PEJABAT KETUA PEGAWAI KESELAMATAN
KERAJAAN MALAYSIA

KETIRISAN MAKLUMAT:

ANCAMAN KEPADA KESELAMATAN NEGARA

OLEH:

JULAILA BINTI ENGAN

BAHAGIAN KESELAMATAN PERLINDUNGAN ICT DAN RAHSIA RASMI

KEPENTINGAN KAWALAN MAKLUMAT KERAJAAN

"Sehari dua ini ada beberapa **kebocoran maklumat** rahsia Kerajaan dilaporkan termasuk kenaikan harga tol. Kalau belum sedia membuat pengumuman, jangan bocorkan kerana dikhuatiri boleh jadi keputusan berlainan kelak." (MAPPA XIV)

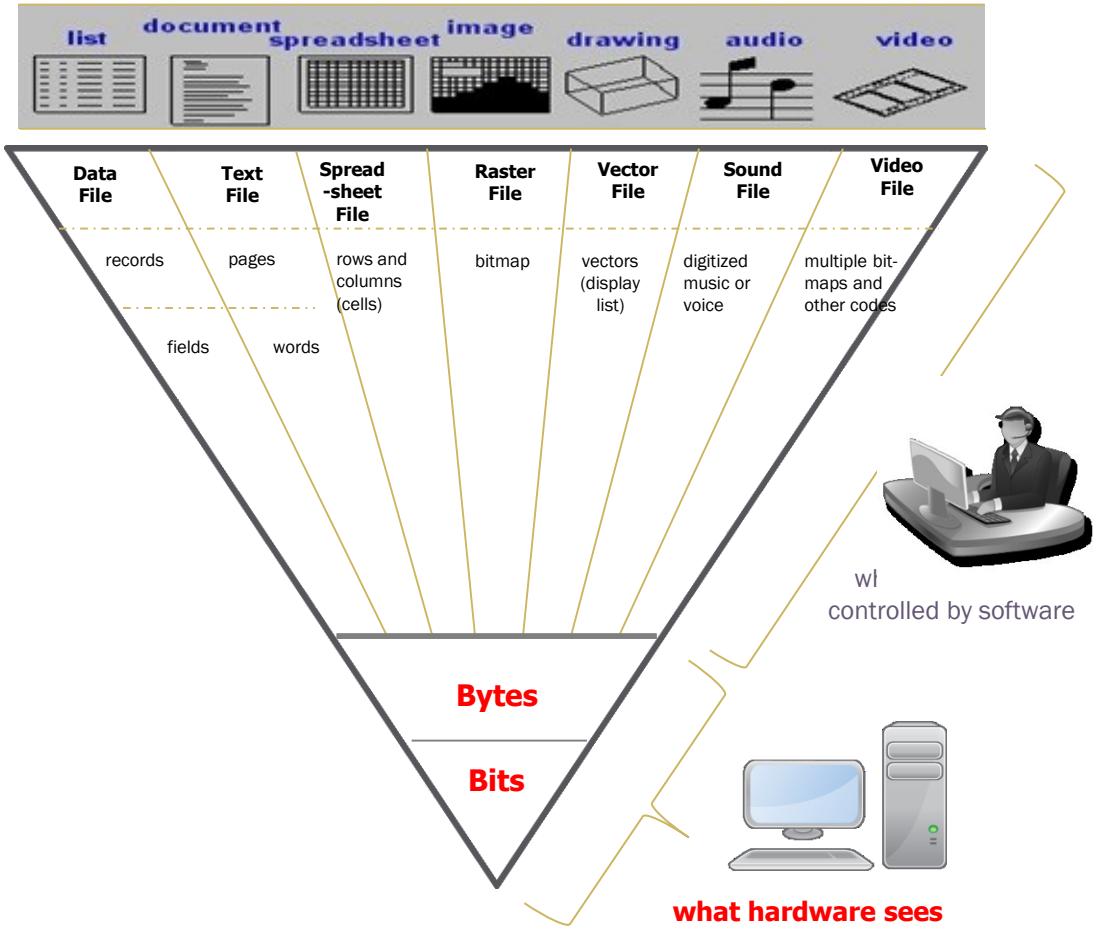
YAB DATO' SRI MOHD NAJIB TUN HAJI ABDUL RAZAK
PERDANA MENTERI MALAYSIA

"Kepentingan kawalan ke atas **rahsia rasmi** dan **aset** Kerajaan perlu sentiasa diberi keutamaan yang tinggi. Ini kerana ia merupakan sesuatu yang tidak ternilai."

YBHG. TAN SRI DR. ALI HAMSA
KETUA SETIAUSAHA NEGARA

"...Information can exist in many forms. It can be printed or written ***on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation.***

Whatever form the information takes, or means by which it is shared or stored, it ***should always be appropriately protected.***"



JENIS/BENTUK MAKLUMAT?

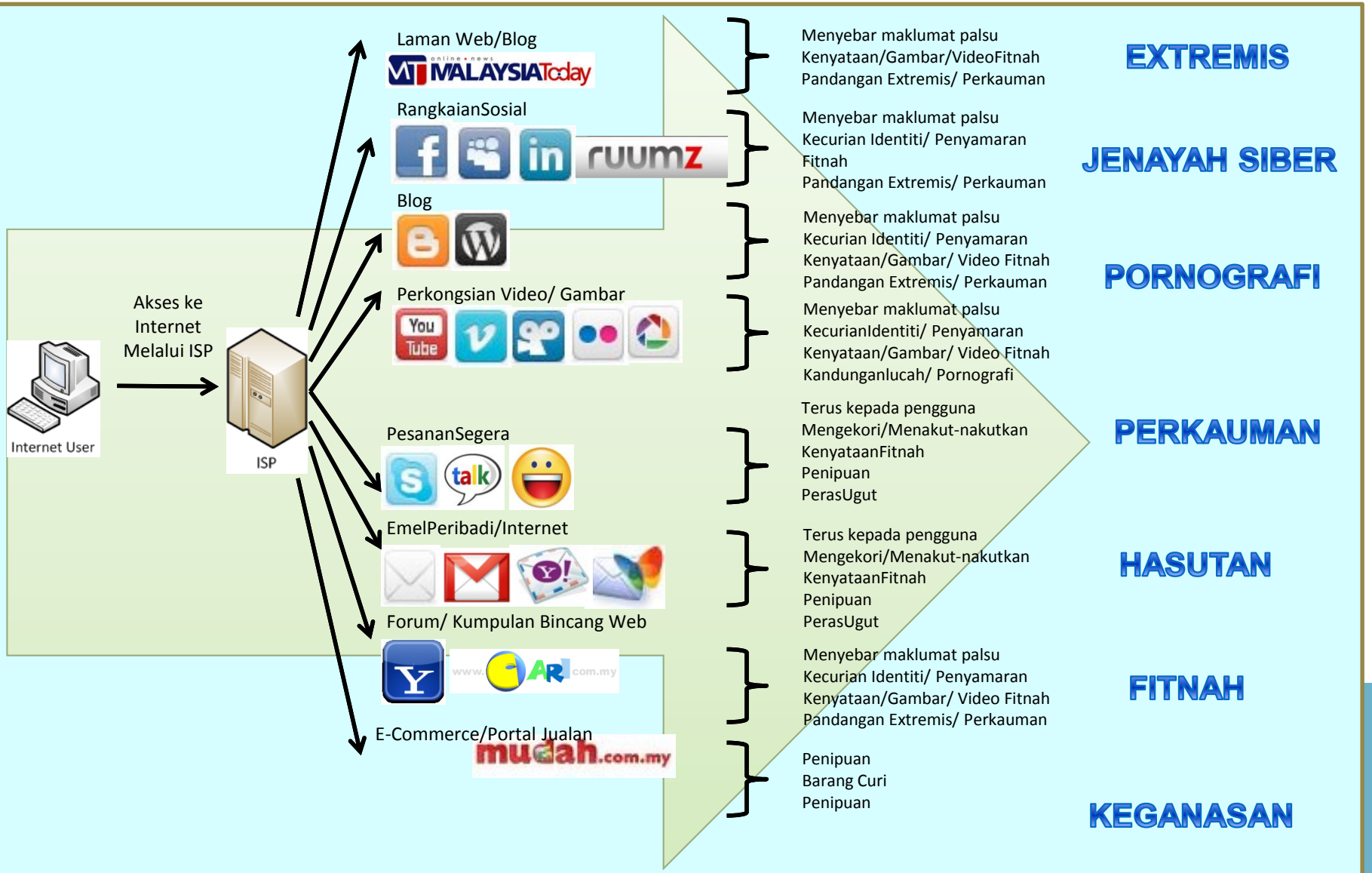
KESELAMATAN MAKLUMAT

“ Perlindungan maklumat dan sistem maklumat daripada sebarang capaian atau akses yang tidak dibenarkan, digunakan, didedahkan, diganggu, diubahsuai atau dimusnahkan oleh mana-mana pihak yang tidak dibenarkan”.

Tafsiran : Arahan keselamatan baharu

(Pindaan 2016)

APAKAH RISIKO ANCAMAN INTERNET/MEDIA SOSIAL?



*** Sumber : SURUHANJAYA KOMUNIKASI MULTIMEDIA MALAYSIA (SKMM)**

The computers gets infected by possibly 3 ways..

Internet

USB

Removable drives (CD rom) , Add on Storage Devices.

- APT (Advanced Persintent Threats)
- RAT / Trojan
- Keyloggers
- Virus
- Worm
- Botnet

- Phishing
- Spam - ransomware
- Man In The Middle Attack
- Social Engineering

- **Email Attachment**
- **Download from Internet**
- **Visiting a malicious webpage**
- **USB / External Hard Drive**
- **Following link in a spam email**
- **Accessing Public Hotspot**

BENTUK ANCAMAN SIBER

ANCAMAN SIBER DI MALAYSIA

Keratan Akhbar

Kandungan Internet
(Laman Web/ Blog/Media Sosial)

Keganasan Siber
Penggunaan Internet oleh pengganas

Jenayah Siber/ Penipuan Dalam Talian
Kerugian wang jutaan Ringgit Malaysia

Infrastruktur Maklumat Kritikal
Sasaran kumpulan pengganas dan penggodam

Maklumat Rahsia Negara
Ketirisan/kecurian maklumat

Kebergantungan Tinggi Terhadap Sistem Elektronik/Internet
Jenayah oleh sindiket/gerakan terancang

KEBOCORAN MAKLUMAT RASMI DAN RAHSIA RASMI DI SEKTOR AWAM

2012 – 2016

TAHUN / MEDIUM	2012	2013	2014	2015	2016 (JUN)
WhatApp/Facebook/SMS	1	-	8	4	-
Laman Web/Blog	1	1	3	5	5
Faksimili/Kenyataan Media	-	2	4	2	-
JUMLAH	**2**	**3**	**15**	**11**	**5**

Kes soalan bocor UPSR macam misteri MH370

» *Mahkamah bebaskan dua guru kerana tiada bukti kukuh*

lan UPSR secara tidak sah, pada September tahun lalu, setel mendapati pendakwaan ga mewujudkan kes prima faci

Beliau sebelum itu mengam masa dua jam untuk memb penghakiman setebal 102 mu surat bagi pertuduhan mem bitkan P Murugan, 37, yang belum ini bertugas di Seko

UPSR subjek Matematik 015/1 di Taman Sri Mawar di sini.

Eksklusif

Hanya satu klik curi data peribadi

» *Taktik terbaharu penjenayah godam e-mel akses maklumat tanpa disedari*

Oleh Syalikha Sazili
syalikha@bh.com.my

Kuala Lumpur

Satu klik pada pautan yang diterima menerusi e-mel boleh menyebabkan seseorang menjadi mangsa sindiket penipuan siber yang mencuri data peribadi.

Kaedah itu menjadi taktik terbaharu penjenayah siber bagi menggodam e-mel tanpa disedari oleh mangsa.

Antara cara dikesan ialah penghantaran e-mel tertera arahan 'klik di sini jika tidak dapat membaca mesej' yang mengandungi pautan khusus.

Apabila mangsa menekan pautan itu, penggodam mendapat akses kepada maklumat senarai kenalan mangsa, termasuk alamat e-mel dan data peribadi.

him, 62, yang pernah menjadi mangsa penipuan internet berkata, mangsa dipercayai dipilih secara rawak.

"Beberapa hari lalu saya menerima e-mel daripada anak lelaki dengan mesej 'klik di sini jika tidak dapat membaca mesej'.

an dibuka oleh penerima kerana nama penghantar adalah kenalan terdekat atau ahli keluarga.

Maklumat sulit

Apa yang membimbangkan, katanya, pelbagai maklumat sulit disimpan dalam e-mel seperti

"Rupanya satu klik membuka ruang kep nayah menggodam m telefon bimbit dan ko ribadi saya.

"Ada rakan menda dapat e-mel yang ko

an menerusi e-mel ber

Eksklusif

Pengintip antarabangsa kerah 'tentera siber'

» *Pakar komputer tempatan syak server mudah diceroboh, curi maklumat*

Oleh Wan Noor Hayati Wan Alias
wanti@bh.com.my

Kuala Lumpur

Pengintip siber antarabangsa disyaki menyerang server (pelayan komputer) di negara ini menggunakan botnet (rangkaian robot) dengan menjadikannya sebagai tentera siber untuk menguasai sistem komputer dan mencuri maklumat.

nuddin, berkata botnet itu yang bertindak sebagai tentera siber boleh menguasai pelayan individu, syarikat atau agensi kerajaan.

"Mereka (penceroboh asing) boleh menggunakan botnet untuk mengambil alih kawalan semua operasi kita yang menggunakan komputer sama ada sistem pengangkutan, perbankan, pertahanan atau kerajaan.

Ceroboh tanpa disedari

"Robot ini dikawal oleh komputer. Sasaran penceroboh adalah server yang tahap pertahanannya rendah atau yang tidak disedari pentadbirnya bahawa serangan itu sedang berlaku.

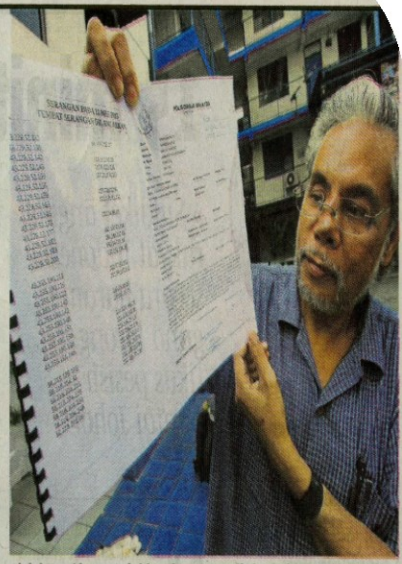
"Bayangkan jika lebih 300,000 server yang ada di seluruh negara diserapi botnet. Botnet ini boleh dijadikan tentera siber untuk melakukan apa sahaja termasuk mengambil alih keseluruhan sistem

mua server kita boleh dikawal oleh penceroboh dari luar negara dan boleh mengeluarkan apa sahaja arahan menggunakan botnet.

"Ketika ini semuanya dikawal komputer. Daripada telefon bimbit, elektrik, air, radar, pengangkutan hingga alat bantuan jantung dan sebagainya. Bayangkan jika seminggu kita tidak boleh keluarkan duit dari mesin pengeluaran automatik (ATM)," katanya kepada *BH*, semalam.

Beliau mengambil contoh bagaimana penceroboh melumpuhkan sistem perbankan Korea Selatan selama 24 jam pada 2013 dengan menyerang 100 server menggunakan botnet.

Abdul Hamid berkata demikian ketika ditemui selepas membuat laporan di Balai Polis Wangsa Maju di sini berikutan serangan terhadap server miliknya, kelmarin.



Abdul Hamid ***menunjukkan laporan polis berkaitan serangan siber terhadap komputer*** *di negara ini, di Balai Polis Wangsa Maju.*

[FOTO SADDAM YUSOFF/BH]

bu serangan sehari, semuanya menggunakan alamat Protokol Internet (IP) dari China dan Israel. Bukti serangan turut diserahkan kepada polis.

Ketua polis balai itu, Superintendan Mohamad Roy Suhaimi Sarif, mengesahkan menerima laporan berkenaan.

Abdul Hamid percaya serangan itu adalah cubaan untuk menjadikan server miliknya sebagai botnet yang boleh dikuasai oleh penceroboh.

tanya, oleh kerana servernya dalam bahasa Melayu tiada sebab orang dari China atau Israel nak capai sistemnya, kecuali mencari dan merekrut botnet.

"Apa yang membimbangkan sampai satu tahap nanti mereka merekrut banyak botnet, negara kita boleh lumpuh sepenuhnya dalam masa beberapa saat sahaja," katanya.

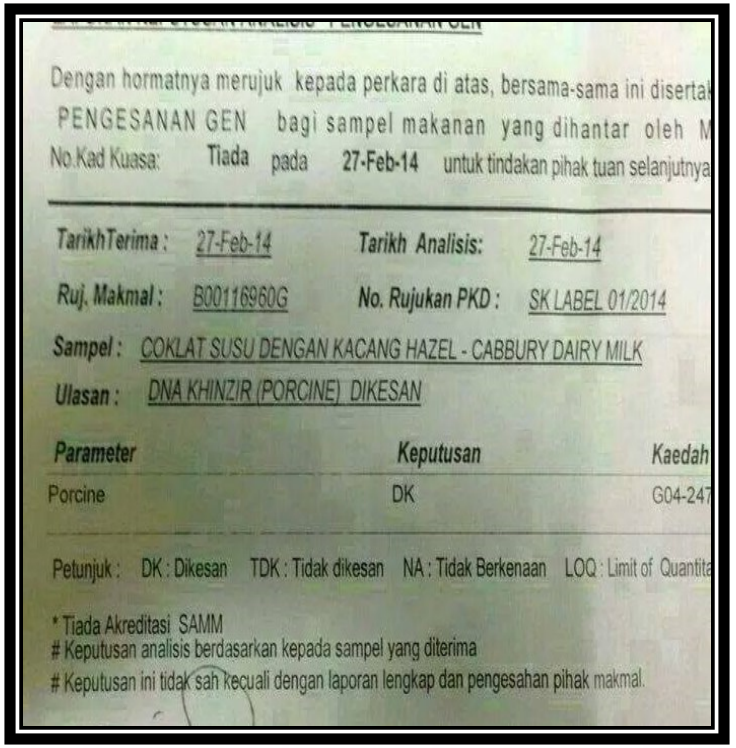
BH dalam laporan eksklusif se jak 4 Mei lalu mendedahkan ha pir setiap hari ruang siber

Tabung Haji sahkan beli tanah 1MDB

Search

FMT Reporters
| May 7, 2015

Tabung Haji bagaimanapun menafikan pembelian Signature Tower (Fasa 2) seperti yang dilaporkan beberapa blog tertentu.



Dengan hormatnya merujuk kepada perkara di atas, bersama-sama ini disertak
PENGESANAN GEN bagi sampel makanan yang dihantar oleh M
No.Kad Kuasa: Tiada pada 27-Feb-14 untuk tindakan pihak tuan selanjutnya

TarikhTerima : 27-Feb-14 Tarikh Analisis: 27-Feb-14
Ruj. Makmal : B00116960G No. Rujukan PKD : SK LABEL 01/2014
Sampel : COKLAT SUSU DENGAN KACANG HAZEL - CABBURY DAIRY MILK
Ulasan : DNA KHINZIR (PORCINE) DIKESAN

Parameter	Keputusan	Kaedah
Porcine	DK	G04-247

Petunjuk : DK : Dikesan TDK : Tidak dikesan NA : Tidak Berkenaan LOQ : Limit of Quantita

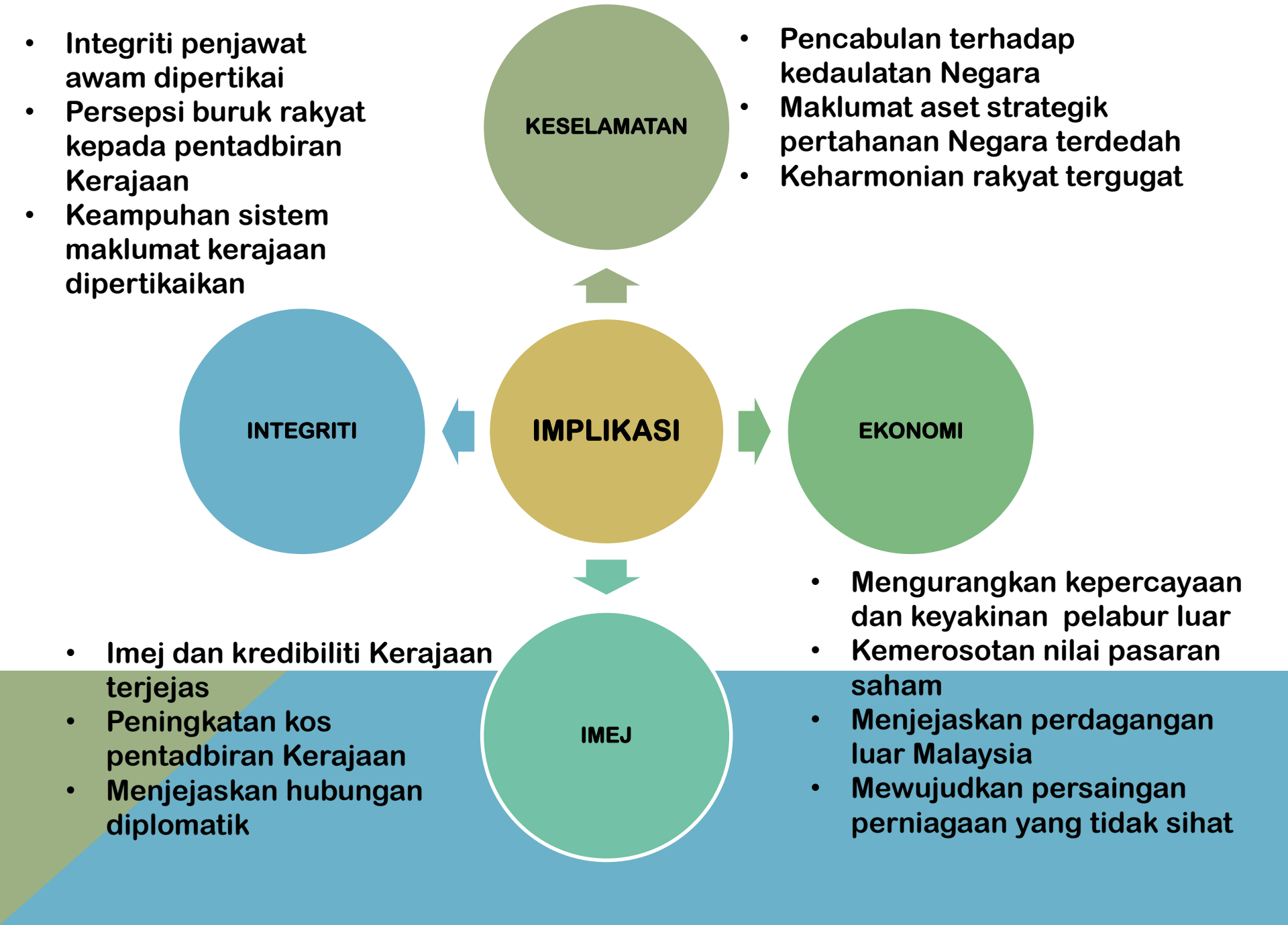
* Tiada Akreditasi SAMM
# Keputusan analisis berdasarkan kepada sampel yang diterima
# Keputusan ini tidak sah kecuali dengan laporan lengkap dan pengesahan pihak makmal.

PETALING JAYA: Lembaga Tabung Haji (TH) mengesahkan membeli sebidang tanah bernilai RM188.5 juta di Pusat Kewangan Tun Razak Exchange (TRX) milik 1Malaysia Development Bhd (1MDB) bagi pembangunan sebuah menara kediaman.

Timbalan Pengarah Urusan Kumpulan dan Ketua Pegawai Eksekutif, Datuk Johan Abdullah, berkata pembelian itu adalah sejajar dengan strategi pelaburan hartanah TH yang memberikan tumpuan kepada sektor domestik.

"Pelaburan ini adalah keputusan komersial yang menepati selera risiko dan telah melalui semua proses penilaian dalaman yang terperinci.

"Pembelian hartanah pada harga RM188.5 juta adalah pada kadar diskaun berlandaskan nilai pasaran semasa dan ia telah dinilai oleh sebuah badan penilai bebas profesional," katanya dalam kenyataan pada Khamis, lapor BH Online.



- Integriti penjawat awam dipertikai
- Persepsi buruk rakyat kepada pentadbiran Kerajaan
- Keampuhan sistem maklumat kerajaan dipertikaikan

- Pencabulan terhadap kedaulatan Negara
- Maklumat aset strategik pertahanan Negara terdedah
- Keharmonian rakyat tergugat

- Imej dan kredibiliti Kerajaan terjejas
- Peningkatan kos pentadbiran Kerajaan
- Menjejaskan hubungan diplomatik

- Mengurangkan kepercayaan dan keyakinan pelabur luar
- Kemerosotan nilai pasaran saham
- Menjejaskan perdagangan luar Malaysia
- Mewujudkan persaingan perniagaan yang tidak sihat

ANTARA KES-KES KEBOCORAN RAHSIA RASMI YANG DILAPORKAN DAN DIAMBIL TINDAKAN

- Pendedahan tidak terkawal salinan asal Buku Arahan Keselamatan di dalam portal / laman web.
- Mendedahkan dokumen berkaitan cadangan kenaikan kadar tol di blog.
- Mendedahkan maklumat mengenai kemasukan bot pancung dipercayai pengganas Sulu melalui Whatsapp.
- Mendedahkan Hasil ujian makmal ke atas Coklat susu dengan kacang hazel – (DNA Khinzir *Porcine* dikesan) di Facebook.
- Mendedahkan kertas soalan peperiksaan UPSR 2014 di laman sosial.
- Menyebarkan *Force Deployment* OPS Tayang melalui aplikasi Whatsapp.
- Mendedahkan Siasatan Kes Kecurian Kenderaan melalui faksimili.

BAGAIMANA KEBOCORAN MAKLUMAT BOLEH BERLAKU?

Mengambil gambar dokumen rasmi / rahsia rasmi menggunakan telefon bimbit dan pelbagai peranti elektronik (milik peribadi).

Tiada kawalan salinan *softcopy* sebagai fail kepilan (*attachment* - salinan kepada (*cc*) dan dimajukan (*forward*)).

Penggunaan *public email (yahoo mail)* dalam urusan rasmi Kerajaan.

Memuat naik (upload) dokumen rasmi / rahsia rasmi dalam media sosial dan *cloud (cth: dropbox, amazon dsb)*.

Menulis maklumat *login* dan kata laluan dan menampalnya di skrin komputer atau *keyboard* dll.

Melaksanakan tugasan rasmi secara jarak jauh.

Berkongsi komputer / katalaluan untuk mengimbas dokumen (*scanner*).

BAGAIMANA KEBOCORAN MAKLUMAT BOLEH BERLAKU?

Meninggalkan pejabat dengan membawa peralatan mudah alih yang menyimpan rahsia rasmi.

Mengakses emel rasmi menggunakan *wireless hotspot* di tempat awam.

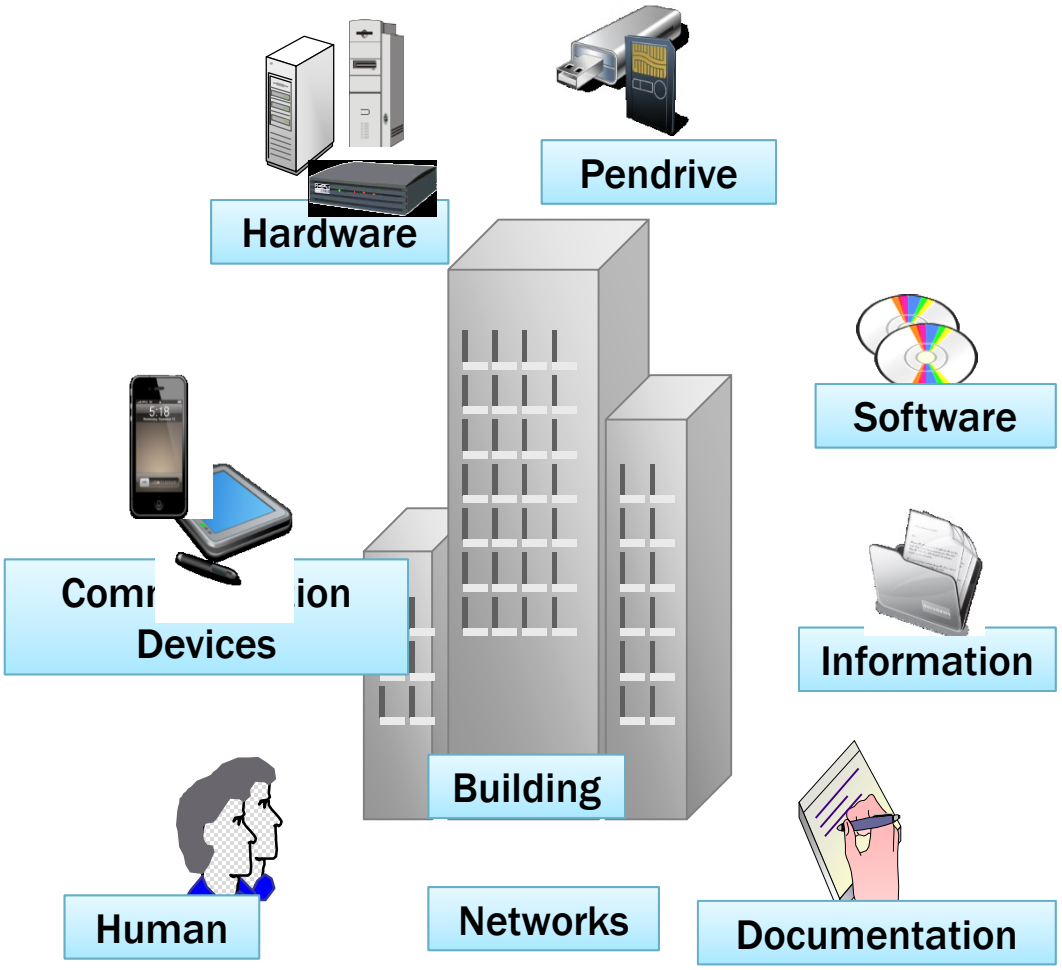
Menyalin dan membawa keluar maklumat Jabatan dengan menggunakan media storan seperti USB, *external HD* dsb

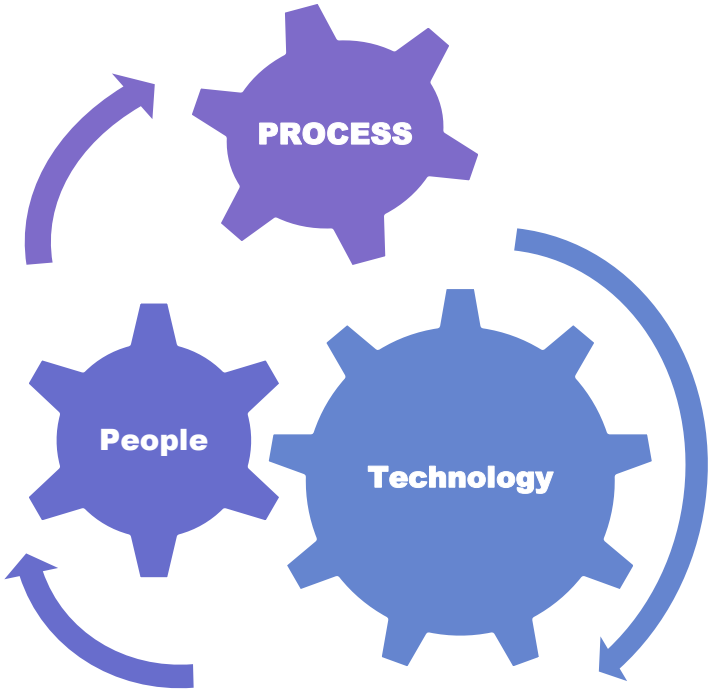
Memadam dokumen elektronik tanpa merincih secara elektronik.

Meninggalkan komputer tanpa '*logoff / lockscreen*' komputer di ruang pejabat yang terbuka.

Berkongsi atau tidak menukar kata laluan mengikut peraturan yang ditetapkan.

‘SECURITY IN-DEPTH’





ASET DAN MAKLUMAT DILINDUNGI MELALUI KONSEP ‘ SECURITY IN-DEPTH’ KEPADA DATA DLM PENGGUNAAN, DATA SEDANG DIPINDAHKAN DAN DATA DALAM STORAN

RUMUSAN

KES KEBOCORAN/KETIRISAN MAKLUMAT KERAJAAN

Pegawai Awam tidak mematuhi sepenuhnya pengurusan melindungi keselamatan dokumen dan maklumat termasuk dalam persekitaran ICT.

Kurangnya integriti dan akauntabiliti pegawai awam dalam melindungi kerahsiaan maklumat rasmi dan rahsia rasmi.

Kurangnya program kesedaran keselamatan untuk pegawai awam yang menguruskan maklumat rahsia rasmi.

Penguatkuasaan dan pemantauan pegawai penyelia serta pegawai atasan tidak menyeluruh.

Kurangnya program bagi meningkatkan pengetahuan dan kemahiran pegawai awam bagi melindungi maklumat rahsia rasmi dalam persekitaran ICT.

LANGKAH-LANGKAH PENAMBAHBAIKAN

Meminda Arahan Keselamatan dengan memasukan perkara -

KESELAMATAN RAHSIA RASMI DALAM PERSEKITARAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

Inisiatif MAMPU dan CGSO bagi menyediakan Dasar Perlindungan Ketirisan Maklumat Kerajaan dan Sistem DLP

Perolehan, penyediaan kelengkapan keselamatan seperti produk sanitasi dan enkripsi – software & hardware

Program NBOS bersama Agensi bagi meningkatkan kesedaran keselamatan maklumat rahsia rasmi dalam persekitaran ICT

Pemantauan dan penyeliaan berkesan dari pegawai penyelia / pegawai atasan

Menyemak dan Meminda Akta Rahsia Rasmi 1972 [AKTA 88]

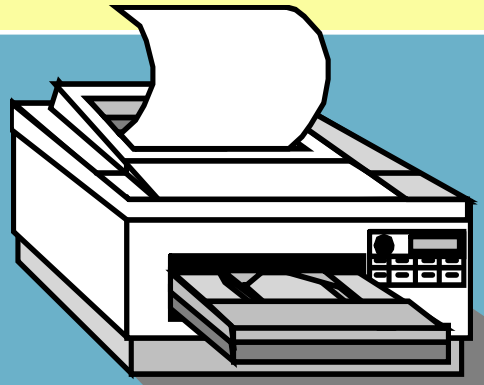
Komitmen, integriti dan sikap bertanggungjawab setiap individu penjawat awam sangat penting sebagai faktor kejayaan bagi menangani kebocoran maklumat Kerajaan.

RAHSIAKAN RAHSIA KERAJAAN

Rakyat Didahulukan, Pencapaian Diutamakan

KESIMPULAN

Bagi menanggani isu kebocoran maklumat Kerajaan langkah-langkah dan tindakan holistik dari pelbagai sudut perlu dilaksanakan meliputi elemen proses, teknologi dan manusia. Semua pemilik maklumat perlu memantapkan tadbir urus keselamatan, tingkatkan pematuhan peraturan, perkasakan keupayaan teknologi dan terapkan budaya keselamatan perlindungan.



Sekian,

Terima kasih.

Bahagian Keselamatan ICT dan Rahsia Rasmi
Pejabat Ketua Pegawai keselamatan Kerajaan Malaysia
Jabatan Perdana Menteri