KONFERENSI ICT 2022

UNIVERSITI TEKNOLOGI MARA

Pejabat Pembangunan Infrastruktur dan Infostruktur

Strengthening Your Cybersecurity Beyond Vulnerabilities

22 November 2022

ICT CONFERENCE 2022

EMBRACING DIGITAL LEARNING TRANSFORMATION

INFOSTRUCTURE OFFICE • UiTM

ASSOC. PROF. COL. (R)
DATO' TS DR HUSIN JAZRI
CYBERCRIMES WATCH

Speaker Summary Profile

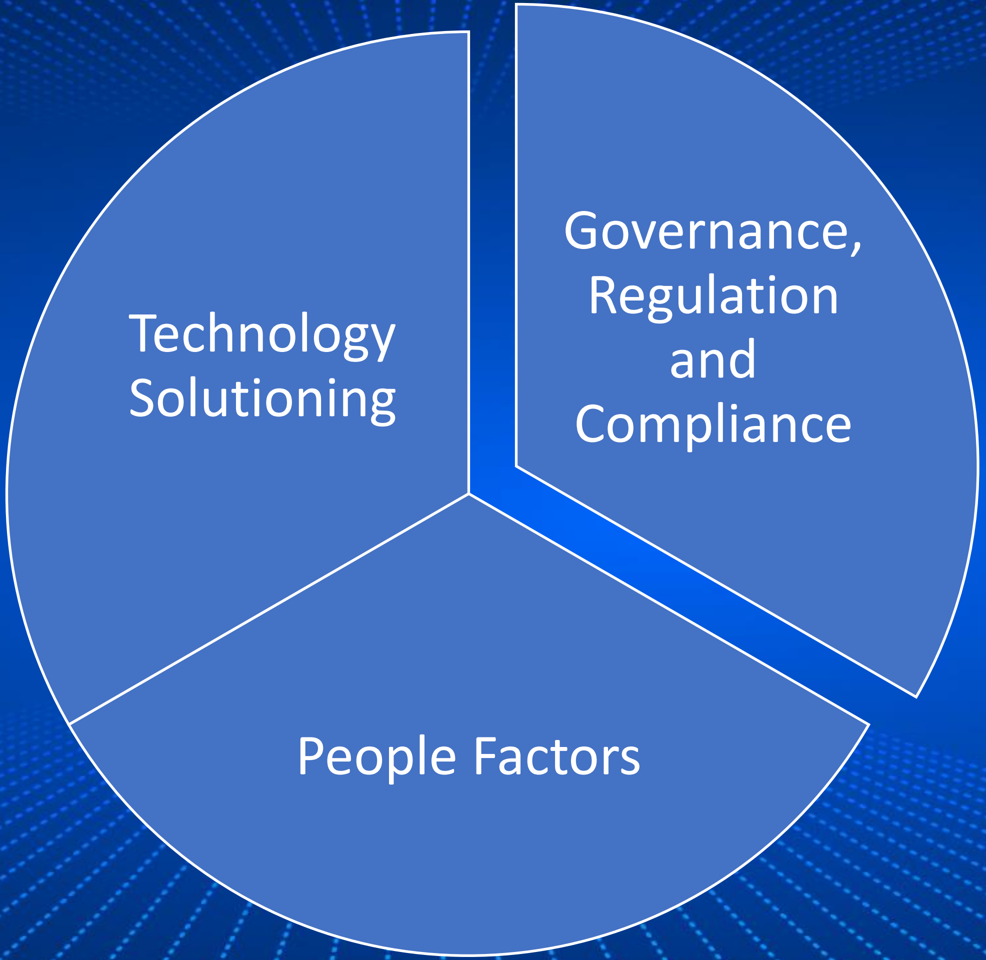
ICT CONFERENCE 2022 · INFOSTRUCTURE OFFICE · UiTM
EMBRACING DIGITAL LEARNING TRANSFORMATION

ASSOC. PROF. COL. (R)
DATO' TS DR HUSIN JAZRI
CYBERCRIMES WATCH

Dato' Dr Jazz
Father of Cybersecurity

- -ISC2 Harold Tipton Lifetime Cybersecurity Award
- -Founder Cybersecurity Malaysia
- -Founder OIC CERT
- -Co Founder APCERT
- -Founder Cyber999
- -Founder Common Criteria Malaysia
- -Founder CyberSAFE
- -Founder CyberClinic
- -Founder Digital Forensic Malaysia
- -Founder ESPC Media
- -Best Professor NUST, Namibia
- -Former Prof Asia Pacific Univ, Malaysia
- -Prof UniMy, Malaysia
- -Director Serba Dinamik Cybersecurity
- -Chief Editor eSecurity & Privacy Channel
- -Executive Chairman Cybercrimes Watch

Segmentation of Cybersecurity



Question 1 : Which one is the most complex issue to address?

Question 2: Which one is the easiest issue to address?

Question 3: Which one is the most invested segmentation by enterprises and governments ?

ICT CONFERENCE 2022 · INFOSTRUCTURE OFFICE · UiTM
EMBRACING DIGITAL LEARNING TRANSFORMATION

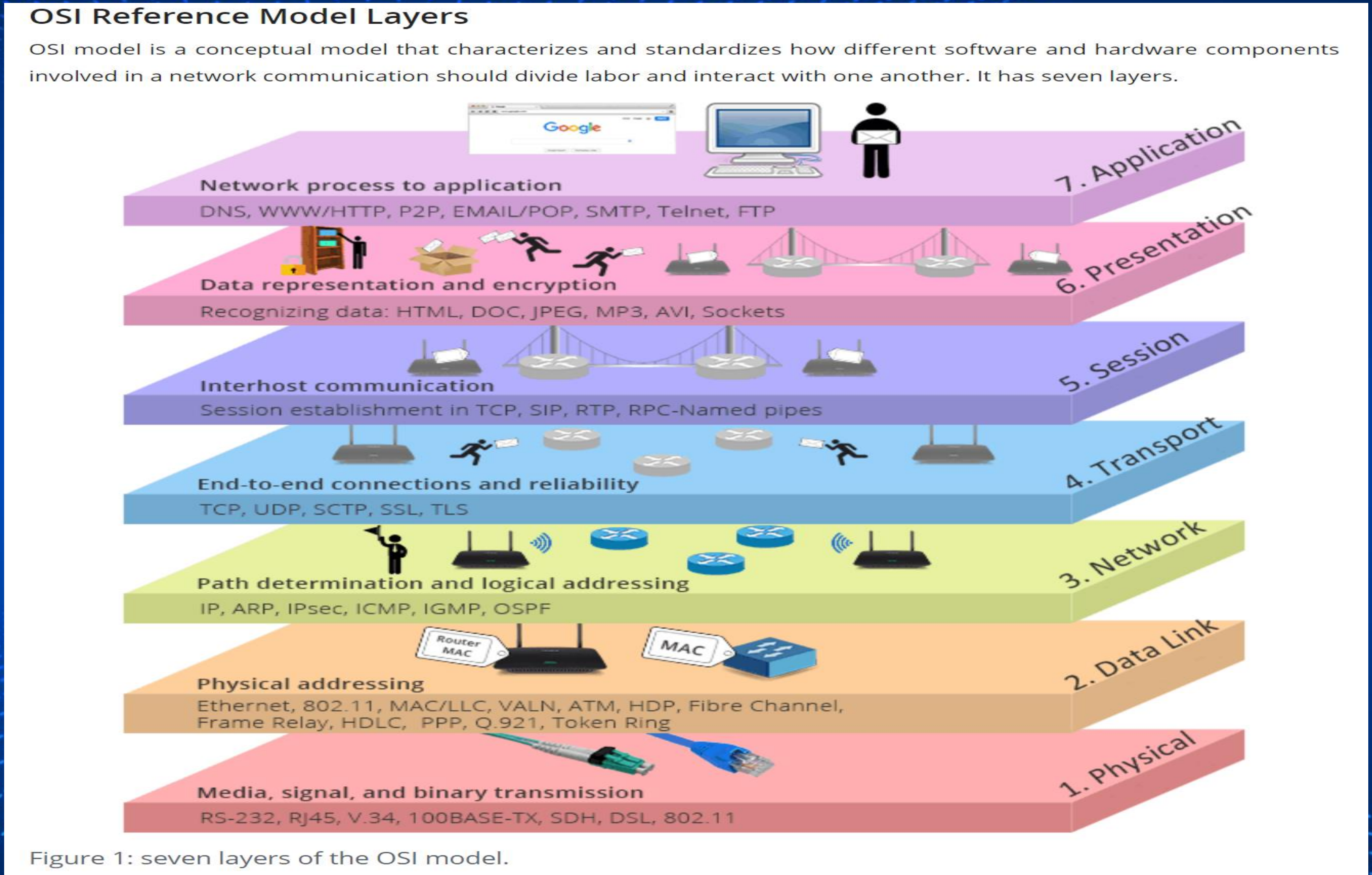
ASSOC. PROF. COL. (R)
DATO' TS DR HUSIN JAZRI
CYBERCRIMES WATCH

Q4: Are all three segmentations are address here ?

ICT CONFERENCE 2022 • INFOSTRUCTURE OFFICE•UiTM

EMBRACING DIGITAL LEARNING TRANSFORMATION

ASSOC. PROF. COL. (R)
DATO' TS DR HUSIN JAZRI
CYBERCRIMES WATCH



OSI Reference Model Layers

OSI model is a conceptual model that characterizes and standardizes how different software and hardware components involved in a network communication should divide labor and interact with one another. It has seven layers.

7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP

6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets

5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes

4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS

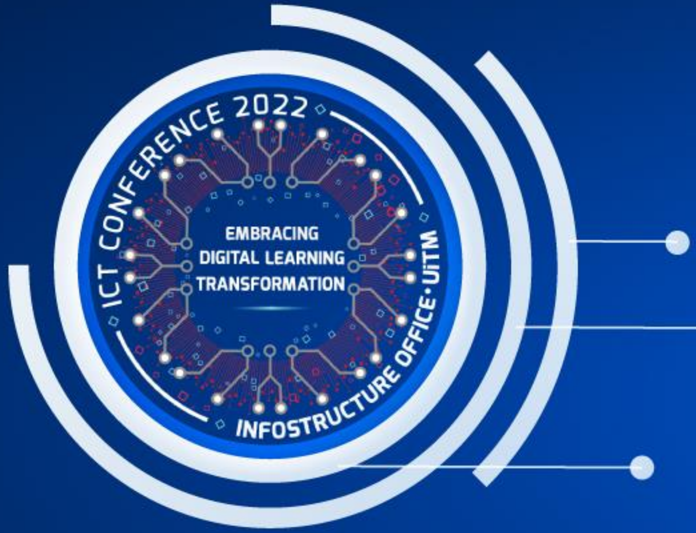
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF

2. Data Link
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring

1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

Figure 1: seven layers of the OSI model.

Cybersecurity & Privacy – Grumble Notes


ICT CONFERENCE 2022
EMBRACING DIGITAL LEARNING TRANSFORMATION
INFOSTRUCTURE OFFICE · UiTM

- Have we really solved the humanity problems or creating another ?
- After more than 30 years, cybercrimes are not coming down and why?
- Fire fighting efforts and soon we can be very tired?
- The agony of being a victim is much more than the burden of preventing it !
- Is it an unsolvable problem technically speaking?
- Are we looking at a wrong perspective?
- Are we not looking good enough?
- Or maybe the OSI model is not yet complete?
- Or perhaps it is time to complete or perfected it?

**ASSOC. PROF. COL. (R)
DATO' TS DR HUSIN JAZRI**
CYBERCRIMES WATCH

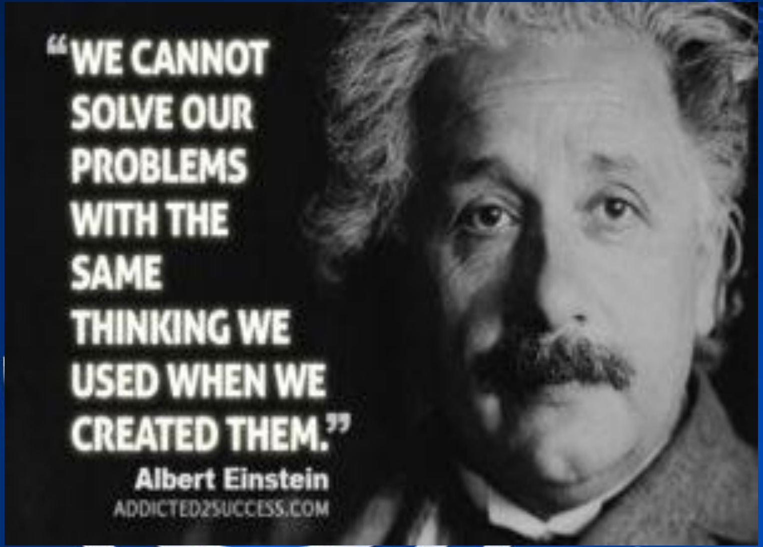
Human Layer – Why Do We Need It ?

ICT CONFERENCE 2022
EMBRACING DIGITAL LEARNING TRANSFORMATION
INFOSTRUCTURE OFFICE · UiTM

- Limitation of OSI Layer 1 – 7 (Technical Centric Perspectives)
- Legal approaches are not fast enough to reduce the numbers
- Victims cannot afford the legal fees and waiting time, not to mention uncertainties of getting back what was stolen
- Challenges in managing crimes in the digital space, if not addressed can be like the pandemic that we are facing now.
- Universe is set in balance, and extreme imbalances will destroy humanities and natural ecosystems
- Complexity in OSI Layer 1 – 7 are not well transited to reach human comprehension properly. Gaps existed and can be exploited.
- People – Process – Technology considered under OSI Layer 1-7 may not be in the right balance.

ASSOC. PROF. COL. (R)
DATO' TS DR HUSIN JAZRI
CYBERCRIMES WATCH

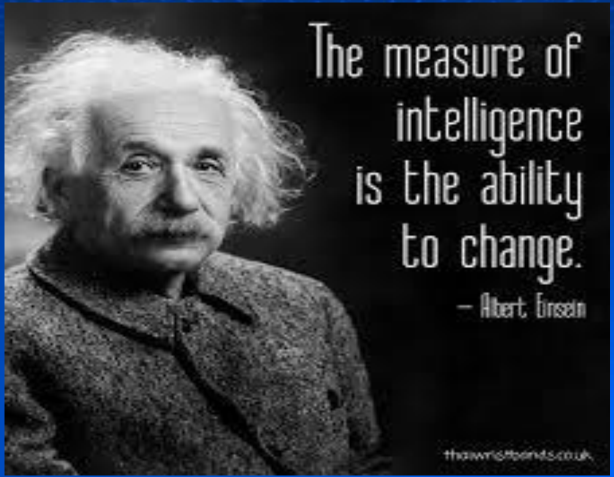
Words of Wisdoms : We already know but we may forget !



"WE CANNOT SOLVE OUR PROBLEMS WITH THE SAME THINKING WE USED WHEN WE CREATED THEM."

Albert Einstein

ADDICTED2SUCCESS.COM



The measure of intelligence is the ability to change.

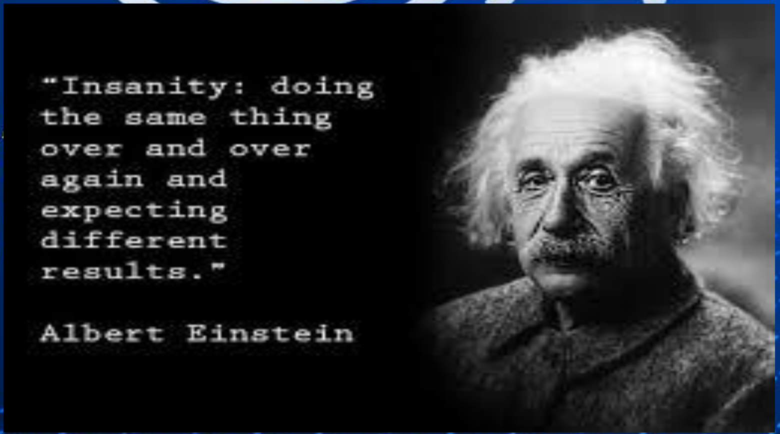
– Albert Einstein

thewristbands.co.uk

Without changing our pattern of thought, we will not be able to solve the problems we created with our current patterns of thought

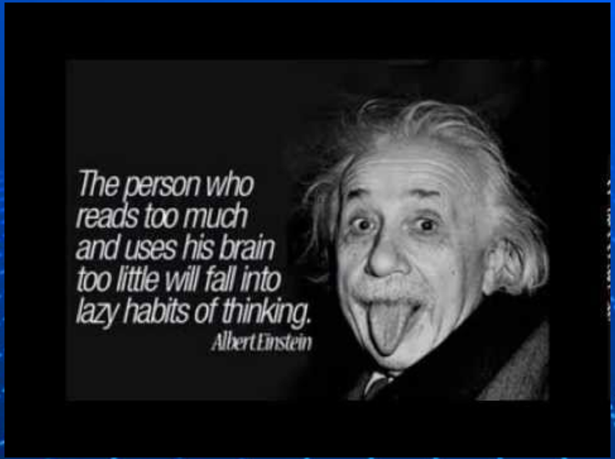
— Albert Einstein —

AZ QUOTES



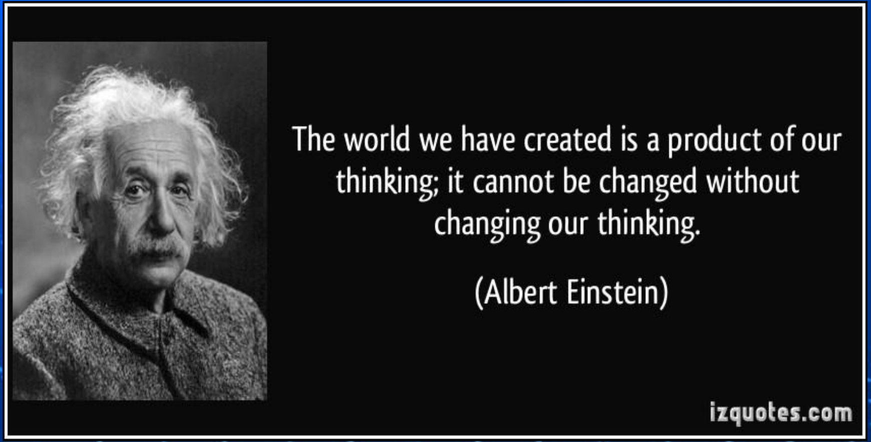
"Insanity: doing the same thing over and over again and expecting different results."

Albert Einstein



The person who reads too much and uses his brain too little will fall into lazy habits of thinking.

Albert Einstein



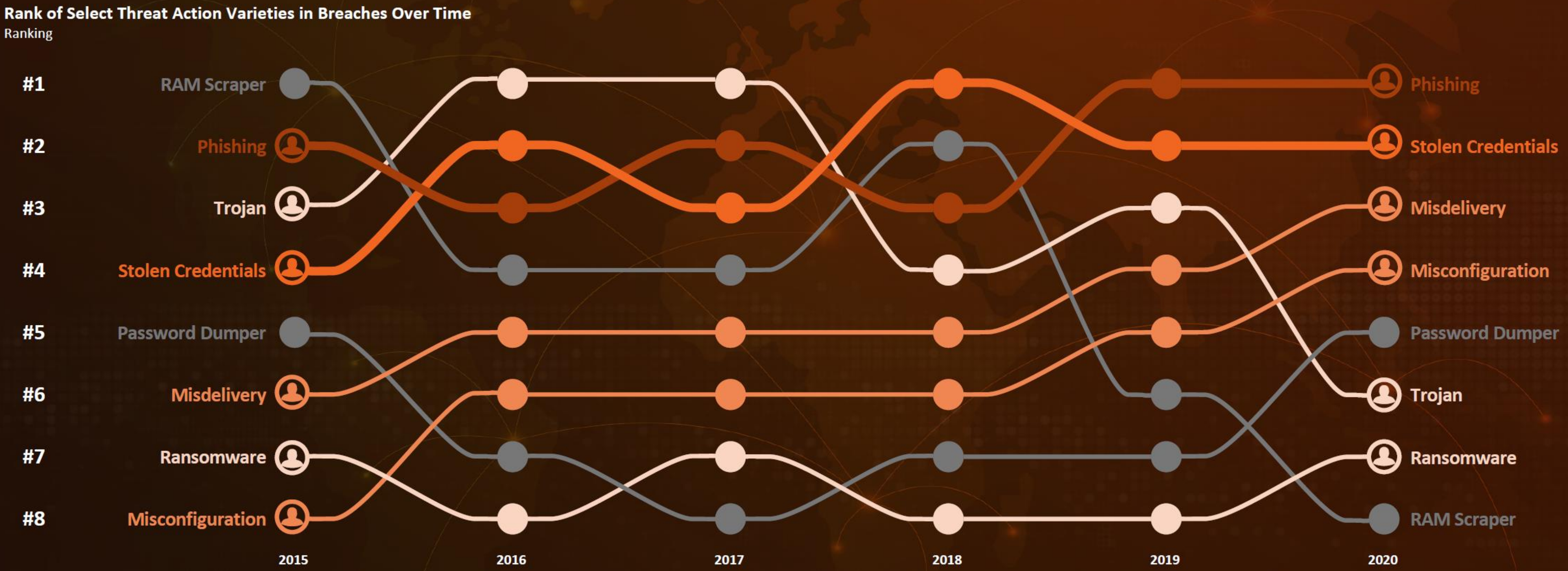
The world we have created is a product of our thinking; it cannot be changed without changing our thinking.

(Albert Einstein)

izquotes.com

People are a critical layer within the fabric of our Security Programs

Humans Have Always Been the Weakest Link in Security



The human layer represents a **high value and probability target** at **low time and cost** to implement for attackers

Source: Verizon 2020 Data Breach Investigations Report

KnowBe4
Human error. Conquered.

How Do You Manage the Ongoing Problem of Social Engineering?

Baseline Testing

We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

Train Your Users

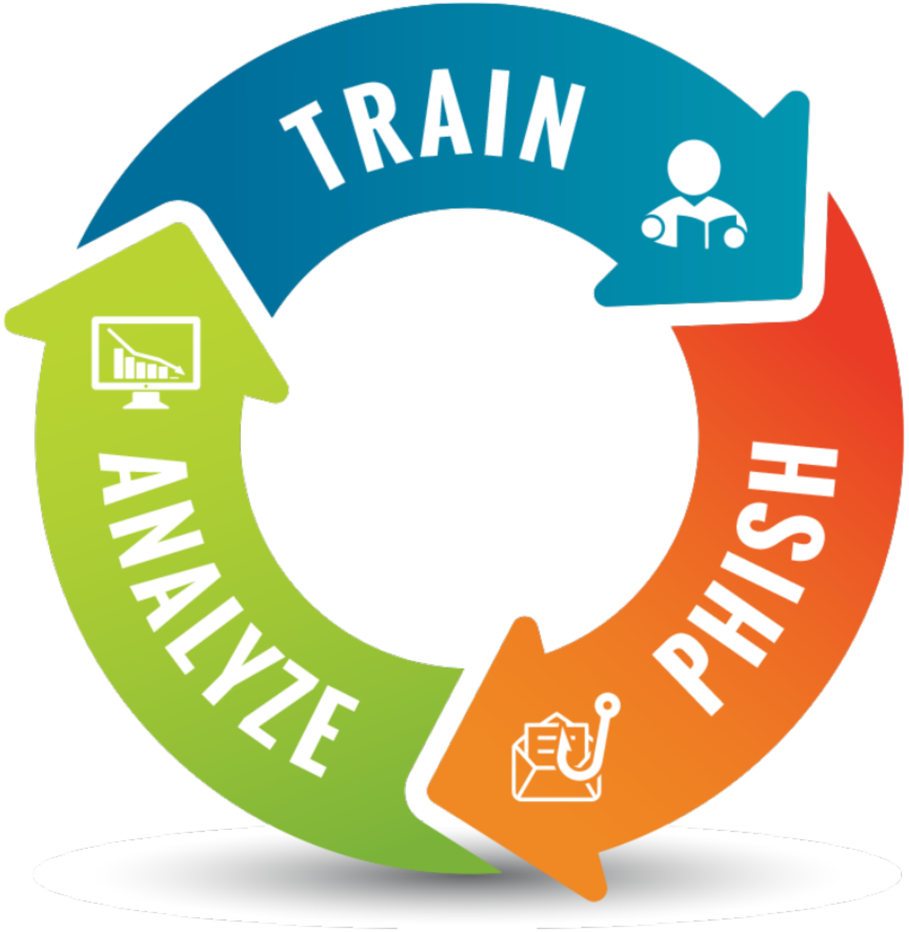
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users

Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results

Enterprise-strength reporting, showing stats and graphs for both security awareness training and phishing, ready for management. Show the great ROI!

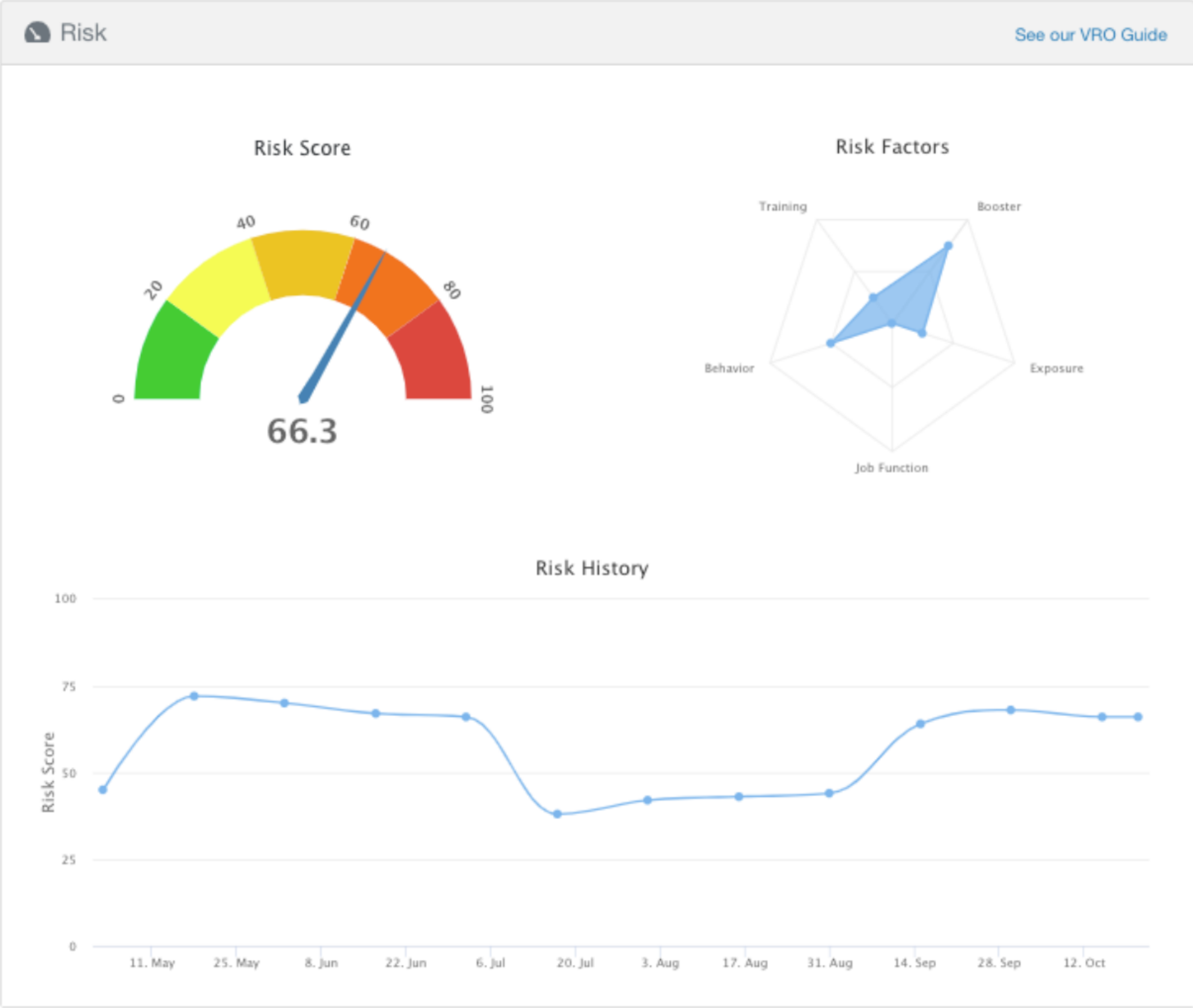


Virtual Risk Officer™

- **Identify risk** at the user, group, and organizational level to enable you to make data-driven decisions for your security awareness plan.

- With Virtual Risk Officer's **Risk Score**, answer questions like:
  - What users are the most vulnerable to a phishing attack?
  - What groups haven't had any training?
  - What types of phishing templates are my users most prone to clicking?
  - What are my highest-risk groups?

- Risk Score enables you to take action and **implement security awareness mitigation plans** for high-risk user groups



EXECUTIVE SUMMARY – Human Behavioural Analysis: Scientific Approach

391 users monitored on 417 devices

36% users exhibited high to medium risks

4 risky modes of PII data handling detected

6 risky user behaviours detected

A data security risk assessment was conducted for Sample Pty Ltd from 12th August to 9th September 2019. The assessment involved monitoring PII and general data movement trends from various data stores.

The risks levels high, medium, and low are defined based on the NDB Scheme, the accuracy of the detected data, and risky user behaviour, in line with current industry trends.

- High Risk involves credit card data and suspicious user activity.
- Medium risk involves TFN, Medicare and risky user activity.
- Low risk involves general PII data and potential risky user activity.

Notable risks included transfer of sensitive PII data in an unsecured manner using USB storage, emails, and cloud services. Large caches of PII were also found stored on local drives. Other findings included the use of personal cloud services, transfer of information when connected to non-corporate networks, and printing using non-corporate printers.

The tables summarise these findings from a user perspective, which are presented in more detail throughout the report. Recommendations for reduction in risk is included in at conclusion of the report. Please contact us should further details be needed to identify a security risk.

Number of users who exhibited risky handling of PII data

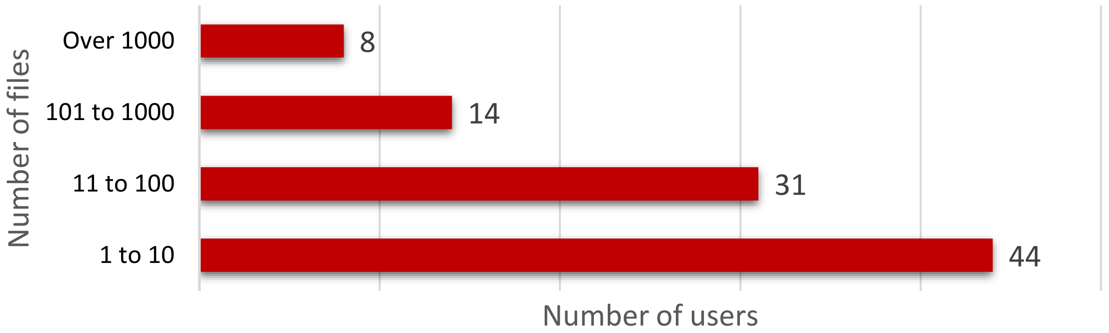
User actions	High Risk	Medium Risk	Low Risk
USB usage	5	16	
Use of cloud and Websites	5	8	
Email Activity	11	37	
Storing PII data in local devices	37	115	262

Number of users exhibiting general risky behaviours

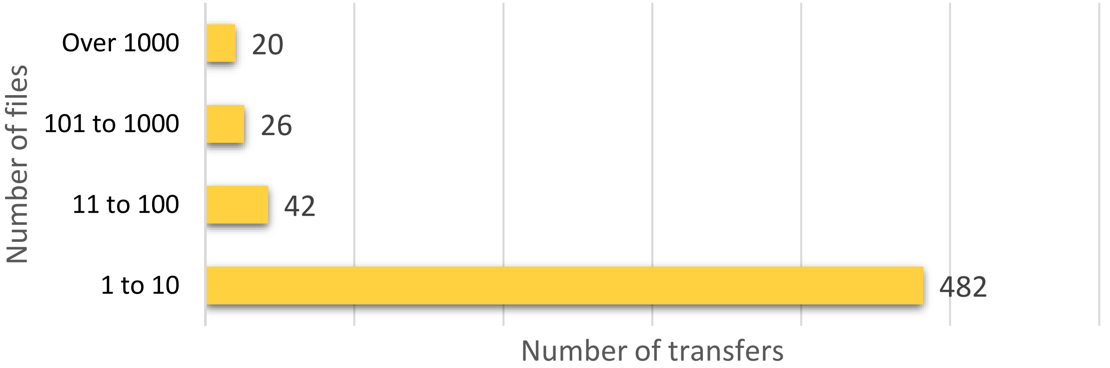
User actions	High Risk	Medium Risk	Low Risk
USB usage	8	98	
Use of non-corporate cloud and websites		42	46
Email Activity		29	221
Non-corporate network usage	14		84
Non-corporate printer usage		14	
Non-corporate application usage		19	

File Transfers To USBs

Number of users transferring files to USBs by file volume (High to Medium Risk)



USB file transfer incidents by volume of files transferred per hour (High to Medium Risk)



Users with over 1000 sensitive files transferred to USB storage	8	High risk
Users with high rate of sensitive files transfers outside working hours	1	High risk
Users transferring sensitive files to USB storage	98	Medium risk
Number of sensitive files transferred to USB storage	59541	

The use of USB storage may be for legitimate reasons and unavoidable, but there are significant risks involved.

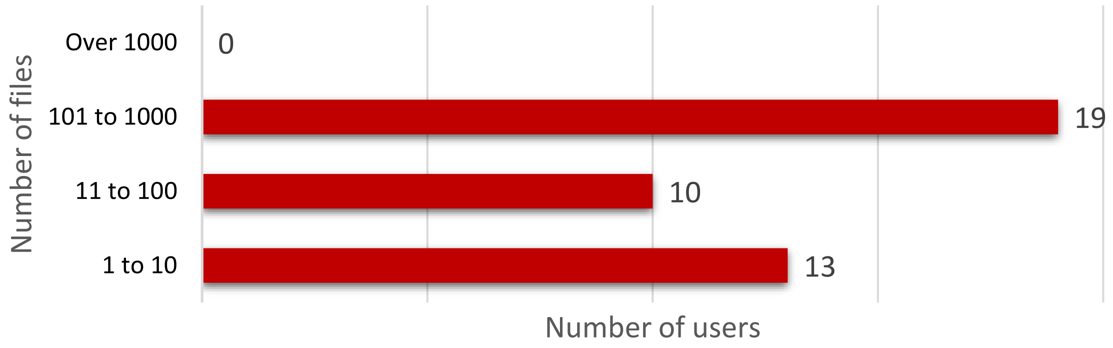
Risk. High transfer rate over a short duration of time is a typical indicator of deliberate data theft and should be reviewed.

Risk. Large transfer of information outside working hours, especially on weekends, can be an indication of attempted data theft and should be reviewed.

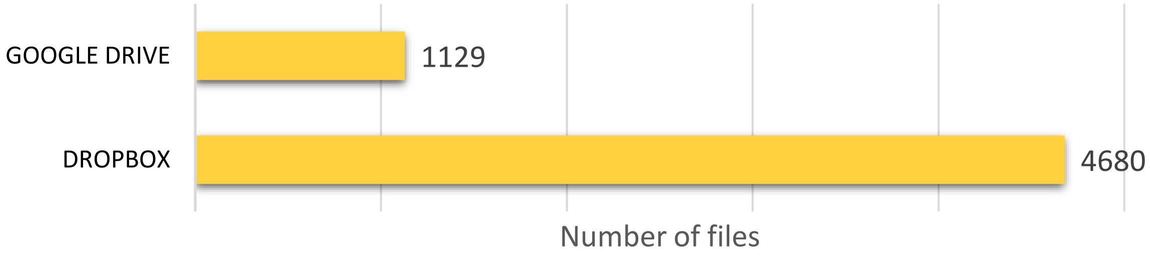
Risk. Loss of information due to information creep. Large movement of data onto USB storage devices indicates a movement of data away from the established information stores.

Non-Corporate Cloud Usage (All files)

Users transferring files to non-corporate cloud providers by volume (Medium Risk)



Number of files transferred in total to non-corporate cloud providers (Medium Risk)



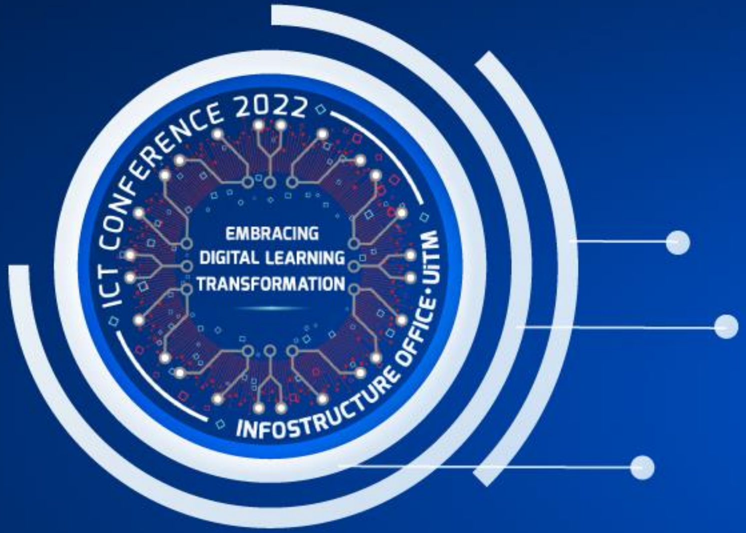
Users transferring files via non-corporate cloud services	42	Medium risk
Number of files transferred on non-corporate cloud services	5809	

The use of personal cloud services and applications may be for legitimate reasons, but there are significant risks involved.

Risk. Unauthorised access by former staff members. Information stored in personal cloud account remains with its user after he leaves a company and therefore can result in a breach as per NDB Scheme.

Risk. Applications like Dropbox, OneDrive, and Google Drive sync files to any device where a user is logged into these applications. This may include their personal devices or, even worse, those of a different company, which could result in the loss of sensitive information.

More Questions:



Q4 – How many OSI Layer ?

Q5 – Has OSI layer 8 being designed ?

Q6 – Weakest link in cybersecurity ?

ASSOC. PROF. COL. (R)
DATO' TS DR HUSIN JAZRI
CYBERCRIMES WATCH

Thank You for Your Attention

ICT CONFERENCE 2022
EMBRACING DIGITAL LEARNING TRANSFORMATION
INFOSTRUCTURE OFFICE · UiTM

- Contact Details:
    - Personal Email – drhjazri@gmail.com
    - Official Email – drjazz@cybercrimeswatch.com.my
    - Mobile/Whatsapp/TG : 019 868 1892

ASSOC. PROF. COL. (R)
DATO' TS DR HUSIN JAZRI
CYBERCRIMES WATCH