are deemed more secure

Table 2.0: CCTV Specifications from Australia and New Zealand, United Kingdom, and United States of America

The analysis of CCTV specifications from the four (4) countries featured in this article shows that the Australia and New Zealand are more specific in camera resolutions requirements, while UK and USA only require general camera specifications but emphasize end objectives as criteria.

2.3 CCTV Installation Recommendations

RECOMMENDATIONS	
Australia and New Zealand	<ul style="list-style-type: none"> Physical Installation – secure from vandalism, weather elements and damage. Resolution – Cover entries, exit, pinch point and point of sales face identification 120%, <ul style="list-style-type: none"> Face Recognition 50% Intrusion Detection 10% Crowd control 5% Cover car entry and exit point with Manual License Plate Recognition Camera Placement <ul style="list-style-type: none"> Overlap camera views to maximize recording a person's movement Avoid back-lit areas/ bright/ flashing light in the camera's field of view Eye-Level camera No object obstructing the view Assess camera placement over entire operating timeframe Optimize Face Identification 120% level camera at entries, exits, pinch point Camera Exposure <ul style="list-style-type: none"> Add lighting in dim surroundings. Avoid bright hot spot. Include day/night cameras, motion sensor lights/ infrared and illumination Frame Rate – set at level that will capture four or more images of the target Motion Detection – if no motion is sensed, set 1fps. Avoid areas of high movement. If pre-roll is available, minimum 10second Compression quality, the less compression, the better recorded detail Time/Date on screen – ensure On Screen Display (OSD) position do not cover the view Overwrite period – store recording for at least 31 days Power Loss Recovery – employ uninterruptible power supply (UPS). Maintenance – ongoing routine maintenance to ensure the CCTV system is fully functional
United Kingdom	<ul style="list-style-type: none"> Quality – based on the purpose of surveillance e.g. recognize the face of someone walking through a doorway/ read vehicle registration number / exchange money Export – operator able to replay and export recording <ul style="list-style-type: none"> System operator's manual must be available to assist System user should be able to export images and information

	<ul style="list-style-type: none"> Exported images and information should not interrupt the operation of the system Exported images must preserve the same quality as the original recording and metadata Exported media in the native file format at the same quality Playback – have variable speed control <ul style="list-style-type: none"> Display single & multiple camera Display single camera at full resolution Permit the recoding from each camera to be searched by time and date Allow printing/saving with time and date Storage – restricted access to avoid tampering or unauthorized view <ul style="list-style-type: none"> Retention should be at least 31 days protect specific sequence Prevent overwriting before extraction
United States of America	<ul style="list-style-type: none"> Lighting <ol style="list-style-type: none"> Fluorescent: used for indoor area Incandescent: used to illuminate large outdoor areas High-intensity discharge (HID): There are two forms – High/Low pressure sodium and metal halide. Require a few minutes to reach full luminance once turned on. Commonly used for street lighting Infrared (IR): used to provide discrete CCTV, minimize light pollution, provide long distance illumination. LED: Provide high levels of brightness and intensity, highly efficient, low operating temperature, low electrical consumption Power Distribution – should have uninterruptible power supplies (UPS) Video Transmission – coaxial cable or unshielded twisted pair (UTP) Scalability - ability of the system to accommodate additional components such as cameras, increased video storage, and additional monitors Cost – cover planning, design, installation, operation, maintenance & personnel cost Define System requirement Lighting strategies, camera selection & camera location – should be considered together, ensure optimum performance Network storage – Direct Attached Storage (DAS) / Storage Area Network (SAN)/ Network Attached Storage (NAS)

Table 3.0: CCTV Installation Recommendations from Australia and New Zealand, United Kingdom, and United States of America

2.4 Camera Placement Recommendations for CCTV

CAMERA PLACEMENT	
Australia and New Zealand	<ul style="list-style-type: none"> Incorporate eye-level cameras Avoid back-lit areas and bright or flashing lights in the camera's field of view Can maximize continuous recording Optimize face identification level camera position (entries, exits, pinch points & point of sale areas) No obstruction of camera views Assess timeframe 24 hours continuous recording- ensure camera view is not compromised
United Kingdom	<ul style="list-style-type: none"> Only deploy in public spaces where people are aware that they are being monitored Avoid private spaces (such as changing rooms etc.)
United State of America	<ul style="list-style-type: none"> The area under surveillance should only be public spaces. Surveillance equipment can use zoom, tilt, and pan to enhance video capture, and enhanced microphones to detect sound. However, technology that is able to intrude beyond reasonable limits of audio and visual capability may be deemed unconstitutional.

Table 4.0: Camera Placement Recommendations from Australia and New Zealand, United Kingdom, and United States of America

Criteria for Public Spaces' Video Surveillance based on Commonly Used and Effectiveness

Spectrum	2.4GHz is one of the most widely used unlicensed bands for public areas but the 4.9G is licensed to public safety agencies, usually the police.
Video Compression	MPEG-4 , MJPEG and ITU standards of H.264
Transmission	Hybrid Network – Fibre Optics and Internet Connection – is the most talked about technology, hailed as the best media conversion system
Cameras	PTZ with Infrared and vandal proof casing with real time zooming up to 300 metres
Storage	IP SANs which have capacity of more than 1,000 terabytes.

Source: Adapted from various sources

3. CCTV Recommendation And Guidelines In Malaysia

The suitable video surveillance systems in public spaces environment excerpted from the article:

Generally, the comparative studies portray two generic approaches in the deployment and implementation of public video surveillance systems and services by UK and New Zealand. The surveillance systems are either deployed solely by the local government authorities or in joint partnership between a local government authority and private security service providers.

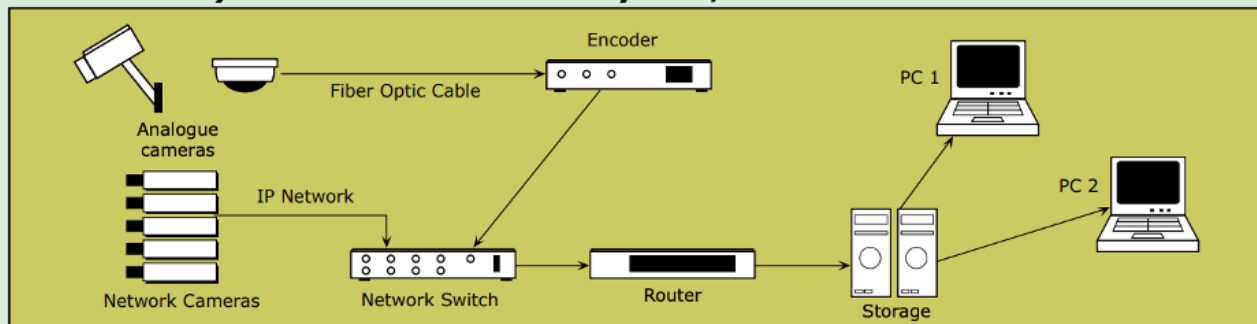
In Malaysia, Malaysian Communications and Multimedia Commission (MCMC) has published a report entitled, "Video Surveillance in Public Spaces". According to MCMC, the public spaces that require installation of CCTV should be clearly defined prior to determining the installation methodology. MCMC defines public spaces as any place that an individual has the right to access and use as opposed to private space which may have restrictions.

4. Conclusion

There are mixed approaches to the management of public video surveillance systems and service deployment in Malaysia. In countries such as UK, Australia, New Zealand and US, public video surveillance are mostly funded by the state government, local city councils or municipal councils. Specific recommendations and guidelines on the technical aspects of CCTV installation have not been issued in Malaysia.

Most local government authorities outsource the entire CCTV deployment works to an external private security party through a contract agreement or joint partnership in leasing, installing and maintaining the systems and equipment. As such, recommendations and installation guidelines are tailored specifically for each project.

Hybrid Video Surveillance System, with Media Conversion



Source: Adapted from various sources

References

1. "Video Surveillance in Public Spaces", *Suruhanjaya Komunikasi dan Multimedia (SKMM)*. (2008).
2. *Australia and New Zealand police recommendations for CCTV systems*. (2014). Docklands, Victoria: ANZPAA.
3. Dowling, Christopher & Morgan, Anthony & Gannoni, Alexandra & Jorna, Penny. (2019). *How do police use CCTV footage in criminal investigations? Trends and Issues in Crime and Criminal Justice*. 575. Retrieved July 26, 2020, from https://www.researchgate.net/publication/332224368_How_do_police_use_CCTV_footage_in_criminal_investigations
4. EESAG. (2014). *Australia and New Zealand police recommendations for CCTV systems*. Retrieved July 26, 2020, from <https://nla.gov.au/nla.obj-275378245/view>
5. Garris, M. D., Laamanen, M. T., Russell, C. S., & Nadel, L. D. (2017). *Assessment of closed-circuit television digital video recording and export technologies*. doi:10.6028/nist.ir.8172
6. Ratcliffe, Jerry. (2010). *Video Surveillance of Public Places*. Retrieved July 25, 2020, from https://www.researchgate.net/publication/252218884_Video_Surveillance_of_Public_Places
7. *Space and Naval Warfare Systems Center Atlantic* (2013). *System Assessment and Validation for Emergency Responder. CCTV Technology Handbook*. Retrieved July 26, 2020 from https://www.dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf
8. *Surveillance camera code of practice*. (2013). London: Home Office. Retrieved July 25, 2020, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

Windows Artifact Analysis : The Importance In E-Discovery Analysis

By | Mohd Zabri Adil Bin Talib, Nor Zarina Binti Zainal Abidin, Muhammad Zahid Bin Ismail & Muhammad Bin Mohd Roslan

Introduction

Microsoft Windows is the most popular operating system used around the world. Windows will generate system artifacts of user activities. As such, Windows artifacts is a crucial area for Digital Forensics analysis in the Microsoft operating system environment but is often overlooked by the forensics analyst.

The artifact can be useful in the case investigation especially to verify what kind of file or folder that has been accessed by a user. In E-Discovery analysis, the artifact analysis offers important information which needs to be analysed especially on data breach incident or domestic inquiry. The artifact contains not only a record of files and folder accessed but the original path, the date and time accessed. This provides key evidence required by the management to verify if their own employee has committed certain acts of misconduct.

Windows system artifacts can be divided into six (6) parts: **event logs, swap file, registry, recycle bin, web cache and prefetch.**

In this article, we will focus on five (5) areas of Windows artifacts of file or folder opening from registry. Registry is a central hierarchal database that maintains configuration setting for applications, hardware device and users. The five key areas are listed below:

- i. Shell Bags
- ii. Shortcut (LNK) files
- iii. Jump Lists
- iv. Open/Save MRU
- v. Recent Files

i. Shell Bags

Windows ShellBag is one of the important artifacts in the Windows operating system. Shell Bags are designed to improve user experience and to remember preferences when browsing the folders. For example, if the user changes a folder view from a "small" icon to "large" icon or "Details," the setting is stored in ShellBags.

Shell Bags records created or updated when a user opens or closes any folder locally or remotely on a computer. These actions are tied according to a user account.

Shell Bag information resides in `UsrClass.dat` hive. The following is the full path location of `UsrClass.dat` in Microsoft Windows 10.

`\Local Settings\Software\Microsoft\Windows\Shell\Bags`

A forensic examiner may use a free and powerful tool developed by Eric Zimmerman's. Shell Bag Explorer, which can be downloaded at <https://ericzimmerman.github.io/#!index.md>.

Value	Icon	Shell Type	MSL Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Extension	Has Shortcut
My Computer		Root Folder (GUD)	1							
Control Panel		Root Folder (GUD)	2							
Exchange 2010		Directory	3	2014-12-01 13:02:14	2014-12-01 13:02:14	2014-12-01 13:02:14	2014-12-01 13:02:14	2014-12-01 13:02:14		NTFS file system
New Folder		Directory	4	2014-12-01 13:04:06	2014-12-01 13:04:06	2014-12-01 13:04:06	2014-12-01 13:04:06	2014-12-01 13:04:06		NTFS file system
User Libraries		Root Folder (GUD)	2					2014-09-21 11:05:15		

Figure 1: ShellBag Explorer

Figure 1 shows the primary interface of ShellBag explorer. On the left panel of the interface, it indicates the folder structure that the user has opened. On the right panel are the details on created, modified, and accessed date. This information is vital to a forensics examiner to identify when the user accessed that specific folder.

ii. Shortcut (LNK) files

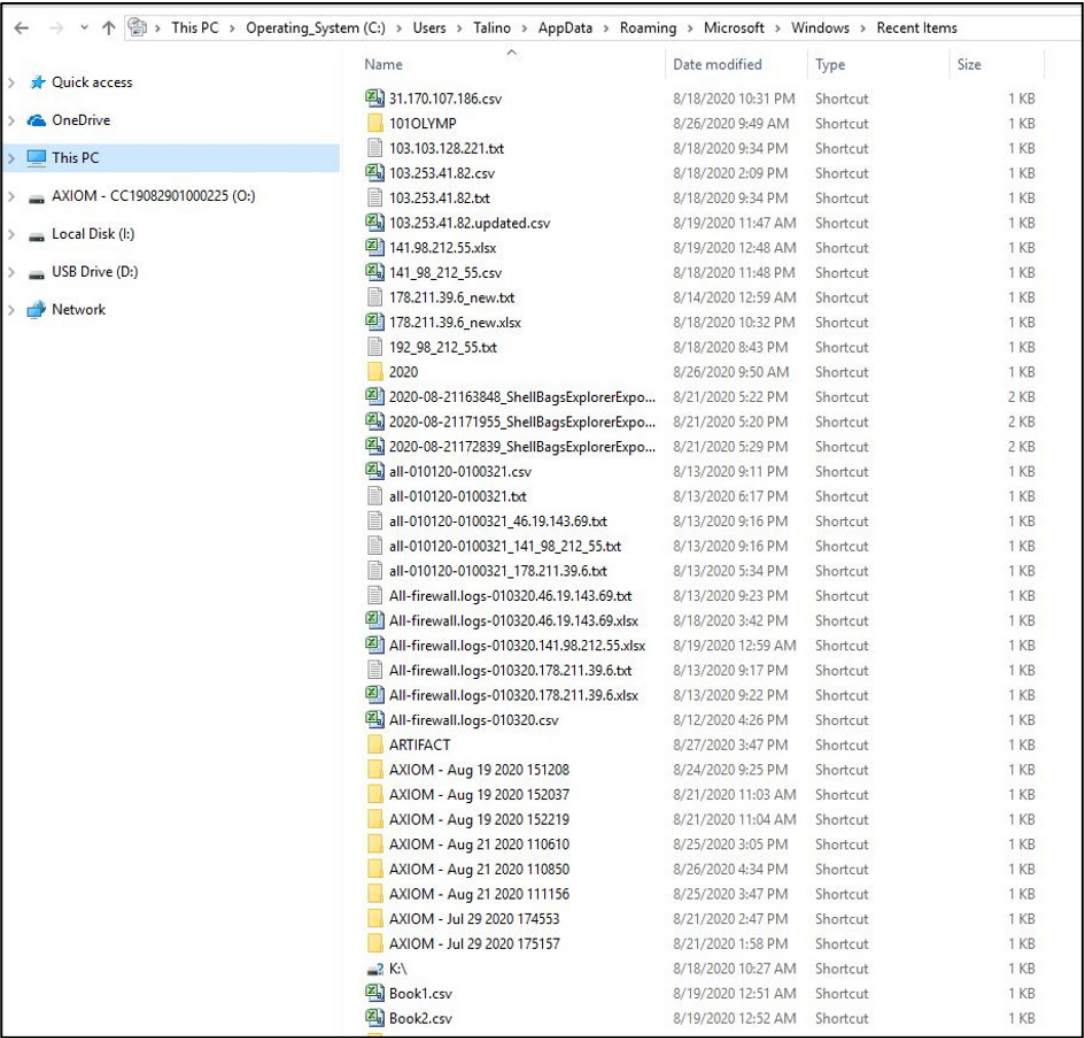
The second Windows artifact that is essential for the forensic examiner to trace down file or folder opening is the LNK file (.lnk). LNK files are shortcut files which automatically created by the Windows operating system. Shortcut (LNK) files are used by Microsoft Windows to point to an executable file.

Shortcut (LNK) files are used as a direct link to an executable file without having to navigate to the executable file location.

Windows creates shortcut files when a user opens and uses media files that show up in the Recent Files folder. If a user opens and edits a file from a USB key but never copied the file to the system, that shortcut is created in the Recent Items folder under that user account.

Microsoft Windows automatically creates a shortcut (LNK) files on user recent item and opening local and remote data files.

Analysis shortcut (LNK) files in Microsoft Windows were able to track Modified, Access, and Creation times of the target file, volume Information (Name, Type, Serial Number), file attributes (system, hidden), MAC address of the machines, network share information, original location, and name of the system on data files user accessed in the exhibit.



Name	Date modified	Type	Size
31.170.107.186.csv	8/18/2020 10:31 PM	Shortcut	1 KB
101OLYMP	8/26/2020 9:49 AM	Shortcut	1 KB
103.103.128.221.txt	8/18/2020 9:34 PM	Shortcut	1 KB
103.253.41.82.csv	8/18/2020 2:09 PM	Shortcut	1 KB
103.253.41.82.txt	8/18/2020 9:34 PM	Shortcut	1 KB
103.253.41.82.updated.csv	8/19/2020 11:47 AM	Shortcut	1 KB
141.98.212.55.xlsx	8/19/2020 12:48 AM	Shortcut	1 KB
141_98_212_55.csv	8/18/2020 11:48 PM	Shortcut	1 KB
178.211.39.6_new.txt	8/14/2020 12:59 AM	Shortcut	1 KB
178.211.39.6_new.xlsx	8/18/2020 10:32 PM	Shortcut	1 KB
192_98_212_55.txt	8/18/2020 8:43 PM	Shortcut	1 KB
2020	8/26/2020 9:50 AM	Shortcut	1 KB
2020-08-21163848_ShellBagsExplorerExpo...	8/21/2020 5:22 PM	Shortcut	2 KB
2020-08-21171955_ShellBagsExplorerExpo...	8/21/2020 5:20 PM	Shortcut	2 KB
2020-08-21172839_ShellBagsExplorerExpo...	8/21/2020 5:29 PM	Shortcut	2 KB
all-010120-0100321.csv	8/13/2020 9:11 PM	Shortcut	1 KB
all-010120-0100321.txt	8/13/2020 6:17 PM	Shortcut	1 KB
all-010120-0100321_46.19.143.69.txt	8/13/2020 9:16 PM	Shortcut	1 KB
all-010120-0100321_141_98_212_55.txt	8/13/2020 9:16 PM	Shortcut	1 KB
all-010120-0100321_178.211.39.6.txt	8/13/2020 5:34 PM	Shortcut	1 KB
All-firewall.logs-010320.46.19.143.69.txt	8/13/2020 9:23 PM	Shortcut	1 KB
All-firewall.logs-010320.46.19.143.69.xlsx	8/18/2020 3:42 PM	Shortcut	1 KB
All-firewall.logs-010320.141.98.212.55.xlsx	8/19/2020 12:59 AM	Shortcut	1 KB
All-firewall.logs-010320.178.211.39.6.txt	8/13/2020 9:17 PM	Shortcut	1 KB
All-firewall.logs-010320.178.211.39.6.xlsx	8/13/2020 9:22 PM	Shortcut	1 KB
All-firewall.logs-010320.csv	8/12/2020 4:26 PM	Shortcut	1 KB
ARTIFACT	8/27/2020 3:47 PM	Shortcut	1 KB
AXIOM - Aug 19 2020 151208	8/24/2020 9:25 PM	Shortcut	1 KB
AXIOM - Aug 19 2020 152037	8/21/2020 11:03 AM	Shortcut	1 KB
AXIOM - Aug 19 2020 152219	8/21/2020 11:04 AM	Shortcut	1 KB
AXIOM - Aug 21 2020 110610	8/25/2020 3:05 PM	Shortcut	1 KB
AXIOM - Aug 21 2020 110850	8/26/2020 4:34 PM	Shortcut	1 KB
AXIOM - Aug 21 2020 111156	8/25/2020 3:47 PM	Shortcut	1 KB
AXIOM - Jul 29 2020 174553	8/21/2020 2:47 PM	Shortcut	1 KB
AXIOM - Jul 29 2020 175157	8/21/2020 1:58 PM	Shortcut	1 KB
K:\	8/18/2020 10:27 AM	Shortcut	1 KB
Book1.csv	8/19/2020 12:51 AM	Shortcut	1 KB
Book2.csv	8/19/2020 12:52 AM	Shortcut	1 KB

Figure 2: LNK file in Windows 10

Figure 2 shows the list of shortcut file or (.lnk) which is created by Windows. The forensic examiner will know which file or folder was opened by the user. The following is the full path location of where the Windows 10 shortcut file (.lnk) resides.

C: \\\USERPROFILE%\\ AppData\\Roaming\\Microsoft\\Windows\\Recent

iii. Jump Lists

The third Windows artifact is the Jump List. Jump List is a feature in the Windows operating system starting in Windows 7 that gives the user quick access to recent application files and actions. This functionality also includes recent tasks. For example, a web browser like edge or chrome uses a Jump list to display websites frequently visited. Microsoft Office program, PowerPoint, Excel, or Word uses the Jump list to display its recent file opening.

Jump List artifact analysis in windows enable a forensic examiner to track on what and when a file opening or website visited by each user account on the computer.

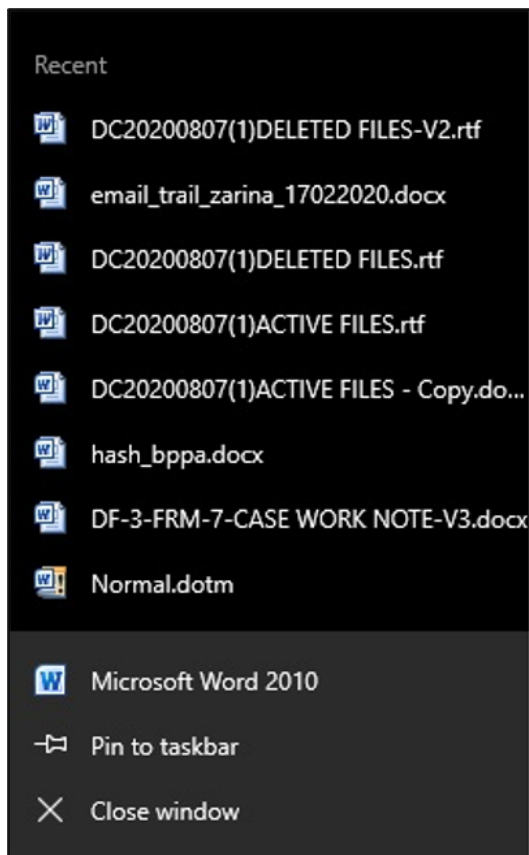


Figure 3: Example of Jump List in Windows 10.

Figure 3 shows a Jump List interface in Windows 10. It is used to provide quick access to recently or frequently-used documents and offer direct links to app functionality. The Jump List content is derived from two sets of Destination file by the Windows operating system.

The first set is automaticDestinations type files. These automaticDestinations type files are created and maintained by the Windows operating system which stores information about data file usage. Items in automaticDestinations type file are sorted either by Most Recently Used (MRU) or by Most Frequently Used (MFU), depending on the application.

The second set is customDestinations type file. These two sets of files can be located in the Windows file system on the following path.

1. **%APPDATA%\\Microsoft\\Windows\\Recent\\AutomaticDestinations\\[AppID].automaticDestinations-ms**
2. **%APPDATA%\\Microsoft\\Windows\\Recent\\CustomDestinations\\[AppID].customDestinations-ms**

For forensic examiner, JumpList Explorer by Eric Zimmerman is a free and efficient tool to analyse the above two sets of files. JumpList explorer allows the forensic examiner to extract JumpList information from the Windows operating system. This tool can be downloaded at <https://ericzimmerman.github.io/#!index.md>.

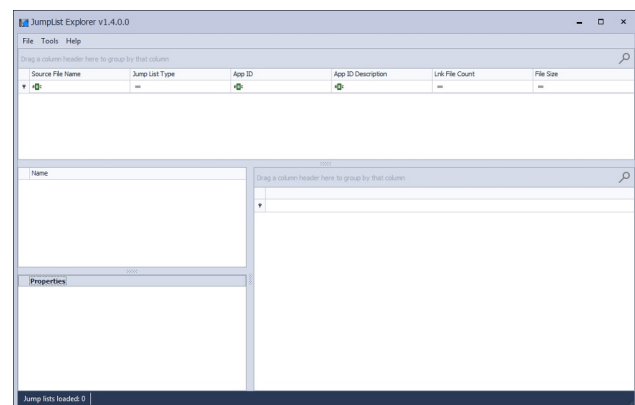


Figure 4: Jump List Explorer's main interface.

Jump List Explorer's main graphical user interface (GUI) is easy to use. A user just has to load the AutomaticDestinations file and CustomDestination file sets.

iv. Open/Save MRU

Another vital artifact to trace a file or folder opening in windows is Open/Save MRU. MRU is an abbreviation for Most Recently Used. Open/Save MRU tracks files that have been opened or saved within a Windows shell dialog box.

The data from Open/Save MRU can be found at the following two registry keys below.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

For forensics examiner to analyze Open/Save MRU registry keys, there are many tools available. One of them is Registry Explorer by Eric Zimmerman. This tool is free to download at <https://ericzimmerman.github.io/#!index.md>.

Figure 6 shows the Registry Explorer's main interface. The forensics examiner needs to upload the Software registry file to get information for Open/Save MRU. Navigate to these two paths for Open/Save MRU details.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

v. Recent Files

The fifth Windows artifact enables one to trace the opening of a file or folder from the Recent Files registry key. Recent Files registry key can be used to track the last file or folder which was opened. This registry key is used to populate data in the "Recent" item in the Windows Start menu.

The forensic examiner needs an NTUSER.DAT registry file to analyze recent file information from the registry key. The registry key for the recent file is located at the following path in the registry hive.

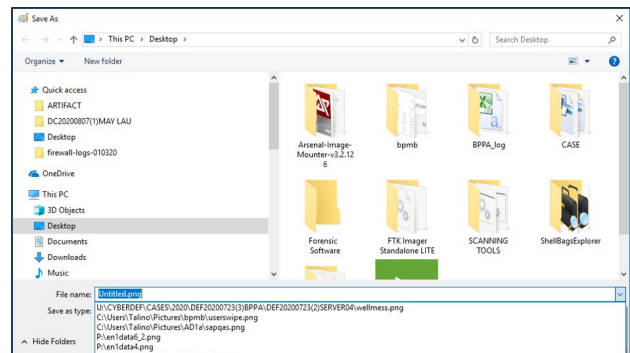


Figure 5: Windows 10 Shell dialog box Autocomplete example.

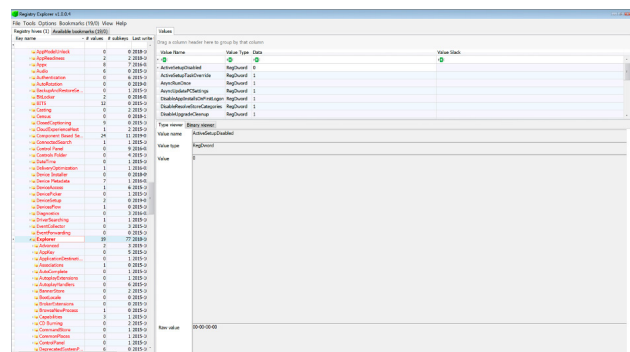


Figure 6: Registry Explorer's main interface.



Figure 7: Windows 10 start menu.

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

An appropriate tool to analyze the recent file registry key is Registry Explorer. From this analysis, forensic examiner gets to identify recent files opened by the user account of the computer.

From these Shell bags, LNK, Jumplist, Open/Save MRU, and Recent file records and registry key, a forensic examiner can access vital information on what and when files or folders were opened by each user account on the computer. This may be crucial for cyber intrusion cases as forensics analyst need to examine what type of files that is aimed by the intruder.

find%20the%20NTUSER,you%20can%20see%20the%20NTUSER.

7. <https://www.blackbagtech.com/blog/windows-10-jump-list-forensics/>
8. https://tzworks.net/prototype_page.php?proto_id=20
9. https://www.nirsoft.net/utils/open_save_files_view.html
10. https://www.nirsoft.net/utils/recent_files_view.html
11. Carvey, H.: *Windows Forensic Analysis DVD Toolkit*, Burlington (2007)

Conclusion

The forensics analyst needs to know the objectives and goals of the investigation. Being made aware of the case details will prevent crucial evidence been left out. A forensics analyst is responsible to target specific data, in specific areas such as Windows artifacts. Therefore, analysis of Windows system artifacts plays significant role in performing an E-Discovery analysis investigation.

References

1. <https://ericzimmerman.github.io/#!index.md>
2. <https://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/#gref>
3. <https://lifars.com/knowledge-center/windows-shellbags-forensics-investigative-value-of-windows-shellbags/#:~:text=Generally%2C%20speaking%20ShellBags%20are%20designed,settings%20get%20stored%20in%20ShellBag.>
4. <https://www.sans.org/blog/opensavemru-and-lastvisitedmru/>
5. <https://www.howtogeek.com/97824/how-to-customize-the-file-opensave-dialog-box-in-windows/>
6. <https://www.faqforge.com/windows/windows-10/what-is-the-ntuser-dat-file-in-windows-10/#:~:text=You%20can%20>

Application of OBD-II Standard In Vehicle Diagnostics

By | Yasmin Binti Jeffry, Fauzi Bin Mohd Darus, Miratun Madiah Binti Saharuddin, Wafa' Binti Mohd Kharudin & Ummu Ruzanna Binti Abdul Razak

Vehicles of today are fitted with electronic dashboards displaying an array of indicators on various systems and sensors within the in-vehicle ecosystem, vehicle body and engine conditions (Figure 1). These indicators and diagnostics follow a certain standard namely the On-Board Diagnostics II (OBD II). Every gasoline powered vehicle in the USA manufactured after 1997 follows OBD II standard and every gasoline powered vehicle in European Union since 2001 has European On-Board Diagnostics (EOBD). On-Board Diagnostic I was the earlier version used to regulate vehicle emission control.

Below are some of the standards that were developed for OBD II:

- SAE J1962 – Documenting the requirements of the OBD II connector and its external test equipment connector.
- SAE J1978 – Defines the requirements of OBD II Scan Tool as legislated by the United States' government.
- SAE J1979 – This standard pertains to the Diagnostic Test Modes. It details the data reporting requirement of OBD II, which

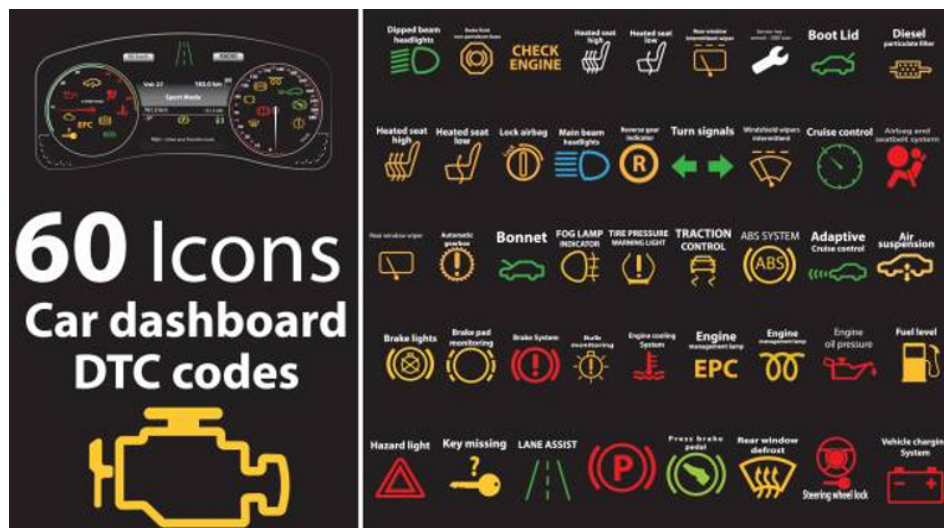


Figure 1: Car dashboard icons

Among the major drawbacks of the older OBD I system was its inconsistency. Different manufacturers have different implementations of a diagnostic system. Two different car models from the same manufacturer might also have different implementation. The difficulty arises when users do not have a single uniform tool to use during diagnosis.

OBD II resolved this issue since it was produced and maintained by several international standards organizations. The primary organization involved in this process is the SAE International (previously known as Society of Automotive Engineers) and International Organization for Standardization (ISO).

includes OBD II's messages format, timing requirement of message transmissions, behavior of vehicles when data is unavailable and diagnostic services. This standard also describes OBD II's Parameter IDs (PIDs), which are codes used in requesting data from vehicles.

- SAE J2012 – This document pertains to the Diagnostic Trouble Codes (DTC) generated when a fault is detected in a vehicle.
- ISO 9141-2, ISO 14230, SAE J1850, and ISO 15765 – These documents describe the basic signaling protocols that is used in OBD II and the interchange of information between vehicles and scan tools.

Diagnostic Trouble Codes

Diagnostic Trouble Codes (DTC) are codes that are used for vehicle diagnostic purposes. It is generated when the vehicle experiences a failure in its internal system. The code can be read by connecting an external scan tool to the vehicle's OBD II port. This feature is not only limited to users who want to diagnose their vehicle's condition themselves but also for auto repair shops to perform diagnosis on a customer's vehicle.

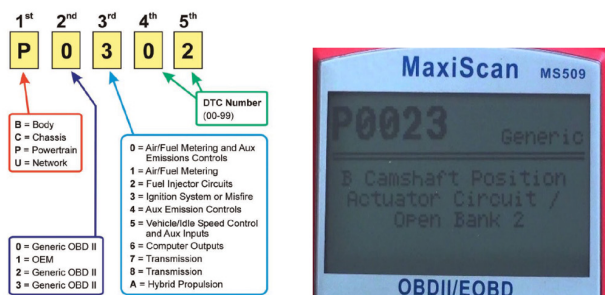


Figure 2: Diagnostic trouble code (DTC) formatting and reading DTC with a scan tool

As previously mentioned, the system of DTCs are detailed in standard SAE J2012. It is formatted in 5 digits (Martin, 2015).

- The 1st digit – Indicates an alphabet which categorizes the vehicle's general operating system that is faulty. There are 4 alphabets: P (Powertrain), B (Body), C (Chassis), U (Network/unknown).
- The 2nd digit – Specifies whether the codes are from the standardized generic set (specified in SAE J2012), or proprietary codes from the manufacturer (manufacturer specific codes).
- The 3rd digit – Signifies the specific system that is faulting. There are 10 categories for the 3rd digit. For example, number 3 in the 3rd digit represent faults in the fuel injector circuits.
- The 4th and 5th digit – indicates further information regarding a malfunction.

It is important to note that the SAE J2012 document only specifies the standardized generic set of codes. These are codes that are uniform across all different types of vehicle models. Vehicle manufacturers usually implement more DTCs on top of the generic set, which is unique to their own vehicles. Most scan tools can access generic DTCs but not all manufacturer

specific DTCs. The scan tools need to have the manufacturer's DTC database to access it. Certain OBD II scan software such as Dash Command (iPhone/Android) charges additional payment for certain manufacturer specific DTC. Some of these manufacturers may not follow the standardized format. For example, the generic DTC for losing GPS connection is U016A; but for Volvo's specific DTC is GPS-0001.

Scan Tool

To read fault codes of OBD II system requires a scan tool. The tool must be connected to the vehicle through a connector called Diagnostic Link Connector. The Diagnostic Link Connector is usually located under the steering wheel or under dashboard on passenger side. It is a 16-pin connector which follows the OBD II Standard, which means its appearance and functions are standardized.

A scan tool can be connected to the Diagnostic Link Connector either using a standalone scan tool or a software installed in laptops or mobile phones. The software use Bluetooth adapter or wired connection to gather information from Diagnostic Link Connector.



Figure 3: Example of standalone scan tool and Android application with Bluetooth reader

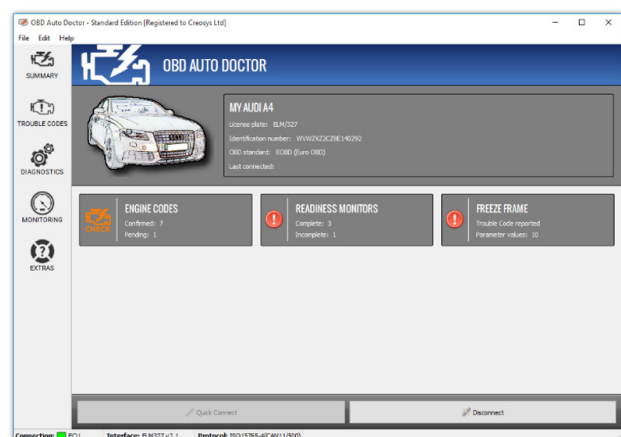


Figure 4: Example of desktop software for OBD II analysis

Importance Of OBD II Standard

The benefits of the OBD II Standard can be seen at many levels of society from individuals, organizations to governments. One of the major advocates of the OBD II standard was the California Air Resources Board (CARB) as they were the first organization which pushed legislation of OBD II requirements in their state. This legislation was soon followed by implementation at the federal level. Auto repair shops were required to perform 'smog check' inspection on customer's vehicles. This is to ensure that the emission control system of the vehicle is functioning properly to reduce the amount of pollutants released into the air. Through OBD II, governments can enforce tighter regulations to reduce air pollution. In certain organizations, OBD II is embedded in their fleet management software. Organizations such as logistics companies that manage a number of vehicles will greatly benefit from this. Companies can remotely generate a report on their fleet's fuel economy.

Individuals can gain the advantage of diagnosing vehicles themselves without the need to have immense automotive knowledge. Users can easily check any faults using a scanner tool, saving time and costs before going to an auto repair shop. Moreover, since OBD II is standardized, having one good scanner tool is sufficient as it can be used across multiple vehicle types.

Forensics Readiness

One major component of the OBD II frame data is the checksum component. Checksum is an error detection method used to ensure that the integrity of data is maintained, and its transmission successful. Each of the OBD II protocol has their own implementation of checksum. The SAE J1979 Standard documents the implementation of checksum for each protocol.

For example, the ISO 15765 CAN protocol uses a checksum method known as Cyclic Redundancy Check (CRC). CAN data frames has a CRC field which consists of 15 bits that are used in the checksum process. Further details on the CRC implementation of the ISO 15765 CAN protocol is written inside the BOSCH CAN Specification 2.0 (BOSCH, 1991). The checksum component is useful when checking the transmitted data to ensure consistency and no unintended changes.

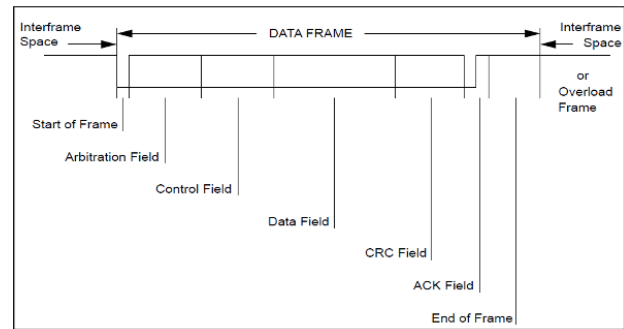


Figure 5: CAN data frame

Whenever possible, the closed loop system of the OBD II and infotainment should be maintained. Enabling connection with other networks (such as mobile carriers or internet provider) creates vulnerability to the system. Maintaining a closed loop ensures that data transferred in the vehicle communication network is secured and cannot be remotely tempered.

Conclusion

This article provides a brief overview of OBD II Standard and explains how a regular user could utilize OBD II. There are several documents that support the OBD II Standard from SAE J1962, SAE J1978, SAE J1979 to SAE J2012. Each of these document covers a different aspect of the OBD II Standard. The DTCs can be utilized to ensure optimum performance of vehicles. By observing the format of OBD II, a checksum component maintains the integrity of data. Implementing best practices will ensure that data in the vehicles are not compromised by external attacks.

References

1. Martin, T. (2015). *How To Use Automotive Diagnostic Scanners*. Wisconsin, United States. Motorbooks International.
2. Robert BOSCH GmbH. (1991). *CAN Specification 2.0*. Retrieved from <http://esd.cs.ucr.edu/webres/can20.pdf>
3. 'What are the benefits of on-board diagnostics (OBD)?'. (n.d.). Retrieved from <https://www.yelowsoft.com/blog/benefits-of-on-board-diagnostics/>

OIC-CERT Contribution To The OIC-2025 Strategic Agenda

By | Ahmad Nasir Udin Bin Mohd Zin

Introduction

International cooperation and collaboration are key components of cyber threat mitigation in a borderless world. Therefore, good international relations is pivotal in strengthening cybersecurity. The International Engagement Department of CyberSecurity Malaysia is tasked to manage international relations for CyberSecurity Malaysia, an agency under the purview of the Ministry of Communications and Multimedia, Malaysia.

OIC-CERT And The OIC

One of the platforms used by CyberSecurity Malaysia in managing and enhancing international relations is through its active participation in the **Organisation of Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT)**. CyberSecurity Malaysia is currently the Permanent Secretariat of the OIC-CERT, a responsibility held since 2012. The OIC-CERT is a collaboration of **Computer Emergency Response Teams within the Organisation of Islamic Cooperation (OIC)** region. To date, it has 47 members from 27 countries. This organisation is managed by an OIC-CERT Board. The current members of the Board are Oman (Chair), Indonesia (Deputy Chair), Malaysia (Permanent Secretariat), Azerbaijan, Egypt, Iran and the United Arab Emirates^[1].

The OIC-CERT is an affiliate member of the OIC since 2009 as per the OIC Resolution No 2/36-INF made during the 36th Session of the Council of Foreign Ministers of the OIC meeting in Damascus, Syrian Arab Republic on 23–25 May 2009^[2]. As an affiliate member of the OIC, the OIC-CERT has since played an active role and made significant contribution to OIC through the OIC-2025 strategic agenda.

The OIC-2025

The OIC-2025 forms OIC's strategic agenda in the current decade. Adopted at the 13th Islamic Summit Conference in Istanbul on 14–15 April 2016, it is currently in its implementation phase guided by the Implementation Plan 2016–2025 document^[3] which set 107 goals across 18 priority areas. The priority areas are:

1. Palestine and Al-Quds
2. Counter-terrorism, Extremism, Violent Extremism, Radicalization, Sectarianism, and Islamophobia
3. Moderation, Cultural and Inter-faith Harmony
4. Peace and Security
5. Environment, Climate Change and Sustainability
6. Poverty Alleviation
7. Trade, Investment and Finance
8. Agriculture and Food Security
9. Employment, Infrastructure and Industrialization
10. Science, Technology and Innovation
11. Education
12. Health
13. Advancement and Empowerment of Women, Family Welfare and Social Security
14. Joint Islamic Humanitarian Action
15. Human Rights, Good Governance and Accountability
16. Media and Public Diplomacy
17. ICT and Digital Information Structure
18. OIC Institutional Reforms

OIC-CERT Contribution To The OIC-2025

The OIC-CERT, as an affiliate member of the OIC, has contributed significantly to the OIC-2025 strategic agenda. The list of contributions by the OIC-CERT to the OIC-2025 as per the Program of Action Progress 2018-2019 are as follow ^[4] :

a. Priority Area 2: Counter-Terrorism, Extremism, Violent Extremism, Radicalisation, Sectarianism, and Islamophobia

1. Goal 2.2.6 – Improve the utilization of ICT in countering the misuse of Cyberspace through terrorist act and recruitment for terrorism purposes.

a. OIC-CERT has been engaged in creating and enhancing a common set of standards, policies, procedures and regulations for OIC-CERT to address cyber security and cyber-crimes. Its focus has been two-fold:

- i. Creating communication channels and communication protocols for incident handling among OIC-CERT members and partners.
- ii. Maintaining an interactive portal that facilitates communication and information sharing.

b. Development of the OIC-CERT cyber security standard operating policies, procedures and best practices.

c. Two new guidelines are currently being developed (2019): (i) Internet of Things (IoT) Security Guidelines (ii) Industrial Control System (ICS) Security Guidelines.

d. Guidelines developed in 2018 include:

- i. Security Framework and Model for Organizational Architecture.
- ii. Security & Privacy Guidelines for Online Social Work.
- iii. Security Requirements for Smartphone App Stores.

2. Goal 2.2.7 – Counter the misuse of cyberspace for terrorism purposes,

including recruitment and financing, and cyber espionage campaigns by illegal organisations.

a. a)OIC-CERT Annual Cyber Drill is conducted annually. The objective of the drill is to test and evaluate the readiness and communication capabilities of the OIC-CERT members.

b. OIC-CERT Annual Cyber Drill 2019, hosted by the Oman National CERT (OCERT), was conducted on 17 September 2019 with participation from: Bangladesh, Brunei, Egypt, Indonesia, Jordan, Malaysia, Morocco, Nigeria, Pakistan, and Tunisia.

c. Asia Pacific Computer Emergency Response Team (APCERT) representatives and the African Computer Emergency Response Team (AfricaCERT) representatives also participated in this drill.

d. OIC-CERT and the APCERT has signed a Memorandum of Understanding (MoU) to collaborate in the areas of cyber security. Based on this MoU, the APCERT invited members of the OIC-CERT to participate in their annual cyber drill and vice versa.

e. The 2019 APCERT Annual Cyber Drill which was conducted on 31 July 2019 involved three (3) OIC-CERT member countries: Brunei, Indonesia and Malaysia.

f. For the 2018 APCERT Annual Cyber Drill, nine (9) OIC-CERT member countries took part as follows: Brunei, Bangladesh, Egypt, Indonesia, Malaysia, Morocco, Nigeria, Oman and Pakistan.

g. OIC-CERT Malware Research and Coordination Facility: this is a collaborative project among the OIC-CERT members to share malware threat research, analysis and response to protect the community against malware threats. It provides an overview of the cyber threat landscape for the OIC-CERT community.

b. Priority Area 17: ICT and Digital Information Structure

3. Goal 2.17.1 – Promote ICT skills and digital technologies and information structure.

- a. COMSTECH participated in the 11th Cyber Security Malaysia Awards, Conference and Exhibition 2019 organized by Cyber Security Malaysia in Kuala Lumpur, 23–26 September, 2019. The role of OIC–CERT in implementing the Cyber security activities outlined in the Implementation Program of the STI Agenda 2026 and a longer term collaboration between COMSTECH and OIC–CERT to achieve these goals was established.
 - b. A strategic collaboration was established between OIC–CERT and the Pakistani universities’ consortium on Cyber Security Research, the NCCS. It was agreed that COMSTECH would make efforts to expand the membership of OIC–CERT and encourage other national cyber security centres to cooperate and collaborate with OIC–CERT.
 - c. Development of training programs for OIC–CERT members during 2019 include:
 - i. CyberSecurity Malaysia has been arranging regular training for OIC–CERT and ASEAN countries.
 - ii. Starting 2017, “Certified Cyber Defender Associate” was introduced. Participation for 2018–2019 are as follows:
 - iii. 2019: 18 participants from 12 countries
 - iv. 2018: 14 participants from 10 countries
 - v. Malaysia is currently developing the Global Accredited Cyber Security Education (Global ACE) Scheme. The objectives of the scheme are:
 - To provide an alternative international information security certification scheme mainly for the OIC–CERT member countries; and
 - To increase the number of cyber security professionals with enhanced skill sets in tandem with the international standards. A soft launch for the Malaysia Chapter was held on 6 August 2018.
- development and access to knowledge and technology.
- a. OIC–CERT organizes an annual conference to exchange ideas and share information through presentations and forum sessions. Cyber Threats to the Public: Social Networks and Mobile Apps was hosted by Iran during 2018.
 - b. Malaysia organized two (2) and Indonesia organized one (1) online training during 2019. Malaysia conducted one in March 2019 on Handling Insider Threats: and the second on 19 June 2019 on “Honeynet Data Analysis through Lebahnet”. On 3 September 2019, Indonesia conducted “Social Engineering Attacks: Common Techniques and How to Prevent”.
 - c. OIC–CERT journal of Cyber Security (OIC–CERT JCS) is a platform for the academia and practitioners in cyber security around the world to share experiences and knowledge through research and publications. The inaugural issue of this journal was published in December 2018.
 - d. For 2019, Oman hosted the annual conference on 27–30 October 2019 in Muscat with the theme, “Cybersecurity Revolution”.
 - e. Developed a system to measure the response awareness of the OIC–CERT members. Azerbaijan through the CERT.GOV.AZ conducts “Awareness test” amongst OIC–CERT members. These tests act as a tool to collect statistical data for measuring response time of the members.
 - f. Indonesia conducted 2 technical events for the OIC–CERT members in October 2018.
 - i. OIC–CERT Cyber Security Technical Workshop on 12 October 2018.
 - ii. CodeBali International Conference on 19–20 October 2018.
 - g. Oman hosted the Forum of Incident and Security Teams (FIRST) Technical Workshop on 30 and 31 October 2019.
4. Goal 2.17.2– Advance the use of ICT as a tool for inclusive economic growth, e–governance and social and human

The OIC-CERT, as an affiliate member of the OIC, has always played a supportive role to the OIC. This can be seen through the various activities conducted in support of the OIC-2025 strategic agenda, specifically in two priority areas namely: Priority Area 2: Counter-Terrorism, Extremism, Violent Extremism, Radicalisation, Sectarianism, and Islamophobia; and Priority Area 17: ICT and Digital Information Structure. The OIC-CERT will continue to support OIC-2025 through its own strategic initiatives such as Standards and Regulations, Technical and Technology, Capacity Building and Awareness. For further information on the OIC-2025, please refer to the following documents:

- a. The OIC-2025 Programme of Action^[5]
- b. The OIC-2025 Programme of Action Implementation Plan 2016-2025^[6]
- c. OIC-2025: Program of Action Progress Report 2018-2019.^[7]

References

1. <https://www.oic-cert.org/en/theboard.html#.X2S6ni1h3UI>
2. <https://www.oic-cert.org/en/themandate.html#.X2QnQy1h1o4>
3. <https://www.oic-oci.org/upload/documents/POA/en/The%20OIC%20-2025%20POA%20Implementation%20Plan%202016-2025%20%28E%29.pdf>
4. https://www.oic-oci.org/upload/documents/POA/en/progress_report_2018_2019_en.pdf
5. <https://www.oic-oci.org/docdown/?docID=16&refID=5>
6. <https://www.oic-oci.org/upload/documents/POA/en/The%20OIC%20-2025%20POA%20Implementation%20Plan%202016-2025%20%28E%29.pdf>
7. https://www.oic-oci.org/upload/documents/POA/en/progress_report_2018_2019_en.pdf

Secure Your Zoom To Prevent Any Cyber-Attack Gloom

By | Mohamad Farhan bin Mohd Rahimi

Introduction

Zoom, a video telephony technology developed by Zoom Video Communications Incorporated, has recently seen a surge in downloads since the protracted COVID-19 pandemic led to quarantine orders being implemented worldwide.

Zoom video-conferencing is easy to manage and user friendly. It allows meetings of up to 100 participants at a time with a 40-minute limit on group meetings. The Zoom client has a simple and user-friendly design. Even the navigation menu makes it easy to manage meetings, contacts and groups. Each user only needs three easy steps to start a Zoom call or conference. Users need to have a Zoom account, a working webcam and stable Internet connectivity speed. Mobile users can download a mobile version to their smartphone to participate in calls compatible with Windows, Mac, Linux, iOS, and Android. By clicking on the Zoom invitation link, users can easily conduct online meetings.

Zoom encourages users to install desktop applications even though Zoom calls are accessible through a web portal. The reason is that using Zoom on web portal may limit access to online calls, particularly inbound. The Zoom web portal is primarily used for changing your profile, meeting settings, or Zoom Phone settings. User can also use the portal to schedule, view, and edit meetings.

Security Concerns

Security concerns over Zoom application have been growing since early April this year. Since the Covid-19 restrictions, Zoom's daily active users shot up as people had to rely on this video conferencing platform for work meetings, online classes, support groups and webinars. At that time, the application lacked secure end-to-end encryption features, which led to widespread data leaks and privacy issues.

With the rise popularity of Zoom around the world now, there is a cyber threat that threatens

the video conferencing platform to the detriment of users' privacy. Zoom bombing occurs when someone gains unauthorized access to directly enter a Zoom meeting and create a disturbance. These uninvited guests share their screens to bombard real attendees with disturbing content or videos. The main purpose of the attacker is to harass meeting participants.

Based on observations, it was found that security issues were triggered due to user failure in understanding the steps for Zoom application settings for the purpose of protection from third parties. Experts felt that the security configurations should be enabled by default, in addition to applications that essentially set that ease of use as a key aspect of the product to attract users.

Mitigation Measures

If you are among millions of users who have become loyal Zoom users, you may be wondering what all this means for you. Is Zoom conferencing safe to use or not? It is best not to use this medium if it involves sensitive and high-profile data especially if you want to discuss national or corporate confidential matters or disclose personal health information to patients.

Government and healthcare sectors which have strict information security and confidentiality policies should avoid video conferencing apps such as Zoom which may potentially compromise their respective agencies.

Users must review the importance of their online meetings as well as the associated risks and consequences before deciding on the use of Zoom. For example, online classes for schools and universities, after-work meetings, or even work-from-home meetings that do not expose confidential matters may be deemed acceptable.

To maintain the security of your next meeting, here are some basic security and privacy tips which can keep your online conferences safe.

1. Strong password for Zoom meeting

Automatically, Zoom will activate the “require meeting password” option when the host creates a new Zoom meeting and sets a random 6-digit password. This setting is one of the default security features that cannot be removed to ensure that only invited participants can access your Zoom meetings. Forgoing this security feature will allow anyone to gain unauthorized access to your meetings. There are additional options to set your own stronger passwords by incorporating features in the recommended password policy. This is one of the more effective ways to increase the level of privacy of an online meeting in the corporate sector.

2. Avoid sharing Meeting IDs

Each Zoom host includes a permanent Personal Meeting ID associated with their Zoom account. If the ID falls into the wrong hands, the perpetrators can check if there is an active meeting and the potential to participate illegally. Sending a Zoom invitation email is more convenient and secure than copying and pasting a URL to someone publicly. Users are encouraged to create a new meeting as a different ID will be generated by Zoom for security purpose.

3. Zoom Waiting Room

The concept of waiting room for the Zoom application can provide a high level of security to the users. For example, if a guest comes to your home, he or she will first be greeted by the host. Next, the host will check and identify who the person is before accepting the guest.

The same goes for Zoom application which also applies a similar concept. If this feature is enabled, the host will be able to determine who is authorized to enter the meeting before or during the meeting. Participants who join the meeting must wait in the waiting room for confirmation from the host. Both parties will receive an alert.

4. Update Zoom Client

You are strongly encouraged to install new update if you receive a notification to update your Zoom client. As we all know, installing the latest updates can prevent threats and fix any shortcomings in the application or system. Therefore, it is important and appropriate for users to scan and install the latest updates for security purposes. As Zoom is one of the most popular communication platforms, it is vulnerable to threats of unethical attackers. It is advisable for users

to install updates to get security patches for the latest vulnerabilities.

5. Disable screen sharing from participants

By default, Zoom has set the participant screen sharing settings without permission. This is to ensure that no participant attempts to distract the presenter or accidentally presses the sharing button while making a presentation.

6. Activate the lock meeting function

After making sure all the above tips are implemented, you can use the lock function of the meeting after ensuring that all the invited participants have joined the meeting. This function is to ensure that no one else can enter the meeting illegally without the permission of the host.

7. Beware of malware

There are various malware threats due to the increase in Zoom users. This includes fraud, phishing, and other COVID-19 themed attacks. Therefore, it is recommended that users install the Zoom installer or any latest security updates from Zoom's own official website (<https://zoom.us/>). Avoid downloading Zoom-related applications from third-party sites which may pose a risk.

8. Use a randomly generated ID

If you use the Zoom Pro version, you can apply your own ID to make it easier for users to remember the ID you have set. Even so, an attacker might be able to guess or carry out a brute force attack to get your ID. It is better to continue using the random ID provided by Zoom. Avoid sharing your ID, especially on social media.

9. Use alternatives

Zoom is not the only video conferencing platform, but it is easily the most popular. Should a user have any concerns about Zoom, there are a number of other useful video conferencing applications too. Secure video conferencing is crucial for any business no matter the size.

Conclusion

Most of us still utilize the Zoom platform to interact virtually with friends and family. If you are using it for social purposes, then the application is quite safe. So far, Zoom has done its best to address reported security issues. Zoom has also added new security features and improved its privacy settings.

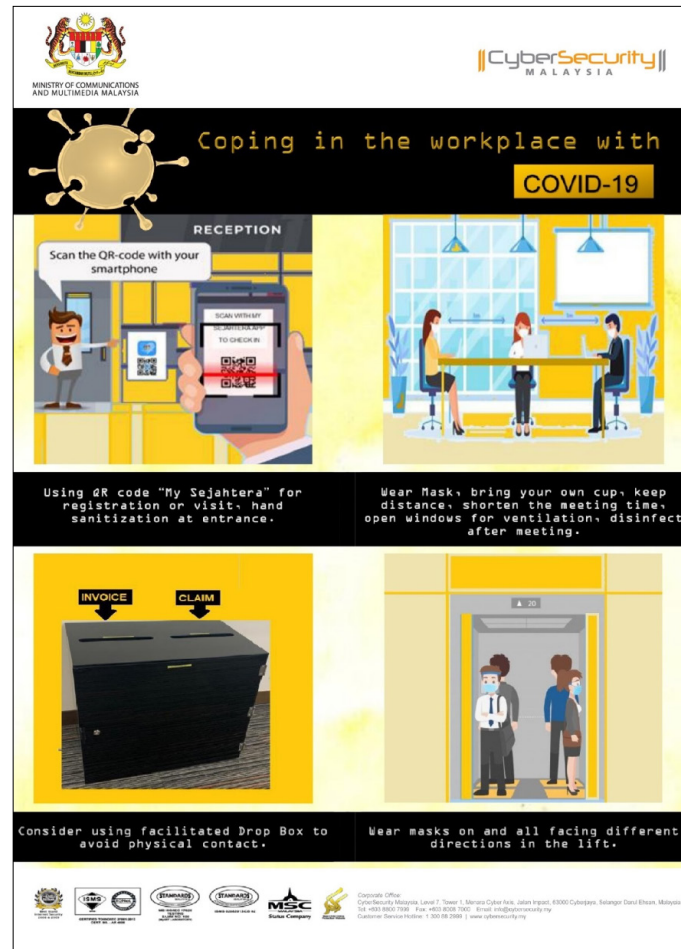
Despite the latest enhanced features on Zoom, companies are advised to remain vigilant by considering the above tips to increase security and productivity of your meetings. Let's keep in mind that no online application or web portal is guaranteed 100% safe from cyber threats. Stay alert and stay safe!

References

1. T. Charlotte, "Zoom explained: Understanding (and using) the popular video chat app", (2020, August 12). Retrieved from <https://www.computerworld.com/article/3570623/the-zoom-meeting-app-explained-understanding-and-using-the-popular-video-chat-software.html>. [Accessed 7-September-2020]
2. W. Paul, "Zoom security issues: Here's everything that's gone wrong (so far)", (2020, July 31). Retrieved from <https://www.tomsguide.com/news/zoom-security-privacy-woes>. [Accessed 7-September-2020]
3. O., Kate, "Zoom Security Tip: Avoid the App and Do This Instead, Here's Why", (2020, April 29). Retrieved from <https://www.forbes.com/sites/kateoflahertyuk/2020/04/29/zoom-security-tip-avoid-the-app-and-do-this-instead-heres-why/#7308578248d9>. [Accessed 7-September-2020]
4. O. Charlie, "Zoom security: Your meetings will be safe and secure if you do these 10 things", (2020, April 22). Retrieved from <https://www.zdnet.com/article/make-sure-your-zoom-meetings-are-safe-by-doing-these-10-things/> [Accessed 7-September-2020]
5. J. Matthew, "Getting Zoom Security Right – 8 Tips for Family and Friends", (2020, May 5). Retrieved from <https://www.tripwire.com/state-of-security/security-data-protection/getting-zoom-security-right-8-tips-family-friends/> [Accessed 7-September-2020]
6. D. Nield, "How to keep your Zoom chats private and secure", (2020, May 4). Retrieved from <https://www.wired.com/story/keep-zoom-chats-private-secure/> [Accessed 7-September-2020]
7. Gadgets Now Bureau, "Government has 9 tips that you must follow for safe Zoom video meetings", (2020, April 22). Retrieved from <https://www.gadgetsnow.com/slideshows/government-has-9-tips-that-you-must-follow-for-safe-zoom-video-meetings/Disable-join-before-host-feature-in-the-settings-menu-of-Zoom-chat-app/photolist/75284794.cms> [Accessed 7-September-2020]
8. R. Hodge, "Using Zoom while working from home? Here are the privacy risks to watch out for", (2020, April 2). Retrieved from <https://www.cnet.com/news/using-zoom-while-working-from-home-here-are-the-privacy-risks-to-watch-out-for/> [Accessed 7-September-2020]
9. L. Abrams, "How to secure your Zoom meetings from Zoom-Bombing attacks", (2020, March 31). Retrieved from <https://www.bleepingcomputer.com/news/software/how-to-secure-your-zoom-meetings-from-zoom-bombing-attacks/> [Accessed 7-September-2020]
10. W. Jane, "Coronavirus: Zoom is in everyone's living room – how safe is it?", (2020, March 27). Retrieved from <https://www.bbc.com/news/technology-52033217>. [Accessed 7-September-2020]
11. "Zoom Help Center", Retrieved from <https://support.zoom.us/hc/en-us>. [Accessed 7-September-2020]

Coping In The Workplace With Covid-19

By | Nur Faridah Binti Mohd Zainudin & Noorhannan Binti Khairuddin



The COVID-19 pandemic has brought an unprecedented impact on companies and workers worldwide. Malaysia recorded a total of 1,240 new COVID-19 cases on 26 October 2020. It is the highest daily increase in new infections since the beginning of the pandemic. In view of this, the Ministry of Health (MOH) has advised for workers to continue following the Standard Operating Procedures (SOP) in place and recommended that employers adhere to safety guidelines as the new normal.

Cybersecurity Malaysia has also taken significant steps to fight this pandemic and to flatten the curve again. To properly manage exposure to risks related to COVID-19, employers must keep their employees updated on the latest health and safety measures to safeguard their well-being. It is important for each of us to do our part by observing safe distancing and practising good personal hygiene to reduce the risk of transmission.

Covid-19 Safety Guidelines In Workplace

1. Visitors are required to wear a mask before entering the office premises. Kindly scan "My Sejahtera" QR code to enable contact tracing. Use hand sanitizer at the office reception
2. Wear a mask, bring your own cup, maintain one-metre distance from each other, keep meetings short, open windows for ventilation, disinfect after meeting
3. Consider using a 'Drop Box' to avoid physical contact
4. Wear a mask and keep apart in the lifts

Signages must be posted to remind employees and visitors to observe all SOPs in place.

Crime Prevention Through Environmental Design: Elements And Illustration

By | Mohd Syamsyul Bin Shuib

Introduction

After midnight, you feel like having a snack but there is nothing at home. The next thing that comes to your mind is the nearby 24-hour convenience store. You walk to the row of shops where the convenience store is located. All the other shops are closed and dark except for the convenience store which is open and brightly lit. There are benches outside the store where two customers are chatting and enjoying their hot coffee. You can clearly see the cashier inside the store as the front glass panels have no poster bills blocking your view. You enter the store through the glass door, purchase your favourite snack and return home. Without you realizing, the convenience store had adopted a few CPTED method as part of its crime prevention strategy.

CPTED or Crime Prevention Through Environmental Design is a multi-disciplinary approach of crime prevention that uses urban and architectural design and the management of built and natural environments. The official definition of CPTED as given by the late Tim Crowe of the US National Institute for Crime Prevention is:

The proper design and effective use of the built environment that can lead to a reduction in the fear and incidence of crime and an improvement in the quality of life. ...The goal of CPTED is to reduce opportunities for crime that may be inherent in the design of structures or in the design of neighborhoods (2000: 46).

CPTED is used worldwide and functions by reducing a criminal's ability to commit crime. It enhances safety by influencing the physical design of our environment and encouraging positive social interaction. CPTED recognizes that our environment directly affects our behavior, because we constantly respond to what is around us. These responses help us to interact safely in our communities.

According to the International CPTED Association (ICA), CPTED has its basic premise that the

opposite design and effective use of the physical environment can lead to a reduction in the incidence and fear of crime, thereby improving the quality of life. It acknowledges the idea that the community residents can play an active part in crime prevention by recognizing the environmental conditions which make certain areas more attractive as targets to criminals. CPTED relies on four elements that are different but complementary, namely

natural surveillance, territorial reinforcement, access control and maintenance.

CPTED Elements

1. Natural Surveillance

Natural surveillance is the state and condition of a site that is observed by eyes and heard by ears. With this concept, various parts of the site are observable through the use of human sense during both day and night without support from any electronic or mechanical devices. In other words, "see and be seen" is the overall goal when it comes to natural surveillance. This strategy works well because criminal will not commit crimes in areas where they feel exposed to witnesses.

Based on the convenience store scenario above, the store maintained its natural surveillance by keeping the front glass panel or windows clear from posters and advertisements. Another example of natural surveillance is the elevators in the shopping malls located in the middle of the building with glass interiors. Everybody can see what is going on inside the elevator as compared to older design where elevators were located at the end of buildings and far from the main aisles. With this approach, crime would decrease and elevators can now be considered as safe areas.

2. Natural Access Control

In CPTED context, natural access control refers to the use of symbolic or actual

barriers to restrict, encourage or channel the movement of people or vehicles into, out of and within designated areas. This can be achieved by designing streets, footpaths and building entrances so that public routes and private areas are clearly indicated and understood. The design will encourage and attract movement of people to some places or certain spaces and restricts them from others.

Natural Access Control also utilizes the use of lighting, fences, walkways, signage and landscape to clearly guide people and vehicles to the proper entrances. The goal with this CPTED principle is not necessarily to keep intruders out, but to direct the flow of people to the designated route while reducing the opportunity for crime. Another type of barrier is bollard which is commonly used by placed at walkway gate to prevent vehicle entry but allow pedestrian entry. This strategy would be effective to discourage vehicle-related crime.

In relation to the convenience store scenario above, the store uses bright lights and signage to attract customers. Another example could be a public park where plants and shrubs are used as barrier for the walkway.

3. Territorial Reinforcement

Territorial reinforcement refers to creating or extending a "sphere of influence" by utilizing physical designs such as landscaping plants, pavements and fences to develop a sense of proprietorship or ownership over certain areas. This would delineate the transition from public space to private space, furthermore discourage potential trespassers.

For example, landscaping plants can be placed around a front yard. The plants separate the public roadway and sidewalk from the front yard and makes a clear statement that non-legitimate users are not welcome in the yard. Using the above convenience store scenario, some stores have decorative, low level fencing at the front. This serves as an indication of the ownership of the area in line with the territorial reinforcement.

4. Maintenance

Care and maintenance of the adopted CPTED strategy need to be in place to allow for continual use and security of the protected area. The upkeep of an area demonstrates

that someone cares and indirectly create the fear of crime. On the other hand, neglected and poorly maintained areas are breeding grounds for criminal activity. In March 1982, an article titled "Broken Windows" by James Q. Wilson and George L. Kelling introduced the broken windows theory whereby if a window in a building is broken and left unrepaired, then all the rest of the windows will soon be broken. Unrepaired broken window is a signal that no one cares, and so breaking more windows would have no impact and costs nothing. This theory suggests that a neglected area will lead to mistreatment by people, while a maintained area will lead to proper treatment.

In most CPTED implementation, lighting and landscape require proper planning and maintenance. For example, there is no point installing a good lighting system for the convenience store if nobody replaces the bulbs when the lights go out. Similarly, keeping the shrubs around the store trimmed is necessary to maintain clear visibility.

Advantages

The main advantages of CPTED usage are convenience and cost which can described as follows:

- CPTED principles are mostly subtle and unobtrusive in contrast to other security measures such as surveillance cameras or metal detectors. People would not even notice the CPTED implementation which is addressing the security while balancing it with comfort.
- CPTED design strategies offer cost effectiveness as it does not require expensive security solutions. At the same time, it also contributes to lower maintenance cost. Instead the cost of complying to CPTED principle such as additional outdoor lighting, glass windows for natural surveillance and landscape design would have been incorporated during building design and construction phase.

Conclusions

CPTED is derived from the idea of proper design and effective use of the built environment leading to reduction of crime potential as well as improvement in the quality of life. If an area is well laid out, the probability for a crime to happen could be much lower. CPTED also combines the effort from law enforcement, architects, city planners, landscape and interior designers together with residents to create a safer environment for the community. Security is built within the infrastructure of the environment and meld into the landscape. Overall, CPTED balances between security and comfort as improper security implementation could lead to sterile areas.

References

1. Crowe, T. (2000). *Crime Prevention Through Environmental Design: Applications of Architectural Design and Space Management Concepts*, 2nd edition. Oxford: Butterworth-Heinemann.
2. *Introduction to Private Security, Fifth Edition* Karen M.Hess, 2009
3. Rick Draper and Emma Cadzow (2004), *Crime Prevention through Environmental Design: International Security Management and Crime Prevention Institute*
4. Jean-Thomas Henderson (2018), *The four pillars of Crime Prevention through Environmental Design (CPTED)* <https://insights.ehotelier.com/insights/2018/05/24/four-pillars-crime-prevention-environmental-design-cpted/>
5. Cozens, P.M., Saville, G. and Hillier, D. (2005). *Crime Prevention Through Environmental Design (CPTED): A Review and Modern Bibliography*. *Journal of Property Management*. Volume 23, Issue 5, pp328-356.
6. Lamoreaux D, Sulkowski ML. *An alternative to fortified schools: Using crime prevention through environmental design (CPTED) to balance student safety and psychological well-being*. *Psychol Schs*. 2020;57:152-165. <https://doi.org/10.1002/pits.22301>

Data Sanitization - Definition, Importance, Methods And Advantages

By | Nurkhairunnisya Binti Mohamad Khairi & Muhammad Anis Farhan Bin Yahaya



Data as the new "oil" (Source: Google)

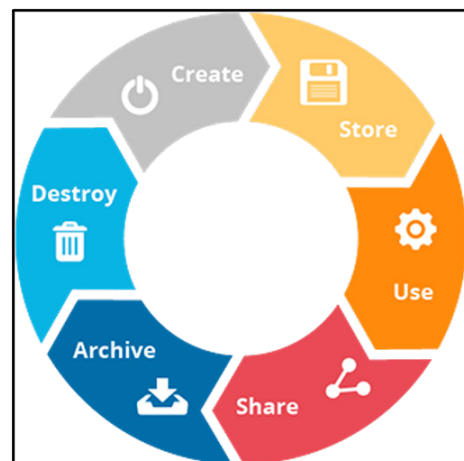
For many years, oil has been one of the main and arguably the most valuable commodities around the world. However, it is no longer considered the main resource. Today, data is considered one of the most important assets for an individual or organization. Data represents one of the main components used to derive better decisionmaking that creates revenue opportunities, cost savings, and more efficient operations (Fauerbach, 2017).

Data needs to be handled and maintained properly once it has reached the end of its life or if it is deemed trivial, obsolete, or redundant. One has to dispose of the data in the right way to prevent any misuse by irresponsible entities which will bring about negative consequences to the individual or organization.

What Is Data Sanitization?

Data sanitization is a crucial and important phase in the data lifecycle management. It is the process of erasing, removing, or destroying

data trails from any data storage devices such as hard disk drive (HDD), solid-state drive (SSD), flash drive, mobile phone, and memory card. Once it has been sanitized, no data can be found and cannot be recovered again by any means, even with the assistance of any advanced data recovery software tools.



Data Lifecycle Management (Source: Google)

Importance Of Data Sanitization

The current trend of accelerated technological developments in the digital devices sector is resulting in frequent hardware upgrades and software updates for better and more efficient business administration and operations. At the same time, the enormous amount of data being digitized and stored in digital devices has made data security critical to everyone. The sanitization of the hard disk becomes a necessity when selling, donating, returning, reusing, or disposing of your hard disk, which is one of your most significant IT assets.

There are several reasons for it. Some are as follows:

1. You and/or your organization potentially could be at risk of losing your personal, private, and confidential information to individuals or organizations with ill means. They may extract data from your hard disk and use it for their benefit or to malign your and/or your organization's reputation.
2. You and/or your establishment could be at risk of losing a large amount of significant information to unauthorized users as they are able to recover the data by using any recovery software or services.
3. The organization, particularly the government departments has legal obligations set up by The Malaysian government that they should always abide by to maintain work culture and task-flow. Organizations should comply with several international laws such as Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act (SOX) and also the Malaysian Personal Data Protection Act (PDPA) 2010 to prevent the breach of your data.
4. Simply deleting data using Delete or Shift + Delete key simultaneously or even formatting your hard disk is still unsafe. It does not remove the data from the hard disk completely, only the link (reference) to the stored data is lost while the data remains on the disk.

What Is MyCyberSecurity Clinic?

MyCyberSecurity Clinic (MyCSC), an initiative by CyberSecurity Malaysia, an agency under the Ministry of Communications and Multimedia Malaysia (MCMC) is a trusted entity that specializes in data recovery and data sanitization. With the tagline "Where trust comes first", MyCSC manages the information security according to the requirements in the ISO/IEC 27001 Standards to achieve an overall information security assurance through the preservation of confidentiality, integrity, and availability.



To protect a business's relevant information during the entire data security lifecycle, ISO/IEC 27001 Standards, which is an international standard on how to manage information security, provides two specific controls, Annex A.8 and Annex A.11 related specifically to information disposal as below:

- a. Control A.8.3.2 – Disposal of Media
 - Whenever a media shall be discarded, the use of procedures should be considered to ensure proper information disposal.
- b. Control A.11.2.7 – Secure Disposal or Reuse of Equipment
 - Equipment containing storage media shall be verified to ensure it is free of sensitive information before disposal or re-use.

Popular Methods Of Data Sanitization

In general, data sanitization services provided by MyCSC are based on the type and characteristics of the digital storage device, state of data, and the required level of data sanitization. There are three well-known methods of data sanitization which are physical destruction, cryptographic erasure, and data erasure.

First, Physical Destruction is a process of destroying the storage devices physically which means, it can be achieved by using a crushing machine, shredder machine, and degaussing machine. Degaussing is a form of physical destruction whereby data is exposed to the powerful magnetic field of a degausser and neutralized, rendering the data unrecoverable, but the drives or tapes cannot be re-used upon completion. However, the Degaussing method is ineffective when applied to SSD. Physical destruction is an effective method of destroying data.



Example of Degaussing Machine (Source: Google)

Second, Cryptographic Erasure is the process of using encryption software (either built-in or deployed) on the entire data storage device and erasing the key used to decrypt the data. While the data remains on the storage device itself, by erasing the original key, the data is effectively impossible to decrypt. As a result, the data inside the storage media is unrecoverable. Cryptographic erasure is a quick and effective method to achieve data sanitization. However, sometimes it does not meet the regulatory compliance requirements.

Finally, Data Erasure is a software-based method of obliterating data by securely overwriting data from any storage device using zeros and ones onto all sectors of the device. By overwriting the data on the storage device, the execution of this process makes the original data impossible to be recovered. In order to achieve data erasure, the software must:

1. Allow for selection of a specific standard, based on the individual's or organization's specific needs and requirements.
2. Verify the overwriting process has been successful and remove data across the entire storage devices.

3. Produce a tamper-proof report containing information of erasure process has been successful and written to all sectors of the device, along with the information about the storage device including the type, manufacturer, model number, serial number & capacity of the particular storage devices, and also the method of data sanitization that has been used.

Although data erasure is the most effective method of data sanitization, it is a time-consuming process compared to physical destruction and cryptographic erasure.

Advantages Of Data Sanitization By MyCyberSecurity Clinic (MyCSC)

Data sanitization ensures the security of data during the hardware upgrading and/or disposal stage by sanitizing the storage devices that are being replaced, thus mitigating the risk of data leaks when the replaced drives are reused by other entities. Furthermore, the replaced or discarded digital storage devices can also be safely reused or recycled. Hence, it will contribute to the eco-friendly movement promoted by the government and reduce the cost to the individual or organization.

Through data sanitization service offered by MyCSC of CyberSecurity Malaysia, we will address your needs for safe and secure deletion of data from storage devices that are to be retired, upgraded, or reallocated. With information security at the core of our service and our identity as the national custodian of cybersecurity specialist agency, engaging standard and secure process, we provide an effective and trustworthy data sanitization service. Over the years, MyCSC has received and handled numerous data sanitization cases from both the public and private sectors.

MyCSC's technical staff are well-trained, highly skilled and knowledgeable. We keep abreast with emerging industry trends and cutting-edge technologies, particularly on data sanitization. Furthermore, MyCSC's data sanitization lab is equipped with the latest software tools and equipment to ensure that the process of data sanitization can be performed well and within a given standard level agreement or SLA. Our team will ensure that our customers always receive the best service.

Deepfake: Fake Videos – Generated by AI

By | Ahmad Haziq Ashroffie Bin Hanafi

Introduction

Fake news has become a matter of grave public concern due to its pervasiveness, impacting our existing civil culture and creating social disturbance in recent years ^[1]. Businesses are increasingly worried about the rise of fake news and how it might affect them. Fake news is fabricated material presented as news which is meant to misinform the public. False information can easily spread to millions of people via social media ^[2]. One of five Internet users frequently receive news updates from social media platforms such as YouTube and Facebook ^[3]. The spike in video popularity demonstrates the need for tools and devices to validate the authenticity of streaming media and its content since new technology can easily manipulate video footages. It is becoming extremely challenging to decide what to believe in, which impacts rational decision-making, acceptance of truth, and validating the source. In today's digital era, information is perceived as "post-truth", and marked by digital misinformation and information warfare led by malicious actors carrying out misleading public opinion campaigns.

Recent technological advances have resulted in a high number of hyper-realistic videos called deepfakes. This technology uses face swaps and leave no evidence of distortion. An example can be seen in **Figure 1** below, where an AI program called DeepFace Lab that is available on Github ^[4] is used to create a realistically-appearing video of the former US president delivering a speech at the White House. The video does not only seem convincing but it also sounds convincing enough to cause individuals with zero knowledge about deepfake to believe the content.



Figure 1: Original video and deepfake video of Barack Obama ^[5]

How Is It made?

Deepfake is a result of the combination of merge, substitution and the superimposition process performed by algorithmic capabilities made by Artificial Intelligence (AI), that generates fake yet authentic videos and pictures. For instance, using facial and vocal data of a person that was taken without consent from their social media page, and converting it into an entirely different video to produce unethical content that leads to humour, pornographic or political content in contrast to the original content.

To create a deepfake ^[6], the "maker" must first train the algorithmic neural network for hours using an actual video footage of a human (or a selected target) to replicate a video of someone, giving it a realistic "understanding" of what it looks like from a range of viewpoints and under different lightings. Next, it will be combined with the trained network using computer graphics to superimpose a clone of the individual to another actor (such as placing the image on top of each other where both look similar and coincide). The image in **Figure 2** below shows how AI trains the model under different lighting and quality to superimpose Elon Musk, the CEO of TESLA Inc. on top of Jeff Bezos, the CEO of Amazon Inc.



Figure 2: Deepfake AI model training using Jeff Bezos and Elon Musk footage ^[7].

AI will try to match the video frame-by-frame between the source (Jeff Bezo's footage) and the learned-source (Elon Musk's footage). While doing this, AI will also calibrate the parameters of the "fake" scene such as the lighting in the scene, the motion of the person, the lip sync and other facial feature matchmaking and alteration

as well as audio tuning for the audio output or in this case, the voice of the individuals in the final product. These components are done every second for each frame alteration until the AI considers the frame good enough to be used for the final deepfake video.

Although the addition of AI and advancement in a more high-end and powerful CPU and GPU speeds up the process, this process requires plenty of time to create a convincing composite that puts a person in a fully fictitious scenario. To avoid blips, distortion and artifacts in the image, the developer must also manually tweak several parameters for the trained AI algorithm. The method is far from simple but still possible for beginners with the availability of developer notes and easy-to-use manuals as the software develops and matures over time.

Detection Through Human Sight

When it comes to deepfakes, the human vision can be used to a certain extent to detect tools used in producing a deepfake video. Deepfakes tend to produce artifacts that when observed close enough can reveal the tampering of videos. Here are a few steps non-professional people can do even without high-end AI detection tools to identify an altered video ^[8]:

1. Most of the time, deepfake videos are about face alteration. So check the face of the individuals in the video for any sign of smoothness, wrinkles, aging effects or even the face bone structure and compare it against the source (the real picture/video of the individual). If it is a deepfake video, you will start to notice glitches or blurred effects each time the person's face move, even slightly.
2. Next, check the eyes. One of the problems with deepfake (if not trained enough) is its transformation of the eye because AI generally struggles to represent the human face's natural features within a video scene. It might be slightly slanted, an eye may appear smaller/bigger or even "lacklustre". Another characteristic that you can look out for is the rate of blinking. Is the eye blinking too much or too little?
3. Pay attention to the glasses and lighting in the scene. Check if the glare is too bright or non-existent and whether the lighting condition changes when the person moves. AI tend to struggle with adapting to proper lighting even in a natural scene from an

unaltered video, let alone an altered one. Glass materials in the scene can also be a reference point for this effect.

4. Finally, most deepfakes can be traced back to its reference videos used to train the AI. As such, when you come accross any of these videos, please search the web for any similar content first. Deepfake creators tend to use popular videos available on social media platforms such as YouTube or Facebook to train AI, especially when it comes to prominent or highly influential individuals.

These are certain steps that can be done to detect common and low-quality deepfakes. If these steps are not convincing enough, you may ask for a proper analysis from experts in this particular area. They have the proper tools and in depth-knowledge to detect high-quality deepfakes.

Why Is It A Concern?

Digital video and picture manipulation is not something new. Advancement in AI, the convenient access to video manipulation software, and the volume of dissemination of doctored videos are growing at an alarming rate. The two latter points are the primary reasons as to why deepfakes are becoming more concerning than any previous photo and video editing software.

Sexual violation allegations can affect the lives of innocents greatly. Brian Banks is an example of a fraudulent sexual harassment claim [9]. Despite being innocent, he was given two difficult choices that would both land him in prison. He was found innocent only after having served a five-year prison sentence and being labelled a criminal. He was robbed out of a bright career in the NFL and five years of his life was wasted on mere allegation [10]. To make matters worst, the accuser was only sentenced to minor charges.

You can imagine how much more powerful an accusation can be if extremely well-doctored footage were to be presented in a court, without clear ways to distinguish whether it is fake or real. This will also be a problem for victims who come forward with an actual video footage. It may be difficult for them to prove that their footage has been doctored. Considering that the court requires time to validate each evidence every time it is presented, this situation can cause a delay and further complicate the case.

Deepfakes are a powerful tool that can affect not only the lives of individuals but also a growing threat to democratic elections of a country. In Malaysia, where Islam is the official religion amongst the majority Muslim–Malay community, subjecting politicians to sex scandals could sway voters away.

Conclusion

The deepfake phenomenon is an issue that must be taken seriously. With various software readily accessible to the public, it is only a matter of time before the technology's full potential is realized. If you are making your own deepfake, ensure that you thoroughly read the terms and conditions of the apps to understand what your information does online and request for your information to be removed from any archive in which it might be kept.

References

1. Statista. *Fake news worldwide - Statistics and Facts*. Available online: <https://www.statista.com/topics/6341/fake-news-worldwide/> (Accessed on 14th October 2020).
2. S. Kumar, N. Shah. *False Information on Web and Social Media: A survey*, *Social Media Analytics: Advances and Applications*, vol.1, no.1, April 2018.
3. E. Shearer, K. E. Mutsaers. *News Use Across Social Media Platforms 2018*. Pew Research Center Journalism and Media. Available online: <https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/> (Accessed on 15th October 2020).
4. I. Pevrov, D. Gao, N. Chervoniy. *DeepFaceLab: A simple, flexible and extensible face swapping framework*. Available online: <https://github.com/iperov/DeepFaceLab> (Accessed on 15th October 2020).
5. J. Vincent. *Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news*. Available online: <https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peepe-buzzfeed> (Accessed on 14th October 2020).
6. S. Adele. *What Are Deepfakes and How Are They Created?*. *IEEE Spectrum*, 29 April 2020. Available online: <https://spectrum.ieee.org/tech-talk/computing/software/what-are-deepfakes-how-are-they-created> (Accessed on 16th October 2020).
7. A. Robertson. *I'm using AI to face-swap Elon Musk and Jeff Bezos, and I'm really bad at it*. Accessed online: <https://www.theverge.com/2018/2/11/16992986/fake-app-deepfakes-ai-face-swapping> (Accessed on 17th October 2020).
8. M. Groh. *Detect DeepFakes: How to counteract misinformation created by AI*. MIT Media Lab. Available online: <https://www.media.mit.edu/projects/detect-fakes/overview/> (Accessed on 18th October 2020).
9. J. Catsoulis. *'Brian Banks' Review: Falsely Accused, and Fighting Back*. *The New York Times*, 8 August 2019. Available online: <https://www.nytimes.com/2019/08/08/movies/brian-banks-review.html> (Accessed on 16th October 2020).
10. A. Brockington. *In 2019, The Real Brian Banks Has His Life Back — & A New Career*. Available online: <https://www.refinery29.com/en-us/2019/08/240005/where-is-the-real-brian-banks-today> (Accessed on 17th October 2020).

Business Continuity And COVID-19

By | Nahzatulshima Binti Zainuddin & Nurin Iman Binti Mohammad Azmi

Introduction

Business continuity is the advance planning and preparation undertaken to ensure that an organization will have the capability to operate its critical business functions during emergency events. Emergency events may include natural disasters, fires, power failures, pandemic, and cyber-attacks.

Today, the world is fighting a global pandemic caused by a virus called the coronavirus (COVID-19). The COVID-19 pandemic has disrupted all aspects of the business chain. Employees are barred from getting back to the office to work. Millions of people are forced to stay at home. One is not allowed to venture unless with valid reason. Work meetings and gatherings are banned to uphold social distancing and prevent the infectious spread of COVID-19. Festivals and international conferences have to be cancelled due to travel restrictions. It is no longer business as usual, and the seriousness of the domino effect towards the end value chain such as households must be recognized. When households are no longer spending, that's when more businesses start to collapse.

Creating A Business Continuity Plan

Business continuity is vital to rebuild the economy during this pandemic. In the event of an outbreak, organizations must be able to respond swiftly to maintain business continuity. Here are some practical tips to ensure your business continuity during the COVID-19 outbreak.

1. Preparation

Prepare a Business Continuity Plan (BCP). The plan ensures your employees and assets are protected and will be able to recover promptly in the event of a disaster. Your BCP must include the following:

- Identify priorities and critical processes
- Plan for working and scheduling arrangements
- Plan for continuity of leadership

- Educate employees on good personal hygiene and infection prevention or control
- Ensure that employees know their roles and responsibilities during the outbreak
- Set up a communication channel so that employees can ask questions or report their status
- Make sure all important documents are in soft copy and they are backup appropriately (cloud storage as a backup is a good option, but ensure the security and confidentiality as well)
- Implement all the recommendations from the World Health Organization (WHO), Kementerian Kesihatan Malaysia (KKM), etc.

2. Finance and Business Management

Reshape the strategy to maintain business continuity, especially in finance management. During the economic uncertainty, managing cash and liquidity is crucial. Here is what you can do:

- Determine how the crisis affects budgets and business plan
- Identify key stakeholders and prepare them on a contingency plan during the outbreak
- Identify the financial and operational levers that can be pulled to conserve and generate cash, and potentially increase access to funding
- Assess financial and operational risks and respond quickly
- Identify alternative supply chain options
- Evaluate short-term liquidity
- Assess prospects for relief from the tax provisions or other local measure
- Effectively manage cash taxes

3. Cyber security and Information Technology (IT) infrastructure

As organizations extend remote working to ensure business continuity, security risks have shifted from the fortified corporate landscape to the more vulnerable off-site areas. What you need to do is:

- Check security and monitoring of applications for remote access
- Test applications for remote access such as Virtual Private Network (VPN)
- Perform awareness campaign for specific cases of social engineering attacks in communication-related to crisis
- Accelerate digital transformations e.g. digital document management system or cloud computing but at the same time do not neglect security features
- Enable the security of Information and communication technologies (ICT) tools such as video conferencing, email and IT infrastructure to empower work from home and online meetings

1. 60% of the organizations managed to get staff involved in time-critical business process to work remotely within 3 days.



2. 88% of the organizations agreed that BCM was helpful to minimize damage in their organizations.

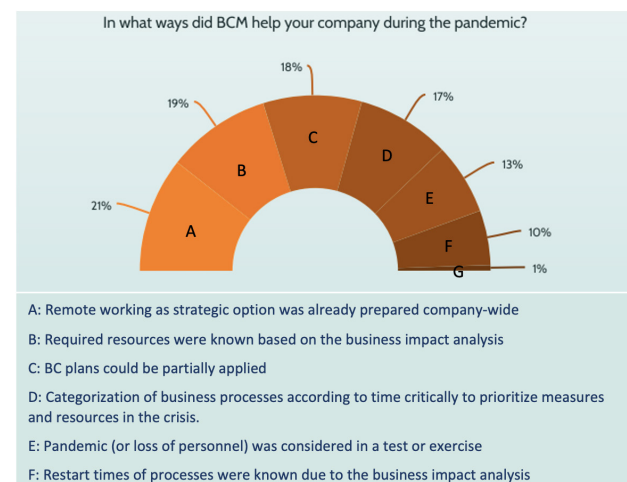


Effectiveness Of BCM During COVID-19

Disaster Recovery Institute defines Business Continuity Management (BCM) as “holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities”. BCM is not a new subject. It has long been practiced by most organizations, especially financial institutions. BCM was widely adopted ever since the September 11 terrorist attack, and even more so now with the recent COVID-19 outbreak. Since the global pandemic has affected many organizations worldwide, it would be interesting to see how BCM could be a critical success factor for organizational resilience.

A study on the effectiveness of BCM during the COVID-19 Pandemic has been conducted by Controllit AG, Germany involving 104 organizations in 19 countries. According to the study, 75% of the correspondence have established BCM in their organizations. The study revealed several interesting findings:

3. Most organizations indicated that BCM is effective as remote working has already been incorporated as part of their strategies while required resources have also been identified before in business impact analysis.



This study showed that BCM has helped organizations in many ways. While existing BCM frameworks did offer benefit, it is evident that they can be improved based on the key learnings over the past few months. These include reviewing employee's arrangement during crisis; revisiting business continuity plan and improving where necessary; evaluating and strengthening supply chain; as well as enhancing communication with key stakeholders.

Benefits Of BCM Certification

There are many ways of developing and implementing BCM in an organization. Renowned international bodies in BCM such as Business Continuity Institute (BCI), Disaster Recovery Institute (DRI) and BCM Institute (BCMI) provide different methodologies for BCM development. Most of the methodologies comply with ISO 22301 Business Continuity Management Systems which is the international standard for business continuity management.

An organization can be certified with ISO 22301 upon successful third-party audit performed by a certification body. The requirements specified in ISO 22301 are generic and intended to be applicable to all organizations, regardless of type, size and nature of the organization. Getting an ISO 22301 certification grants several benefits which include:

1. Compliance to legal and regulatory requirements;
2. It guarantees organization a competitive advantage and enhances corporate reputation; and
3. Annual independent assessment of organization's performance in BCM.

The ISO 22301 was first published in 2012. It was recently revised and published as ISO 22301:2019 on 30th of October 2019 with 3-years transition period. Due to the COVID-19 pandemic, the transition period has been extended to another 6 months.

Conclusion

BCM is an ongoing pursuit, not a one-time project. This pandemic is a unique opportunity for organizations to learn how to better prepare and equip themselves for future uncertainty. For organizations with BCM in place, this would be the best time to review and assess its corporate preparedness and resilience. For organizations which have none, it is an opportune time to consider implementing a BCM in their organization.

References

1. Anonymous. (2020, Jun 22). *BUSINESS CONTINUITY: HOW INDUSTRIES ARE ADAPTING TO A POST-COVID-19 WORLD*. Retrieved from Management Events: <https://managementevents.com/news/business-continuity-how-industries-are-adapting-to-a-post-covid-19-world/>
2. Anonymous. (n.d.). *Business continuity management standard ISO 22301 revision*. Retrieved from bsi.: <https://www.bsigroup.com/en-my/iso-22301-business-continuity/revision/>
3. Anonymous. (n.d.). *ISO 22301:2012 Business Continuity*. Retrieved from Certification Europe: <https://www.certificationeurope.com/certification/iso-22301-business-continuity-management-certification/>
4. Harsha Basnayake, C. M. (2020, March 18). *COVID-19 business continuity plan: Five ways to reshape*. Retrieved from EY: https://www.ey.com/en_my/strategy-transactions/companies-can-reshape-results-and-plan-for-covid-19-recovery
5. Kelton, W. (2020, July 24). *Business Continuity Planning (BCP)*. Retrieved from Investopedia: <https://www.investopedia.com/terms/b/business-continuity-planning.asp>
6. Long, R. (2017, August 1). *What is Business Continuity? - Business Continuity 101*. Retrieved from MHA CONSULTING: <https://www.mha-it.com/2017/08/01/what-is-business-continuity/>
7. Said, A. M. (2020, May 4). *The financial impact of COVID-19*. Retrieved from Deloitte: <https://www2.deloitte.com/my/en/pages/financial-advisory/articles/financial-impact-of-covid-19.html>
8. Anonymous. (n.d.). *The effectiveness of BCM in the current pandemic*. Retrieved from Controllit AG: <https://www.controllit.de/de/blog/category/news/die-wirksamkeit-von-bcm-in-der-aktuellen-pandemie>
9. Thum, Y. (2020). *Coronavirus (COVID-19): 8 Practical Tips For Business Owners With Physical Stores*. Retrieved from StoreHub: <https://www.storehub.com/blog/coronavirus-covid-19-business-owner-tips/>

Remote Audit As A Continuity Tool During Covid-19

By | Razana Binti Md Salleh & Noor Aida Binti Idris

Introduction

COVID-19 is an infectious disease caused by a newly discovered strain of coronavirus, a type of virus known to cause respiratory infections in humans (Coronavirus disease (COVID-19) pandemic, 2020). This new strain was only discovered in late December 2019, when an outbreak involving pneumonia of an unidentified cause emerged in Wuhan, China. The COVID-19 pandemic caused a lockdown in Wuhan on 23 January 2020. The purpose of this lockdown was to prevent the COVID-19 outbreak to other cities or even countries. The World Health Organization (WHO) called it "unprecedented in public health history" (Coronavirus disease (COVID-19) pandemic, 2020). By 30 January 2020, WHO declared the COVID-19 outbreak as a Global Public Health Emergency. As of 18 Oct 2020, COVID-19 has affected more than 200 countries with 39,596,858 cases reported (World Health Organization, 2020).

Malaysia is one of the many countries affected by the COVID-19 pandemic. Its first COVID-19 case was detected on 24 January 2020. In March 2020, Malaysia faced an alarming high number of COVID-19 cases, dubbed as "second wave", as a result of one cluster involving a large gathering in Sri Petaling. On 18 March 2020, Malaysia government instituted a Movement Control Order (MCO) lockdown as an effort to "flatten the curve". Other countries also adopted similar measures in an effort to bring down the COVID-19 cases as well as to stop the pandemic outbreak. Figure 1 shows the alarming numbers of COVID-19 cases in Malaysia (as of 5.00pm, 18 March 2020) which prompted the Movement Control Order.

Remote Audit

As Malaysian business and services came to a grinding halt in March 2020 due to the MCO, most employees suddenly found themselves in a completely new norm. For the employees of Information Security Certification Body (ISCB), a department within CyberSecurity Malaysia, this new norm involved remote auditing. When the

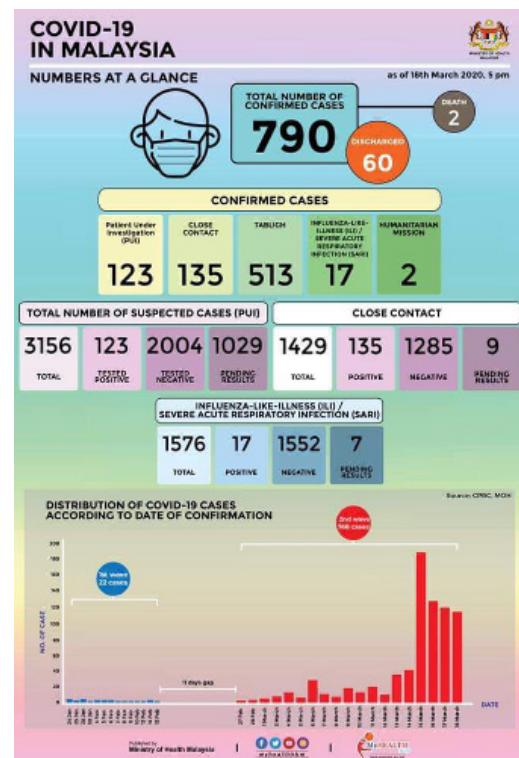


Figure 1 COVID-19 cases in Malaysia (as of 5pm, 18 March 2020) (source: (COVID-19 MALAYSIA, 2020))

clients closed their premises and worked from home, ISO/IEC 27001 audit fieldwork has to be accomplished using technology means. The traditional model of working at client sites and interviewing clients face-to-face were rendered impossible during the Covid-19 pandemic.

A remote audit process is described in ISO 19011:2018 as a process using interactive communication methods that involve human interaction (e.g. interview, observing process performed by client personnel) and non-human interaction (e.g. document review, data analysis, observing process performed by surveillance means) (ISO 19011 Guidelines for auditing management systems, 2018). The remote audit is conducted using technology and electronic methods such as video conferencing, email and telephone to verify audit evidence and conduct interviews with relevant personnel. This remote audit may be conducted from the homes of auditors as opposed to the normal audit conducted at the client's premises. Nevertheless,

62

the purpose of remote audit remains the same which is to evaluate the evidence objectively and to achieve the audit objectives.

Benefits And Barriers Of Conducting Remote Audit

Remote audit is an electronic audit that uses technology to evaluate compliance. There are a variety of reasons that an audit may be needed to be conducted remotely such as safety issues, physical or logistics constraints, pandemics or travel restrictions. The voluntary or mandatory movement restrictions due to the current COVID-19 pandemic is a perfect example where auditing remotely is beneficial to both auditor and client.

There are several reasons why conducting remote audits can be beneficial for clients and audit team members. Here are the most relevant ones:

1. Avoid travelling to difficult or unsafe location

Situations where travelling to difficult or unsafe location can be solved with remote auditing. Difficult locations can refer to locations which are remote or difficult to access due to in an isolated area, or strict permits are needed to enter the location. Logistics arrangement related to these issues are not needed when conducting remote audit. Unsafe locations may be caused by riots or demonstration gone wrong, and also posed a risk to traditional face-to-face audit. Remote audit may also be beneficial for locations that are very huge to cover such as plantation or manufacturing plant. Live video or even surveillance video can be used to gather the necessary audit evidence.

2. Cost saving

Information and communication technologies (ICT) have made remote auditing more feasible. As access to ICT has increased, remote auditing has become more commonly used globally. Remote auditing means that an auditor can easily interview any key personnel in any part of the world without incurring travelling cost.

3. Flexible schedule

There can be situations where an auditor is on the road travelling from one audit site to another site to fulfil the audit fieldwork. This can be avoided via live video of the site, which

can save the auditor's time in travelling. At the same time, it provides auditor with flexibility and visual access to the audit site.

On the other hand, remote auditing has its hindrance. The followings are some of the barriers while conducting a remote audit:

1. Issues with technology

Limitations and risks posed by ICT should be well considered by auditor. The location of the client or auditor may cause issues and limitations with technology and network. Such examples include unreliable or slow Internet connections which may impede the fulfilment of audit objectives. Online interviews can be interrupted and evidence stored in cloud may be inaccessible. Due to these issues, there may be insufficient time to conduct the audit as more time is spent on troubleshooting or re-connecting to the Internet connection.

2. Trusting the audit

Another challenge in remote auditing is the auditor does not have physical access to audit evidence and face-to-face interview with the client. The physical communication may be useful to provide subtle signs to the auditor that there are conflicting messages during the interview. The auditor may not be able to detect inconsistencies in the areas of audit. Being not physically present on the client's site also make it possible for the client to hide issues and even possible non-conformities during a remote audit.

3. Insufficient training / experience

Depending on the technology used by the client, there may be key challenges faced by the auditor in remote auditing. Lack of experience and/or training of conducting remote audits can lead to an inability to collect sufficient audit evidence using the technology.

There are a variety of ICT tools which can help facilitate remote auditing such as file-sharing via cloud, desktop access, screen sharing, video conferencing and live data analysis. Competency is crucial in ensuring that remote audit is conducted efficiently and meets its intended objective.

Preparing And Conducting Remote Audit

Once a remote audit is mutually agreed by both the audit team and client, preparation needs to be done to ensure a smooth and effective audit conducted despite using online methods. The ISO 19011 Guidelines for Auditing Management Systems (ISO 19011 Guidelines for auditing management systems, 2018) provides a guide on how to conduct a management system audit and specifications for conducting remote audits.

There are several items which must be prepared by both the auditor and client. These are based on ISO 19011 Guidelines for Auditing Management Systems (ISO 19011 Guidelines for auditing management systems, 2018) as well as some personal experience of CyberSecurity Malaysia in preparing and conducting remote audits. The key items include, but not limited to, the followings:

- ICT tools and good network connection
- Competency and availability of personnel
- Document accessibility
- Time management
- Security and confidentiality consideration

ICT tools and good network connection

ICT and network connections are important elements in ensuring that remote audit can be conducted effectively. Having a laptop easily helps an auditor to audit from their homes. The auditor also need to use ICT tools. There are a variety of ICT tools that can assist the auditor in conducting remote audit efficiently. For example technology solutions such as Zoom and WebEx have made this remote audit possible.

A simple video conference or telephone call could also be used in a remote audit. Using a combination of ICT tools will help both the auditor and client to switch to the best and suitable method. Table 1 provides a list of ICT tools that can be used during various stages in a remote audit.

Audit Activities	Example of ICT Tools
Opening / Closing meeting	Video conferencing, Tele conferencing, Phone call
Document review	Cloud sharing, Video conferencing, Email
Interview personnel	Video conferencing, Tele conferencing, Phone call
Observation of activities/processes	Video conferencing with screen share, Real time video, Access to video monitoring of sites
Sites visits	Real time video, Access to video monitoring of sites

Table 1 Examples of ICT tools

The network connection is another challenge faced by the auditor. It is difficult to predict the connection especially during the remote audit. Nevertheless, a connection testing prior to the audit can be beneficial and helpful to determine if remote auditing will be a success. Furthermore, the auditor should have an alternative solution if there are difficulties regarding the network connection.

In a remote audit situation, there may also be challenges to understand what the other party is trying to explain. As such, one needs to be diplomatic, to listen attentively and to be respectful. This applies to both auditor and client.

Competency And Availability Of Personnel

Just having a reliable network connection is not enough during a remote audit as both the auditor and the client must also be competent in utilizing ICT tools. It is crucial for the auditor to have the necessary knowledge to correctly conduct audits using the technology. Since there is a variety of tools which can be applied in remote audit, the client may decide which one they prefer. In any audit situation, ISO/IEC 27001 ISMS (ISO/IEC 27001 Information Security Management System – Requirements, 2013) requires the auditors to adopt standard auditing techniques which include interviewing key personnel. Auditors will need to ask relevant questions related to the scope of the audit. Therefore, the client's key personnel must be ready for online interviews during the remote audits.

Document Accessibility

ISO/IEC 27001 ISMS (ISO/IEC 27001 Information Security Management System – Requirements, 2013) audit requires mandatory documented information to be established by the client. Some examples of these documented information are risk assessment and risk treatment methodology (clause 6.1.2), Statement of Applicability (clause 6.1.3 d), Risk treatment plan (clauses 6.1.3 e and 6.2) etc. Thus, the ISMS auditor must have access to these documented information as well as other relevant documents that can provide assurance of the client's management system. Clients who have cloud-based audit management systems and document imaging will be at an advantage when auditing remotely. It will be easier for both client and auditor if the client has move towards digital document system. The more documented information auditors have access to, the more remote auditing is possible.

It will make the process of remote auditing much easier if relevant documents can be accessed by the auditors via the agreed ICT methods (e.g. email, cloud sharing) and in accordance with the agreed information security arrangement. For ISMS audits, the documents may include (but not limited to) the client's Statement of Applicability, ISMS internal audit report, management review records, risk assessment report and risk treatment plan. The relevant policy and procedure, records and evidence of ISMS implementation and information security controls should also be accessible during remote audit.

Time Management

In any auditing exercise, time management is critical in meeting auditing objectives within the agreed audit timeline. Network interruption or other technical issues can also cause a delay in the remote audit process. The auditors should manage their time well during these interruptions and be flexible in carrying out the audit plan. Any deviation to the audit plan though, will need to be discussed and agreed with the client.

There can be situations where the auditor may be unable to observe the implementation of processes and / or activities during the remote audit. The auditor should not waste time but instead proceed to observe and audit other relevant areas. In certain situations, the auditor may have to arrange a follow-up audit including but not limited to an on-site audit. If necessary,

he or she has to cover the area which cannot be accessed during the remote audit. Alternatively, the auditor may need to reschedule the remaining on-site audit activities to a later date when scheduling allows appropriate supporting evidence to be captured. This will ensure ISMS requirements are met to support the client's certification.

Security And Confidentiality Consideration

Security and confidentiality need to be emphasized in any audit, more so if it involves remote audits. As documents, records and evidence may be transferred using ICT tools to the auditor, extra precaution should be taken to ensure these are protected accordingly. Information security controls such as encryption and password-protected documents can be applied to ensure the security and confidentiality of these documents and records.

Furthermore, auditors would have signed a confidentiality agreement with the Certification Body and/or with the client. They are required to keep all information obtained from a client during their audit as confidential. At the end of a remote audit, auditors are also required to delete every document and record received from the client.

Conclusion

Malaysia is now experiencing its third wave of the COVID-19 pandemic (based on 18 October 2020, the date this article is written). The country has registered a triple-digit rise in new COVID-19 cases since 1 October 2020 with 869 and 871 cases reported on 17 and 18 October 2020, respectively (COVID-19 MALAYSIA, 2020). The total number of cases in Malaysia has reached 20,498, as of 12 noon of 18 October 2020 (COVID-19 MALAYSIA, 2020).

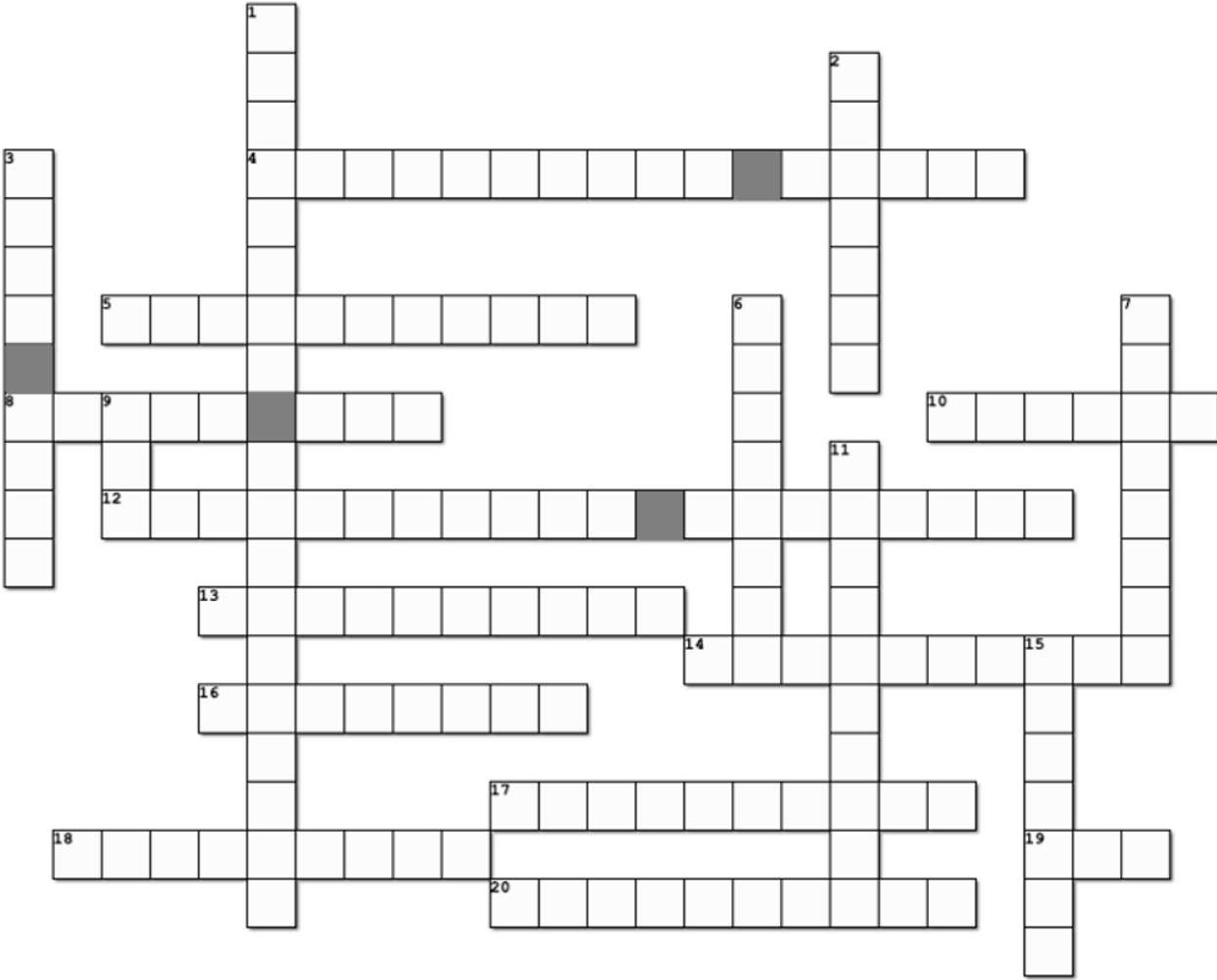
As the COVID-19 pandemic is unlikely to be over in the next few months, remote audit remains a viable alternative continuity tool for a more efficient and productive method of auditing. While online and virtual methods for auditing needs to be explored further, the traditional face-to-face audits should not be ignored. There must be a balance for conducting both traditional and virtual audits to ensure effective ISO/IEC 27001 ISMS audits.

References

1. COVID-19 MALAYSIA. (2020). Retrieved from Kementerian Kesihatan Malaysia COVID-19 : <http://covid-19.moh.gov.my/>
2. Coronavirus disease (COVID-19) pandemic. (2020). Retrieved from World Health Organization: <https://www.who.int/>
3. World Health Organization. (2020). Retrieved from WHO Coronavirus Disease (COVID-19) Dashboard: <https://covid19.who.int/>
4. International Standard (2013). ISO/IEC 27001 Information Security Management System - Requirements. Switzerland: International Organization for Standardization.
5. International Standard (2018). ISO 19011 Guidelines for auditing management systems. Switzerland: International Organization of Standardization.

Crossword Puzzle: Understanding ISO 22301:2019

By | Nahzatulshima Binti Zainuddin



Across

4. An individual or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.
5. The process to determine a value.
8. A business continuity activity that takes participants through the process of dealing with a simulated disaster scenario.
10. The outcome of a disruption affecting objectives.
12. An activity to which urgency is given to avoid unacceptable impact to the business during a disruption.
13. Selection of _____ shall be based on criteria that will meet the requirements to continue and recover prioritized activities within identified time frames and agreed capacity.
14. An organization shall ensure that applicable legal and _____ requirements are considered when implementing its BCMS.
16. An event that can be, or could lead to, a disruption, loss, emergency, or crisis.
17. Fulfilment of a requirement.
18. Based on the result of the BIA and risk assessment, an organization should identify and select business continuity strategies. The strategies shall be comprised of one or more _____.
19. The process of analysing the impact of a disruption over time in an organization.
20. The ability of an organisation to absorb and adapt to a changing environment in order to enable it to deliver its objectives.

Down

1. Pre-defined capability of an organization to continue to deliver their products and services within acceptable time frames during a disruption.
2. When there is a need for this, the organization shall consider its purpose and consequences; the integrity of its BCMS, the availability of resources and allocation of responsibilities.
3. A layered hierarchical communication model that is used to notify specific individuals about an event and coordinate recovery, if necessary.
6. Its purpose is to validate the business continuity strategy, activities, assumptions regarding times (maximum tolerable period of disruption, recovery time objectives), procedures and work instructions as specified in the business continuity plan.
7. The process to restore and return business activities from the temporary measures adopted during and after a disruption.
9. Documented information that guides an organization to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.
11. An incident, whether anticipated or unanticipated, which causes an unplanned, negative deviation from the expected delivery of products and services according to the organization's objectives.
15. The new version of ISO 22301 was published this month in 2019.

Answer:

1. Business Continuity; 2. Changes; 3. Call Tree; 4. Interested Party; 5. Measurement; 6. Exercise; 7. Recovery; 8. Table Top; 9. BCP; 10. Impact; 11. Disruption; 12. Prioritized Activity; 13. Strategies; 14. Regulatory; 15. October; 16. Incident; 17. Conformity; 18. Solutions; 19. BIA; 20. Resilience

Cyber Security Marketing Strategy - What Hiking Can Teach Us

By | Balamurugan Nallapan



What Is hiking?

Sir Edmund Hillary, the first man credited to have successfully conquered Mount Everest once famously said, "It is not the mountain we conquer, but ourselves". And so we decide to scale the highest and toughest mountains. When we do, we experience a sense of achievement, fulfilling certain specific goals unique to every individual. Hence, while attempting a hike, more than the sight offered by the mountains, we soon discover a lot more of ourselves. Hence, it is not the mountain we conquer, but ourselves.

Talking about mountain climbing or hiking, here are some fun facts on mountains. Oxford English dictionary defines a mountain as "a natural elevation of the earth surface rising more or less abruptly from the surrounding level and attaining an altitude which, relatively to the adjacent elevation, is impressive or notable". What a boring definition!

For most mere mortals however, a mountain is a place which makes you want to slap the person

who suggested and convinced you that hiking is FUN. Researchers vary in their opinion on the very definition of a mountain. Some argue that anything higher than 1,000 feet should be considered a mountain, whereas some will insist that anything above 2000 feet is a proper mountain and everything shorter than that is just a hill. For most of us, if it is just call it a "Gunung".

Marketing is rather subjective, more so in marketing cyber security solutions. Cyber security is a complex and intangible subject that makes it difficult to grasp, particularly for customers.

The right marketing strategy must be deployed to ensure the solutions are brought to the right customer at the right moment, bringing the right value.

In this article, we explore a few lessons from hiking that can be used in building a strong marketing strategy for cyber security products.

What Happens While Hiking?



To put it in the simplest way, when one goes for hiking, there will be a high level of physical exertion. It involves the sweat, the never ending climb, the exhaustion, the thirst, the insect bites and most annoyingly the super fit fellow climbers who zip past you.

At the start of the climb, no matter how well prepared, most have us will have a sense of trepidation, a slight doubt if we will be able to scale the mountain and return safely. You will also feel the excitement of what you may discover. These days, people are also thinking of all the “instagram-worthy” photographs they can take and the amount of likes and comments it may amass. With that setting, you begin your journey, pushing through your limits, enduring the pain, taking scheduled and unscheduled stops along the way. The moment you reach the summit, you will always feel a sense of calm and relief. Relieved because you have made it to the summit. It will be quickly followed by a sense of achievement. You have conquered yourself. You reward yourself with the much-earned rest, taking in the sight and enjoying the fresh mountain air. You repeat the entire process to get yourself back down from the mountain.

Lesson #1: Continuous Effort without complacency

I have climbed Gunung Angsi more than 15 times and Gunung Datuk more than 5 times. No matter how many times I have climbed these mountains, each new attempt requires equal effort and preparation. I still need to go through the path, I still need to pay attention to my every step to ensure I can climb the mountain safely and return. In short, each climb is a new climb. What is the lesson? We got to where we are today because of our efforts in the past. To continue to grow we must continue to put in the effort. There is no room for complacency. Although the path may appear familiar, you are required to give full

attention and put in equal if not more effort. You cannot rest on your past achievements and expect doors to open for you. It is said that the position we find ourselves at today is the result of our actions six months ago. In the same vein, it also means that our actions today determines where we will be in six months' time. If you decide to stop learning, stop improving, stop giving your best each time because you are already where you want to be, then you are setting yourself up for disappointments in the very near future. Imagine cruising on the highway, reaching the desired speed (110km/h for most of us) and upon reaching the speed level, you do not need the engine to be running anymore. The inertia will take you a few extra meters but inevitably your car will come to a stop. The effort must be sustained no matter what.

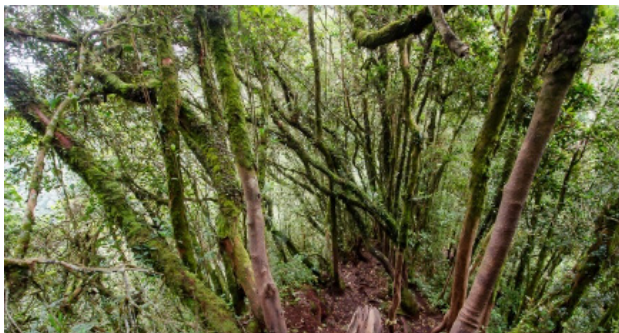
Similarly, our marketing strategy for cybersecurity solutions must be a continuous engagement. The marketing efforts we put in place today will bear results in 6 to 12 months' time. The benefits of cyber security solutions are not visible immediately and hence, longer and continuous engagements are required to acquire customers. The effort must be repeated continuously to build the momentum. As such, each effort is similar to a new attempt to scale a mountain.

Lesson #2: Implementation of Each Action Items

When climbing you are advised not to look up the trail but focus on each of your steps. Seeing the tough trail ahead can mentally tire you. I personally prefer the early morning climbs before the sunrise where even if you looked up you will not see a thing. My torchlight is to find my next step and not to see how steep the trail is so that I do not feel defeated even before I started. Talking about torchlights in the jungle, one of the unwritten rules of hiking is that you are not allowed to shine your torchlight wherever you wish especially not up at those trees. You would not want to discover what may be staring back at you. That is just a small digression. Getting back to our main story, hiking teaches you to focus on each step you take to ensure it is firm and secure. One small misstep could cause severe damage to you and may end your adventure prematurely. Take one step at a time and make that a solid step. When you decide to hike a mountain, you must find out the height of the mountain, how long the journey will take (up and down), how many rest areas and other basic information.

This is an important lesson on how we develop our cyber security marketing strategies. When given a responsibility by management to develop the marketing strategy or to win a specific key account, it may appear like a mountain you have never climbed before. Just like hiking, understand the full scale of the “mountain” before you. Do not let the enormity of the task defeat you even before you start. Always remember to take one step at a time. With the right focus and sheer determination, you will reach the summit. Desmond Tutu, a famous South African anti-apartheid and human rights activist once famously said, “there is only one way to eat an elephant: a bite at a time”. Everything in life that seems daunting, overwhelming or even impossible can be gradually achieved by taking one step at a time.

It is important to have clarity when developing your marketing strategy. The key to success is in the implementation of each action item. Break down the strategies into singular actionable items and focus on executing one at a time while constantly remain aware of the big picture.



Lesson #3: Play To Your Strength

Despite the challenge, risk and intangible nature of its reward, hiking is still a popular activity among the young and enthusiastic Malaysians. Most often than not, the enthusiasm is not matched by the physical ability.

When you start your climb, you will find individuals or groups moving way slower than you. The slower ones will give way with a smile and I have given way to many younger, fitter climbers without a fuss. Despite not being the fittest or the youngest, sometimes I do find myself climbing faster than others. I walk past the slow climbers, offering some words of encouragement to them and feeling very good about myself, feeling fit and strong—but only to have some annoyingly fit individuals run past me. Yes! You read it correctly, RUN past me up the mountain.

That is the rule of our land. You find some climbers faster than you and some slower than you. There will be older climbers faster than you and younger climbers slower than you. However, the mountain is indifferent to the speed at which you climb. It will not grow shorter because you climb fast or grow taller because you are a slow climber. Each climber will climb at his or her own pace. It is one's own journey. This is one key lesson in hiking that resonates with me every time.

All of us have our own journey. It does not matter if someone is faster or slower than you. It is important to focus on our journey and take the steps needed to ensure we reach our goals. Do not allow the journey of others distract you or more importantly, demotivate you. The ones climbing faster than you could be on their 100th trip to the mountain. It is therefore irrelevant and unfair to compare their speed to your first attempt and vice versa. Your success depends on your total commitment to the cause and your sheer determination to achieve your goals.

Taking cue from this, in forming our own marketing strategies we should not be deterred by the emergence of newer entities bringing in the latest cyber security solutions, state-of-the-art technologies or strong strategic partnerships.

It is important to conquer our own “mountain”. Similar to the pace of each climber which is based on the individual's strength and preparedness, we should identify and focus on our core strengths and capabilities. This does not mean we should ignore the competitive landscape. Find out what other industry players are doing. Let's chart our own journey and bring the right cyber security solutions to the right customer at the right time. We should always play to our strength.

References

1. <https://medium.com/the-ascent/its-not-the-mountain-we-conquer-but-ourselves-af86e2500d37>
2. <https://www.oed.com/>
3. <https://www.geographyrealm.com/mountain/>
4. <https://www.psychologytoday.com/us/blog/mindfully-present-fully-alive/201804/the-only-way-eat-elephant>

How To Reduce Gadget Addiction For Kids

By | Azatulsheera Binti Mohd Azman, Atikah Binti Baharudin, Niroshini Madi Palan & Nor Fatihah Binti Mohd Zabidi

It is not uncommon to see young kids glued to their electronic gadgets. They are so caught up in the Internet world through their devices that they completely disregard people and their physical surroundings.

Even when they are in a family gathering, some children just stare at their devices watching video or playing games. As a result, they spend less time bonding with family members. A lot of parents are expressing worries that their kids are addicted to their devices.

Challenges Of Gadget Addiction

1. Limit Your Child's Exposure to Gadgets

In raising kids today, the biggest challenge for every parent is to limit their kids' exposure to smartphones and gadgets. A study found that about 92.5 percent of adolescents (between the ages of 13 and 17) are hardcore Internet users.^[1] The study revealed that kids use the Internet for a combined duration of one to four hours every day. The Internet can pose serious dangers to children such as cyber-bullying, sexual predators and excessive use of social media. Internet addiction among children must be seriously looked into as such addiction can 'take control' of their lives and compromise family relationships. Moreover, it also reduces their interest in sports and recreational activities.^[1]

2. Psycho-social Impact

There are serious psycho-social risk factors associated with Internet addiction. The consequences include psychological distress, lack of family ties, social problems and insufficient role models to educate on responsible attitudes.^[1] People depend on gadgets to get information and thus, ignore the physical world and people around them.^[2]

3. Less Communication

This situation is very worrying especially when we see a group of teenagers or adults consisting of peers or even a family sitting together but not communicating with each other because they are busy using their gadgets and digital devices. It is even more disturbing when kids as young as two to three years old have started using digital devices such as tablets and smartphones. More so, these tech devices were actually gifted by either parents or friends.

4. Lower Productivity

Gadget addiction could take up a disproportionate amount of time and thus, lower productivity.

5. Cyber Crime x Cyber Victims

Excessive Internet usage is an inter-generational problem that can increase the risk of kids becoming victims and predators of cyber-crimes.^[1]

Preventing Gadget Addiction

To prevent kids from being addicted to gadgets, parents can do the following:

1. Set a Daily Limit of Screen Time

Allocate an appropriate amount of screen time for your child, irrespective of the gadget. Give your child the option to watch TV, use the computer, etc. and let him choose what time of the day he wants to use the device. This gives him a sense of freedom and it involves him in making decisions too.

2. Listen Attentively

Everyone needs to be understood. The big mistake is thinking kids are different from adults. Parents need to listen to their kids attentively and stop using their own gadgets when their kids are communicating with them.

3. Acknowledge Their Feelings

Paraphrase what kids say. Do not simply say that you understand, but show them that you really do. Do not ignore your kids' emotions.

4. Give Their Feelings a Name

Naming feelings is the first step in helping kids learn to identify themselves. It allows your child to develop an emotional vocabulary so they can talk about their feelings.

5. Spend Quality Time with Your Kids

Turn off tech devices during play time with kids. Try not to answer a text or a call or even scroll through social media. Take the initiative to spend more time with your kids and do things that interest them.

6. Ask Questions

You may want to understand their underlying emotional needs but at the same time, try not get into a debate. Ask them questions. This will help to develop their thinking skills.

[3]

References

1. <https://www.bharian.com.my/berita/nasional/2017/10/340635/remaja-kanak-kanak-ketagihan-internet-serius>
2. <https://www.bharian.com.my/berita/nasional/2019/09/604548/tpm-bimbang-masyarakat-ketagih-teknologi-media-sosial>
3. <https://www.bakadesuyo.com/2015/10/out-of-control-kids/>
4. <https://kidshealth.org/en/parents/nine-steps.html>
5. <https://tekkiehelp.com/top-5-dangers-kids-face-online-how-to-keep-your-children-safe-online/>

Conclusion

In summary, parents play an important role in supervising what their children watch and read on the Internet. They must realize that a tech gadget is not a caregiver tool. Without parental guidance on their Internet activities, there is a high possibility that children will be exploited in the cyber space. Whilst there are tools to control Internet usage, it is important to recognize that perhaps the most effective way to help raise a digitally responsible generation is through open communication, proper education and awareness.

Can WPA3 Be The Game Changer In Wi-Fi Security?

By | Mai Syasya Ilyana Binti Meor Abdul Wahab, Zarina Binti Musa, Ahmad Dahari Bin Jarno & Noor Asyikin Binti Zulkifli

Abstract

Wireless networks are available everywhere from the local coffee shop, shopping mall, or at home to which we can connect. The question is how do we know which ones are safe. Network security protocols are designed to address Wi-Fi security issues.

Wi-Fi Protected Access (WPA) is an essential security standard for wireless Internet connection for wireless networking. Other wireless security protocols include WEP, WPA, WPA2–Personal, WPA2–Enterprise. Wireless network security has since evolved from WEP protocol to WPA3 protocol. WPA3 is expected to be a more robust Wi-Fi security protocol. This article discusses the security challenges in WPA2 and upcoming features in WPA3 which will bring about vast improvements in wireless networking security.

The Evolution Of Wi-Fi Security

WPA was developed by the Wi-Fi Alliance in 2003 to provide better wireless network security through advanced data protection and enable user authentication as compared to the Wired Equivalent Privacy (WEP) wireless security technology.

Security should be one of the major concerns when planning a wireless network. However, a lot of users are not aware that it is possible to sense, capture, and analyze network traffic from a distance without being detected. In 2004, WPA2 was introduced for Personal and Enterprise. There were many vulnerabilities discovered on the WPA2 wireless security protocol, which warranted attention. Finally, after a long wait and usage of WPA2, WPA3 was introduced in 2018. Can WPA3 solve the issues and challenges faced by WPA2?

WPA2 Security Challenges

Let's delve deeper into WPA2 vulnerabilities. First and foremost, WPA2–Personal is vulnerable to passphrase brute force attacks, where an attacker injects brute force with random passphrases with the expectation of being able to guess correctly the passphrase, especially the simple ones. Once the attacker manages to guess the correct passphrase, data in the wireless traffic can be decrypted. This would allow the attacker to snoop on other users' traffic and sniff out the network traffic content without authorization.

Should the user move to the WPA2–Enterprise configuration compared to WPA2–Personal? Unfortunately, this configuration requires an additional component which is a RADIUS server. Due to the requirement of a RADIUS server, it is more applicable for an organization with an enterprise network system to use WPA2–Enterprise compared to a home set-up. Although it may sound effective in reducing the risk of wireless hacking, this standard is not so flexible for home user network security.

The biggest downside of Wi-Fi since its introduction is probably the lack of any built-in authentication, encryption, or privacy on open public networks. In public places such as cafes, airports that provide public Wi-Fi hotspots, the person right beside you could be an attacker who is snooping on your wireless network activity. All it takes is just a few wireless hacking tools.

Ever heard of a key reinstallation attack (KRACK)? KRACK is one of the biggest vulnerabilities for WPA2. Any hacker will spend every millisecond of trial and error in exploiting the wireless network protocol just to gain sensitive information that brings benefits to them. Attackers gain passwords, e-mails, and other data – that are presumed to be encrypted, and for some cases, the attacker will inject ransomware or any other malicious content into a website that a client is viewing. On the surface, it does not look that dangerous but if only people can see bits of their transmitted data being decrypted by these hackers, it could be horrendous.

WPA3 Wireless Security Overview

As vulnerabilities are uncovered, advancements and patches have been made. WPA3 is believed to simplify Wi-Fi security, enable more robust authentication, and deliver increased cryptography strength for highly sensitive data stored. It comes with some improvements, additional features together with a new protocol called Dragonfly. In anticipation of its commercialization, some companies have started to manufacture new devices which have built-in support for WPA3. Not to be left out, devices loaded with WPA2 security standards are also being updated with WPA3.

WPA3 is more secure as it delivers improvements to the general Wi-Fi encryption. Firstly, WPA3 acts as a shield against brute-force attacks that were previously used against WPA2. Additional steps for a sealed handshake are compulsory when devices are connected to any WPA3 access points, all because of Simultaneous Authentication of Equals (SAE) or referred to as "Dragonfly Key Exchange" that replaces PSK protocol. To connect with a closed Wi-Fi network using passphrases, there will be a four-way handshake between the client and the access point. To fortify security, WPA3 uses SAE protocol as a new 802.11 authentication method to secure the process, avoiding attacks on wireless connection even though the wireless passphrase/password is simple (weak) – either abcd1234 or 12345678. As for WPA3-Personal, it requires the use of Protected Management Frames (PMF). It allows for improved security. WPA3-Personal networks with simple passphrases make it difficult for hackers to crack using off-site, brute-force, dictionary-based cracking attempts, unlike WPA/WPA2., even if another person is connected to the network, they cannot even snoop, passively observe your traffic and cannot even decrypt any of your captured data. Besides, SAE functions in preventing notorious key reinstallation attack (KRACK) for WPA2-Personal.

Secondly, one of the improvements in WPA3 is advanced enterprise security, especially in WPA3-Enterprise mode. This involves the expansion of security for enterprise environments from 128-bit security level along with the usage of WPA2-Enterprise to 192-bit key-based encryption. The new standard uses an identical 192-bit cryptographic intensity in WPA3-Enterprise mode (AES-256 in GCM mode with SHA-384 as HMAC) and also mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum cryptographic algorithm in WPA3-Personal mode.

This is especially crucial for cryptographic strength when the wireless network is transmitting sensitive data. Oriented to the Commercial National Security Algorithm (CNSA) suite, this new standard will cover the 48-bit initialization vector targeting government entities, large corporations, and organizations, and highly-sensitive environments, to ensure a maximum degree of protection. As new features come with the latest updates, therefore anything related to the EAP server component of the RADIUS server also requires a new installation.

Thirdly, the most formidable feature of WPA3 is its robust security in open or public Wi-Fi networks. This new feature is known as Wi-Fi Enhanced Open that makes WPA3 deliver secure connection in public areas. This latest standard by Wi-Fi Alliance allows communication of open networks especially one without any password or passphrase to be uniquely encrypted between individual clients and the access point based on Opportunistic Wireless Encryption (OWE). It will prevent attacks like snooping on traffic or session hijacking. This is an optional feature available for all vendors. Each connection between a user and the access point will be encrypted with a unique key to avoid the most common Man-in-the-Middle attacks.

Fourthly, WPA3 also offers another new feature called Wi-Fi Easy Connect. The feature enables easier connection for devices without displays. It is common to see Wi-Fi activated devices without displays. Anything from Google Home to smart outlets and light bulbs can be linked to a Wi-Fi network. But it is always tedious to connect these machines to a Wi-Fi network because it does not have screens or keyboards that you can use to type passwords so smartphones are needed to type in complicated passphrases. WPA3 guarantees to "simplify the security configuration process for devices with limited display interface and IoT devices." One could just simply add these devices using a QR code.

This is the part where Dragonfly's new handshake is featured. This handshake performs its task by forcing network interaction on a potential login, thereby preventing hackers from using dictionary hack, which is a login by downloading its cryptographic hash and then run cracking software to break it before using other tools to snoop on network activity. Dragonfly Handshake is a key exchange using discreet logarithm cryptography that is authenticated using a password or passphrase. This is immune to active attack, passive assault, and offline dictionary attacks. WPA3 has full forward confidentiality – which is lacking in WPA2 –

and defends against offline brute force attacks. Unlike WPA2, WPA3 is only required to use the "Advanced Encryption Standard" (AES) and no longer utilize obsolete protocols such as the "Temporal Key Integrity Protocol" (TKIP) or the "Wired Equivalent Privacy" (WEP) protocol. The WPA2 Pre-Shared Key (PSK) approach is replaced by Simultaneous Authentication of Equals (SAE), which provides more reliable password-based authentication. It is now possible to authenticate each other at the same time and independently of any position in SAE. With this new approach, the system (STA) and access point (AP) are now obsolete. SAE uses the Diffie-Hellman (DH) key exchange.

By the time WPA3 is launched, Qualcomm would have started making chips for phones and tablets that fully support WPA3. Cisco is also in the process of creating support and updating existing devices in anticipation of long-term use in compliance with new security standards. TP-Link has started manufacturing WPA3 devices such as Archer C6, RE505X, Deco X60, and Omada EAP. Lastly, Extreme Networks has listed out WPA3-certified devices such as wireless adapters and Enterprise APs which are available on the market today.

Conclusion

The industry is constantly working to improve wireless security standards. No doubt every security standard has limitations and challenges which may create vulnerabilities that are susceptible to new attacks. Even with WPA3, wireless network flaws are bound to be uncovered. Thus, it is always prudent to ensure all networks are secured from any intrusion by using a VPN. It is important to regularly change the passphrases and practice good cybersecurity sense when using public wireless networks.

References

1. Bednarczyk, M., & Piotrowski, Z. (2019). *Will WPA3 really provide Wi-Fi security at a higher level? [Abstract]. XII Conference on Reconnaissance and Electronic Warfare Systems.* doi:10.1117/12.2525020
2. Geier, E. (2018, November 02). *What is WPA3? And some gotchas to watch out for in this Wi-Fi security upgrade.* Retrieved October 21, 2020, from <https://www.networkworld.com/article/3316567/what-is-wpa3-wi-fi-security-protocol-strengthens-connections.html>
3. Hoffman, C. (2018, October 21). *What Is WPA3, and When Will I Get It On My Wi-Fi?* Retrieved October 21, 2020, from <https://www.howtogeek.com/339765/what-is-wpa3-and-when-will-i-get-it-on-my-wi-fi/>
4. *What is WPA3? Explore WPA3 Devices: TP-Link.* (n.d.). Retrieved October 21, 2020, from <https://www.tp-link.com/my/wpa3/>
5. [Wireless] *What is WPA3? What are the advantages of using WPA3?: Official Support: ASUS Global.* (2020, April 14). Retrieved October 21, 2020, from <https://www.asus.com/support/FAQ/1042478/>
6. *What is WPA3 and what you should test in WPA3 enabled devices.* (n.d.). Retrieved October 21, 2020, from <https://www.qacafe.com/articles/what-is-wpa3-how-to-test-wifi/>
7. *WPA3: The Next Generation of Wi-Fi Security.* (2019, November 14). Retrieved October 21, 2020, from <https://www.extremenetworks.com/resources/at-a-glance/wpa3-the-next-generation-of-wi-fi-security/>

Book Review – Interesting Read on Big Tech: Yahoo, Amazon & Netflix!

By | Mohammad Fahdzli Bin Abdul Rauf

Many people do not realize the power of the written word. In fact, many have not read a book since they left school or university. This is rather unfortunate since one of the secrets of self-development is reading. One could always find an answer to a problem in a book.

A book, especially a non-fiction one, reflects a set of ideas straight from the author. A book is a medium of transfer for knowledge, wisdom, and ideas.

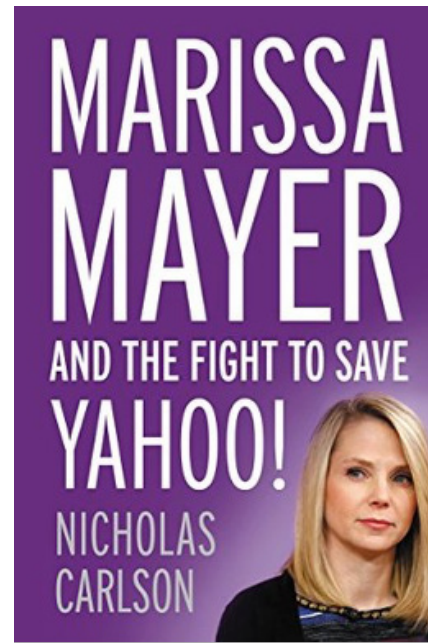
The right book can open your mind to new ideas, inspire you to invent or innovate or transform to become a winner in some key areas of your life. Malaysians read an average of about 15 books a year based on an interim study done by the National Library in 2014. But this is still a long way to go compared to those from developed countries who read an average of 40 books a year. ^[1]

To be honest, to finish even 15 books in a year seems a longshot for me. Since the beginning of this year, I have only managed to finish reading a total of eight books, just slightly over half of the national average. Of which, three of them are related to the information technology industry and known to be disruptors of the traditional economy.

I am sharing my reviews of three technology related business books with the hope of encouraging others to pick up reading. There is so much we can learn from these books. Just keep in mind that this is my personal opinion, but nevertheless the books chosen are either best sellers or highly recommended by the industry.

Below is a list of books which I recently reviewed:

1. Marissa Mayer and the Fight to Save Yahoo! by Nicholas Carlson
2. The Everything Store by Brad Stone
3. This Will Never Work by Marc Randolph



1. Marissa Mayer and the Fight to Save Yahoo! by Nicholas Carlson^[2]

The author of this book is Nicholas Carlson who is Business Insider's Chief Correspondent on technology.

The book is not just about the dwindling influence of Yahoo! and the effort of its founders and Board of Directors in rejuvenating the brand name, but is also about Marissa Mayer, in her younger days, and her rise to become one of Google's most prominent executives and eventual appointment as Chief Executive Officer of Yahoo!

Yahoo! is a big name in the tech industry. It was among the early adopters of the Internet in the 90's.

The book is divided into 4 parts. It is written in such a way that each part is standalone respectively. For example, I find that Part 2 has no continuity from part 1 while readers will only find out the conclusion of the first part later in Part 3.

Part 1 is about the rise of Yahoo! It tells about

how the dot com bubble of the early 2000's and the rise of Google had impacted Yahoo!'s business. Part 2 focuses more on Marissa Mayer's upbringing and her time as one of the earliest employees of Google and her subsequent rise to become the Vice President of Google Consumer Products. Part 3 deals with the continuous debacle within Yahoo! that left its market share and most importantly its reputation further down and its subsequent loss to Google. While Part 4 is all about Marissa Mayer's appointment as Yahoo! CEO and her struggle to turn around the organization.

The most interesting parts of this book captures both the human part of Marissa and her steely resolve and determination to save the once behemoth organization that has lost hope and conceded defeat to Google.

I will definitely recommend this book for those who want to understand more about the early days of the Internet boom and also pitfalls awaiting any companies that is not agile enough in innovating new ideas and adapting to new technologies.



2. The Everything Store by Brad Stone^[3]

Published in 2013, this book won the 2013 Financial Times and Goldman Sachs Business Book of the Year.

I previously read another book written by Brad Stone titled, **'The Upstarts: How Uber, Airbnb, and the Killer Companies of the Silicon Valley Are Changing the World'** and personally, the author is a great storyteller and investigative

journalist. He knows his subject thoroughly and interviews scores of people and present his story in such a compelling manner that will captivate readers.

'The Everything Store', as implied on its cover, is all about visionary founder Jeff Bezos who was not content with being a bookseller. He wanted Amazon to become 'the everything store'. This book is Brad Stone at his best.

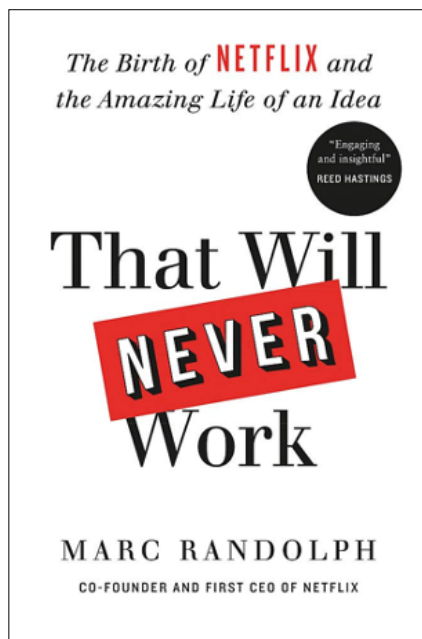
Personally I can find no fault in the way this book is written, since it follows a mostly linear timeline from the inception of an idea to creation of Amazon, its struggle during the dot com bubble of the early 2000's, rapid growth and effects of Amazon on the economy. Basically Amazon has single handedly transformed the retail industry for the entire world.

The author keeps the above premise interesting by filling in bits of information about Jeff Bezos (who now is the richest man in the world), his upbringing, mental fortitude, ruthlessness, compassion and thirst for continuous improvement and innovating. A brief story about Blue Origin, the space company founded by Jeff Bezos is also included in the book.

I highly recommend this book as it encapsulates all the ingredients needed to build a successful empire, a true story of the first big disruptor to our economy, Amazon, which changed the way we buy things and will keep evolving as the years go by. Jeff Bezos is also a nerd who never ceases to innovate.

Here is a quote from Jeff Bezos which reflects his persistent drive for improvement, innovation, and iteration:

"When you are eighty years old, and in a quiet moment of reflection narrating for only yourself the most personal version of your life story, the telling that will be most compact and meaningful will be the series of choices you have made. In the end, we are our choices".



3. That Will Never Work by Marc Randolph^[4]

This particular book was more of an impulse buy during one of my regular visits to Kinokuniya Bookstore. I was rather astonished that the author was not a correspondent from a business publishing company or even a journalist, but co-founder of the company itself. I found it refreshing to learn more about the company from the first-person's perspective, especially from the founder.

The book narrates in linear timeline from the Eureka! moment up until to the point of Netflix becoming the biggest producer of streaming services in the world for movies, TV shows, and documentaries.

Through the author, which is also Netflix first CEO before he stepped down to make way for fellow co-founder Reed Hastings, we can learn about his mindset on starting his own company from throwing ideas after ideas to finding the most feasible one. The author also tells about the hardship in the early years as a start-up company (Netflix started as a DVD rental company via website), and the challenges faced against the incumbent and biggest competitor at that time – Video Rental company Blockbuster. As a disruptor of the industry, which changed the usual way of consumer renting a movie via brick and mortar shop, several hard decision were made at Netflix. What built and shaped the company was hiring the right people and establishing a culture that reflected the author's vision. Netflix's corporate culture has since

been a hit in Silicon Valley fraternity. It has been heralded as a game changer in Human Resource management by the Harvard Business Review.

This book is a refreshing take on one of the most iconic economic disruptors of the decade. It is highly recommended since it is written by the founder who shares the transformational journey of a company through grit, gut, instincts and determination to change the world. The impact of Netflix is still being felt across the world today, as traditional media powerhouses are at loss to catch up. Its biggest competitor in the industry, Blockbuster, has already filed for bankruptcy.

References

1. *Research conducted by the National Library in 2014 – www.pnm.gov.my*
2. *Marissa Mayer and the Fight to Save Yahoo! by Nicholas Carlson. Published by TwelveBooks.com in January 2016*
3. *The Everything Store – Jeff Bezos and the Age of Amazon by Brad Stone. Published by Little, Brown and Company in 2013.*
4. *That Will Never Work – The birth of Netflix and the Amazing Life of an Idea. Published by Little, Brown and Company in 2019.*

Global ACE Certification

By | Nor Radziah Binti Jusoh & Nur Liyana Binti Zahid Safian

Global ACE Certification

Organizations are expected to keep their customers' data safe and secure, but the growing shortage of qualified cybersecurity professionals is making it extremely tough to do so. The industry will need to look at new ways to cast a wider net if we are to grow the talent pool and attract career changes into the cybersecurity industry.

To alleviate the shortage of skilled professionals, CyberSecurity Malaysia (CSM), an agency under Ministry of Communication and Multimedia Malaysia, decided to develop a professional certification for the cybersecurity sector. The Global ACE Certification is a holistic framework of cyber security professional certification that outlines the overall approach, independent assessments, impartiality of examinations, competencies of trainers, identification and classification of cyber security domains and the requirements of professional memberships.

It is a large-scale systematic plan of actions to certify and recognise cyber security workforce developed in collaboration with government agencies, industry partners and academia.

The establishment of the certification with international standards such as ISO/IEC 17024 on certification of persons, ISO/IEC 27001 on security management and ISO/IEC 9000 on quality management, is vital to:

- Assure workforce capability and experience;
- Secure and validate core skills, knowledge, attitude, and experience; and
- Assure trustworthiness, ethical conduct, and responsibility

The Global ACE Certification is aimed at enhancing the skill-sets of cyber security workforce congruent with local and international requirements. Global ACE Certification Recognition Arrangement allows for mutual recognition of certified cyber security

professionals, which creates value for the cyber security industry and participating countries.

This certification's vision is to create a critical mass of qualified and competent workforce with shareable expertise across the country boundaries. The objectives of this certification are:

- To establish a professional certification programme that is recognized globally;
- To provide cyber security professionals with the right knowledge, skills, attitude (KSA) and experience;
- To promote the development of cyber security professional programmes globally; and
- To ensure accredited personnel has been independently assessed and committed to a consistent and high-quality service level

The core of this certification is the framework that provides a standard base and means of recognizing the "knowledge, skill and attitudes" of our cybersecurity workforce. The framework encompasses two broad categories:

1. **The "Cyber Security Technical Competencies"** – related to technical skills and knowledge required by a professional to conduct its task as a certified professional.

The domains are:

- Digital Forensics
- Incident handling and response
- Security Assurance
- Cryptography
- Governance
- Risk
- Compliance

2. The “CyberSecurity Generic Competencies”

– related to the necessary cyber security soft skill-sets in delivering service and consultation. The domains are:

- People skills domains:
 - » Leadership
 - » Mentoring & Coaching
 - » Diversity Management
 - » Communications
 - » Strategic Thinking
- Process skills domains:
 - » Change Management
 - » Organizational Management
 - » Information Management
 - » Financial Management
 - » Conflict Management
- Business acumen skills domains:
 - » Entrepreneurship
 - » ICT Literacy
 - » Customer Services
 - » Partnership & Coalition
 - » Innovation & Creation

At this moment there are five certification programs:

1. **CSAP** (Certified Secured Applications Professional)
2. **CISAM** (Certified Information Security Awareness Manager)
3. **CISMS** (Certified Information Security Management System – Auditor)
4. **CDFFR** (Certified Digital Forensics First Responder)
5. **CPT** (Certified Penetration Tester)

To promote this certification throughout the country, CyberSecurity Malaysia participated in various events under the Malaysian government and commercial platforms. CyberSecurity Malaysia also participated in World Summit on the Information Society Prizes (WSIS Prizes) 2020 to gain international recognition.

In September 2020, CyberSecurity Malaysia was named project winner through the Global Accredited Cybersecurity Education Scheme: Centre of Excellence for Capacity Building and Lifelong Learning. The prize was conferred under Category 5 – Action Line C5: ‘Building Confidence and Security in Use of ICTs’.

WSIS Forum 2020 is the world's largest ICT annual gathering of the ‘ICT for development’ community hosted by the International Telecommunication Union (ITU), and co-organized by ITU, UNESCO, United Nations Conference on Trade and Development (UNCTAD) and United Nations Development Programme (UNDP) in close collaboration with all WSIS Action Line Facilitators/Co-Facilitators.

Over 800 projects around the world submitted their entries for WSIS Prizes 2020 and 90 projects were selected as champions by WSIS multi-stakeholder community based on a total of 18 WSIS Action Lines. Under each Action Lines, one winner will be identified.

Out of 20 shortlisted projects under WSIS Prizes 2020 Action Line C5: Building Confidence and Security in Use of ICT, among the champions are Sri Lanka – ‘NextGen Girls–Internet Security Ambassadors’; Oman – ‘Oman National Public Key Infrastructure’; Cuba – ‘Security Antivirus’ and China – ‘The Cloud-Linked Privacy Security Protection System and Public Welfare Services’.

The Global ACE Scheme COE builds a single converging platform for cybersecurity capacity building and lifelong learning within the region to allow individuals to develop capabilities at their own pace and permit continual enhancement through lifelong learning pathways.

Global ACE Certification is now recognized by the ITU and WSIS stakeholders. This is an acknowledgement of its effort to develop professional programmes and quality education courses as well as nurture effective cyber defenders.

In Malaysia, the Global ACE Certification certifies cybersecurity professionals at the national level. Credential holders are recognised by the Malaysia Board of Technologists (MBOT)

through Malaysia Act 768 and the Department of Skills Development Malaysia through Malaysia Act 652 which also incorporated the Scheme's syllabuses for the relevant National Occupational Skills Standards (NOSS) development. About 60 percent of public universities have started aligning cybersecurity academic modules with the Global ACE Certification to incorporate professional credentials.

For further information, please visit:
<https://www.cybereducationscheme.org/web/guest/certified-training-programme>
or email training@cybersecurity.my.

References

1. <https://www.itu.int/en/myitu/News/2020/09/04/15/50/2020-WSIS-Prizes-winners>

Drones – Models Of UAV And The Evolution Of The Future

By | Amirah Syazwani Binti Ahmad Suparmin

Drones are officially known as an Unmanned Aerial Vehicle (UAVs) or Unmanned Aircraft Systems (UAS). Fundamentally, a drone is also known as a flying robot that can be remotely controlled or fly autonomously through a software-controlled flight plans in their embedded systems, working in conjunction with onboard sensors and GPS.

Commercial usage of drones is gaining steady momentum as various industries are currently working with drones to see how they could fit into their daily business functions. Apart from that, drones are used in military services such as anti-aircraft target practice, intelligence gathering and then, more controversially, as weapons platforms. Drones are also used by the citizens, either for businesses or personal. The range of usage can be for surveillance, traffic and weather monitoring, food delivery or even the ever-popular photography and videography.

As flying has always been a dream for humanity, especially for kids, drones controlled remotely is a safe way for us to enjoy flying and being able view on the screen a bird's eye view of the surroundings. A drone is equipped with various state of the art technology, such as infrared cameras, GPS or even laser. This device is controlled by a remote ground control system which also known as the ground cockpit.

The Technology Of Drones

Drone technology is constantly evolving as new innovation and big investment are bringing more advanced drones to the market every few months. The UAV which is literally the brain of a drone describes the aerodynamics, the manufacturing physicals materials, chipsets and software, as well as the circuit boards. The UAV component consists of the body, power supply and platform, computing, sensors, actuators, software, loop principles and communications.

Types Of Drones

There are four (4) major types of drone which are commonly used. These drones can be classified based on usage such as for surveillances, personal usage, or aerial mapping.

1. Multi Rotor Drones



Multi Rotor drones are the most common types of drones that are used by professionals and drone enthusiast. They are mostly used for conventional applications such as aerial photography, aerial video surveillance, drone racing or even leisure flying. Multi Rotor Drones can be further categorized based on the quantity of rotor on them, some of which are Tricopter (3 rotors), Quadcopter (4 rotors), Hexacopter (6 rotors) and Octocopter (8 rotors). The most popular drone used is the quadcopter. This drone is the easiest and cheapest to manufacture. However, they tend to have limited flying time, durability, and speed. Therefore, it is not suitable for long distance aerial mapping or surveillance.

2. Fixed Wing Drones

Fixed Wing Drones are very similar to the likes of a normal airplane, with wings that are uniquely designed for its purpose. This type of drone is not able to hover in mid-air thus uses less energy. Its forward movement is controlled by the remote guide but dependent on permissible energy source. On average, a Fixed Wing Drone can fly for

a few hours based on the fuel efficiency and flying time. This drone is mainly used for long distance operation. Besides being quite



costly to manufacture, a Fixed Wing Drone requires special training and a runway for it to start its course on air. It also requires a parachute or a net to land it safely on the ground.

3. Single Rotor Drone



A Single Rotor Drone is like a mini version of a helicopter, with a big rotor and a small one on its tail that controls its course. This type drone is one of the most efficient drones with a higher-flying time. It can even be fuelled by gas engines. This type of single rotor drone has higher capabilities compared to the multi-rotor drone. Nevertheless, these machines come operational dangers. The manufacturing cost is also higher compared to the other drones. The huge measured rotor edges regularly represent a danger, some lethal fatalities have been recorded if the drone is mismanaged or it has been involved in an accident.

4. Hybrid VTOL

Designed for longer flying time, the Hybrid VTOL is a combination of Fixed Wing and

rotor-based models. Although this concept was tested in the 60's with many failures, the new generation technology and sensors



have given this design a boost. This type of drone is operated with a combination of computerization and manual flying. A vertical lift is utilized for the drone to be lifted in the air, while the Gyros and Accelerometers work in autopilot mode to keep the drone stabilized. This drone can run on programme or manual basis.

Evolution Of The Modern World

Drone technology has evolved tremendously over the past few years. One of the latest high-tech evolution is the Collision Avoidance System, an obstacle detection sensor technology that scans the environment, while the software algorithms generates the images into 3D maps, enabling the drone to detect and avoid any obstacles. The most common model is the recently released DJI Mavic 2 Pro and Mavic 2 Zoom which have obstacle detection on each of the 6 sides of the drones. These models also have the '**No Fly Zone Feature**' to increase the safety as well as to avoid accidents in restricted areas which is regulated by the Federal Aviation Administration (FAA). Furthermore, these drones are also equipped with the FPV (First Person View) Live Video Transmission technology which has a video camera and transmits the live video using the radio signal to guide on the ground. It allowed them to experiment on flying distance rather than looking at the drone from the ground.

With the world running on smartphones and applications, these drones can also be flown remotely on an application which can be easily downloaded from Google Play or App Store. The manufacturer will give the user full control of the drone. Although drones are widely available, there are the security aspect that needs to be taken into consideration.

- Ensure the drone's firmware is updated regularly. The major drone manufacturers will issue patches when new security threats emerge, so regular updates should keep the drones ahead from the hackers. After hackers breached the manufacturer's website, DJI releases a safety patch enabling them to access flight logs, videos, images, and map views from the user in real time.
- Use a strong password for your base station application. Using a combination of numbers, letters and special characters to create a solid password will deter hackers. Most will give up and go after easier prey. This should help avoid a malefactor hacking the drone signal.
- Keep your smartphone and laptop secure. Don't let it get infected by malware. Install a reliable anti-virus software and do not download any suspicious files
- Subscribe to a Virtual Private Network (VPN) to prevent hackers from accessing your communication while you are connected to the Internet. A VPN serves as a secure gateway to the Internet and encrypts your network, so that it is impossible for a hacker to get in.
- Ensure your drone has "Return to Home" (RTH) mode. Once you have set the home point, this will enable the drone to return if it loses signal, or when the signal is jammed or even if the battery is running out. This will enable you to recover your drone from a hijack situation. However, because RTH depends on GPS to work, it's not immune to GPS spoofing.

In 2019, Average Drone Sdn Bhd started a three-month trial on delivering food to their customers using a drone in Cyberjaya. The food would be delivered within a two-kilometre radius and take no more than 12 minutes once an order is placed. With the current water supply issue in Selangor, the state government has also decided to deploy drones to monitor rivers as well as collect samples from remote areas for inspection. According to Malaysia's national aviation authority, the Civil Aviation Authority of Malaysia (CAAM), flying a drone is legal in Malaysia. However, there are several drone rules and regulations that must be followed.

Drones may not be flown in Class A, B, C or G airspace; within an aerodrome traffic zone; or more than 400 feet above the ground, drone pilots must maintain a direct visual line of sight with their drones during operations, permission

from the Director General must be obtained for commercial drone operations and drones weighing more than 20 kilograms may not be flown without permission from the Director General.

As much as drones provide solutions for us, they are also not secure for our privacy as these spies in the sky can take pictures of our homes and has been found unsafe if they are flown in the city or airports. Collision in mid-air due to high drone traffic has also increased these days. In June 2019, Iran shot down a US military surveillance drone. Drones can also be used as a method of hacking as it is like minicomputers with operating system and programmable codes that can hack into wireless network and breaching others privacy.

Drone has been one of the most powerful technological inventions in recent times. Many countries are leveraging this technology to develop their own drones for multiple applications. These drones are combination of innovative technology with the likes of GPS Tracker, Wi-Fi or microcontrollers that gives plenty of company's business opportunity as well as chances to start-up companies to venture into these field.

With large amount of drone kits and course materials available on the Internet, makes it easy for beginners to build and program a drone. Therefore, the role of the government is crucial in such scenarios in enforcing the rules and regulation of the drones' law in order to spot malicious drones as well as build a strong regulation, so as to ensure no misuse of such valuable technology.

References

1. <https://www.circuitstoday.com/types-of-drones>
2. <https://readwrite.com/2020/04/23/what-the-drones-of-future-can-do/>
3. <https://www.kaspersky.com/resource-center/threats/can-drones-be-hacked>
4. <https://www.nst.com.my/lifestyle/bots/2019/06/497157/food-delivery-drones-cyberjaya-end-month>
5. <https://uavcoach.com/drone-laws-in-malaysia/>
6. <https://www.thestar.com.my/news/nation/2020/10/20/rm2mil-drones-to-be-used-to-catch-polluters>

Crypto-Ransomware Behaviour On Infected Machine

By | Wira Zanoramy Ansiry Bin Zakaria

Crypto-ransomware is a type of malware that encrypts the files of a user. The intruder then requests a ransom from the victim to restore access to the data upon payment. Users are given instructions on how to pay a fee to get a decryption key. Costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

Crypto-ransomware uses many forms of infection vectors to infect a machine. One of the most popular distribution mechanisms is phishing spam — an attachment that comes to the victim in an email, masquerading as a file they can trust. If downloaded and opened, they can take over the victim's device, particularly if they have built-in social engineering tools that trick users into allowing administrative access. Other more violent types of ransomware (such as NotPetya) exploit security holes to infect machines without needing to trick users.

Ransomware has been found to use standard cryptographic algorithms. This made the production of ransomware a relatively small endeavour, as these libraries are already available. Poorly crafted ransomware has also been effective as they use scare tactics on victims who would still pay the ransom ^[1].

Listed below are the behaviours of a crypto-ransomware on an infected machine:

a. Contacting command and control (C&C) server and cryptographic key exchange

When contacting their C&C servers using secure protocol, crypto-ransomware hides its network communication through the use of compromised web proxy servers. The exchange of cryptographically generated key was implemented securely using Transport Layer Security Version-1 (TLSv1) protocols ^[1].

b. Encryption of Targeted Files

Encryption is an essential characteristic of crypto-ransomware. It encrypts files with targeted extension and changes the extension's current name to other names.

c. File Search and Enumeration

Crypto-ransomware displays a typical behaviour, which is the enumeration of all interesting files on the computer. It is a plausible feature for ransomware detection and classification ^[3].

d. Delete Backup Files

Additional operations may be performed to frustrate recoverability. Ransomware could, in some cases, delete shadow copies that contain old copies of files ^[4]. For example, ransomware family TeslaCrypt disables and removes the Windows volume shadow copies, and other variants to wipe out the disk's free space. This operation is performed to avoid recoverability on the victim's side ^[5]. For example, Cerber ransomware escalates its privileges to administrator level, after which it deletes shadow copies. Ransomware deletes multiple files from the infected machine. This trait is clear evidence that it is either ransomware, wiper malware, or system destruction malware. The ransomware developer wants to ensure that the victim cannot recover the encrypted files without paying the ransom ^[1].

e. Terminating Selected Active Processes

Some ransomware terminates the running processes of productivity applications such as Microsoft Office, databases, and antiviruses.

f. Generating Cryptographic Key

Ransomware uses Windows APIs to generate the cryptographic key. An asymmetric key generation algorithm is employed to create a secure key used to encrypt files in the infected system. The generated key is shared with the attacker's C&C server.

g. Hidden TOR Browser

Ransomware has been known to use the Tor browser to maintain its anonymity, making it challenging to discover the source of the attack. For example, WannaCry ransomware dumped Tor link in the memory. Later, through the ransom-note, the victim will be instructed on how to use the provided Tor link to download and install the Tor browser. Henceforth, the victim will be required to use the Tor browser for any other communication with the attacker ^[1].

h. Moving and Appending New File Extensions

Ransomware performs write, move, delete, and rename the encrypted files by appending a new file extension over the existing extension. In the case of WannaCry ransomware, the appended file extension was .WNCCRY ^[1].

i. Payload Persistence

This action is to ensure that the attack remains persistent even after the system is rebooted. Standard techniques include placing an executable file in the start-up directory, adding a new registry key, and setting a scheduled task ^[2].

j. Restrict System Restore

This action is to prevent the victim from restoring the system to the pre-infection state. Commonly used techniques are deleting a scheduled backup and deleting backup files ^[2].

k. Stealth Mode

This action is to prevent the attack from being visible to the victim. Common approaches are executing from %AppData% directory and using the same name as the standard system executable ^[2].

l. Environment Mapping

This trait ensures that the infection is actually in the victim's system and not in a sandbox. A sandbox is a typical setup for the dynamic analysis of malware. Standard techniques used include checking the security setting

and policies, geographical location, user language, file system architecture, and network drives ^[2].

m. Privilege Elevation

This action will enable the attacker to perform actions as an administrator. The administrator can only perform system-related actions. Therefore, elevating to administrator level will ensure all activities can be performed without restriction ^[2].

In conclusion, a thorough examination of crypto-ransomware activity will help anti-ransomware researchers build a framework to detect and eradicate an impending ransomware attack.

References

1. S. Kihui and E. Abade, "Comparative Analysis of Distinctive Features of the Ransomware Tactics in Relation to Other Malware Comparative Analysis of Distinctive Features of the Ransomware Tactics in Relation to Other Malware," no. July, 2020.
2. S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Ransomware, Threat and Detection Techniques: A Review," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 2, pp. 136–146, 2019.
3. R. Moussaileb, B. Bouget, A. Palisse, H. Le Bouder, N. Cuppens, and J.-L. Lanet, "Ransomware's Early Mitigation Mechanisms," 2018, pp. 1–10.
4. U. Adamu and I. Awan, "Ransomware Prediction Using Supervised Learning Algorithms," 2019.
5. N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 2016-Augus, pp. 303–312, 2016.

Courses Of Action Matrix: The Cyber Kill Chain Complement For Incident Handlers

By | Afiq Ashraf Bin Mohd Azhar, Muhammad Azri Rafiuddin Bin Basri, Imran Bin Hasnan & Wan Lukman Bin Wan Junoh

Cyber Kill Chain is a seven-step process which adversaries have to execute in order to gain an entry into a network. Established in 2011 by aerospace and defence company, Lockheed Martin, the Kill Chain, has been widely used by blue-team members in an attempt to analyse the discrete, deterministic steps executed by adversaries in an intrusion. The cyber kill chain provides valuable information to both security analysts and computer network defenders in a way which would allow them to break down phases of a cyber intrusion and apply the necessary action (responsive/prevention) to ensure a thorough, meticulous outcome.

While there are many variations for such model, the cyber security community has largely made use of the model developed by Lockheed Martin.

Lockheed Martin's cyber kill chain breaks down an external-originating cyberattack into seven steps:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

1. **Reconnaissance** in the cyber kill chain refers to all of the upfront work needed to be done before executing the next move. This phase can be described as an assessment phase by the adversaries in which they assess all available information pertaining to their target and the suitable tactics and techniques they could deploy against the target victim.
2. **The Weaponization** and **Delivery** stage of the kill chain describes both the process of configuring the tools/malware/payload to exploit the vulnerability discovered in the reconnaissance phase and delivering the artefacts from the adversary's machine to the victim organization.

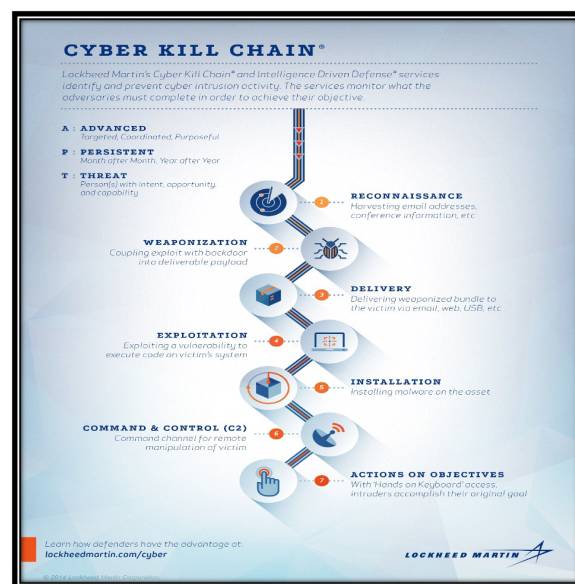


Figure 1: 7 Step process of the Cyber Kill Chain

3. **Exploitation** can be explained by the process of executing code on the victim's system. This could be achieved either through using exploits guided by CVEs or in some advanced cases through zero-day exploits.
4. **Installation** describes the action taken once the exploitation is successful. This includes files creation, modification, changes in registry and any other external components created or modified.
5. **Command and Control** or C2 is the sixth phase of the cyber kill chain. During this stage, the adversary has managed to gain a foothold in the target organization and generally tries to establish communication between adversary and victim machine.
6. **Actions on objectives** entails all the action taken by adversary once they have gained full operational control of the victim's system. This includes files exfiltration and transferring of tools to victims machine to facilitate the mission scope of adversary

Courses Of Action Matrix

During analysis of a security incident, one will undoubtedly encounter various indicators associated with the different stages of the cyber kill chain. This raises questions by analysts on what is the best course of action to be applied, without losing any crucial information pertaining to the adversary, their TTPs and the mission focus (intent) while also simultaneously trying to curb the on-going intrusion.

For example, if you found a piece of indicator such as an IP address performing some malicious activity and a suspicious email address in a user's mailbox, will you simply block or quarantine those said IP address and email? Will your action allow you to gain some knowledge (intelligence) on the adversary using those infrastructures? This is where the courses of action matrix comes into play. It would allow analysts to determine the actions available to them, prioritize initial efforts, categorize indicators, as well as identifying gaps in their organization such as data collection (log retention), preparedness of security team, etc.

The courses of action matrix can be divided into two categories namely active and passive.

The following are categorized active courses of action:

1. Discover

The discover action is a "historical look at data". This may include running a piece of indicator against your local data/log storage or SIEM environment and determine whether you have seen the specific indicator in the past. This action will provide valuable insight on the intrusion being analysed if a match was found in your network environment. Analysts could then pivot through the information to gain insight on the nature of attacks and plan their next move.

2. Detect

When you obtain an indicator in your analysis and have confirmed that the information is accurate and viable, you must tune and set up your local systems such as your Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Firewall Rules, SIEM, etc to allow any future events associated with the particular Indicator to be detected and triggered by your local systems.

	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Log /data correlations	Web analytics	Policy to prevent forum use/traffic filtering			Create fake posting	
Weaponization							
Delivery	Log /data correlations	NIDS, user education	Email AV scanning		Email queuing	Filter but responds with out-of-office message	
Exploitation	Log /data correlations	Hids	Patch	DEP			
Installation	Log /data correlations						
Command and Control	Log /data correlations	NIDS	HTTP Whitelist	NIPS	HTTP throttling		
Action on objectives	Log /data correlations	Proxy detection	Firewall ACL	NIPS	HTTP throttling	Honeypot	

Figure 2: Sample courses of action matrix detailing actions to be taken in every phase of the cyber kill chain

The following are categorized as passive courses of actions.

1. Deny

As the name suggests, when you discover an indicator, you will outright deny it from being run or executed in your system environment. However, this course of action may limit your intelligence analysis as the full extent of the adversary's tactic and technique may not be captured.

2. Disrupt

The disrupt course of action aims to make an event fail as it is occurring. Several examples include quarantining of suspicious emails, session termination, etc.

3. Degrade

Degrading generally means to take actions to slow down an ongoing attack. This would allow system engineers and security analysts to buy some time to further understand the scope of an attack. However, precautionary steps must be taken as the ongoing attack may eventually succeed. Example of this action would be throttling of bandwidth or limiting certain system functionalities.

4. Deceive

Deception is a process in which we try to deceive the attackers by supplementing false knowledge that their action was successful. Some examples would be the usage of honeypots and rerouting suspicious emails to "black-holes"

5. Destroy

Destroy is defined by taking offensive actions against the attackers. This may include "hacking back", performing physical destructive action as well as law enforcement arrests. This course of action is rarely used by organization as most lack the legal aspect of performing such activities.

In short, the courses of action matrix will vastly improve the capabilities and decision-making for analysts involved in research and analysis of a security incident.

Combined with the cyber kill chain, the courses of action matrix would be a fantastic complement for incident responders to handle an ongoing incident without losing precious intelligence pertaining to attack methods employed by the adversary.

For this to work seamlessly though, analysts and incident handlers must have a clear understanding and knowledge of their internal organization's structure, resources and associated knowledge gaps, to ensure the best course of action is implemented in dealing with cyber security intrusions.

References

1. <https://www.sans.org/security-awareness-training/blog/leveraging-human-break-cyber-kill-chain>
2. <https://www.researchgate.net/figure/Kill-Chain-course-of-action-matrix-7D-Model-derived-from->
3. APT-groups-APT28-Red_tbl1_330071595
4. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

Understanding Human Elements In Inculcating Information Security Culture In An Organization

By | Sharifah Sajidah Binti Syed Noor Mohammad

Accessing the Internet today is no longer limited to hard wired terminal, you could now go online just about anywhere seamlessly. Within an organization, employees, contractors, business partners are also connected to Internet and Intranet at all time. Information is one of the valuable assets for an organization. Whilst information security is an activity to secure the information and to protect it against disclosure or leakage of sensitive or confidential information, modification of critical information either accidentally or intentionally, lost of any important business information and unavailability of any important business information. The increasing number and diversity of cyber security breaches and threat has made safeguarding information more complex. One of the main causes of information security breaches are ignorance and ill will by current and former employees – the primary users of information and it is challenging to manage them. According to Pahlila, Siponen, & Mahmood^[1], human element is the weakest link in information security.

Information security risks can create negative effects on business processes and lead to financial loss. Human errors are usually made due to negligence, accident, or deliberate action. According to Rhee et al^[2], a conscious practice has been acknowledged to be an effective approach of reducing the risk of information security incidents in organizations. A conducive culture favorable to information security practice is vital for organizations since the human dimension of information security cannot be totally addressed by technical and management measures^[3]. According to Carlin^[4] the spread of “Wannacry” ransomware that crippled businesses and government entities exposed the weaknesses in how government and business sectors approach cyber security issues with non-compliance being the main contributing factor. Based on the report by Ponemon Institute^[5], the average cost of Data Breach in the information security industry in 2020 is US\$3.86 million. Meanwhile, Verizon Data Breach Investigations Report 2018 disclosed that human error is the second most common cause of breaches. In addition, Okere, J. van Niekerk, and M. Carroll^[6] in their report highlighted that security breaches cost

organizations billions of dollars including the costs of data clean up, loss of data, liability and loss of customer confidence. Human behaviour is heavily influenced by respective culture. Our human interactions, be it formal or informal, are shaped by the environment and the group they are in, and they can be both creating risks and also mitigating security breaches.

Due to rise of information security breach resulting from employees/human error, negligence, ransomware, malware, phishing, denial of service, botnets, computer viruses and worms, cryptocurrency hijacking, there is a need to inculcate an Information Security Culture (ISC) in which it will become a driving force and control mechanism to mitigate risks and vulnerabilities on information assets. To achieve a secure environment for information assets, information security practices should become part of the corporate culture of an organization. The organization culture dictates on activities and behaviour of employees and what the organization and its employees must, can, or cannot do. Information Security Culture acts as a firewall for organisations. As stated by A.Alhogail^[7] organization must develop a ISC to lessen potential risks posed by employees and empowers members of an organization to reduce security incidents. A.Alhogail and Mirza^[8] defines ISC as a collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction in regard to information assets in an organization with the objective of influencing employees’ behavior to preserve its security. There are numerous factors that can mould ISC and this would be depend on the organization itself. The following are factors that influence the human side of information security.

a. Management Commitment (MC)

Knapp^[9] defines Management Commitment (MC) as the level of preparedness and commitment of the highest ranked personnel in the organization in supporting information security initiatives. Management commitment is vital in developing an ISC. Continuous support from this group which includes budget, technology, and human capital and leadership are key contributors to a successful implementation. The top management must promote and communicate a clear message on its information policies and goals to all employees. Narain Singh. A , Gupta, M.P , Ojha A^[10] said that the management are not only required to support and provide adequate funding, but must also commit and participate in all process including objective setting, planning which is not limited policies and procedures development, guidelines and also decision making. On the other aspects, management commitment in information security programmes have great influence on employees' behaviour towards compliance with information security policies, and hence has an impact towards the organizational security culture^[11].

b. Information Security Policies & Procedures (ISPP)

Information Security Policies & Procedures (ISPP) is a written document which spells out an organization's strategies and security posture that governs both the management and employees' behaviour. ISPP is created to communicate information on security protocols, job descriptions, how to handle information security incidents and provide guidelines to employees on standard operating procedure as per PK Sari, Candiwan, N Trianasari^[12] . K Renaud, W Goucher^[13] assert that ISPP should be concise, straight forward, relevant and easy to understand as a complicated document will result in non-compliance. According to N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell^[14] , clear information security policies, adequate security education, training and awareness programs alongside constant monitoring are necessary to bring about a progressive security culture within an organization.

To implement ISPP effectively requires a combination of people, processes and technology controls. Hence, ISPP is key ingredient to cultivate employees' knowledge, understanding towards the ISPP governance and influence their information security behavior.

c. Training & Awareness (TNA)

Training and awareness are a fundamental aspect of thriving information security cultures. It provides employees with the appropriate knowledge needed to use the systems properly. Maeyer^[15] , defines security awareness as an organized and ongoing effort to guide the behaviour and culture of a corporation about security issues. Employees need to be equipped with training and certification on various information security aspects to manage associated risk, damages and threats to their information assets^[16] . Parsons in "A study of information security awareness in Australian government organizations. Information Management & Computer Security"^[17] concluded that Information security Training & Awareness (TNA) implementation is to educate employees on the risk associated with information and appropriate controls necessary and been proven to have a positive impact on the ISC. It is the prerogative of the Management to ensure that training and awareness programmes are available to promote the importance of information security management and safeguarding from threat^[18] .

d. Perceived Sanctions

Mulder, L.B^[19] says sanction is often associated with something negative, namely a punishment for undesired behaviour. Conversely, one may use rewards to encourage desired behaviour. In addition to that he says that sanctions can act as an enabler not only in deterring people from unwanted behaviour but also to convey ethical norms. Perceived sanctions could affect both in a positive and negative way as it may come in the form of a reward or punishment. Herath and Rao^[20] asserts that, sanctions and rewards can alter behaviour and shape culture of the employees. Cheng et al. (2013) in his research highlighted that sanctions and rewards is to encourage behavioural changes amongst employees.

On the other note, Park^[21], Kim, and Park , Siponen, Pahnla, and Vance^[21] emphasized that the level of compliance with information security policies is dependent upon the consequence of non-adherence. Enforcement of penalties in monetary terms would reduce the likelihood of misbehaviour as asserted by D'Arcy, Herath, and Shoss^[23] , Knapp and Ferrante^[24] .

e. Information Security Compliance (C)

Information Security compliance is defined as set of core information security activities to enforce information security as defined by information security policies. Humaidi & Balakrishnan^[25] asserts that having a clear set of security guideline and strict monitoring of employees', will increase information security policies compliance. Whilst Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C.^[26] highlights that the employees' knowledge and adequate understanding of information security policy and procedures will determine the level of compliance. Regardless of their objection, all employees must follow all information securities and procedures in their daily work activities Vroom and von Solms^[27], information security management theorists assert that the behaviour of employees must be guided and monitored to ensure compliance to security requirements.

Y Chen, K Ramamurthy, KW Wen^[28] study says that organizations should put an effort to reward or punish security-related behavior or employees' individual attitudes or motivation to comply with information security policies in an organization. Organizations require their employees to have a well verse understanding and compliance towards information security^[29]. S.Woodhouse studies^[30] shown that the effectiveness of information systems security can be achieved through promoting adequate information security behaviour and constraining unacceptable information behaviour among employees in the organization. Dhillon, Gurpreet; Abdul Talib, Yurita Yakimini; and Picoto, Winnie Ng^[31] pointed out the concern on the non-compliance in information security keep arising due rises due to the possibility of aggressive information security threats and stress out there are limited attention paid to the relationship between work structures such as, intermediating role of psychological empowerment in the relationship and employee's intention to comply to information security policies.

f. Information Security Management System (ISMS)

Liao and Chueh (2012) noted that data security breaches are a result of inefficient management of the availability, integrity, and confidentiality of information. To ensure the information asset remains intact, many organisations must implement Information Security Management (ISM). Current existing standard that provides guidance on ISMS is International Standards Organization (ISO) 27001, which is aimed

at establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) through confidentiality, integrity and availability of the information, It provides a framework for the management of security within an organization. It gives a best practice management framework for implementing and maintaining security.

In a nutshell, ISMS addresses the identification of security needs, objectives, implementation of strategies to support these needs, measurement of results, and improving both the protection strategies. It also consists of instrument, method and leadership that ensure consistent application of the information security principles and policy statement in all tasks and activities^[32]. ISMS introduce continuous improvement process that requires organisations to review their ISMS regularly to ensure its effectiveness^[33] known as "Plan-Do-Check-Act" (PDCA). This ISMS become a driving forces which the orchestrate in organizational context that support change in the desired culture^[34]. To have a check and balance of the ISMS implementation, an audit should be conducted. Audit findings will reveal opportunities for improvement and identify weaknesses in the ISMS itself. The effectiveness of ISMS is subject to many human factors, such as information security awareness, top management support, information security training & awareness, skillsets, and communication^[35].

Conclusion

High dependency on Internet connection has exposed many organisations to potential cyber threats from various sources. Deployment of powerful firewalls, antivirus software and complicated intrusion-detection systems does not ensure zero information security incidents. The organization should focus on the most important and vulnerable security component which is the human resources. According to Von Solms various information security controls can only be managed properly if a comprehensive information security culture is in place, where employees know, understand, and accept that precautions are necessary. S. Furnell in his 2007 publication said that an organization should lead initiative towards building an ISC and integrate information security practices into its corporate culture as this will ensure that employees have the required knowledge and skills to behave appropriately. Information Security Culture guides employees on how to protect and secure

the information assets and as assert by A. Da Veiga and J. Eloff organizations need to create an environment where security is “everyone’s responsibility” and do the right thing. A strong ISC in organizations may able to address many of the human and behavioral issues that cause information security breaches in organizations. A robust ISC would be more likely to result in employees being more engaged, accountable and compliant with information security and ensure protection of information assets. Every employee in the organization should always be alert and aware of the risks that is associated with information. There are factors that determine the effectiveness of ISC such as leading by example – top management support, documentation good practice into policies and procedures, enforcement and imposition of penalty and reward, ongoing training and awareness as well as a structured information security management system.

References

1. Okere, I., Niekerk, J.V., & Carroll, M. (2012). *Assessing information security culture: A critical analysis of current approaches*. 2012 *Information Security for South Africa*, 1-8.
2. M.Daud, R.Rajah, G. Mary, A. David & T. Govindamal (2018). *Bridging The Gap Between Organisational Practices And Cyber Security Compliance: Can Cooperation Promote Compliance In Organisations*. *International Journal of Business and Society*, Vol. 19 No.1, 2018, 161-180
3. Carlin, J. (2017, May 17). The ‘WannaCry’ ransomware attack could have been prevented. Here’s what businesses need to know. CNBC. Retrieved from <http://www.cnbc.com/ Titcomb & McGoogan, 2017>
4. Ponemon Institute’s Data Breach Report 2020
5. Verizon Data Breach Investigations Report 2018
6. Tessem, H.M. and Skaaraas, K.R. (2005), “Creating a security culture”, *Information Society and Security*, p15.
7. MT Siponen (2000) “A conceptual foundation for organizational information security awareness” - *Information Management & Computer Security*, 2000.
8. Abhishek Narain Singh , M.P. Gupta , Amitabh Ojha (2014). “Identifying factors of “organizational information security management””. *Journal of Enterprise Information Management*. 2014
9. Rhee, H.S., C. Kim, and Y.U. Ryu, *Self-Efficacy in Information Security: Its Influence on End Users’ Information Security Practice Behavior*. *Computers & Security*, 2009. 28(8): p. 816-826.
10. A.AlHogail, “Design and Validation of Information Security Culture Framework,” *Computers in Human Behavior*, vol. 49, no. August, (2015), pp. 567-575.
11. T Herath, HR Rao (2000) “Protection motivation and deterrence: a framework for security policy compliance in organisations” *European Journal of Information Systems*, 2009
12. A. AlHogail and A. Mirza, "Information security culture: A definition and a literature review," 2014 *World Congress on Computer Applications and Information Systems (WCCAIS)*, Hammamet, 2014, pp. 1-7, doi: 10.1109/WCCAIS.2014.6916579.
13. PK Sari, Candiwan, N Trianasari (2014) “Information security awareness measurement with confirmatory factor analysis”. *Technology Management and Emerging Technologies (ISTMET)*, 2014
14. K Renaud, W Goucher (2012) “Health service employees and information security policies: an uneasy partnership?” *Information Management & Computer Security* 2012
15. Safa, N. S., Von Solms, R., & Furnell, S. (2015). *Information security policy compliance model in organizations*. *Computers & Security*, 56, 70-82.
16. Adéle Da Veiga (2015). According to ISF (2000), Box and Pottas (2013),
17. Maeyer D.D (2007). *Setting up an effective information security awareness program*. ISSE/SECURE 2007 *Securing Electronic Business Processes Highlights of the Information Security Solutions Europe/ SECURE 2007 Conference (part 1)* 49-58.
18. K. Renaud. (2012). *Blaming noncompliance is too convenient: What really causes information breaches*. *Security & Privacy, IEEE*, vol. 10, no. 3, pp. 57-63, 2012.
19. Sami M. Alageel, (2003). *Development Of An Information Security Awareness Training Program For The Royal Saudi Naval Forces (RSNF)*. Naval Postgraduate School

20. A. Da Veiga, J.H.P. Eloff (2010). A framework and assessment instrument for information security culture *Computers & Security*, Volume 29, Issue 2, March 2010, Pages 196 – 207
21. Ponemon Institute. 2017 cost of data breach study: Global overview. In IBM Security, 2017.
22. Alavi, R., Islam, S. & Mouratidis, H., 2014. LNCS 8533 - A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations. LNCS, 8533, pp.297-305.
23. Mulder, L.B. When sanctions convey moral norms. *Eur J Law Econ* 46, 331-342 (2018). <https://doi.org/10.1007/s10657-016-9532-5>
24. Park, E. H., Kim, J., & Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, 65, 64-76.
25. Mikko Siponen, Seppo Pahnla Motivating IS security compliance: Insights from Habit and Protection Motivation Theory Anthony Vance*, *Information & Management*. Volume 49, Issues 3-4, May 2012, Pages 190-198
26. J D'Arcy, T Herath, MK Shoss (2014) "Understanding employee responses to stressful information security requirements: A coping perspective" *Journal of management information systems* 31 (2), 285-318
27. Knapp, KJ, and Ferrante, CJ 2012. "Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations," *Journal of Management Policy and Practice* (13:5), Dec 2012, pp 66-80
28. Humaidi, N., & Balakrishnan, V. (2012). The Influence of Security Awareness and Security Technology on Users' Behavior towards the Implementation of Health Information System: A Conceptual Framework. *International Proceedings of Economics Development & Research*, 35.
29. Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organizations. *Information Management & Computer Security*, 22(4), 334-345
30. Vroom, C., & von Solms, R. (2004). Towards information security behavioral compliance. *Computer Security*, 23(3), 191-198.
31. Y Chen, K Ramamurthy, KW Wen (2012) "Organizations' information security policy compliance: Stick or carrot approach?" *Journal of Management* 2012
32. Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), 635-645.
33. S. Woodhouse (2007). Information security: End user behavior and corporate Culture. presented at 7th IEEE International Conference on Computer and Information Technology- CIT 2007, 2007.
34. Dhillon, Gurpreet; Abdul Talib, Yurita Yakimini; and Picoto, Winnie Ng (2020) "The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions," *Journal of the Association for Information Systems*: Vol. 21 : Iss. 1 , Article 5.
35. ISO/IEC 27001:2013 - International Organization for Standardization and International Electrotechnical Commission, 2013
36. Heru Susanto, Mohammad Nabil Almunawar and Yong Chee Tuan (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences IJECS-IJENS* Vol: 11 No: 05
37. Kumah, P. (2020). The Role of Human Resource Management in Enhancing Organizational Information Systems Security. In Misra, S., & Adewumi, A. (Eds.), *Handbook of Research on the Role of Human Factors in IT Project Management* (pp. 278-303). IGI Global.

Cyber Security: Putting Resilience Before Insurance

By | Ida Rajemee Binti Ramlee, Ahmad Sirhan Bin Abdul Ghazali, Ahmad Khabir Bin Shuhaimi, Adam Bin Zulkifli, Nurfaezah Hanis Binti Halim & Mayasarah Binti Maslizan

Overview

Cybercrime cost the global economy almost USD600 billion or approximately about 0.8% of global gross domestic product (GDP), according to a 2018 report by the Centre for Strategic and International Studies (CSIS) and McAfee. The elements of cybercrime include theft of Intellectual Property (IP), financial losses arising from online fraud and financial crimes, as well as reputational damage.

Cybersecurity firm Kaspersky reported that Malaysia was ranked 17th in ransomware attacks and recorded losses to the tune of RM22 million as a result ^[1].

What do these statistics tell us? Due to rampant cyber-attacks, we are losing enormous amounts of money, potentially tarnishing reputation, and jeopardizing customers and employees as a result. To mitigate financial losses, lawsuit or privacy investigation as a result of cyber-attack or other technical risks, one can turn to cyber insurance.

Insurance is a risk transference method by which an organization can hedge against uncertainty. An organization agrees to pay a fixed premium and the insurance company agrees to compensate in the event of adverse outcomes.

Cyber security insurance or cyber insurance is a form of risk management solution to protect businesses or individuals from cyber risks not limited to information infrastructure, information privacy, information governance liability, and activities related thereto ^[2].



Cyber insurance is a comprehensive financial solution that covers business interruption loss due to a network security failure, data loss and restoration, liability arising from failure to maintain confidentiality data, defense cost, personal and corporate data liability, extortion, hacking, theft, denial of service attacks as well as others that are deemed appropriate.

Know Your Information Security Readiness

Cyber insurance is not a replacement for cybersecurity. The need for cyber insurance should be considered after all information security risk mitigations have been fully exhausted. This include putting a comprehensive suite of security tools in place and conducting regular due diligence to secure your information. By knowing your organization's information security readiness level, you can identify key areas that need further improvement. Therefore, these elements should be considered in identifying your readiness level towards information security:

1. Employ Information Security Governance

Information security governance is an organization's structure, policies and practices to ensure controls are adequately communicated, carried out, and enforced by engaging direction and support at the appropriate organizational



level. It is important for information security roles and responsibilities to be clearly defined and assigned to relevant parties. Thus, they know what are supposed to do in protecting organization's information.

Organizations can refer to one of the most globally recognized standards for information security: the ISO 27001:2013 Information Security Management System (ISMS). ISMS comprehensively address information domains and controls in relation to process, people, and technology (PPT).

Organization should ensure processes meet business requirements and are aligned with policy, as well as adopt new technologies that are adaptable to changing requirements. The processes needs to be well documented and communicated to relevant human resources personnel, and periodically reviewed to monitor its effectiveness.

Implementing information security in an organization can protect the technology and information assets it uses by preventing, detecting and responding to threats. People

play an important role in enforcing information security. Organization should provide information security awareness and training to their staff, addressing information security concerns in recruitment such as access to background checks, access to system tools and data on employment and termination.

Putting strategic processes and competent people in place ensure a more assuring deployment of technology.

Enforcing compliance helps organizations secure information, increase resilience to cyber-attack, accelerate response to evolving security threat, improve organization culture, protect confidentiality, integrity and availability (CIA) of data, as well as provide organization-wide protection. The aforementioned advantages will contribute to lower dependency on cyber insurance.

2. Establish Risk Management

To support the implementation of ISMS, there are several general risk assessment ^[3] measures that organizations should undertake to minimize the level of risks by adding possible counter

measures. Firstly, identify and manage the risk through an asset and risk management strategy and development of cybersecurity policies. Next, mitigate the risk by establishing data security protection to protect the confidentiality, integrity, availability of data and empowering staff within the organization through cybersecurity awareness and training. Monitor the occurrence of risks, ensuring anomalies and incidents are detected, understand its potential impacts, and verify the effectiveness of protective measures is also vital in risk assessment. Finally, organizations need to ensure their response planning processes are executed during and after an incident and analyze the effectiveness of response activities in order to reduce the threats.

This comprehensive process of risk assessment is crucial for all organizations to protect their assets, finances, and operations. An effective risk management will protect the reputation, credibility, and status of the organizations from any damages due to unexpected cybersecurity incidents.

3. Assure Data Protection and Privacy Practices

Businesses that use, collect and process personal data of their customers should acknowledge and comply with the relevant data protection acts such as Malaysian Personal Data Protection Act (PDPA). The concept of data privacy is premised on the rights of the data subject. Data subject is an individual person who can be identified directly or indirectly based on the identifier such as name, IC number, address, email, etc. Data subjects have the right to know the purpose of data collection, processing, and the way organizations process and manage their personal data. Therefore, the purpose of data protection and privacy is to keep information private so that individuals' identities stay as safe and anonymous as possible. Basic principles [4] that will help organizations manage and protect their personal data include but not limited to the following:

- i. Encourage education and awareness on data privacy protection among the personnel and data subject;
- ii. Provide a clear privacy policy – organizations must inform data subject on how organizations will collect, store, protect and utilize their personal data (e.g. name, email, phone number, birth

date, financial info, etc.);

- iii. Provide SLAs/Data Processing Agreement with Third Parties to have a mutual understanding in ensuring that data processor provides sufficient guarantees in respect of security and privacy and organizational measures governing the processing of personal data;
- iv. Complying with the seven (7) principles of Malaysian PDPA which are General, Notice and Choice, Disclosure, Security, Retention, Data Integrity and Access Principles;
- v. Practice minimal data collection – organizations must determine the type of information they want to collect from the data subject and the purpose of collecting the information;
- vi. Apply consent mechanisms whenever the organizations want to collect and use personal information. At the same time, to allow data subject to correct, modify or terminate their personal information;
- vii. Implementing Privacy by Design (PbD) approach using technology by integrating data protection and privacy features into the system and application engineering, practices and procedures;
- viii. Conduct a Privacy Impact Assessment (PIA) that scrutinizes the privacy implications of the operations and personal data handling practices.

Data protection and privacy laws represent a complex collection of differing guidelines over processing of users' data (e.g. customers). Most of the privacy guidelines stipulate the rights of data subject to control the party using their data. It is difficult to determine one single framework that would allow organizations to protect the data. However, by implementing the aforementioned best practices, organizations will minimize the impact of privacy breaches, better manage their reputation and avoid additional liability for concealing a privacy breach incident.

4. Ensure Resilience

Implementation of Business Continuity Management (BCM) helps in ensuring an organization's resiliency. According to DRI International Glossary for Resiliency, BCM is defined as a holistic management process that identifies potential threats to an organization and the resulting impact to business operations. It provides a framework for building organizational resilience by leveraging the capability in effective response and action that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities [5].

One of the important parts of the BCM process is to conduct Business Impact Analysis (BIA) which will help organizations identify critical business functions, product or services. Based on the BIA, organizations need to develop or update their Business Continuity Plan (BCP) where they can review its incident management, disaster recovery and business continuity strategy. The strategy includes backup and recovery as well as testing exercise to ensure effectiveness.

Conclusion

Cyber security has become one of the most essential sectors in today's environment. The rise in cybercrime incidents has made organizations more cautious in dealing with cyber threats. Prior to resorting to cyber insurance, organizations should employ information security governance with the support of their top management. It is important to establish risk management by conducting risk assessment whenever there are new changes to the existing processes, or when hazards are identified. Strengthening data protection and privacy practices help reduce the impact of privacy breaches.

Finally, organizations should cultivate resiliency by implementing BCM strategies to respond to threats such as natural disasters or data breach. This would help ensure continuity in daily business operations. Having these elements in place will at least give the organisations a peace of mind and reduce reliance on cyber security insurance.

References

1. Muhammad Saufi Hassan (November 12, 2019) Title: "Serangan Ransomware meningkat di Malaysia". Retrieved on 21st October 2020 from URL: <https://www.hmetro.com.my/itmetro/2019/11/516501/serangan-ransomware-meningkat-di-malaysia>
2. Organisation for Economic Co-operation and Development (OECD) (2017) Title: "Enhancing the Role of Insurance in Cyber Risk Management". Retrieved on 21st October 2020 from URL: <https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf>
3. US National Institute of Standards and Technology (August 10, 2018) Title: "CyberSecurity Framework: The Five Functions". Retrieved on 21st October 2020 from URL: <https://www.nist.gov/cyberframework/online-learning/five-functions>
4. Stephanie Torto (June 18, 2020) Title: "Best Practices for Managing Data Privacy & Responding to Privacy Breaches". Retrieved on 21st October 2020 from URL: <https://securityintelligence.com/posts/manage-data-privacy-breaches-response/>
5. [5]DRI International. Title: "What is Business Continuity Management?" Retrieved on 21st October 2020 from URL: <https://drii.org/what-is-business-continuity-management>

A Brief Review Of Authenticated Encryption

By | Nik Azura Binti Nik Abdullah, Norul Hidayah Binti Ahmad Zawawi, Liyana Chew Binti Nizam Chew & Faridatul Akhma Binti Ishak

This article provides a brief review of Authenticated Encryption and some of its common schemes.

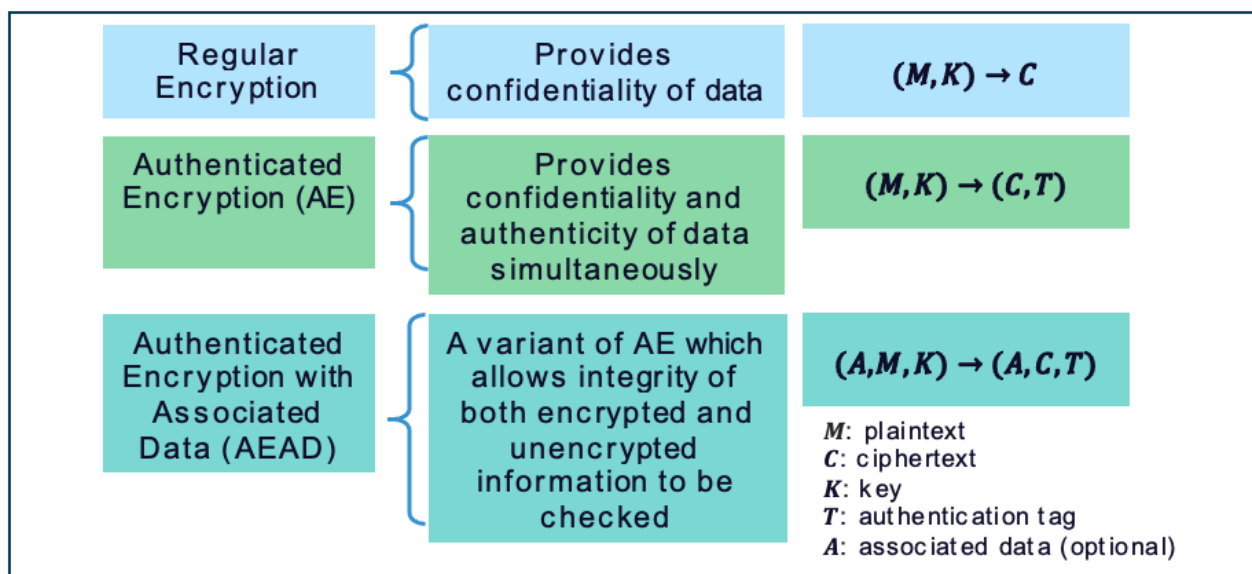
What Is AE And AEAD Compared To Regular Encryption

Why should I use an authenticated encryption mode rather than just an encryption mode?

In today's corporate world, secure communication is absolutely crucial. To fully trust a communication channel, two issues are important: security and authentication. We must secure the contents of the message and authenticate to ensure the message is genuine. Encryption is a process of hiding the content of a message so that only the intended recipient can read it. This provides confidentiality of the message. On the other hand, authentication

confirms that the encrypted message comes from the correct sender. Authenticated Encryption (AE) and Authenticated Encryption with Associated Data (AEAD) are forms of encryption that provide the assurances of confidentiality and authenticity of data

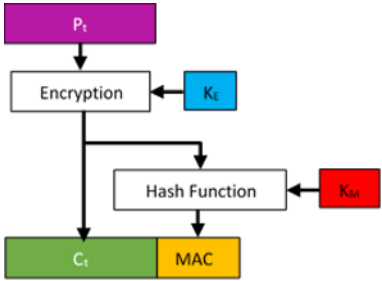
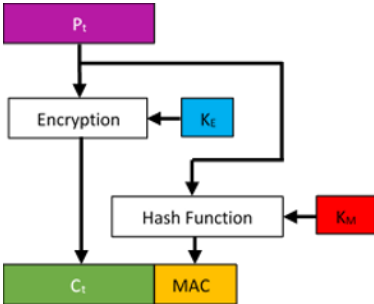
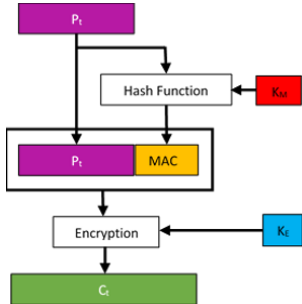
The main difference between standard encryption and authenticated encryption (AE) is that AE provides confidentiality and authenticity, while standard encryption provides only confidentiality. Securely combining separate schemes for confidentiality and authenticity could be error-prone and difficult. This weakness has been the motivation behind the development of AE. An AE scheme is usually more complicated than confidentiality-only or authenticity-only schemes. However, it is easier to use because it usually needs only a single key and is more robust. Throughout the years, enhancement was further made to consider the associated data, which are not confidential but must authenticate the encrypted data.



AE Scheme By Generic Composition

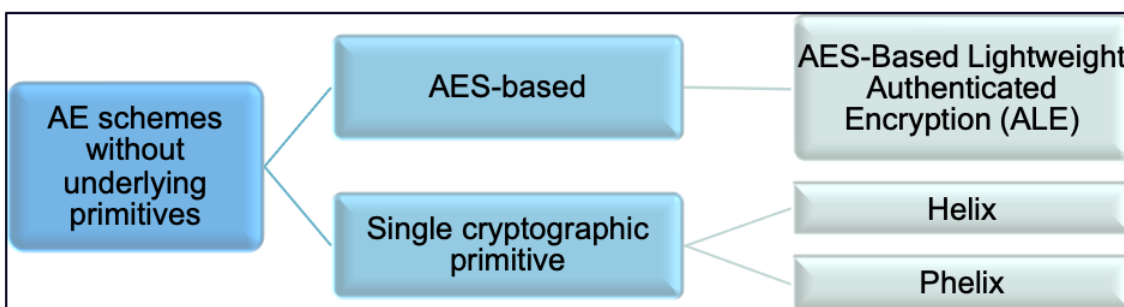
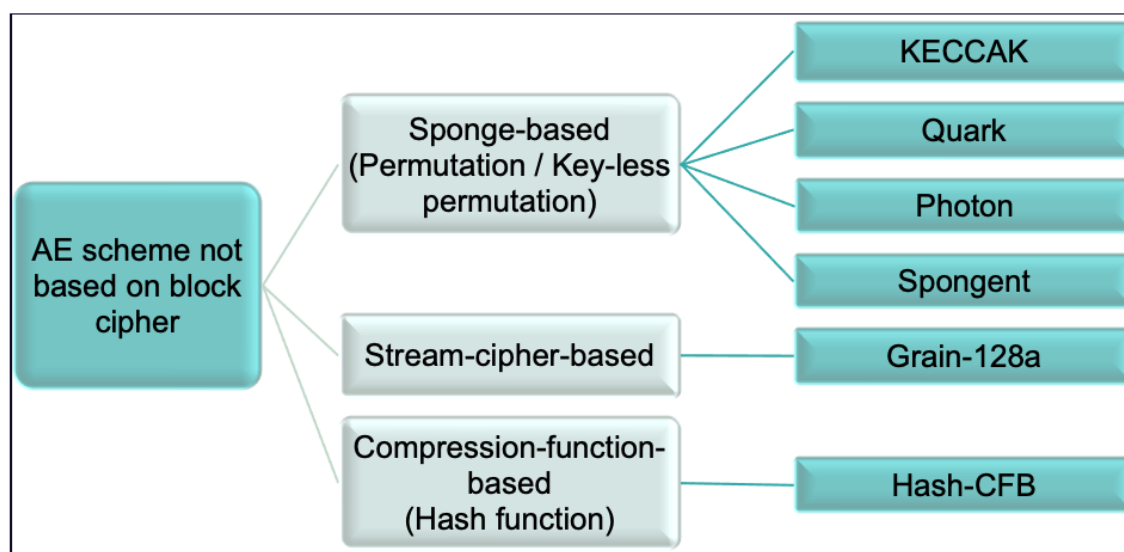
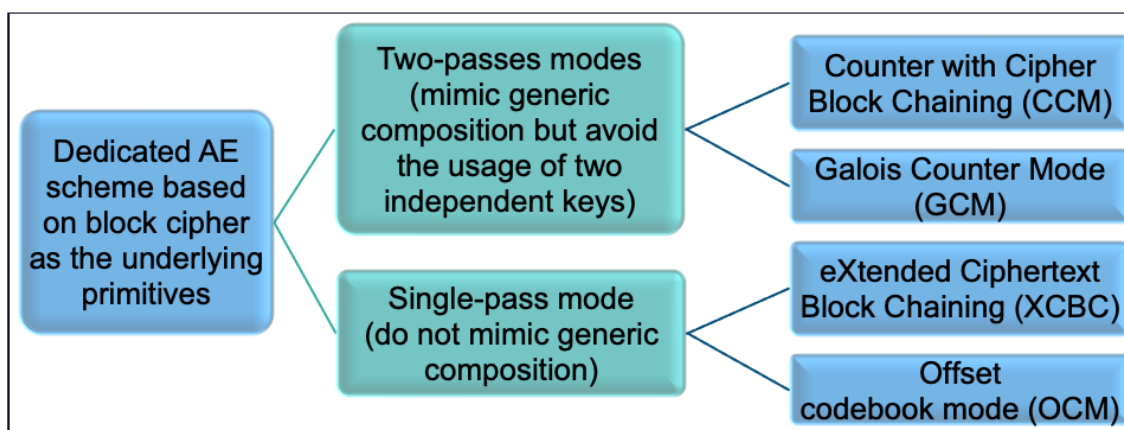
A way to design an AE scheme is by using the generic composition which combines a secure encryption function with a secure message authentication code (MAC) using two independent keys.

There are three types of AE generic composition scheme:

Encrypt-then-MAC (EtM)	Encrypt-and-MAC (E&M)	MAC-then-Encrypt (MtE)
		
<p>The plaintext is first encrypted using an encryption key. Then MAC is produced based on the resulting ciphertext together with a different MAC key. Finally, both ciphertext and MAC are sent together.</p>	<p>The plaintext is first encrypted using an encryption key to produce ciphertext. The same plaintext is hashed using a MAC key to produce a MAC. Then both ciphertext and MAC are sent together.</p>	<p>Plaintext with a MAC key is first used in hashing to produce a MAC. The plaintext, together with the resulting MAC, is encrypted using an encryption key to produce the ciphertext. Finally, the ciphertext containing the MAC is sent.</p>
Used in IPsec	Used in SSH	Used in TLS
Most secure variant	Generically insecure	Mildly insecure

Alternative To AE Scheme By Generic Composition

Among the three generic AE Scheme described earlier, EtM (Encrypt-then MAC) is guaranteed to be most secure. However, this variant has some flaws. It uses two different keys for encryption and authentication and has low performance. The alternative to AE by generic composition and its example of standard cryptographic algorithms are: –



Conclusion

Authenticated encryption (AE) has been a vital operation in cryptography as it assures confidentiality, integrity, and authenticity at the same time.

References

1. Authenticated encryption - Wikipedia. https://en.wikipedia.org/wiki/Authenticated_encryption
2. General classification of the authenticated encryption schemes for the CAESAR competition. Farzaneh Abed, Christian Forler, Stefan Lucks. *Computer Science Review* 22 (2016) 13-26.
3. Authenticated Encryption in Theory and in Practice. Jean Paul Degabriele. Thesis for University of London. 2014.
4. A Survey on Authenticated Encryption - ASIC Designer's Perspective. Elif Bilge Kavun, Hristina Mihajloska, Tolga Yalcin. *ACM Comput. Surv.* 50, 6, Article 88 (December 2017).

Effective Communication In Digital Age

By | Zul Akmal Abdul Manan & Nur Ainin Aida Binti Ahmad Juanda

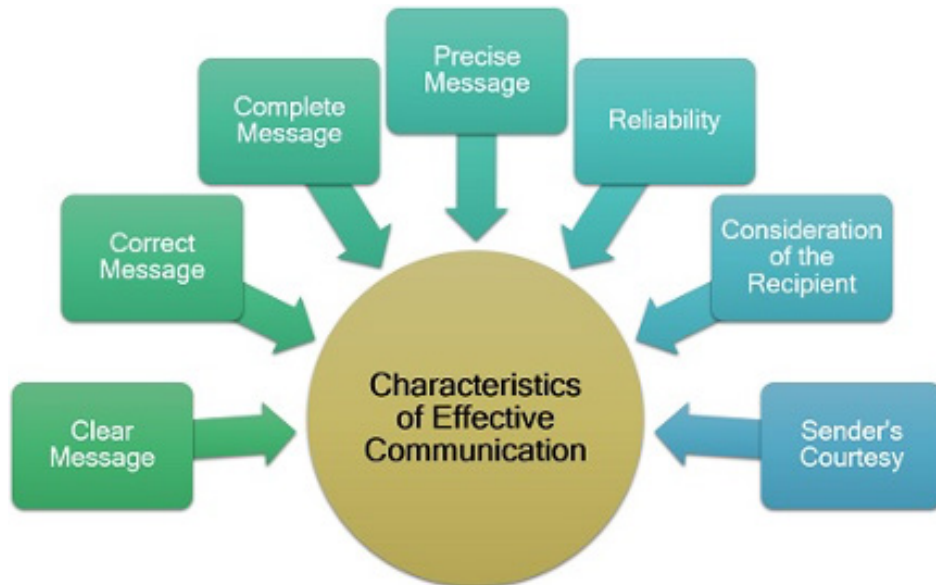


Figure 1: Characteristics of Effective Communication

Humans are social creatures who instinctively use communication everyday. However, the process of sending and receiving the right messages can only be achieved through effective communication. (refer to Figure 1)

With rapid changes in the digital age, today's art of communication is drastically different from two decades ago, as almost everything is now digitized. Businesses and organizations go online and use social media for all kinds of communication. According to the latest statistics (January 2020) by Statista Research Department, about 81% of the Malaysian population were active social media users. This is the research figure before the global pandemic COVID-19.

Content producers from various organizations see the rise of video, audio, graphics, and interactive features. Companies need to differentiate from the competition through digital marketing channels.

Here are a few suggestions on how to communicate more effectively in the digital age:

Be Interactive And Dynamic

Understand the differences between static, dynamic, and interactive content. Static content is advantageous as it is more controlled with relatively low time commitment. However, the Internet is saturated with static content. Instead of relying solely on static content such as standard static web pages or banner ads for brand exposure, create a more dynamic experience for users when collecting information.

Take advantage of dynamic content that adapts to the user based on data giving them a more authentic feel. Interactive content provides social proof of the company standing, making the brand/organization stand out and create an impression. This is how to maintain engagement with the audience.

Visual Communication

We respond to and process visual data better than any other type of data. Research proves that the human brain processes images 60,000 times faster than text, and 90% of the information processed by the brain is visual. Opt for a more exciting and eye-catching visual

through an infographic, for example, instead of long paragraphs.

In the context of social media posting, only posting visuals for the sake of posting won't generate good engagement. Media audiences need it to be compelling, engaging, and relevant.

Channel Of Communication

Other than discussing how to create the digital messages, we should also look into what electronic communication channels should be utilized for a given message? According to the Written Communication Module by lumen, several criteria should be considered when deciding which channel to use:

1. Who is the audience?
2. The importance of the message.
3. Level of confidentiality.
4. Amount of interactivity needed.
5. Amount of information to be conveyed.
6. Although it is listed separately above, all five factors need to be considered collectively in the decision-making process to choose the most effective communication channels.

Transparency

Companies must commit to improving their transparency, both internally and externally in an effort to build trust and company brand. The rise of technology may contribute to improving transparency, but it also can cause substantial distrust.

As written text could easily lead to miscommunication, especially in the corporate world, phone calls and video conferencing are preferred over text messaging platforms, particularly in remote working environments.

Companies' decisions of maintaining confidentiality are legitimate concerns. There have been several incidents previously. Before deciding to shut off information, remember that executive presence on the Internet is essential for a competitive benefit, and risks are unavoidable. Besides, keep in mind that transparency is not full disclosure, but disclosing relevant information to the right people or party at the right time in the right manner.

Communication Shortcuts: Emojis

In many cases, emojis provide added value to written language, going as far as adding clarity to textual communications, and is becoming part of organisation's corporate culture. Of course, the appropriateness depends on the situation, context, the company, and clients. The more you can personalize communications, the stronger relationship you can build.

It is in human nature for people to want to communicate within their natural comfort zone. The lack of tone and context in textual message can leave out important information. There is no harm including one or two emojis in messaging to convey complex emotions that are difficult to put into words. However, it is also essential to know the limit and avoid going overboard.

Digestible And Engaging Content

Digitally minded audiences like short, crisp, and straight to the point content. Try to avoid producing a dense content, thus enabling the brain to easily absorb the information consumed. Shorten the words, but keep it relevant and enjoyable to view.

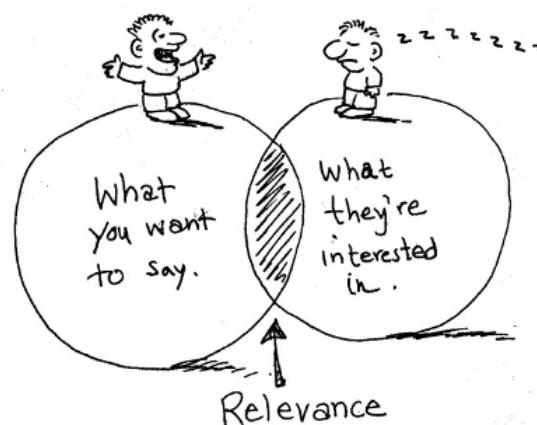


Figure 2: Relevant Content

Engagement will generate interest, loyalty, and respect, simultaneously drawing visitor with more in-depth content into the brand. Do not limit to just static content, use interactive tools ranging from flowcharts to data visualizations, existing tools consumers are familiar with such as mini-quizzes or timelines.

Face-to-Face Communication

Digital communication is definitely recognized as the primary method today. However, nothing can yet replace F2F communication. It is about how you balance these two without sacrificing clarity. An unclear email thread may actually cause even more confusion between two parties. In fact, it could be better resolved with just a quick 10-minute in-person meeting. In any case, clarity is the key.

Conclusion

The rapid rise of social media communication tools has profoundly impacted communication management and planning in an organization. In keeping up with the target audiences' loyalty, it is vital to be competent in using the latest in presentation technology and be savvy in knowing which platform to communicate effectively in a digitalized era.

Finally, it is important for companies to stay up to date on tech trends so that they do not risk falling behind their competitors. Businesses which use the latest technologies are often more efficient and successful.

References

1. <https://www.thoughtleadersllc.com/2014/10/7-ways-to-communicate-more-effectively-in-a-digital-age/>
2. <https://www.kunocreative.com/blog/bid/88040/static-dynamic-and-interactive-content-pros-and-cons>
3. <https://www.statista.com/statistics/883712/malaysia-social-media-penetration/>
4. <http://www.t-sciences.com/news/humans-process-visual-data-better>
5. <https://www.business2community.com/content-marketing/produce-digestible-content-audience-will-eat-01455525>
6. <https://courses.lumenlearning.com/wmopen-businesscommunicationmgrs/chapter/using-the-right-communication-channel/>

Damn Vulnerability Web Application: Command Injection

By | Fateen Nazwa Binti Yusof

Command injection is an attack in which the goal is to execute arbitrary commands on the host operating system (OS) via a vulnerable application ^[1]. The attacks are possible when an application passes unsafe user-supplied data such as forms, cookies, and HTTP headers to a system shell. In this attack, the commands supplied by an attacker are usually executed with the privileges of the vulnerable application. The attacker who is able to inject commands, can read and steal data, or engage in other damaging activities. Command injection attacks are possible primarily due to insufficient input validation. This attack differs from code injection, in which code injection allows the attacker to add his code into the original code. The application then executes the modified code. Meanwhile, in command injection, the attacker extends the default functionality of the application, which runs system commands, without the necessity of injecting code.

There are two types of command injection attacks, which direct and indirect. Direct command injection is the most basic whereby malicious commands are directly supplied to the vulnerable application. Meanwhile, indirect command injection consists of providing malicious commands to the vulnerable application, possibly through a file or an environment variable. This article will discuss the methodology and example of direct command injection attacks on an application with different security levels.

How Direct Command Injection Works

A direct command injection can occur via three (3) steps as follow:

- *Step 1:* The attacker discovers that the application invokes a system command by directly passing user-supplied data as arguments to the command, usually through an input mechanism such as a form field, cookies, or HTTP header.

- *Step 2:* The attacker then supplies the malicious command as part of the expected arguments
- *Step 3:* The application executes the original command and then the malicious command

Simulation of Command Injection On Damn Vulnerable Web Application (DVWA)

This section discussed on command injection attack with different levels of security. The simulation is executed on Damn Vulnerable Web Application (DVWA), run on the localhost server. DVWA is a vulnerable PHP/MySQL web application that has different levels of security deployed. This web application is used by security professionals to test their skills and tools in a legal environment and help web developers to understand better the processes of securing web applications. There are four (4) levels of security that can be set on DVWA, which are Low, Medium, High, and Impossible. However, only Low, Medium, and High level will be executed and compared in this article.

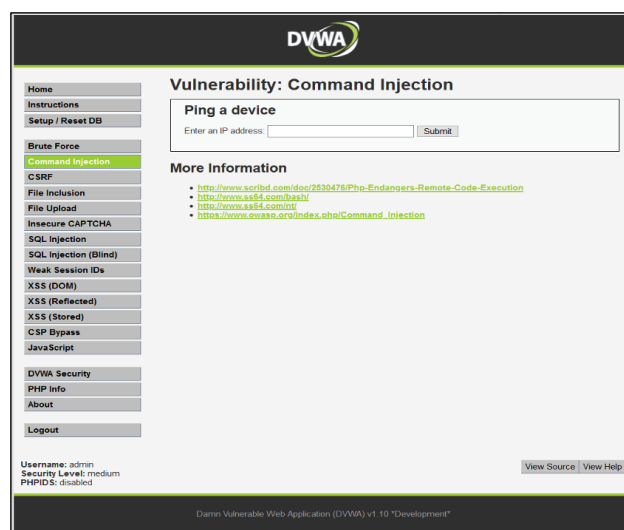


Figure 1: DVWA page for command injection

The page for command injection vulnerability provides an input box with functionality to ping a device. Users need to enter a valid IP address to ping the device. The input box is where the command injection attack will be executed. Before proceeding with the attack, users need to decide the security level under the 'DVWA Security' tab and then proceed to select which security level they want. The simulation of the attack for each security level is described in the next sub-sections.

a. Low-Security Command Injection Source Code

A low-security level means there is no security mechanism implemented in the code. Clicking on the 'View Source' button will display the source code for the low-security level, as shown in Figure 2.

The two 'shell_exec' lines are the lines that execute ping function depending on which

Operating System (OS) is being used. In Unix/Linux command, you can run multiple commands separated by a ' ; '. There are other characters that can be used in order to append commands in the input box. The simulation for this article was run on Windows OS. Therefore, the commands used throughout the simulation may be different from the standard commands for Unix/Linux OS.

Back to the code, it does not check if '\$target' matches an IP Address, and there is no filtering on special characters. This requirement means the system allows for appending commands behind the IP Address. As the simulation was done on Windows, alternatives to the character ';' should be used. Among other characters that can be used are AND (&&) Operator or PIPE (|) Operator. Use of PIPE Operator will completely remove the IP address from the output in this case.

```
<?php
if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if( striistr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

Figure 2: Source code for low-security command injection

Ping a device

Enter an IP address:

```

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=64
Reply from 127.0.0.1: bytes=32 time<1ms TTL=64
Reply from 127.0.0.1: bytes=32 time<1ms TTL=64
Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Volume in drive C is OS
Volume Serial Number is C87D-B007

Directory of C:\xampp\htdocs\DVWA-master\vulnerabilities\exec

01/07/2020  12:10 PM
.
01/07/2020  12:10 PM
.
01/07/2020  12:10 PM
help
01/07/2020  01:03 AM          1,830 index.php
01/07/2020  12:10 PM
source
1 File(s)          1,830 bytes
4 Dir(s)  433,276,645,376 bytes free

```

Figure 3: Successful command injection execution with low-security

```

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Set blacklist
    $substitutions = array(
        '&&' => '',
        ';' => '',
    );

    // Remove any of the characters in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( strpos( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

```

Figure 4: Source code for medium-security command injection

In a normal situation, users will only need to enter a valid IP address such as 127.0.0.1 to display the ping result. Figure 3 shows that when users enter IP address 127.0.0.1 and append command '&& dir' after the IP address, the result displays ping statistic and a full directory of where the DVWA application is located on the server. This result means that the code is vulnerable and command injection is successfully executed.

b. Medium-Security Command Injection Source Codev

Viewing the source code as shown in Figure 4, there is a blacklist filter that has been set to exclude '&&' and ';' character from being added into the input. That is why, when '&&' is used to execute the arbitrary command, the application returns 'Bad

Ping a device

Enter an IP address:

Bad parameter dir.

Figure 5: Execution result of blacklist character for medium-security

Ping a device

Enter an IP address:

Pinging 127.0.0.1 with 32 bytes of data:
 Reply from 127.0.0.1: bytes=32 time<1ms TTL=64
 Reply from 127.0.0.1: bytes=32 time<1ms TTL=64
 Reply from 127.0.0.1: bytes=32 time<1ms TTL=64
 Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 127.0.0.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
 Volume in drive C is OS
 Volume Serial Number is C87D-B007

Directory of C:\xampp\htdocs\DVWA-master\vulnerabilities\exec

01/07/2020 12:10 PM

01/07/2020 12:10 PM

01/07/2020 12:10 PM

help

01/07/2020 01:03 AM 1,830 index.php

01/07/2020 12:10 PM

source

1 File(s) 1,830 bytes

4 Dir(s) 436,646,191,104 bytes free

Figure 6: Successful command injection execution with medium-security

parameter dir.’ as the result as shown in Figure 5. However, changing the character to any other that is not on the blacklist still allows command injection. As previously mentioned, some alternatives can be used to replace the blacklist characters such as ‘&’ or ‘|’ character. For note, ‘&’ and ‘&&’ are two (2) different characters. For ‘&&’, command after ‘&&’ is executed if, and only

if, command before ‘&&’ returns an exit status of zero. The logic is the same as the AND operator. Meanwhile, for ‘&’ character, the shell executes the command terminated by ‘&’ in the background. It does not wait for the command to finish and immediately returns exit code 0.

c. High-Security Command Injection Source Code

For the high-security level, a more extensive blacklist has been set, as shown in Figure 7. It is slightly trickier and more difficult to bypass in the real situation. Since the source code in the DVWA can be opened, the list of blacklist characters is known. As previously done for medium-security level, the use of alternative characters besides the one on the blacklist, still allows command injection to occur. A closer look at blacklist character “|” ‘=> ‘ ‘, will show that there is a space after the | character. Thus, if the command ‘| dir’ is to be used, output ‘Bad parameter dir.’ will be returned, as shown in Figure 8.

However, if the command ‘|dir’ is to be used, the output will be returned, as shown in Figure 9, indicating that command injection is a success. For note, the output does not display the ping result due to the use of a PIPE Operator that will remove the IP address from the output. In conducting a command injection attack in a real environment, please be reminded that users will not always have access to the source code. Thus, ‘trial and error’ testings should be conducted. For example, the use of commands with and without a space between them. It is also essential to take note of what type of OS that the target uses so that the commands can be specific to the OS.

```
if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        'g' => '',
        ';' => '',
        '|' => '',
        '-' => '',
        '$' => '',
        '(' => '',
        ')' => '',
        '*' => '',
        '!' => '',
    );

    // Remove any of the characters in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stripos( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}
```

Figure 7: Source code for high-security command injection

Ping a device

Enter an IP address:

Bad parameter dir.

Figure 8: Execution result of blacklist character for high-security

Ping a device

Enter an IP address:

Volume in drive C is OS
Volume Serial Number is C87D-B007

Directory of C:\xampp\htdocs\DVWA-master\vulnerabilities\exec

01/07/2020 12:10 PM

01/07/2020 12:10 PM

01/07/2020 12:10 PM

help

01/07/2020 01:03 AM 1,830 index.php

01/07/2020 12:10 PM

source

1 File(s) 1,830 bytes

4 Dir(s) 434,785,951,744 bytes free

Figure 9: Successful command injection execution with high-security

Impact of An Attack

Problems resulting from a command injection attack can range from minor to highly disruptive. An attacker can take advantage of this weakness to execute arbitrary commands, disclose sensitive information, alter or corrupt a database, and cause a denial of service (DoS). If the attacker is able to perform an OS command injection, he may gain access to the server and exploit the underlying application. Worse, the attacker may retain access to the systems even after the vulnerability has been detected and fixed.

Area Of Improvement For Command Injection

After discovering that a command injection attack has taken place, it is crucial to block access to the application or vulnerable script that has been compromised. It is a temporary solution until the issue is resolved by the development or security team. Blocking the access can be done in one of two ways, either making changes using the native functionality of the webserver or altering system access permissions to the affected file. However, it is vital to address potential vulnerabilities that could lead to the command injection attack since prevention is better than cure.

There are several ways to avoid the command injection attack. One of them is never to use calls such as 'shell_exec' in PHP to execute any host operating system commands. Instead, equivalent commands should be used from the programming language. But, this approach may be difficult if there is no equivalent command in the programming language. In such cases, input sanitization should be used before passing the value to a shell command. Whitelisting is a good example of input sanitization, and it is applicable for all types of injections. These methods are summarized as below:

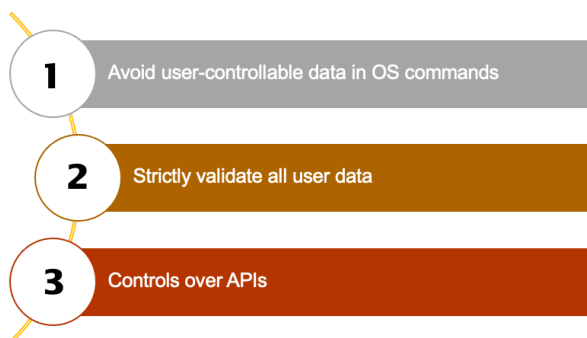


Figure 10: Area of improvement to prevent command injection

Conclusion

Command injection vulnerability exists due to poor input validation and sanitization on the dynamically-generated, user-supplied inputs used by functions that interact with the operating system (OS) shell. Any attacker with control of these parameters can execute arbitrary commands that allow him to read, steal, and even manipulate data as he wants. It is strongly recommended that to never call out to OS commands from application-layer code. If unavoidable, then strong input validation must be performed to ensure the application is secure from command injection attacks.

References

1. *Command Injection*, https://owasp.org/www-community/attacks/Command_Injection
2. *Damn Vulnerable Web Application*, <http://www.dvwa.co.uk/>
3. *DVWA - Command Injection*, <https://chris-young.net/2018/03/28/dvwa-command-injection/>

Security Concerns On Online Meeting Applications

By | Fateen Nazwa Binti Yusof

An online meeting application is an online service that lets people connect and participate in meetings from remote locations through audio, video, or chat. Web conferencing is a popular term for online meetings in the field of business and other sectors. Since it is online, the meetings can be done anytime, anywhere as long as there is an Internet connection. Not only the application convenient to use, but it also saves costs for organizations. Organizations do not need to spend money on business trips or gathering business partners, shareholders, or staff, just for holding a meeting. Other advantages of online meetings are uninterrupted communication and time-saving.

However, the online meeting also has its disadvantages, especially in the aspect of cybersecurity. Aside from a decrease in personal contact and internet connection interruption, there is a high risk of security by performing online meetings. There is a chance of cyberattacks like Man-in-the-Middle (MiTM). MiTM occurs when an adversary successfully intercepts communication between two parties, secretly eavesdrops, or can even modify data that being exchanged. This situation leads to a leak of confidential information in the case of business. Therefore, security issues are a great concern in ensuring the online meeting is conducted securely.

Before a further discussion on the security concerns in online meeting applications, it is a good step to compare a few applications or software existing in the market. Nowadays, most of the applications are not limited to chat-based communication only. There are advanced functionalities such as desktop and application sharing, one-click recording, drawing tools, video-conferencing abilities, and more. With both free and paid versions available, users can choose which option is suitable based on their requirements. Table 1 below shows some examples of online meeting applications with brief explanations and their security features.

No	Online Meeting Application	Explanation	Security Feature(s)
1	Microsoft Team	Microsoft Team is designed to provide an easier way for small groups of users to communicate and collaborate. Microsoft Teams is enabled by default for subscribers using Microsoft Office 365. Aside from chat-based communication, it also integrates with other Microsoft services. This way, users will be able to access shared files and calendars, collaborative editing, and easy switching between voice, video, and text chat.	<ul style="list-style-type: none"> • Advanced Threat Protection (ATP) • Conditional access • Authentication based on Azure Active Directory Authentication Library (ADAL) • AppLocker • Data Loss Prevention (DLP)
2	Cisco WebEx	Cisco WebEx is considered one of the oldest yet commonly used online meeting application. It allows users to join or hold meetings while sharing screens or chatting face-to-face with other users. Users can have up to 25 users in a meeting and see up to 6 webcams on screen at a time. Other services available are schedule appointment and email the attendees.	<ul style="list-style-type: none"> • Data encryption • Role-based access • Administrative capabilities • Single Sign-On • Cloud Connected Audio (CCA) • Network access control • Privacy Shield Framework-certified

Table 1(a): Examples of Online Meeting Applications

No	Online Meeting Application	Explanation	Security Feature(s)
3	GoTo Meeting	GoToMeeting is built for collaboration for any type of business. It can be used for online meetings, web conferences, and webinars. It allows for screen sharing and personalized meeting URLs with interactive whiteboard features. One of the highlights for this application is the Cloud Recording feature, whereby users do not need to take notes while hosting a meeting on the go.	<ul style="list-style-type: none"> • Single Sign-On • Role-based access • Account & session authentication • End-to-end Secure Socket Layer (SSL) • 128-bit Advanced Encryption Standard (AES) encryption
4	Zoom	With HD video conferencing, this feature making Zoom the ideal application for meetings. Even with the free version, users can make unlimited one-to-one calls and hold unlimited meetings for up to 25 users. Not limited to online meetings and phone calls, this application also offers video webinars, online conference rooms, virtual workspaces, and cross-platform file sharing.	<ul style="list-style-type: none"> • Data encryption • Multi-factor authentication • Single Sign-On • Archives data for up to 10 years

Table 1(b): Examples of Online Meeting Applications

Even though these applications come with security features, the possibility of being hacked are still exist. Last year, a security team discovered a vulnerability in Cisco WebEx and Zoom that may expose online meetings to snooping or also known as Prying-Eye vulnerability [7]. The platform could potentially allow an adversary to enumerate and view active meetings that are not protected. The Prying-Eye vulnerability is an example of an enumeration attack. It targets web conferencing APIs with a bot that cycles through (enumerates) and discovers valid numeric meeting IDs [7]. Passwords are enabled as the default setting for online meetings on both Cisco WebEx and Zoom. However, users have the option to set password-free for online

No	Online Meeting Application	Explanation	Security Feature(s)
5	Google Hangouts	With Google Hangouts, a large group of users can be connected despite the distance and via multiple different types of hardware. Google Hangouts is more like a conversation application that allows users to video call, phone call, or message with each other. For the video call, users can talk one-on-one or invite others for a group chat with up to 10 users at a time. Users can join a Hangouts session via Gmail, the Hangouts mobile app, the Hangouts site directly, and with a Chrome extension.	<ul style="list-style-type: none"> • G Suite's security • Data encryption (in transit) • Single Sign-On • Two-factor authentication • Administrative capabilities • Vault support

Table 1(c): Examples of Online Meeting Applications

meetings. If disabling security functionality or not assigning a password is being practiced, then the adversary would be able to view an active meeting. Not only that, if users have chosen the option of configuring a personal meeting ID to simplify meeting management, the adversary can also store that information for future snooping activity. The vulnerability is expected to affect nearly 40 vendors. However, both Cisco and Zoom have posted advisories on how to address this vulnerability.

In another case, Google Hangouts is also riddled with privacy and security concerns. Though hangout conversations are encrypted, it does not use end-to-end encryption [8]. Instead, messages are encrypted "in transit," which means the messages are only encrypted between users' devices and Google's servers. Once they are on a server, Google has complete access to them. Google can tap into private communication sessions and relay that information to government agencies if being ordered to do so. Furthermore, the Google Transparency Report reveals that the company does receive and often fulfill requests for customer information. Additionally, images sent via Hangouts are shared through public URLs,

meaning that virtually anyone (who has the basic knowledge about URLs) can view the images, including private and sensitive images.

Zoom's vulnerability is not limited to the Prying-Eye only. It has other vulnerabilities listed under the Common Vulnerabilities and Exposures (CVE) system. CVE is a list of entries, each containing an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities [9]. The vulnerabilities were discovered as early as 2004, with the latest vulnerability found in July 2019. The vulnerability with ID CVE-2019-13567 allows remote code execution on the Zoom Client before version 4.4.53932.0709. The Citrix GoToMeeting application also has one (1) vulnerability listed with ID CVE-2014-1664. The vulnerability affects version 5.0.799.1238 for Android, whereby it logs HTTP requests containing sensitive information such as user IDs, meeting details, and authentication tokens. This situation may allow an attacker to obtain the information via an application that reads the system log file. Meanwhile, Cisco WebEx tops the list with a total number of nine (9) CVEs discovered. The latest discovery was CVE-2017-3823 in 2017 that allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system.

No	Online Meeting Application	CVE ID
1	Zoom	CVE-2019-13567
		CVE-2019-13450
		CVE-2018-15715
		CVE-2014-5811
		CVE-2004-0680
2	GoToMeeting	CVE-2014-1664
3	Cisco WebEx	CVE-2017-3823
		CVE-2013-3425
		CVE-2012-6399
		CVE-2009-2880
		CVE-2009-2879
		CVE-2009-2878
		CVE-2009-2877
		CVE-2009-2876
		CVE-2009-2875

Table 2: List of CVEs

Like any other thing, online meeting applications have their pros and cons. While it is cost-effective, convenient, and time-saving, it also greatly reduced a personal connection as well as make an organization vulnerable to cyberattacks. It is impossible to ensure an application is free from vulnerability or cyber risk, but best practice is to reduce them into an acceptable level. Users' actions play a big part in helping to keep data safe. Use of reliable and secure software, together with responsible actions, online meeting applications will help users to stay informed and updated in a secure environment, regardless of time zone, location, and financial situation.

References

1. Microsoft Team, <https://products.office.com/en-my/microsoft-teams/group-chat-software>
2. Zoom, <https://zoom.us/>
3. Cisco WebEx, <https://www.webex.com/>
4. Cisco WebEx Meetings Security, <https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf>
5. Hangout Chat, <https://gsuite.google.com/products/chat/>
6. GoToMeeting Web Conference Security, https://logmeincdn.azureedge.net/gotomeetingmedia/-/media/pdfs/ucc_security_white_paper.pdf
7. Vulnerability In Cisco WebEx And Zoom May Expose Online Meetings To Snooping, <https://www.helpnetsecurity.com/2019/10/01/prying-eye-vulnerability/>
8. The Very Best Encrypted Messaging Apps , <https://www.avg.com/en/signal/secure-message-apps>
9. Common Vulnerabilities and Exposures, <https://cve.mitre.org/>

Covid-19: Landskap Keselamatan Siber Di Malaysia Semasa PKP

By | Nurfarhana Nasrulhaq Binti Mohd Zulkifli

Pendahuluan

Pada awal tahun 2020, kita dikejutkan dengan wabak penyakit berjangkit yang menyerang seluruh dunia. Wabak penyakit ini merebak dengan cepat merentas sempadan, sepantas rangkaian Internet di hujung jari. Wabak penyakit tersebut ialah pandemik Covid-19 yang berasal dari Wuhan, Hubei, China dan mula dikesan pada Disember 2019. Pada 11 Mac 2020, Pertubuhan Kesihatan Dunia (World Health Organization atau WHO) mengumumkan bahawa wabak penyakit Covid-19 adalah pandemik berikutan peningkatan kes yang mendadak di seluruh dunia selain China, kadar kematian yang tinggi, penyebaran jangkitan Covid-19 yang cepat dan kerugian ekonomi.

Berikutan krisis Covid-19, skop kertas ini akan memfokuskan kepada perubahan landskap siber serta ancaman siber yang berlaku di Malaysia. Selain itu, setiap ancaman siber yang berlaku juga turut diterangkan agar langkah pencegahan yang dirancang oleh Kerajaan bagi membendung jenayah siber dan kesan Covid-19 terhadap masyarakat khususnya dan negara amnya, dapat dilaksanakan.

Latar belakang

Malaysia juga tidak terlepas daripada serangan wabak ini. Keadaan ini menyebabkan Kerajaan Malaysia mengumumkan Perintah Kawalan Pergerakan (PKP) bagi mencegah lebih ramai lagi rakyatnya daripada dijangkiti wabak Covid-19. Ketika PKP diumumkan pada 16 Mac 2020, bilangan kes pada masa itu telah meningkat kepada 553 kes dan Malaysia adalah negara dengan jumlah jangkitan Covid-19 tertinggi dalam kalangan negara ASEAN. PKP dilaksanakan secara berperingkat seperti yang berikut:

FASA 1 : 8 Mac – 31 Mac 2020

FASA 2 : 1 April – 14 April 2020

FASA 3 : 15 April – 28 April 2020

FASA 4 : 29 April – 12 Mei 2020

FASA 5 : 13 Mei – 09 Jun 2020 (Perintah Kawalan Pergerakan Bersyarat atau PKPB)

FASA 6 : 10 Jun – 31 Ogos 2020 (Perintah Kawalan Pergerakan Pemulihan atau PKPP)

FASA 7 : 1 September – 31 Disember 2020 (Perintah Kawalan Pergerakan Pemulihan atau PKPP)

Dalam tempoh PKP, rakyat dinasihatkan untuk duduk di rumah dan keluar apabila perlu sahaja seperti untuk membeli barangan harian dan hanya ketua keluarga yang dibenarkan keluar. Sekatan jalan raya diadakan di plaza tol utama di lebuh raya dan rakyat dikehendaki menunjukkan surat majikan sekiranya ada keperluan untuk ke pejabat. Pelbagai lagi arahan dan sekatan dikeluarkan bagi membendung penularan serta menangani dan mengurangkan jangkitan wabak Covid-19. Pihak Majlis Keselamatan Negara (MKN) telah mengeluarkan arahan PKP mulai 18 Mac 2020 hingga 12 Mei 2020. Walau bagaimanapun, apa-apa perubahan terhadap tarikh tersebut bergantung pada bilangan kes dan faktor lain yang berkaitan. Arahan PKP ini melibatkan seluruh Malaysia dan dibuat berdasarkan Akta Pencegahan dan Pengawalan Penyakit Berjangkit 1988 serta Akta Polis 1967.

Terdapat enam (6) arahan yang terkandung dalam Perintah Kawalan Pergerakan ini.

1. Larangan menyeluruh pergerakan dan perhimpunan besar termasuk aktiviti keagamaan, sukan, sosial dan budaya;
2. Sekatan menyeluruh semua perjalanan rakyat Malaysia ke luar negara;
3. Sekatan kemasukan semua pelancong dan pelawat asing ke dalam negara;
4. Penutupan semua Taska, sekolah Kerajaan dan swasta serta institusi pendidikan rendah, menengah dan prauniversiti yang lain;
5. Penutupan semua Institusi Pengajian Tinggi (IPT) Awam dan Swasta serta Institut Latihan Kemahiran di seluruh negara; dan
6. Penutupan semua premis kerajaan dan swasta kecuali yang terlibat dengan perkhidmatan perlu negara (essential services)

Landskap Ancaman Keselamatan Siber

Wabak Covid-19 ini telah mengubah ekosistem dunia secara drastik, menjejaskan semua lapisan masyarakat dan memberi ruang kepada penjenayah siber mengambil kesempatan dalam suasana krisis yang dihadapi. Pelaksanaan Perintah Kawalan Pergerakan menyebabkan rakyat Malaysia yang bekerja diarahkan untuk bekerja dari rumah. Keadaan ini telah meningkatkan kebergantungan masyarakat terhadap teknologi bagi tujuan komunikasi, berita, hiburan, perniagaan dan interaksi sosial.

Menurut laporan berita The Sun Daily pada 14 April 2020, Malaysia menghadapi cabaran mencapai digitalisasi secara menyeluruh. Operasi dan urusan dalam talian di Malaysia didapati gagal memenuhi permintaan semasa berlakunya krisis Covid-19. Sebagai contoh, beberapa syarikat telah mengemukakan permohonan secara dalam talian kepada Kementerian Perdagangan Antarabangsa dan Industri (MITI) melalui laman web MITI, untuk meneruskan operasi perniagaan ketika krisis Covid-19. Namun, laman web tersebut tergendala disebabkan hampir 100,000 syarikat berusaha mendapatkan kelulusan untuk beroperasi daripada kementerian menerusi laman web tersebut dan bilangan ini telah melebihi kapasiti bagi mengakses laman web itu pada satu-satu masa.

Menurut Francois Mouton, Profesor Madya Cyber Security di Noroff University College, Oslo, Norway dan Arno De Coning, Jurutera Sistem di University of Pretoria, Afrika Selatan, peningkatan ancaman keselamatan siber adalah disebabkan oleh perkara berikut:

1. Masyarakat mempunyai kebergantungan yang tinggi terhadap infrastruktur digital;
2. Konsep bekerja dari rumah belum diamalkan sepenuhnya oleh semua organisasi;
3. Kebergantungan yang tinggi pada sambungan dalam talian dan infrastruktur rangkaian setiap negara;
4. Sifat manusia yang ingin tahu terutamanya dalam keadaan yang tidak pasti;
5. Masyarakat menghabiskan sebahagian besar masa mereka menggunakan perkhidmatan dalam talian, yang boleh mendorong ke arah tingkah laku yang berisiko;
6. Individu yang tidak 'pandai teknologi' secara automatik atau secara tiba-tiba menjadi mahir menggunakan teknologi dalam kehidupan seharian mereka.

Faktor ini telah menyebabkan peningkatan jenayah siber sepanjang berlakunya krisis Covid-19. Krisis sebegini membuka peluang kepada penjenayah terutamanya melalui alam siber atau alam maya untuk mengaut keuntungan. Antara ancaman keselamatan siber ketika krisis Covid-19 yang mengubah landskap keselamatan siber adalah seperti di bawah:

i. Berita Palsu

Berita merupakan maklumat atau keterangan yang sangat penting apabila berlakunya krisis. Rakyat menanti perkembangan terkini tentang sesuatu krisis yang berlaku. Krisis Covid-19 telah mewujudkan bermacam-macam berita yang melahirkan pelbagai perasaan seperti takut, panik, marah, sedih dan sebagainya dalam kalangan masyarakat. Berita Covid-19 begitu banyak dilaporkan sehingga terdapat wabak berita palsu yang mencetuskan suasana panik dalam kalangan rakyat. Antara berita palsu yang mencetuskan suasana panik sehingga mengakibatkan tindakan yang drastik adalah penyebaran berita palsu tentang pelaksanaan perintah berkurung (Lockdown) di Malaysia pada 16 Mac 2020. Mesej tersebut tular dalam media sosial termasuk Facebook dan WhatsApp dengan tanda pagar #MalaysiaLockdown. Berita palsu ini telah menyebabkan rakyat mengambil tindakan drastik dengan berpusu-pusu pergi ke pasar raya untuk membeli barang keperluan sehingga penuh troli sebagai persediaan kerana tidak boleh keluar rumah dalam tempoh yang lama. Malah, tindakan ini telah mencetuskan pergaduhan kerana berebutkan barang yang hendak dibeli dan sebagainya.

Oleh yang demikian, beberapa laman media sosial Telegram diwujudkan ketika krisis Covid-19 untuk menyampaikan dan mengesahkan berita/kandungan palsu yang diterima secara dalam talian. Sebagai contoh, Telegram 'Sebenarnya' diwujudkan oleh Pihak Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM). Platform ini boleh digunakan oleh orang awam bagi mendapatkan berita yang sahih dan terkini tentang Covid-19, pengumuman, mesej kesedaran, peringatan dan soalan lazim yang disahkan oleh Kementerian Kesihatan Malaysia. Namun, terdapat juga individu atau kumpulan yang memanipulasikan krisis Covid-19 dan mengambil kesempatan mewujudkan platform yang dinamakan dengan nama rasmi agensi/jabatan untuk Covid-19.

Pihak penguatkuasa seperti polis, akan menjejaki individu yang menyebarkan berita palsu bagi membolehkan tindakan diambil dan pesalah dijatuhi hukuman agar menjadi peringatan kepada masyarakat supaya mendapatkan kepastian sebelum menyebarkan sesuatu berita.

ii. Media Sosial

Penggunaan media sosial meningkat kerana penyampaian maklumat kepada rakyat kebanyakannya dibuat menerusi media sosial seperti Facebook, Twitter dan Telegram. Facebook dan Twitter digunakan oleh badan rasmi kerajaan seperti Kementerian Kesihatan Malaysia bagi membolehkan rakyat mendapat maklumat terkini berkenaan jumlah jangkitan Covid, penerangan tentang kluster semasa dan peringatan tentang langkah-langkah untuk mengelakkan jangkitan. Malah, media berita turut menggunakan Facebook untuk menyiarkan secara langsung sidang media Perdana Menteri, Menteri Kanan Pertahanan dan Ketua Pengarah Kesihatan. Berikutan pewujudan platform 'Sebenarnya' dan beberapa platform lain yang dibuka menerusi Telegram, dan berdasarkan notifikasi daripada kawan-kawan penulis, penulis mendapati bahawa penggunaan Telegram telah meningkat. Perkara ini diketahui kerana penulis akan mendapat notifikasi tentang nombor telefon kawan yang baru menggunakan Telegram.

Malah, media sosial juga digunakan untuk mengutip derma bagi membantu mereka yang ditimpa kesusahan kerana sumber pendapatan yang terjejas ketika Covid-19 sebelum masing-masing menerima bantuan melalui Bantuan Prihatin Nasional (BPN). Selain itu, menerusi media sosial, bantuan dan kutipan dana juga dibuat untuk membantu hospital dan petugas barisan hadapan (frontliner) yang terlibat dalam usaha membasmi jangkitan Covid-19 melalui penyediaan peralatan yang diperlukan seperti pakaian PPE, kipas, penyaman udara dan pelbagai kemudahan lain.

Media sosial juga menyebarkan aura positif tentang cara Malaysia menangani krisis Covid-19 dengan begitu efisien berbanding dengan beberapa negara lain. Terdapat penggiat YouTube (YouTuber) luar negara yang begitu kagum dengan cara kerajaan menangani krisis Covid-19, membuat kandungan video Covid-19 Malaysia lwn London dan Malaysia lwn Amerika Syarikat. Malah, rakyat Malaysia turut memberikan kata-kata semangat kepada petugas barisan hadapan di Indonesia yang sudah berputus asa dalam usaha membendung

penularan wabak Covid-19, menerusi Twitter dengan tanda pagar #IndonesiaBisa.

iii. Penipuan dalam talian

Apabila arahan duduk di rumah dikeluarkan berikutan pelaksanaan Perintah Kawalan Pergerakan, maka masyarakat banyak menghabiskan masa dengan media sosial bagi mendapatkan maklumat terkini tentang Covid-19 dan mencari idea untuk melakukan aktiviti di rumah. Penjenayah siber juga mengambil kesempatan untuk melakukan jenayah mereka melalui penipuan. Tambahan pula, masyarakat digalakkan untuk membeli dan menjual barangan secara dalam talian.

Berdasarkan statistik aduan yang diterima oleh pihak CyberSecurity Malaysia menerusi Malaysia Computer Emergency Response Team (MyCERT), jumlah aduan tentang penipuan pada bulan April, iaitu tempoh PKP dilaksanakan, adalah sebanyak 1,180. Aduan yang diterima pada bulan April merupakan jumlah yang tertinggi dalam tempoh antara Januari hingga Julai 2020. Terdapat peningkatan sebanyak 163.98% berbanding jumlah penipuan pada tahun 2019, iaitu sebanyak 447 aduan yang diterima. Terdapat 9 subkategori penipuan. Antara tiga subkategori utama penipuan pada bulan April adalah:

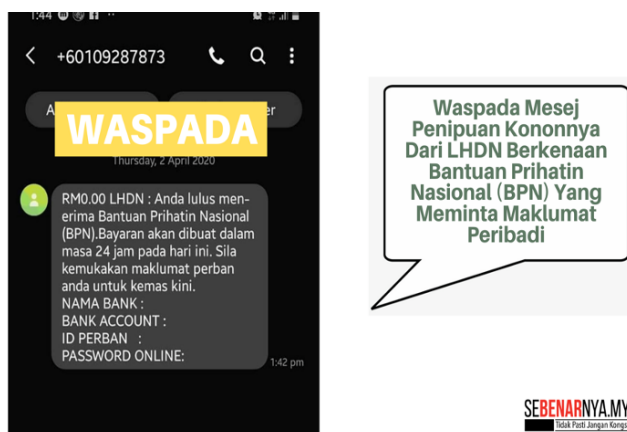
- a. Memancing data (Phishing)
- b. Penipuan dalam talian
- c. Penipuan pembelian dalam talian

Subkategori ini diulas dengan lebih lanjut dalam topik yang seterusnya.

iv. Memancing data (*Phishing*)

Memancing data merupakan perbuatan mencuri data yang bersifat peribadi dan sensitif seperti nama, katalaluan, kad kredit/debit menggunakan e-mel, sistem pesanan ringkas (SMS) atau laman web. Ketika PKP dilaksanakan, banyak golongan yang terjejas dari segi kewangan atau punca pendapatan kerana tidak boleh bekerja dan perlu duduk di rumah. Maka, kerajaan telah mengumumkan Pakej Rangsangan Ekonomi Prihatin Rakyat (PRIHATIN) bernilai RM250 bilion. Sebanyak RM10.92 bilion daripada jumlah tersebut telah disalurkan kepada rakyat setakat bulan Julai menerusi Bantuan Prihatin Nasional (BPN). Penjenayah juga mengambil kesempatan daripada penyediaan bantuan ini dengan memancing mangsa.

Penjenayah melakukan sindiket penipuan dengan mewujudkan mesej berantai yang dihantar secara rambang melalui sistem pesanan ringkas (SMS) tentang semakan BPN bagi mendapatkan butiran peribadi mangsa. SMS tersebut meminta penerima BPN memberikan maklumat perbankan termasuk nama bank, nombor akaun, identiti peribadi dan kata laluan, kononnya bagi tujuan kemas kini. Selain itu, mesej tersebut mendakwa penerima disahkan layak menerima bantuan dan bayaran akan dibuat dalam tempoh 24 jam.



Contoh SMS penipuan BPN. Sumber: Sebenarnya.my

Oleh yang demikian, pihak yang menguruskan BPN, iaitu Lembaga Hasil Dalam Negeri (LHDN) telah membuat kenyataan menyangkal perkara tersebut kepada pihak media untuk disebarkan dan dijadikan peringatan kepada orang ramai. Selain itu, LHDN turut memberikan panduan bagi membolehkan orang ramai membuat semakan menerusi laman web rasmi LHDN.

v. Penipuan pembelian dalam talian

Jumlah pembelian dalam talian meningkat ketika PKP kerana premis atau kedai fizikal tidak boleh dibuka kecuali kedai yang menjual keperluan asas (makanan, barangan basah dan bahan mentah), farmasi dan beberapa kedai keperluan yang lain. Malah, untuk keluar ke kedai, hanya seorang wakil keluarga yang dibenarkan. Oleh yang demikian, terdapat golongan yang mengambil kesempatan melakukan penipuan berkenaan dengan barangan yang sangat tinggi permintaan ketika PKP seperti pelitup muka dan pensanitasi tangan.

Modus operandi penipuan adalah dengan mengiklankan penjualan pelitup muka dalam media sosial seperti Facebook, Instagram dan beberapa aplikasi lain. Mangsa yang melihat iklan ini akan menghubungi penipu menerusi aplikasi WhatsApp dan penipu memberikan nombor akaun bank (akaun palsu) untuk proses pembelian. Malangnya, selepas pembayaran

dibuat, barang yang dijanjikan tidak dihantar. Menurut laporan berita, Jabatan Siasatan Jenayah Komersial telah menerima 556 laporan membabitkan kes penipuan jualan pelitup muka secara dalam talian dengan kerugian lebih RM4.2 juta bagi tempoh Januari hingga awal April. Harga bagi pelitup muka dan pensanitasi tangan adalah sangat tinggi, tetapi barangan yang ditawarkan oleh penjual yang mengambil kesempatan ini biasanya tidak berkualiti.

vi. Ucapan Kebencian dalam media sosial

Akhbar Malay Mail melaporkan tentang peningkatan insiden siber berbau perkauman dan ucapan kebencian dalam talian sepanjang tempoh Perintah Kawalan Pergerakan (PKP). Provokasi perkauman tersebut mula meningkat dalam media sosial terutamanya apabila terdapat kes jangkitan Covid-19 yang melibatkan "kluster Tabligh". Kononnya, insiden tersebut telah mengakibatkan penambahan hampir separuh daripada keseluruhan jumlah kes jangkitan wabak tersebut. Susulan daripada itu, pengguna Internet juga telah menjadikan jangkitan ke atas kumpulan pelarian, pendatang dan pekerja asing sebagai penyebab kepada peningkatan jumlah jangkitan Covid-19. Menurut pensyarah di Universiti Putra Malaysia, isu perkauman ini berlaku disebabkan kebimbangan terhadap kumpulan tertentu dalam kalangan masyarakat yang didakwa boleh mendatangkan ancaman kepada negara.

Media sosial berupaya mempengaruhi persepsi masyarakat dan penggunaannya perlu dipantau agar ia tidak dieksploitasi oleh kumpulan tertentu untuk membangkitkan sentimen perkauman. Jika tidak dibendung, ia boleh memberikan implikasi buruk terhadap aspek keamanan dan kesejahteraan negara. Justeru, penguatkuasaan aspek perundangan yang melibatkan isu berkaitan perkauman dan penyebaran berita palsu perlu diperketatkan dari semasa ke semasa. Program kesedaran dan etika penggunaan media sosial juga perlu dipertingkatkan bagi mewujudkan pengguna media sosial yang lebih bertanggungjawab. Sehubungan itu, CyberSecurity Malaysia menerusi program CyberSAFE sentiasa berusaha memupuk aspek pembudayaan siber bagi melahirkan pengguna Internet yang beretika dalam kalangan masyarakat.

Krisis Covid-19 ini memberikan kesan yang mendalam terhadap keseluruhan ekosistem di seluruh dunia. Semua lapisan masyarakat terkesan, malah masyarakat kini berubah dengan melakukan sesuatu mengikut norma baharu agar Covid-19 dapat ditangani walaupun akan mengambil masa lebih daripada setahun. Berdasarkan persepsi keselamatan siber, Covid-19 akan memberikan kesan terhadap beberapa perkara ini:

1. Maklumat yang salah

Maklumat yang tidak tepat dan palsu yang disebarkan memberikan kesan yang lebih negatif berbanding tidak mendapat apa-apa maklumat langsung. Apabila maklumat palsu disebarkan, usaha bersepadu dari segi mental diperlukan untuk membetulkan maklumat tersebut kerana orang ramai telah mempercayai maklumat palsu. Kemudahan media sosial turut mempercepat penyebaran sesuatu berita palsu. Rakyat juga dilihat menjadi ejen yang pantas menyampaikan sesuatu berita tanpa mengesahkannya terlebih dahulu. Kesedaran tentang pengesahan sesuatu berita amat kurang dalam kalangan rakyat negara kita.

2. Perniagaan

Semua perniagaan terpaksa melakukan dan membenarkan pekerja bekerja dari rumah dengan serta-merta. Kebanyakan perniagaan masih belum bersedia dengan perkara ini. Mereka perlu menyusun strategi perniagaan secara norma baharu untuk meneruskan kelangsungan perniagaan mereka. Apabila pekerja bekerja dari rumah, suasana di rumah terdedah kepada kelemahan keselamatan kerana tiada tembok keselamatan (firewall) yang dapat melindungi pekerja sepertimana di tempat kerja. Selain itu, individu terpaksa berusaha keras untuk membiasakan diri dengan penggunaan teknologi. Terdapat syarikat yang tidak dapat menampung penggunaan VPN apabila akses melebihi kemampuan rangkaian.

3. Ekonomi

Krisis Covid-19 telah mengganggu aktiviti perniagaan yang merupakan tunjang utama ekonomi negara. Sektor pelancongan antara yang pertama terjejas sejak Covid-19 melanda pada Januari 2020. Sekatan kemasukan pelancong asing dan PKP telah menjejaskan aktiviti pelancongan domestik. Syarikat penerbangan terpaksa

mengehadkan atau memberhentikan seketika operasi ke luar negara. Rantaian bekalan global terjejas apabila negara pengeluar bahan mentah seperti China juga turut terjejas akibat Covid-19. Walau bagaimanapun, kerajaan Malaysia bertindak menangani kelembapan ekonomi dengan menyediakan pakej rangsangan. Jangka masa yang lama diperlukan bagi memulihkan aktiviti ekonomi.

Kesimpulan

Ancaman siber ini telah lama berlaku dan sentiasa akan berlaku. Namun, krisis Covid-19 menyebabkan ancaman siber menjadi perhatian seiring dengan kebergantungan masyarakat terhadap penggunaan teknologi dan Internet yang meningkat ketika krisis Covid-19. Perubahan landskap keselamatan siber ketika krisis Covid-19 ini mendorong pemimpin untuk membuat keputusan yang wajar demi masa depan negara. Masyarakat tidak pasti dengan apa yang berlaku dan tidak tahu cara untuk bertindak dan penjenayah siber mengambil peluang yang ada untuk melakukan serangan. Selain itu, tahap kesedaran tentang keselamatan siber dalam kalangan masyarakat yang masih rendah turut menyumbang kepada peningkatan jenayah siber.

Oleh yang demikian, pihak penguatkuasa dan pakar dalam keselamatan siber perlu berganding bahu untuk menyusun strategi, memberikan panduan dan peringatan kepada masyarakat tentang keselamatan siber agar semua lapisan masyarakat dapat dilindungi. Memandangkan tahap kesedaran terhadap keselamatan siber dalam kalangan masyarakat masih lagi rendah, maka penularan wabak Covid-19 ini memaksa masyarakat untuk sentiasa berwaspada. Krisis Covid-19 ini juga menjadi penyebab untuk memulakan pendidikan keselamatan siber secara menyeluruh. Organisasi perlu meningkatkan tahap keselamatan siber masing-masing dan memberikan latihan kepada pekerja tentang keselamatan siber apabila bekerja dari rumah.

Rujukan

1. World Health Organization. WHO announces COVID-19 outbreak a pandemic. <https://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/news/news/2020/3/who-announces-covid-19-outbreak-a-pandemic>
2. Rochester Regional Health. Pandemic vs Epidemic: What's the Difference? <https://www.rochesterregional.org/news/2020/03/pandemic-vs-epidemic>
3. Fareez Azman. 556 laporan polis, RM4.2 juta kerugian dicatat berhubung penipuan jualan topeng muka. <https://www.astroawani.com/berita-malaysia/556-laporan-polis-rm42-juta-kerugian-dicatat-berhubung-penipuan-jualan-topeng-muka-236764>
4. Mahaizura Abd Malik dan Nurul Hidayah Bahaudin. Tak habis-habis menipu. <https://www.hmetro.com.my/mutakhir/2020/04/561748/tak-habis-habis-menipu>
5. Astro Awani. Ini perkara yang anda perlu tahu tentang Bantuan Prihatin Nasional (BPN). <https://www.astroawani.com/berita-malaysia/ini-perkara-yang-anda-perlu-tahu-tentang-bantuan-prihatin-nasional-bpn-235824>
6. Alzahrin Alias. Bantuan keseluruhan BPN cecah RM10.92 bilion. <https://www.bharian.com.my/berita/nasional/2020/07/708630/bantuan-keseluruhan-bpn-cecah-rm1092-bilion>
7. Nor Azizah Mokhtar. COVID-19: Hati-hati dengan mesej berangkai berkaitan BPN. <https://www.bharian.com.my/berita/kes/2020/04/672846/covid-19-hati-hati-dengan-mesej-berangkai-berkaitan-bpn>
8. Milad Hassandarvish. Cyber Racism And Covid-19: Expert Weighs In On Hate Speech In Malaysia. <https://www.malaymail.com/news/life/2020/05/29/cyber-racism-and-covid-19-expert-weighs-in-on-hate-speech-in-malaysia/1870481>
9. Rafidah Mat Ruzki. Kutipan Tabung COVID-19 cecah RM22.66 juta. <https://www.bharian.com.my/berita/nasional/2020/04/674220/kutipan-tabung-covid-19-cecah-rm2266-juta>
10. Syairah Abdul Lajis. Frontliners Malaysia beri semangat kepada Indonesia. <https://www.sinarharian.com.my/article/85400/BERITA/Viral/Frontliners-Malaysia-beri-semangat-kepada-Indonesia>
11. Astro Awani. COVID-19: Ekonomi Malaysia dijangka berdepan cabaran luar - Penganalisis <https://www.astroawani.com/berita-bisnes/covid19-ekonomi-malaysia-dijangka-berdepan-cabaran-luar-penganalisis-238064>
12. Prof Madya Dr Mohd Yusof Saari. COVID-19: Malaysia sedang alami perubahan ekonomi total, ini 8 langkah persediaan. <https://www.astroawani.com/berita-malaysia/covid19-malaysia-sedang-alami-perubahan-ekonomi-total-ini-8-langkah-persediaan-236161>
13. Francois Mouton & Arno de Coning. Research Gate. COVID-19 : Impact on the Cyber Security Threat Landscape. 23 Mac 2020.

Mengenali Ancaman Dalam Siber Ke Atas Sistem Pembuatan Pintar

By | Rabiah Binti Ahmad, Universiti Teknikal Malaysia Melaka (UTeM) & Zahri Bin Yunos

Pengenalan

Teknologi siber berkembang pesat semenjak diperkenalkan pada awal tahun 1995. Protokol Internet membolehkan komunikasi digital dilakukan dalam pelbagai medium. Penghantaran data berlaku dalam dua mod, iaitu segerak dan tidak segerak. Dunia komunikasi digital bertambah maju dengan kemudahan komunikasi terbuka. Model OSI, iaitu *Open System Interconnection* menerangkan prinsip 7 lapisan bagi membolehkan penghantaran data berlaku dalam pelbagai rangkaian.

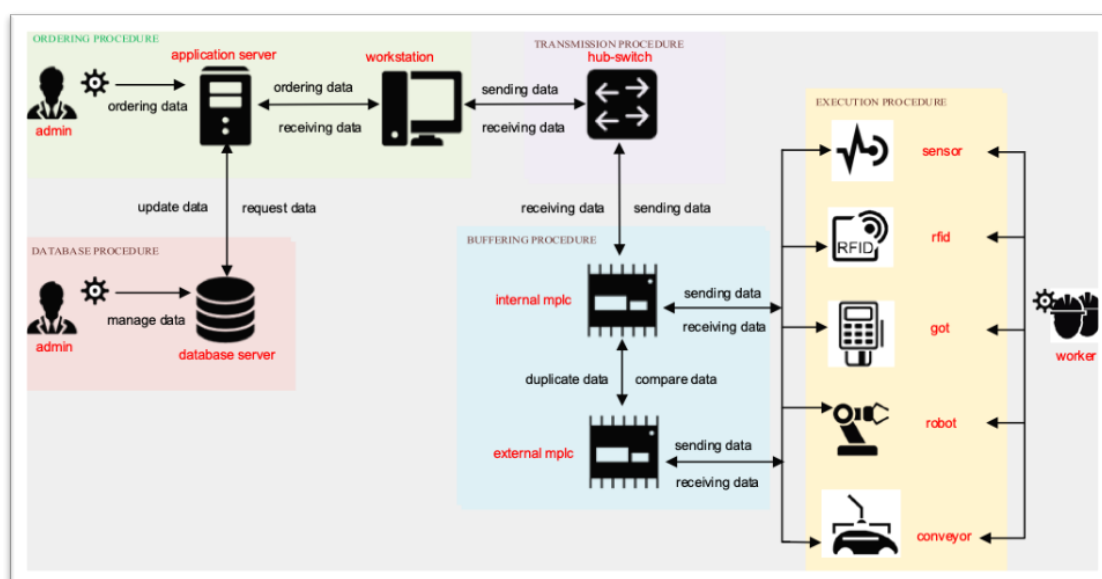
Komunikasi data dan rangkaian menjadi lebih umum dan dikenali sebagai Internet. Internet membenarkan setiap rangkaian berhubung antara satu sama lain melalui protokol yang dikenali sebagai Protokol Internet. Evolusi teknologi maklumat dan komunikasi terus berkembang dengan kemunculan teknologi pengkomputeran awan, teknologi pintar dan banyak lagi.

Keterbukaan komunikasi dalam dunia Internet mengundang pelbagai ancaman seperti kebocoran data, kecurian maklumat, prestasi rangkaian dan kerosakan perkakasan. Ancaman

Internet sering dirujuk sebagai ancaman siber yang boleh berlaku dalam dua keadaan, iaitu dirancang atau tanpa sengaja. Secara umum, ancaman siber boleh dilakukan oleh entiti dalaman atau kadangkala disebut **Entiti Yang Sah**, dan juga entiti luaran. Entiti luaran seperti **penggodam, pencuri maklumat, pemecah masuk sistem** merupakan kejadian norma biasa dalam sesebuah rangkaian komputer.

Ancaman Dalam Siber Dan Sasaran Serangan

Ancaman Dalaman atau dalam bahasa Inggeris disebut *Insider Threats*, merupakan sejenis ancaman siber yang semakin meningkat seperti yang dilaporkan oleh majalah *Cybersecurity Insider* terbitan tahun 2020 dengan 56% serangan ancaman dalaman sukar untuk dikesan berbanding dengan ancaman luaran [1]. Selain itu, kajian ini juga melaporkan bahawa ancaman dalaman kerap berlaku pada teknologi pengkomputeran awan. Teknologi ini kerap diguna pakai dalam sistem pembuatan pintar atau *Smart Manufacturing*.



Sistem Pembuatan Pintar (Smart Manufacturing System)

Secara umumnya, sektor pembuatan melibatkan kumpulan pengguna sistem dalam kalangan kakitangan, pembekal dan pengilang. Kakitangan pula boleh terdiri daripada kakitangan pengurusan, operasi, juruteknik dan banyak lagi. Kaedah kawalan capaian berasaskan peranan amat penting. Namun, ancaman daripada mereka yang mempunyai kuasa atau autoriti mudah berlaku dan biasanya berpunca daripada salah guna kuasa. Terkini, ancaman dalaman penggunaan teknologi siber kerap dilaporkan di negara-negara membangun.

Kelemahan sistem mengundang ancaman serangan oleh kakitangan dalaman dan boleh mengganggu operasi sistem komputer sedia ada. Akhirnya, ancaman dalaman boleh mengganggu operasi harian dan produktiviti.

Kajian oleh Profesor Ts Dr Rabiah Ahmad, profesor dalam bidang keselamatan siber dan juga penyelidik **Universiti Teknikal Malaysia Melaka**, mendapati bahawa penyerang dalaman merupakan antara individu yang mempunyai keistimewaan atau *privilege users* yang berpotensi tinggi melancarkan serangan dalaman terhadap sistem rangkaian komputer [2]. Kajian yang sama menyebut bahawa faktor ketidakpuasan hati terhadap majikan menjadi punca individu merancang untuk melancarkan serangan dalaman dalam pelbagai mod. Dalam era dunia digital, serangan dalaman seperti pencurian maklumat, perencanan operasi sistem komputer dan serangan virus sering dilaporkan secara rasmi di luar negara, namun hal ini bukan perkara biasa bagi penduduk negara membangun seperti Malaysia.

Serangan yang kerap dilakukan adalah seperti buli siber, penukaran kata laluan tanpa kebenaran, ubah suai maklumat dan banyak lagi. Dalam konteks sektor pembuatan, serangan dalaman yang sering dilaporkan melibatkan operasi pengeluaran dan pengubahsuaian pengkodan atur cara oleh pesalah merupakan antara perkara yang kerap dikaitkan dengan serangan dalaman.

Ancaman serangan dalaman siber boleh dianggap sebagai penyakit barah dalam industri perkilangan. Salah sebuah syarikat komputer di Jerman pernah berkongsi pengalaman dengan penyelidik dan menyatakan bahawa syarikat kerugian berbilion ringgit disebabkan oleh kelemahan sistem dan ancaman kakitangan syarikat.

Sistem Keselamatan Siber Yang Kukuh

Penggodam sebenar wujud dalam kalangan pekerja syarikat sendiri. Oleh itu, bagi memastikan sistem rangkaian komputer dalaman terus kukuh, setiap organisasi perlu melaksanakan kawalan keselamatan digital yang merangkumi empat (4) komponen utama, iaitu manusia, proses, prosedur dan teknologi. Sistem keselamatan yang mengambil kira empat komponen ini pastinya akan lebih utuh dan kesannya akan menyeluruh.

Keutuhan sesebuah sistem komputer perlu diuji ketahanannya oleh penganalisis profesional. Ujian ketahanan terhadap sistem keselamatan mesti dilakukan mengikut sela masa tertentu. Perisian komputer mempunyai tempoh luput dan perlu dikemas kini. Kegagalan mengemas kini perisian merupakan faktor utama kepada pertambahan kelemahan sistem dan menjadikan sistem mudah diserang. Oleh itu, ujian harus dilakukan terhadap sistem bagi memastikan tiada kebocoran dalam atur cara, tiada ruang untuk digodam dan tiada kod atur cara yang menjalankan fungsi intipan.

Pengetahuan dan kemahiran tentang proses ujian ketahanan sistem mesti dimiliki oleh setiap pakar keselamatan siber dalam setiap organisasi. Kegagalan pengurusan organisasi mencari pakar bagi mengemudi sistem komputer dalaman bakal mengundang bahaya kepada operasi syarikat, seterusnya menyebabkan kejatuhan reputasi dan akhirnya merencatkan peningkatan produktiviti.

Penulis ingin merakamkan penghargaan dan terima kasih kepada Kementerian Pendidikan Tinggi Malaysia atas penajaan bagi penyelidikan A Multi-perspective Insider Threats Detection and Control Framework Towards Protecting Critical Infrastructure melalui dana TRGS dengan rujukan TRGS/1/2016/UTEM/01/3.

Rujukan

1. <https://www.cybersecurity-insiders.com/portfolio/2020-insider-threat-report/>
2. Al-Mhiqani, M.N.; Ahmad, R.; Zainal Abidin, Z.; Yassin, W.; Hassan, A.; Abdulkareem, K.H.; Ali, N.S.; Yunus, Z. A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. *Appl. Sci.* 2020, 10, 5208

Insiden Keselamatan Siber – Ini Yang Anda Perlu Tahu Dan Lakukan!

By | Norhuzaimi Bin Mohamed

Apa Itu Cyber999?

Pusat Bantuan Cyber999 (Cyber999) yang bertindak sebagai pusat maklum balas tentang insiden keselamatan siber menerima lebih daripada 100,000 laporan pelbagai jenis insiden keselamatan siber dari tahun 2011 hingga September tahun 2020.



Cyber999 menyediakan perkhidmatan bagi membolehkan pengguna Internet melaporkan pelbagai jenis insiden keselamatan siber yang disebabkan oleh kejadian dalam ruang siber yang mengancam keselamatan atau privasi mereka. Insiden keselamatan siber ialah istilah umum yang digunakan oleh Cyber999 untuk apa-apa jua bentuk ancaman, gangguan atau serangan keselamatan siber yang dihadapi oleh orang awam dan organisasi.

Ketahui Jenis-jenis Insiden Keselamatan Siber

1. Penipuan (*Fraud*)

Penipuan secara amnya merujuk apa-apa jenis skim penipuan yang menggunakan satu atau lebih perkhidmatan dalam talian untuk mengumpukan bakal mangsa, untuk menjalankan urusan niaga penipuan atau untuk menghantar hasil penipuan kepada institusi kewangan atau kepada orang lain yang terlibat dengan skim tersebut. Penipuan Internet boleh berlaku dalam talian melalui ruang sembang, e-mel, papan mesej, laman web dan sebagainya. Antara contoh penipuan termasuk memancing data (phishing), penjualan barang tiruan, penipuan dalam talian (online scam), pencurian identiti, pelaburan haram, penipuan loteri (lottery scam) dan penipuan Fi Pendahuluan (Advance Fee scam).

2. Gangguan Siber (*Cyber Harassment*)

Gangguan siber merangkumi pelbagai bentuk tingkah laku di alam siber yang bertujuan mengganggu, mengancam dan menyakitkan hati. Antaranya seperti buli siber (cyber-bullying), intipan siber (cyber stalking), gangguan seksual serta penghinaan kaum dan agama.

3. Berkaitan Kandungan (*Content Related*)

Bahan yang bersifat jelik, tidak bermoral dan tidak memenuhi standard tingkah laku semasa. Antaranya termasuk kandungan lucah dan seks, pornografi dan ancaman ketenteraman awam.

4. Cubaan Menceroboh (*Intrusion Attempt*)

Cubaan menceroboh merangkumi proses proaktif yang mengenal pasti kerentanan rangkaian sistem pengkomputeran bertujuan untuk dieksploitasi dan/atau dicerobohi. Imbasan pangkal (port scanning) boleh dilakukan oleh pihak yang berniat jahat untuk mencari kelemahan dan mencerobohi komputer anda. Login Brute Force pula merupakan salah satu kaedah yang boleh digunakan dengan mencuba semua kata kunci yang mungkin untuk memecahkan sistem enkripsi keselamatan.

5. Pencerobohan (*Intrusion*)

Pencerobohan disebut sebagai akses yang tidak dibenarkan atau akses yang tidak sah kepada sistem atau rangkaian komputer seperti root compromise, web defacements dan pemasangan program hasad, seperti program pintu belakang (back door) atau trojan.

6. Kod Hasad (*Malicious Code*)

Kod hasad ialah sistem perisian atau skrip komputer yang boleh menyebabkan kesan yang tidak diingini, pelanggaran keselamatan atau kerosakan pada sistem komputer. Kod hasad mempunyai kategori yang luas dari segi keselamatan sistem yang merangkumi skrip serangan, virus, cecacing, Trojan, program pintu belakang, dan kandungan aktif yang berbahaya.

7. Spam

Spam lazimnya bersifat komersial dan dihantar sewenang-wenangnya kepada senarai e-mel, individu, atau newsgroup.

8. Gangguan Perkhidmatan (*Denial of Service*)

Serangan gangguan perkhidmatan ialah satu insiden apabila pengguna atau organisasi dihalang daripada mendapat perkhidmatan yang biasa digunakan. Dalam serangan Distributed Denial of Service (DDOS), sebilangan besar sistem yang dikompromikan (dipanggil botnet) menyerang sasaran tunggal.

9. Laporan Kerentanan (*Vulnerabilities Report*)

Kerentanan keselamatan adalah suatu kelompokan keselamatan dalam sesebuah produk ICT yang menjadikannya terdedah kepada penggodam untuk merampas akses pengguna dan seterusnya mengawal operasinya dan menjejaskan integriti data.

Apa Yang Anda Perlu Lakukan?

Sekiranya anda mengalami dan menghadapi apa-apa insiden keselamatan siber seperti yang telah diterangkan, sila laporkan kejadian tersebut kepada Pusat Bantuan Cyber999 melalui salah satu saluran berikut:

1. Aduan melalui laman web (borang dalam talian) – <https://www.mycert.org.my/portal/online-form?id=7a911418-9e84-4e48-84d3-aa8a4fe55f16>
2. Aduan melalui e-mel, hantarkan ke cyber999@cybersecurity.my
Sertakan juga maklumat berikut (jika berkenaan) dalam e-mel anda:
 - Punca insiden
 - Destinasi insiden
 - Pangkal e-mel yang berkenaan (E-mail header)
 - Fail log (Log files)
 - Tarikh dan waktu kejadian
3. Aduan melalui perkhidmatan pesanan ringkas (SMS), hantarkan ke 15888

Sila berikan penerangan ringkas insiden yang ingin dilaporkan dan hantarkan SMS ke 15888 menggunakan format teks seperti yang berikut: CYBER999 REPORT (email)(complaint). SMS yang dihantar akan dikenakan caj sebanyak RM0.35

4. Aduan melalui telefon

- Semasa waktu bekerja, sila dial: 1-300-88-2999
- Jika berlaku kecemasan keselamatan siber selepas waktu bekerja atau semasa cuti umum, sila dial atau SMS ke nombor ini +6019 266 5850 (24 jam)

5. Datang terus ke Pusat Bantuan Cyber999 beralamat di:

Malaysia Emergency Response Team (MyCERT)
CyberSecurity Malaysia, Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan, MALAYSIA

Waktu bekerja:

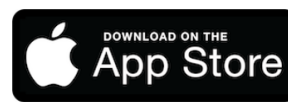
9.00 pagi hingga 6.00 petang, Isnin hingga Jumaat.

Hari cuti:

Sabtu, Ahad, Hari Kelepasan Am di Malaysia dan Negeri Selangor.

Adakah Aplikasi Cyber999 Disediakan Untuk Telefon Pintar?

Ya. Anda boleh memuat turun aplikasi Cyber999 secara percuma di Google Play Store (Android) dan App Store (iOS)



Rujukan

1. <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=4997a4a8-b05d-47d4-8e51-3c5b063a67fd>
2. <https://www.cybersecurity.my/>

Kenali Jenis-jenis Perisian Hasad (*Malware*)

By | Norhuzaimi Bin Mohamed





Apa Itu Perisian Hasad?






Perisian hasad (Malicious Software) merupakan apa-apa program yang dicipta dan dirancang dengan tujuan jahat untuk mendatangkan kerosakan dengan cara menyusup masuk ke dalam sistem komputer. Perisian hasad menyerang komputer melalui e-mel, muat turun Internet, program yang telah dijangkiti, pemacu boleh alih dan sebagainya.

Perisian hasad boleh menyebabkan kerosakan pada sistem komputer dan boleh mengakibatkan berlakunya kecurian data atau maklumat. Perisian hasad boleh dibahagikan kepada beberapa jenis seperti virus, cecacing (worm), kuda trojan (trojan horse), kit akar (rootkit), perisian intip (spyware), perisian iklan (adware), perisian tebusan (ransomware), keylogger, pintu belakang (backdoor) serta perisian lain yang berbahaya dan tidak diinginkan oleh pengguna komputer.

Rujukan

1. <https://www.educba.com/what-is-malware/>
2. <https://windowsmaximizer.com/blog/about-types-of-malware/>
3. <https://www.lemoncomm.com/9-types-of-malware-and-how-to-identify-them/>
4. <http://perpustakaanjbpmb.blogspot.com/2015/01/kenali-jenis-malware.html>
5. <https://amt-it.com/mengenal-jenis-malware-data-perusahaan/>
6. <https://catatanteknisi.com/pengertian-dan-jenis-malware/>
7. <https://www.facebook.com/pusatinternettititeras/photos/kenali-jenis-jenis-malware-yang-menyerang-peranti-anda/1237727213024297/>
8. <https://www.drupalnote.my/komputer-masalah-dan-penyelesaian/malware-dan-langkah-mengatasinya>
9. <https://idcloudhost.com/mengenal-apa-itu-malware-penyebab-dan-mengatasinya/>

Jenis Perisian hasad	Keterangan
 Virus	Program yang apabila diaktifkan, mempunyai kebolehan untuk menggandakan dirinya (self replicate) dengan menjangkiti program lain atau fail yang ada dalam komputer. Program ini boleh mendatangkan pelbagai kesan (bergantung pada penciptanya) seperti memadamkan semua data daripada cakera keras, menayangkan tettingkap mesej daripada penciptanya, atau hanya menggandakan dirinya dan memberatkan komputer anda. Virus tidak boleh merebak dengan sendiri ke komputer lain. Cara paling biasa bagi virus untuk merebak ialah melalui pemacu boleh alih.
 Worm	Program yang mempunyai kebolehan untuk menjangkiti komputer lain dengan sendirinya apabila diaktifkan, sama ada melalui e-mel dengan menggunakan alamat e-mel yang dijumpai pada komputer yang dijangkiti, atau melalui Internet dengan mengeksploitasi kelemahan sekuriti.
 Trojan	Program yang direka untuk kelihatan seperti program yang tidak berbahaya, tetapi sebenarnya dicipta dengan tujuan jahat melalui program pintu belakang (backdoor) untuk mendedahkan komputer anda kepada ancaman. Sebaik sahaja pengguna memuat turun program ini, trojan akan terus menjangkiti sistem mereka.
 Rootkit	Kit akar (Rootkit) ialah teknik pelindung (masking) bagi perisian hasad, tetapi tidak mengandungi perisian yang merosakkan. Teknik kit akar ini dicipta oleh penggodam untuk menyembunyikan perisian hasad supaya tidak dapat dikesan oleh antivirus dan program penyingkiran yang lain.

Jenis Perisian hasad	Keterangan
 <p>Spyware</p>	<p>Berfungsi untuk mengintip aktiviti pengguna, mengumpul maklumat, dan menghantar maklumat itu kepada penciptanya atau kepada penggadam (hacker). Ia memiliki mekanisme jangkitan dan lebih cenderung kepada ancaman kewangan. Perisian intip akan terpasang dengan sendirinya dan menyusup masuk secara senyap bagi mengelak daripada dikesan.</p>
 <p>Adware</p>	<p>Program yang menghasilkan popups atau menayangkan iklan pada komputer anda. Tidak semua perisian iklan boleh dianggap sebagai perisian hasad kerana kebanyakan program atau aplikasi, terutamanya aplikasi percuma, menayangkan iklan dalam program mereka untuk memberikan pulangan atau menjana pendapatan kepada penciptanya. Program ini biasanya tidak akan dianggap sebagai perisian hasad selagi maklumat yang disampaikan itu boleh dipercayai.</p>
 <p>Ransomware</p>	<p>Perisian tebusan (Ransomware) ialah sejenis perisian hasad yang menyulitkan data anda dengan menyimpannya seperti tebusan. Penyerang akan menuntut bayaran daripada mangsa untuk melepaskan kembali data yang telah dikunci (sebagai tebusan). Perisian tebusan akan menyekat akses pengguna kepada sistem dan menyulitkan mangsa untuk mengakses fail yang berada dalam cakera keras dengan memaparkan mesej yang bertujuan untuk memaksa mangsa membayar penyerang mengikut jumlah amaun yang dikehendaki bagi mendapatkan kembali akses kepada sistem anda.</p>
 <p>Keylogger</p>	<p>Keylogger pula merekodkan data penting seperti nama pengguna, kata laluan, nombor kad kredit dan alamat e-mel. Perisian hasad ini digunakan dalam serangan berniat jahat seperti memancing data (phishing), kejuruteraan sosial dan kecurian identiti. Ia juga direka untuk mencuri wang daripada pengguna komputer, perniagaan dan bank tanpa disedari.</p>
 <p>Backdoor</p>	<p>Program yang membolehkan penciptanya mengawal komputer anda untuk menjalankan arahan dan tugas tanpa kebenaran anda. Program pintu belakang merujuk mekanisme yang dapat digunakan untuk memintas dan mengakses sistem, aplikasi dan rangkaian. Program pintu belakang biasanya akan dipasang terlebih dahulu sebelum perisian hasad lain bagi memudahkan dan membenarkan program ini masuk dan menyerang.</p>

Cara Mendidik Anak-Anak Agar Berintegriti Semasa Menggunakan Internet

By | Alifa Ilyana Chong Binti Abdullah, Nur Haslailly Binti Mohd Nasir & Redy Jeffry Bin Mohamad Ramli

Media, terutamanya media interaktif merupakan wahana yang sangat bermanfaat untuk mendidik anak-anak tentang integriti kerana mereka boleh mempraktikkan apa yang dipelajari dan mendapat maklum balas dengan serta-merta.

Sewaktu anak-anak masih kecil, didik mereka supaya tahu menggunakan Internet secara berhemah, bertanggungjawab dan sentiasa menghormati orang lain semasa dalam talian.

Wujudkan prinsip moral yang kukuh dalam diri anak-anak dengan memberitahu mereka tentang apa yang boleh dan tidak boleh dilakukan semasa dalam talian.

1. Didik anak-anak agar sentiasa menghormati orang lain semasa dalam talian.
2. Jadikan diri anda sebagai suri teladan kepada anak-anak agar tindak-tanduk kita semasa dalam talian menjadi ikutan mereka. Laksanakan apa yang anda sering ucapkan.
3. Jangan sesekali biarkan mereka berasa 'tidak apa' tentang perbuatan memuat turun sesuatu secara haram, menghantar mesej atau berselindung di sebalik identiti palsu bagi menyatakan apa-apa perkara yang tidak elok.

BAGAIMANA MENDIDIK KANAK-KANAK TENTANG INTEGRITI SEMASA MENGGUNAKAN INTERNET?

Media terutamanya media interaktif merupakan alat yang banyak manfaatnya untuk mendidik kanak-kanak tentang integriti kerana mereka boleh mempraktikkan apa yang dipelajari dan dapat maklum balas segera.

Sewaktu muda, didiklah kanak-kanak menggunakan Internet secara berhemah, bertanggungjawab dan mengamalkan tingkah laku menghormati orang lain sewaktu dalam talian.

Berikan mereka asas yang kukuh mengenai integriti dengan memberitahu mereka tentang apa yang boleh dan tidak boleh sewaktu dalam talian.

**1**

Didiklah kanak-kanak agar sentiasa menghormati orang lain semasa dalam talian.

**2**


Jadilah sebagai model contoh kepada kanak-kanak sewaktu dalam talian agar tindak tanduk kita menjadi ikutan mereka. Praktikkan apa yang anda sering ucapkan.

**3**

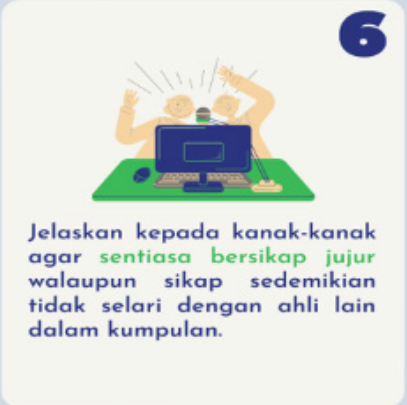
Jangan sesekali biarkan mereka merasa 'tidak apa' tentang muat turun secara haram, menghantar mesej atau berselindung di sebalik identiti palsu untuk meluahkan perkara yang tidak elok.

**4**

Didik kanak-kanak untuk melaporkan sebarang tindak tanduk yang salah semasa dalam talian.



Didik kanak-kanak tentang etika dalam talian, penipuan dan pelanggaran hak cipta.




Jelaskan kepada kanak-kanak agar sentiasa bersikap jujur walaupun sikap sedemikian tidak selari dengan ahli lain dalam kumpulan.

Dengan asas integriti yang kukuh dalam diri kanak-kanak, mereka lama kelamaan mampu berdikari apabila berada dalam talian tanpa pengawasan ketat ibu bapa atau orang dewasa.

Anda boleh menggunakan Internet sebagai inspirasi integriti dengan mendidik kanak-kanak menggunakan apa jua peralatan digital secara beretika dan bertanggungjawab pada usia muda.

Galakkan kanak-kanak agar menyedari tentang kesan dan akibat bagi setiap tindakan mereka semasa dalam talian serta ajak mereka menonton bersama video yang menekankan nilai-nilai integriti.



Rujukan :

- CommonSenseMedia, Character Strenghts and Life Skills
- Berita Harian Online, Menjaga Integriti Penggunaan Media Sosial
- Greater Good Magazine, How To Raise A Kid With Conscience in The Digital Age

4. Didik anak-anak untuk berani melaporkan apa-apa tindak-tanduk yang salah semasa dalam talian.
5. Maklumkan kepada anak-anak tentang etika semasa dalam talian, penipuan dan pelanggaran hak cipta.
6. Terangkan kepada anak-anak betapa pentingnya untuk sentiasa bersikap jujur walaupun sikap sedemikian tidak selari dengan ahli lain dalam kumpulan.

Anda boleh menjadikan Internet sebagai inspirasi untuk mengukuhkan integriti dengan mendidik anak-anak menggunakan apa-apa jua peralatan digital secara beretika dan bertanggungjawab pada usia muda.

Pastikan anak-anak sedar tentang kesan dan akibat bagi setiap tindakan mereka semasa dalam talian serta ajak mereka sama-sama menonton video yang menekankan nilai-nilai integriti.

Dengan asas integriti yang kukuh dalam diri anak-anak, lama-kelamaan mereka akan mampu berdikari apabila berkomunikasi secara dalam talian tanpa pengawasan ketat ibu bapa atau orang dewasa.

Buli Siber Di Media Sosial

By | Faiszatul Nasro Binti Mohd Maksom

Pengenalan

Berdasarkan statistik tahunan MyCERT sejak 2017 sehingga 2020, jumlah laporan buli siber dilihat menunjukkan peningkatan pada tahun 2020. Kenaikan pelaporan mungkin disebabkan situasi semasa pandemik COVID19, di mana penggunaan internet yang lebih kerap sebagai medium komunikasi dan pencarian maklumat.

Tahun	Jumlah
2017	292
2018	266
2019	204
2020 (Sept)	322

Statistik buli siber

Sehubungan dengan itu, menurut Jabatan Statistik Malaysia^[1] pada tahun 2019 penggunaan media sosial merupakan aktiviti tertinggi yang dilakukan iaitu sebanyak 97.1% berbanding dengan tahun sebelumnya iaitu 96.5%.

Penggunaan media sosial juga sering dikaitkan dengan buli siber yang dilihat semakin membimbangkan dalam kalangan rakyat Malaysia. Penggunaan media sosial pada asalnya yang merupakan medium komunikasi dan pemudah cara bagi mendapatkan maklumat, tetapi disalahgunakan oleh sesetengah individu bagi melakukan buli siber terhadap individu lain.

Statistik MyCERT juga menunjukkan buli siber boleh berlaku kepada individu pelbagai peringkat umur. Namun demikian, peringkat umur 26 sehingga 40 tahun merupakan golongan yang paling ramai melaporkan buli siber ke Pusat Bantuan CYBER999.

Umur	Jumlah
Di bawah 18 tahun	13
19-25	58
26-40	78
41-55	16
56 ke atas	3

Umur mangsa yang melaporkan

Menurut satu kajian yang dijalankan, platform media sosial yang paling banyak dilaporkan berlakunya buli siber adalah Facebook dan Instagram^[2]. Maklumat ini selari dengan statistik yang dilaporkan oleh Statcounter, iaitu penggunaan laman Facebook merupakan platform yang tertinggi di Malaysia dengan jumlah sebanyak 84.62% setakat bulan Ogos 2020. Di susuli oleh Twitter sebanyak 2.78%, Youtube 2.62% dan Instagram sebanyak 2.39%.

Penggunaan media sosial sebagai medium buli siber adalah disebabkan berapa faktor^[3].

1. Pembuli siber sukar untuk dikenalpasti kerana mereka boleh merahsiakan identiti sebenar.
2. Pembuli siber lebih mudah bersekongkol kerana bilangan individu yang boleh turut serta tidak dihadkan dalam dunia siber.
3. Buli siber boleh berlaku tanpa mengira masa dan tanpa perlu bersemuka.

Jenis-Jenis Buli Siber

Berdasarkan laporan yang diterima Pusat Bantuan CYBER999, berikut merupakan beberapa jenis buli siber yang sering dilaporkan oleh mangsa:

1. Ugutan sebar video

Mangsa lelaki dihubungi oleh gadis yang berperwatakan menggoda dan mengajak melakukan aksi yang kurang sopan dengan menggunakan aplikasi video sembang. Akhirnya, mangsa diugut sekiranya tidak mahu video tersebut disebar, mangsa perlu membuat bayaran pada waktu yang ditetapkan.

2. Profail palsu

Gambar mangsa digunakan sebagai gambar profail dan menjadikan rakan-rakan mangsa sebagai senarai kenalan. Profail palsu ini juga berpotensi digunakan untuk melakukan penipuan.

3. Mesej yang mengganggu

Mangsa diganggu dengan mesej yang tidak berpuas hati di atas hubungan mangsa dengan pasangannya atau mengugut dengan mesej yang boleh mengganggu emosi mangsa, sekiranya tidak melayani kehendak pembuli siber.

4. Penyebaran maklumat palsu/fitnah

Pembuli siber mereka-reka cerita dan membuat hantaran di media sosial dengan tujuan memburukkan imej mangsa.


5. Komen yang mengejek atau mengutuk

Pembuli siber merendah-rendahkan mangsa dengan kata-kata ejekan dan kejian.


Apa Yang Perlu Dilakukan?

Mangsa dinasihatkan untuk membuat laporan melalui langkah yang disediakan oleh pihak penyedia perkhidmatan (Facebook, Instagram dsb yang berkenaan), iaitu dengan menggunakan butang pelaporan.



I. FACEBOOK ^[4]

1. Pergi ke profil yang ingin melaporkan.
2. Di bahagian bawah sebelah kanan foto muka depan, klik  dan pilih **Report it**.
3. Ikut arahan pada skrin.
4. Sekat akaun pembuli siber.

Melaporkan komen di Facebook ^[5]

1. Pergi ke komen yang ingin melaporkan.
2. Klik  di sebelah komen.
3. Klik **Give feedback or report this comment**
4. Untuk memberikan maklum balas, klik pilihan terbaik yang menerangkan sebab komen tersebut bertentangan dengan Standard Komuniti Facebook. Jika tiada sebarang pilihan yang sesuai, klik **Something Else** untuk mencari lebih banyak pilihan.
5. Bergantung pada maklum balas, mangsa kemudiannya boleh menghantar laporan ke Facebook.


II. INSTAGRAM ^[6]

1. Klik  pada *iPhone* atau  pada *Android* di bahagian atas sebelah kanan profil.
2. Klik **Report it**.
3. Ikut arahan pada skrin.

Melaporkan komen di Instagram ^[7]

1. Klik  di bawah komen.
2. Leret ke kiri pada komen (*iPhone*) atau klik komen (*Android*) yang ingin melaporkan.
3. Klik  (*iPhone*) atau  (*Android*).
4. Klik **Report This Comment**.
5. Klik **This is Spam** atau klik **It's inappropriate**.
6. Pilih satu pilihan yang menerangkan sebab komen tidak sopan.

III. TWITTER ^[8]


1. Pergi ke *Tweet* yang hendak dilaporkan
2. Klik ikon 
3. Pilih **Report**.
4. Pilih **It's abusive or harmful**.

5. Kemudian, Twitter akan bertanya maklumat berkenaan isu yang hendak dilaporkan.
6. Twitter akan memasukkan teks laporan di dalam email susulan yang akan dihantar.
7. Setelah laporan dihantar, Twitter akan menyediakan beberapa tindakan yang perlu dilakukan semasa menggunakan Twitter.

IV. TELEGRAM

1. Tekan pada gambar ikon **Channel**.
2. Tekan **...** dan pilih **Report**.

V. YOUTUBE ^[9]

1. Pergi ke video yang hendak dilaporkan.
2. Tekan **More** **:** di bahagian atas video.
3. Tekan **Report** .
4. Pilih sebab membuat laporan.

V. WHATSAPP ^[10]

1. Buka *chat*.
2. Tekan pada kontak atau nama dan buka **profile information**.
3. Skrol ke bawah dan tekan **Report contact** atau **Report group**.

Kesimpulan

Buli siber berpotensi berlaku kepada sesiapa sahaja. Pembuli siber selalunya akan cuba menakutkan, merendah-rendahkan, mengejek atau membalas dendam secara maya. Disebabkan itu, kesan yang dihadapi oleh mangsa adalah pelbagai dan mereka juga menghadapi tekanan ke atas apa yang berlaku.

Adakalanya, mangsa terlampau tertekan sehingga mahu membunuh diri bagi melepaskan tekanan yang dihadapi. Mangsa dinasihatkan untuk mendapatkan khidmat nasihat daripada badan yang berkecualan memberi khidmat kaunseling bagi menangani tekanan perasaan akibat buli siber.

Perlu diingatkan bahawa, tempoh masa dan tindakan yang diambil setelah melaporkan profil pembuli siber adalah bergantung sepenuhnya

kepada pihak penyedia perkhidmatan (Facebook, Instagram dsb yang berkenaan).

Pihak MyCERT tidak bertanggungjawab ke atas tindakan penyekatan profil atau mengenalpasti identiti individu sebenar disebalik akaun pembuli siber tersebut. Ini adalah kerana, hanya pihak penyedia perkhidmatan sahaja yang mempunyai maklumat itu dan mangsa perlu melalui proses perundangan bagi mendapatkan maklumat berkaitan dengan akaun media sosial tersebut. ^[11]

Rujukan

1. *ICT Use and Access By Individuals and Households Survey Report, Malaysia, 2019* https://www.dosm.gov.my/v1/index.php?r=column/cthemeByCat&cat=395&bul_id=SFRacTRUMEVRUFo1Ulc4Y1JILzBqUT09&menu_id=amVoWU54UT10a21NWmdhMjFMMWcyZz09
2. Sharifah Roziah et al. (2018). *Cyber Harassment Trends Analysis: a Malaysia Case Study*. *International Journal of Engineering & Technology*, 7 (4.15) (2018) 109-112
3. *What is cyberbullying?*, <http://www.myhealth.gov.my/en/cyberbullying-2/>
4. *How to Report Something*, <https://www.facebook.com/help/263149623790594>
5. *How to Report Things on Facebook* <https://www.facebook.com/help/reportlinks>
6. *How do I report a post or profile for abuse or spam on Instagram?*, <https://help.instagram.com/192435014247952>
7. *Abuse and Spam* <https://help.instagram.com/165828726894770>
8. *Report abusive behavior*, <https://help.twitter.com/en/safety-and-security/report-abusive-behavior>
9. *Report inappropriate content* <https://support.google.com/youtube/answer/2802027>
10. *Staying safe on WhatsApp* <https://faq.whatsapp.com/general/security-and-privacy/staying-safe-on-whatsapp/?lang=en>
11. *Law Enforcement & Third-Party Matters*, <https://www.facebook.com/help/473784375984502?page=211462112226850>

Integriti Dalam Dunia Siber, Tanggungjawab Bersama

By | Alifa Ilyana Chong Binti Abdullah, Nur Haslaila Binti Mohd Nasir & Redy Jeffry Bin Mohamad Ramli

Pengenalan

Apakah yang masyarakat umum faham tentang 'integriti'? Kamus Dewan Edisi Keempat mendefinisikan 'integriti' sebagai kejujuran, keadaan sempurna dan utuh.^[1] Ia selari dengan perkataan asalnya daripada Bahasa Inggeris iaitu integrity yang bermaksud berpegang teguh kepada prinsip kejujuran serta mempunyai prinsip moral yang tinggi.

Perkataan integrity berkembang daripada kata adjektif Bahasa Latin, integer yang antara lain bermaksud jujur, keseluruhan atau lengkap.^[2] Walau bagaimanapun, sebelum perkataan integer ini diterima pakai sebagai kosa kata pada 1659 bagi membezakan konsep 'benar dan salah' dalam kehidupan manusia, perkataan tersebut pada asalnya diguna pakai untuk menggambarkan keutuhan sesuatu struktur atau binaan (structural integrity).^[3]

Oleh yang demikian pemahaman integriti dari sudut bahasa belum cukup bagi setiap individu menjadikan ia sebagai budaya dalam kehidupan. Namun memahami definisi integriti itu secara harfiah adalah suatu permulaan terbaik.

Penulis ingin mengajak pembaca menelusuri sejarah budaya integriti di Malaysia bagi memberi sedikit pemahaman betapa negara ini melalui kerajaan yang dipilih telah melakukan perkara yang betul dan tepat dengan memupuk budaya integriti dalam kalangan penjawat awam bagi membentuk masyarakat Malaysia yang berintegriti.

Komitmen kerajaan dalam memerangi budaya rasuah, memperkasakan tadbir urus dan integriti masyarakat secara tegas serta menyeluruh pada tahun 2018 menerusi Pusat Governans, Integriti dan Anti Rasuah Nasional (*Global Infrastructure Anti-Corruption Centre* – GIACC) mula menampakkan hasil yang memberangsangkan.

Penghujung Januari 2020, *Transparency International* (TI) telah mengumumkan Indeks Persepsi Rasuah (CPI) yang mana Malaysia telah memperbaiki kedudukannya pada tahun 2019 sebanyak 10 anak tangga dengan 53 mata sekali gus menduduki tangga ke-51 berbanding 47 mata dan kedudukan di tangga ke-61 pada tahun 2018.

Integriti Di Malaysia

Kerajaan Malaysia pada 4 Mac 2004 secara rasminya telah menubuhkan Institut Integriti Malaysia (IIM) yang bertanggungjawab menyediakan perundingan mengenai integriti, anti-rasuah dan tadbir urus di negara ini.

Melalui IIM, Pelan Integriti Nasional (PIN) yang merupakan satu pelan atau rancangan yang memfokus kepada usaha menanam dan memupuk budaya etika dan budaya integriti bagi segenap lapisan masyarakat Malaysia telah dilancarkan pada 23 April 2004.

Bagi membudayakan integriti dalam masyarakat, kerajaan juga telah menubuhkan beberapa agensi penguatkuasaan antaranya Suruhanjaya Integriti Agensi Penguatkuasaan dan Suruhanjaya Pencegahan Rasuah Malaysia (SPRM) yang suatu ketika dahulu dikenali sebagai Badan Pencegah Rasuah (BPR).

Namun sebelum terma integriti menjadi sebutan masyarakat beberapa tahun kebelakangan ini, konsep jujur, beretika dan bermoral tinggi sebenarnya telah lama diterapkan oleh Kerajaan Malaysia.

Bagi penulis, kempen 'Bersih, Cekap dan Amanah' yang diperkenalkan di Malaysia pada bulan April 1982 merupakan salah satu langkah awal kerajaan membentuk sikap positif, bermoral tinggi serta jujur dalam pengurusan, pentadbiran dan rakyat keseluruhannya.

Konsep 'Bersih, Cekap dan Amanah' ini ditanam dalam kalangan penjawat awam agar lahir

penjawat awam yang menjalankan tugas dan tanggungjawab yang bukan sahaja cekap malah bersih (jujur) serta beramanah tanpa sebarang elemen penipuan, penyelewangan ataupun rasuah.

Tidak berhenti hanya dengan kempen tersebut, kerajaan memperkenalkan pula kempen 'Kepimpinan Melalui Teladan' pada 19 Mac 1983 sebagai kesinambungan konsep 'Bersih, Cekap dan Amanah'.

Walaupun bagaimanapun, angka statistik bagi tempoh sembilan tahun iaitu 2005 hingga tahun 2014 menyatakan bahawa Malaysia telah kehilangan RM1.8 trillion menerusi aliran kewangan tidak sah yang mana sebahagiannya berpunca daripada amalan rasuah. ^[4]

Justeru, Pelan Antirasuah Nasional (*National Anti-Corruption Plan* – NACP) 2019–2023 telah dilancarkan pada 29 Januari 2019 bagi menggantikan Pelan Integriti Nasional. ^[4]

Pelan khusus ini dibangunkan oleh GIACC yang diletakkan di bawah Jabatan Perdana Menteri dengan visi iaitu "Malaysia dikenali kerana integriti dan bukannya rasuah". ^[4]

Pelan ini mengambil kira pandangan pelbagai lapisan masyarakat dalam usaha pencegahan rasuah yang lestari di Malaysia. Ia bermatlamat mengekang campur tangan politik, menghapuskan penyalahgunaan kuasa, menghentikan budaya kronisme dan nepotisme serta menghapuskan penyelewangan dan kelemahan tadbir urus. ^[5]

NACP menyediakan pelan lebih menyeluruh merangkumi enam sektor utama iaitu Tadbir Urus Politik, Perolehan Awam, Penguatkuasaan Undang-undang, Pentadbiran Sektor Awam, Perundangan dan Kehakiman serta Tadbir Urus Korporat, sama ada di sektor awam mahu pun swasta. ^[5] ^[4]

Integriti Dalam Dunia Siber

Malaysia seperti kebanyakan negara di dunia sudah memasuki era siber yang menyaksikan pelbagai urusan kerajaan dilakukan secara dalam talian. Selaras dengan perkembangan ini, penjawat awam bukan sahaja harus berintegriti semasa berada luar talian malah sentiasa menegakkan nilai-nilai integriti ini semasa dalam talian terutama ketika berurusan dengan orang awam.

Berintegriti Dalam Talian Setiap Masa

Sebagai penjawat awam, tanggungjawab menyampaikan aspirasi kerajaan amat mustahak tanpa mengira masa dan tempat. Seorang penjawat awam yang berintegriti akan sentiasa mendukung tanggungjawab tersebut termasuklah ketika menggunakan teknologi dan Internet.

Penjawat awam hendaklah sentiasa mengamalkan sikap positif dan membudayakan integriti keselamatan siber sepanjang berada dalam talian agar setiap tindak tanduk mereka, sama ada membuat hantaran komentar mahupun menular perkongsian maklumat adalah selari dengan sikap bertanggungjawab iaitu menyampaikan perkara yang benar dan sahih.

Pemahaman dan pengamalan integriti juga amat perlu dilaksanakan oleh setiap individu. Di zaman yang sarat dengan gaya hidup berorientasikan teknologi ini maka penggunaannya perlu selari dengan penerapan integriti untuk mencegah pelbagai bentuk ancaman atau cabaran yang memudaratkan. Sebagai contoh, melayari laman-laman yang tidak bermoral dan tidak berfaedah. Oleh itu, setiap individu perlu lebih bertanggungjawab dan beretika ketika berada dalam alam siber.

Model Contoh

Penjawat awam, khasnya serta pekerja swasta dan masyarakat Malaysia amnya hendaklah menjadi model untuk dicontohi sesama individu lain ketika melayari Internet. Tindakan yang tidak emosional, tidak berkongsi maklumat tanpa pengesahan serta tidak menggunakan pengucapan kesat, berbaur hasutan ataupun fitnah dan adu domba merupakan amalan-amalan penggunaan Internet yang positif. Justeru, amalan ini sudah pasti akan mewujudkan suasana persekitaran dunia siber yang selamat dan sejahtera.

Penjawat awam atau sesiapa sahaja yang memahami konsep integriti sudah pasti akan sentiasa beringat dan seterusnya memastikan setiap tindak-tanduk semasa berada dalam talian menjurus kepada pengutamaan keselamatan siber.

Syor Dan Rujukan

Sebagai individu yang sentiasa berintegriti, khasnya penjawat awam mahupun mereka yang mempunyai peranan penting dalam organisasi ataupun masyarakat, menjadi sumber rujukan orang ramai adalah satu tanggungjawab yang besar.

Apabila tindak-tanduk dalam talian terpancar sifat-sifat berintegriti, maka sudah pasti segala pandangan yang dilontar akan dipercayai dan dihormati. Secara tidak langsung individu tersebut akan menjadi rujukan sekiranya orang awam berhadapan dengan isu-isu ancaman siber seperti penipuan dalam talian, scam, pembuli siber dan jenayah siber yang lain.

Dalam hal ini, orang awam yang menghadapi masalah berkaitan keselamatan siber perlu mengambil langkah-langkah wajar berdasarkan amalan terbaik (best practice) sekiranya menjadi mangsa ancaman jenayah siber. Sementara itu, pihak berwajib atau agensi kerajaan juga harus memainkan peranan dengan membangunkan inisiatif serta program secara berterusan demi membendung jenayah siber. Contohnya: Menasihati mangsa untuk membuat laporan kepada pihak berkuasa seperti Polis atau Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) ataupun menghubungi Cyber999 yang dikendalikan oleh CyberSecurity Malaysia

Kerjasama Kerajaan Dan Masyarakat

Kerajaan sudah melakukan banyak perkara dalam memastikan penjawatan awam menjadi individu yang berintegriti. Namun usaha yang dilakukan oleh kerajaan menjadi sia-sia sekiranya rakyat tidak menjiwai dan menjadikan amalan baik itu sebahagian daripada budaya hidup.

Oleh kerana integriti berhubung kait dengan nilai-nilai amanah, jujur, dan kebolehpercayaan, maka adalah wajar untuk rakyat memikul tanggungjawab ini dan menjadikannya integriti sebagai budaya hidup sama ada di dunia fizikal mahupun di alam siber.

Pendidikan Integriti

Sementara itu, penerapan nilai-nilai berintegriti secara berterusan adalah kunci dalam menjayakan budaya integriti sebagai gaya

hidup. Pendidikan budaya integriti khasnya dalam talian hendaklah bermula dari peringkat sekolah agar pembentukan sahsiah dan karakter seseorang individu berintegriti itu bermula seawal mungkin.

Pembudayaan ini tidak berakhir hanya di peringkat persekolahan seseorang individu, malah dalam masyarakat yang merangkumi institusi keluarga, kampung, daerah dan seterusnya negeri.

Penonjolan budaya integriti harus dilaksanakan secara berterusan agar pendidikan mengenai budaya integriti ini berkesinambungan dan secara kolektif diterima sebagai amalan bersama.

Kesimpulan

Jadikanlah budaya integriti sebagai amalan hidup yang berterusan dan bukan hanya diamalkan dalam sesetengah perkara sahaja. Amalannya harus dilakukan sama ada semasa dalam talian atau luar talian, kesungguhan dan keteguhan hati dalam mengamalkan budaya integriti harus wujud dalam sanubari setiap individu dan semuanya harus bermula dengan diri setiap individu sendiri terlebih dahulu.

Jika setiap individu percaya dan yakin bahawa mereka boleh menjadikan budaya integriti sebagai amalan hidup, maka keseluruhan struktur dalam masyarakat bermula dari keluarga, kampung, daerah, negeri, organisasi sehingga ke peringkat negara akan membentuk budaya integriti yang diamalkan bersama.

Sudah pasti apabila budaya integriti diterima menjadi amalan hidup oleh semua lapisan masyarakat, ruang dan peluang untuk berlakunya ketidakjujuran dalam berurusan, pecah amanah, rasuah mahupun penyalahgunaan kuasa dapat dihindari oleh setiap individu dan peringkat.

Ikan kerisi, ikan tenggiri,
Ikan kesukaan Pak Musa;
Amalan rasuah amalan keji,
Kerana rasuah pemusnah bangsa.

Ikan keli disiat-siat,
Masak bersama buah keras;
Integriti diamal sepanjang hayat,
Lakukanlah tugas penuh ikhlas.

Utamakanlah integriti semasa dalam talian kerana amalan tersebut akan mewujudkan dunia siber yang lebih selamat dan mendamaikan buat semua yang berada di dalam dunia siber. Tanpa sifat integriti, sudah pasti keselamatan siber tidak akan wujud khasnya dalam melindungi orang awam seperti wanita dan kanak-kanak yang lebih cenderung menjadi mangsa pelbagai jenayah siber.

Rujukan

1. *Definisi Integriti* : <https://prpm.dbp.gov.my/cari1?keyword=integriti>
2. *Integar Wiktionary* : <https://en.wiktionary.org/wiki/integer>
3. *Integriti Dalam Kehidupan* : <https://www.kemas.gov.my/integriti-dalam-kehidupan/>
4. *Pelan Antirasuah Nasional 2019-2023* ,<http://giacc.jpm.gov.my/wp-content/uploads/2019/01/PELAN-ANTIRASUAH-NASIONAL-2019-2023.pdf>
5. *NACP ganti Pelan Integriti Nasional (PIN), NKRA perang rasuah* : <https://www.bharian.com.my/berita/nasional/2019/01/525281/nacp-ganti-pelan-integriti-nasional-pin-nkra-perangi-rasuah>

Corporate Office:

CyberSecurity Malaysia

Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.


Tel: +603 8800 7999


Fax: +603 8008 7000

Email: info@cybersecurity.my

www.cybersecurity.my

 @cybersecuritymy

 CyberSecurityMalaysia

 cybersecurity_malaysia

 CyberSecurityMy

© CyberSecurity Malaysia 2020 – All Rights Reserved



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA



ISSN 1985-1995

