MAPITA

MINISTRY OF COMMMUNICATIONS AND DIGITAL

CyberSecurity MALAYSIA

CYBER HYGIENE AND CYBER RESILIENCE

16th of August 2023

JAZANNUL AZRIQ BIN ARIPIN
Manager, Outreach & Corporate Communications
CyberSecurity Malaysia

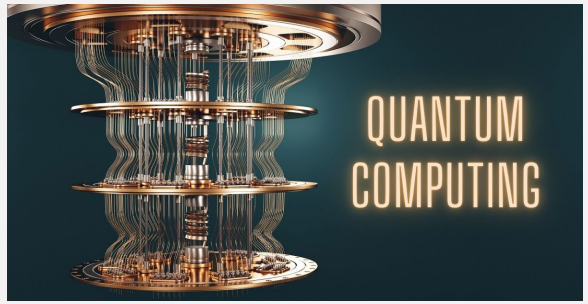
SECURING OUR CYBERSPACE

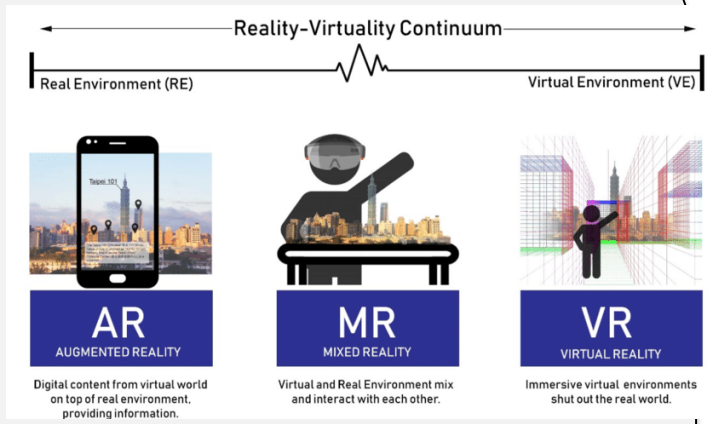
WE ARE MOVING INTO A MORE INTERCONNECTED CYBERSPACE

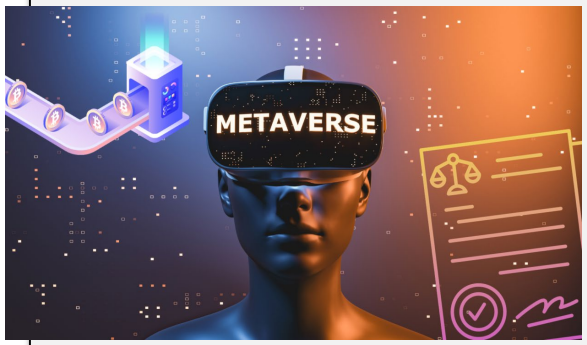
Digital 2023: Global Overview Report — DataReportal – Global Digital Insights

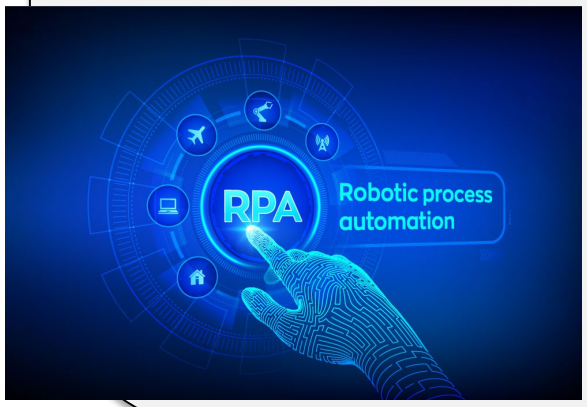
CONVERGENCE OF TECHNOLOGIES

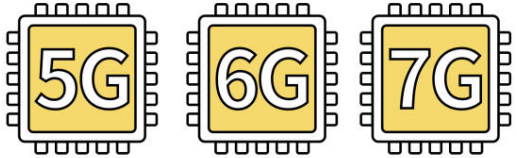
Add More Complexities to Cyber Space





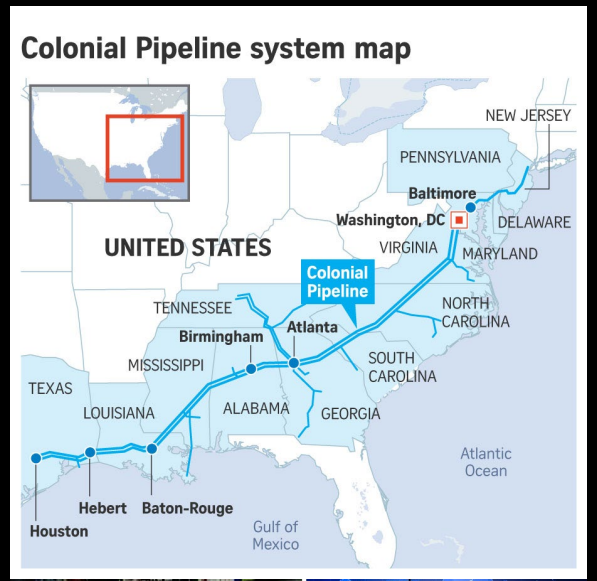


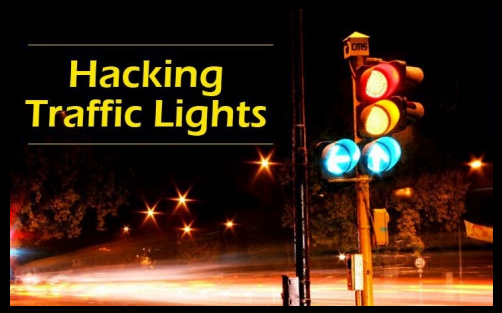




DIGITAL TRANSFORMATION IS NOT WITHOUT ITS **RISK**

CYBER-ATTACKS MAY HAVE PHYSICAL CONSEQUENCES





Technology such as wireless technology has changed the way we conduct business, offering workers with constant access to business-critical applications and data. While this flexibility is convenient and expands productivity, it ***introduces complexity and security risk*** *as these new technology and devices become* ***new target for hackers*** *looking to infiltrate a corporate network.*

EVOLUTION OF CYBER THREATS

Tools and techniques has also evolved from Viruses to the Ransomware attacks that have high pay off for the cyber-criminal community.

2004

- **Malware**
- Worms
- Trojan

2007

- **Social Engineering**
- Impersonate
- Theft
- **Phishing**

2010

- DNS Attack
- Botnets
- SQL Attacks
- Anti-Spam
- Sites
- Competitive
- Sabotage

2013

- Social Engineering
- **DoS**
- Botnets
- Malicious Email

Present

- Banking malware
- Key Logger
- Bitcoin Stealer
- Identity Theft
- Phone Hijacking
- Cyber Warfare
- Mobile Attacks
- APT
- DDoS
- Ransomware
- **Man in Middle Attack**

THE MORE WE ARE INTERCONNECTED THE MORE WE ARE EXPOSED GLOBALLY

Possible Cyberattack Disrupts The Philadelphia Inquirer

The Inquirer, citing "anomalous activity" on its computer systems, said it was unable to print its regular Sunday edition and told staff members not to work in the newsroom at least through Tuesday.

3CX's supply chain attack was caused by…another supply chain attack

Carly Page @carlypage_ / 8:00 PM GMT+8 • April 20, 2023

Russian Man Charged for $200 Million in Ransomware Crimes Involving Crypto

Author: Andrew Throuvalas • Last Updated May 21, 2023 @ 07:30

The hacker was allegedly involved with multiple ransomware strains that attacked police departments, hospitals, and the Colonial Pipeline.

Toyota Japan confirms decade-long security breach affecting more than 2M customers

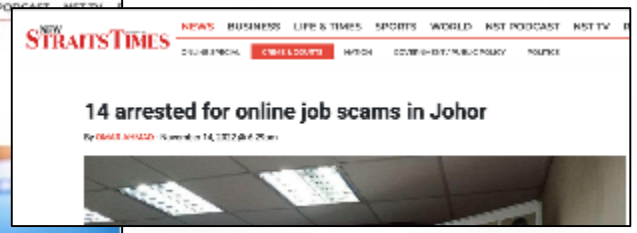
by The Gurus — May 19, 2023 in Featured

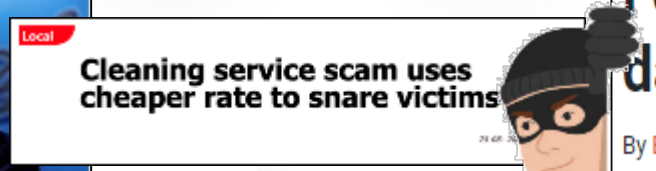
Cyberattack On European Spacecraft! How 'Hackers' Took Control Of Satellite's Imaging Sensors & Jeopardized Its Data

EUROPE EXPERT REVIEWS By Guest Author | May 21, 2023

By Group Captain Arvind Pandey (Retd)

CYBERCRIME OCCURS EVERYWHERE EVEN IN MALAYSIA



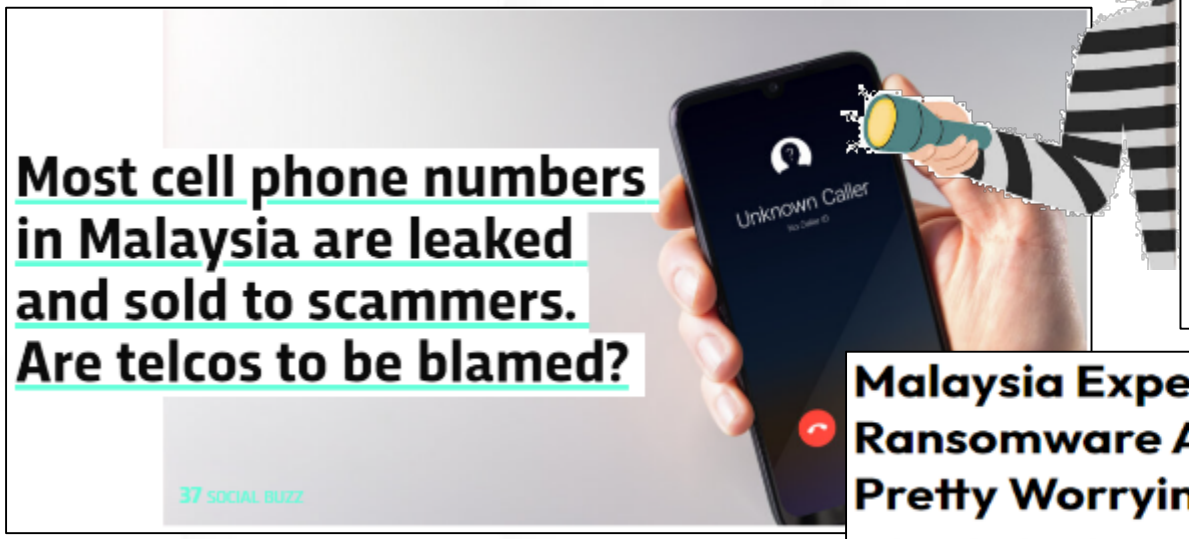


Varsity lecturer loses RM1.3mil to Macau scam syndicate

Bernama - January 8, 2023 6:29 PM

Fortinet: Malaysia recorded 84 million cyber attacks daily in fourth quarter last year

By Bernama - February 22, 2023 @ 10:16am



Immigration Department Confirms Site Is Down After Alleged Cyberattack By Hacker

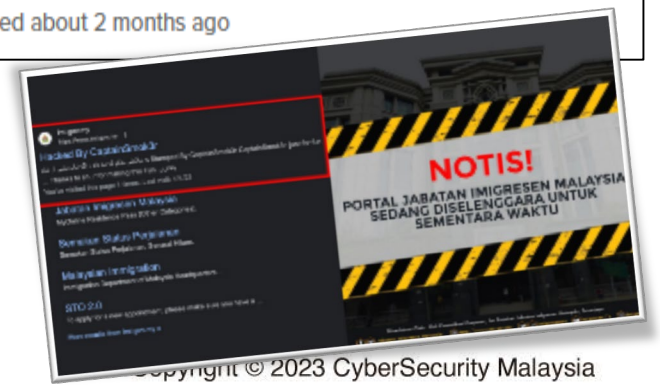
In the website description, the hacker stated that they hacked the website "just for fun".

By Aqasha Nur'aiman — 04 Apr 2023, 02:24 PM — Updated about 2 months ago

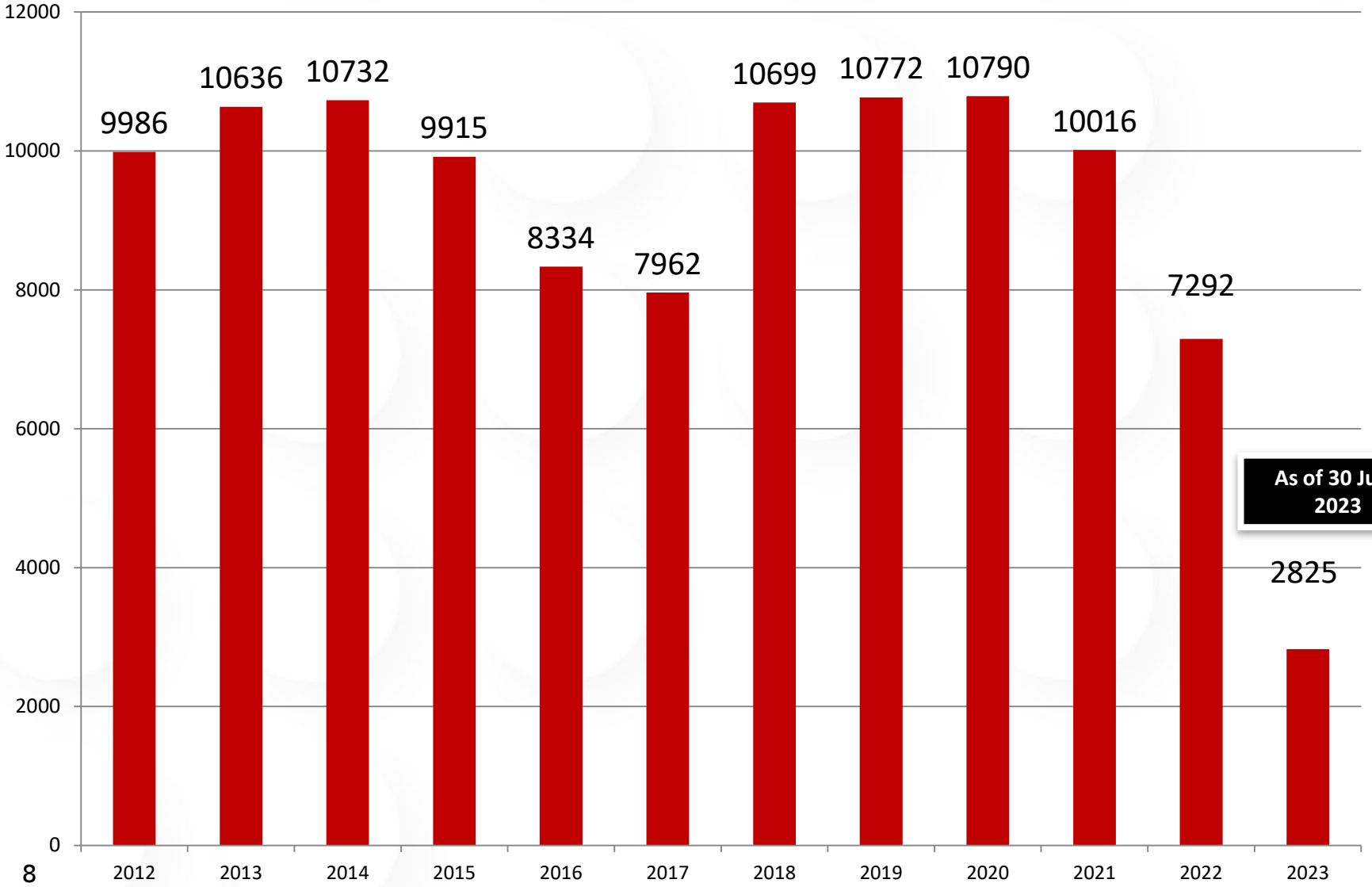
Malaysia Experienced 37% More Ransomware Attacks in 2022, and That's Pretty Worrying

Malaysia has been hit more times than usual.

By Dale John Wong March 22, 2023



CYBER INCIDENTS REFERRED TO CYBERSECURITY MALAYSIA (2011 – 30 June 2023)



MyCERT Incident Statistics

Security Alert

TOP FOUR CYBER INCIDENTS IN MALAYSIA (CYBER999)

1. Fraud
2. Malicious Code
3. Intrusion
4. Content Related

Types of incidents

1. Intrusion
2. Intrusion Attempt
3. Denial of Service Attack (DOS)
4. Fraud
5. Spam
6. Content Related
7. Vulnerabilities Report
8. Malicious Codes

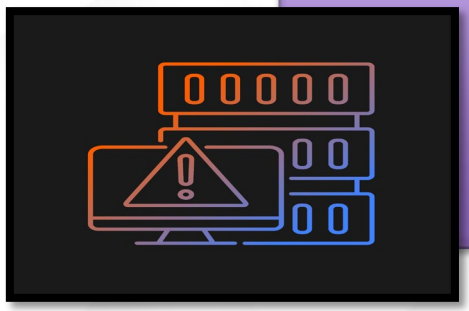
INSECURITY CAUSES DEVASTATING IMPACTS
- Risks and Impacts of Cyber Attacks

Brand
- Sensitive media scrutiny
- Public Relations
- Loss of intellectual Property / Asset

Financial
- Detection and escalation
- Notification
- Lost business / contract
- Response Costs
- Competitive disadvantage
- Insurance premium cost

CYBERSECURITY

Operational
- Diversion of employees from strategic initiatives to work on damage control
- Cybersecurity improvement
- Operational Disruption



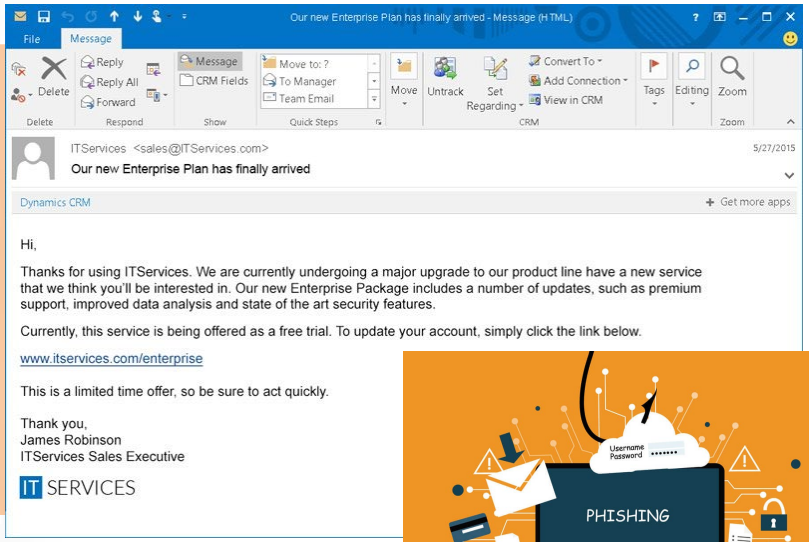
Regulatory
- Independent audits
- Regulatory fines
- Restriction on information sharing
- Implementation of comprehensive security solutions

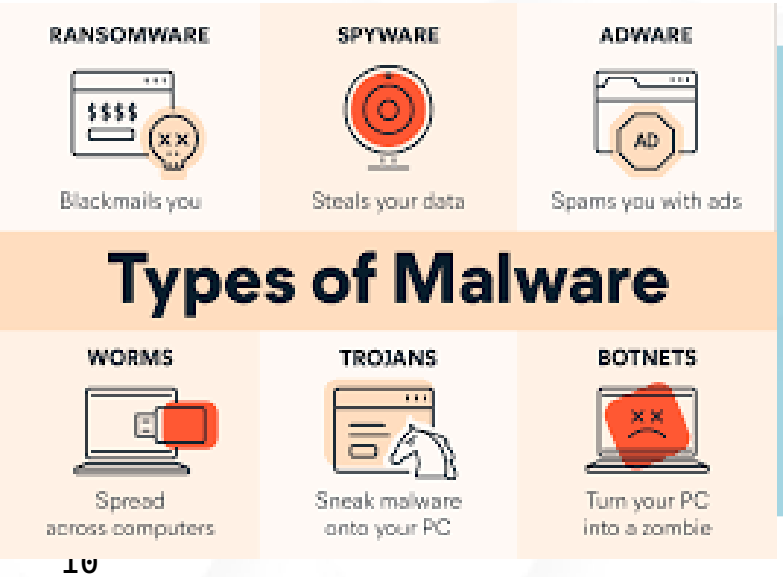
COMMON CYBER ATTACK

PHISHING ATTACKS

The practice of sending **fraudulent communications that appear to come from a reputable source**.

Commonly involves deceptive emails or messages to trick individuals into revealing sensitive information.



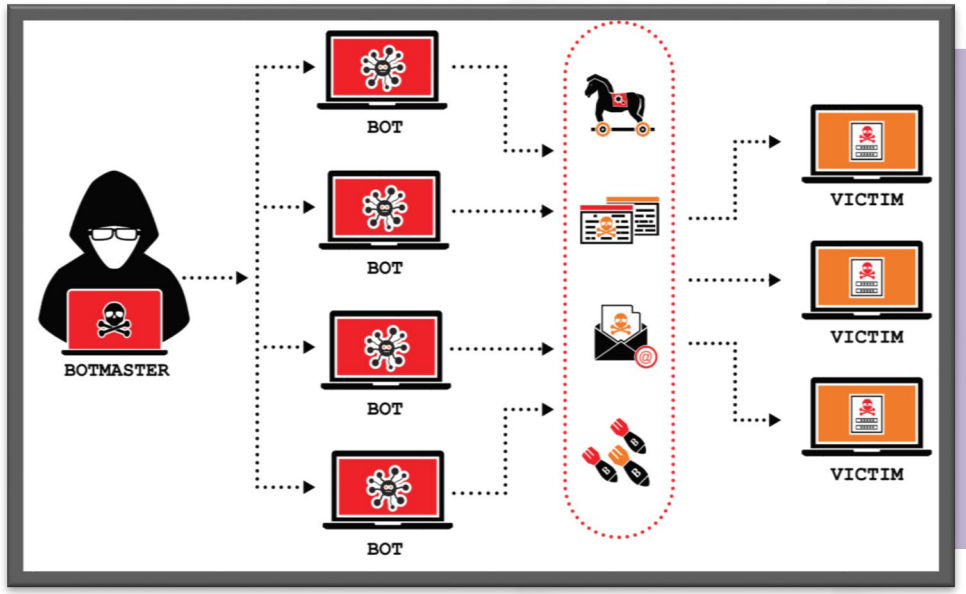


MALWARE AND RANSOMWARE

Malware is any software used to gain unauthorized access to IT systems in order to steal data, disrupt system services or damage IT networks in any way.

Ransomware is a type of malware identified by specified data or systems being held captive by attackers until a form of payment or ransom is provided

COMMON CYBER ATTACK



DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS

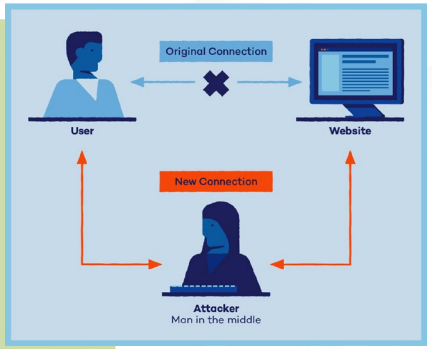
A malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Commonly DDoS attack involve multiple sources and its focused on service disruption and financial losses.

Man-in-the-Middle (MitM) ATTACKS

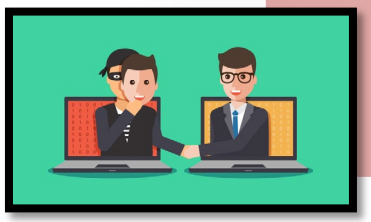
Intercepting and altering communication between two parties without their knowledge.

The potential risks, including unauthorized access, data manipulation, and eavesdropping.



Social Engineering Attacks

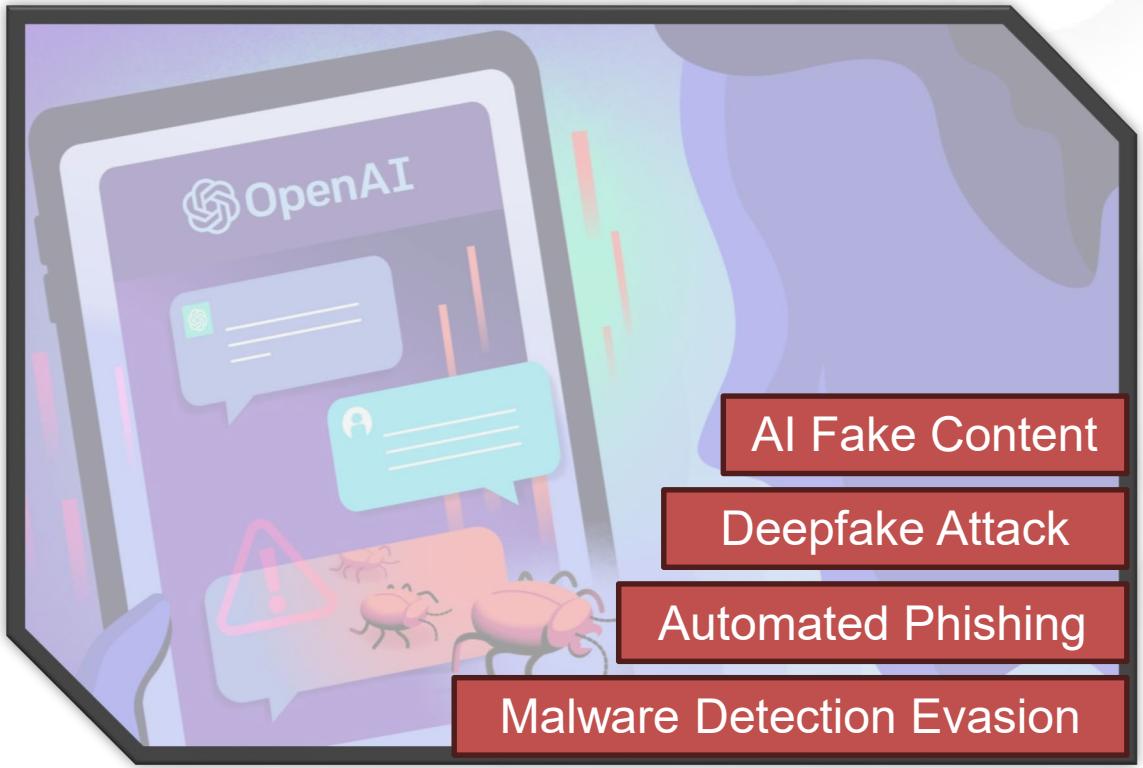
Utilize through the manipulation of individuals to disclose sensitive information or perform certain actions.



Commonly employ techniques like pretexting, baiting, and tailgating.

EMERGING CYBER THREATS

Artificial Intelligence (AI) In Cyber Attacks

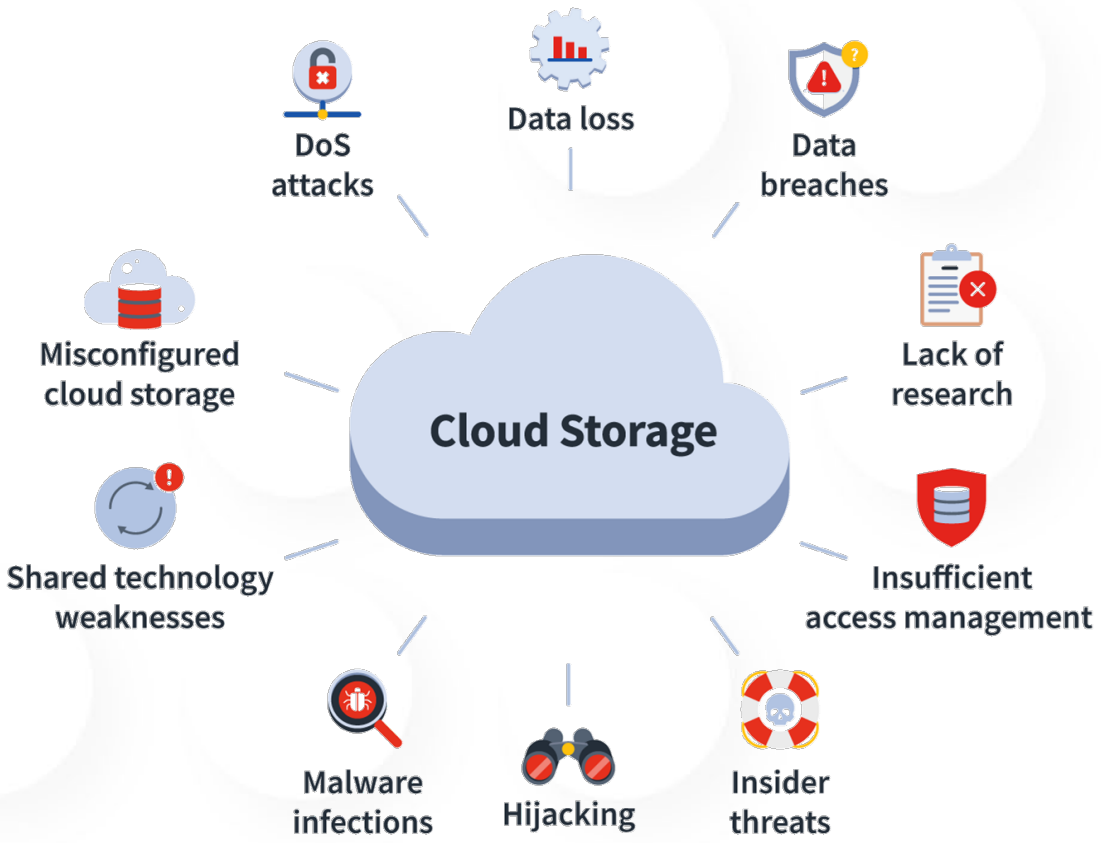


Sophisticated Evasion Techniques	Fast Adaption and Evolution
CHALLENGES	
Blending with Legitimate Traffic	Increasing Attack Scale

Internet of Things (IoT) Vulnerabilities

EMERGING CYBER THREATS

Cloud Security Risk



Mobile Device Threats

EMERGING CYBER THREATS

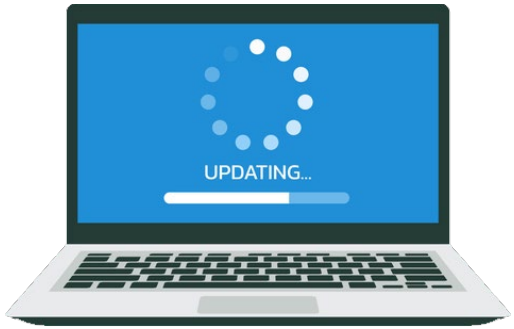
Advanced Persistent Threats (APT)

APT uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences.

CHALLENGES IN CYBERSECURITY

Insider Threats

Vulnerability Management



Patch Management

Increase of Cyber-attack Surface

Human Error And Lack Of Cybersecurity Awareness

Data Breaches And Privacy Concerns

BEST PRACTICES

CYBER HYGIENE

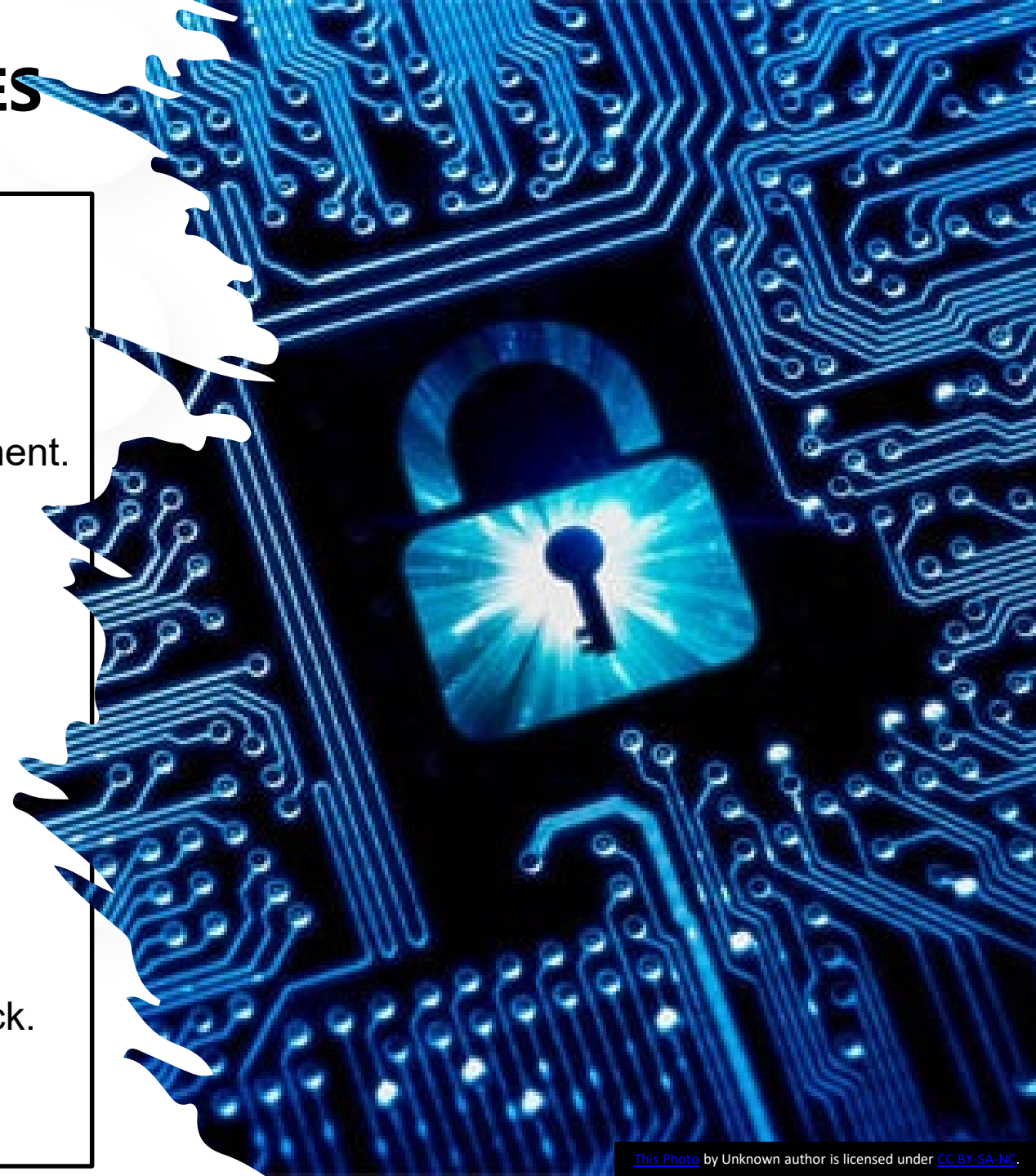
Refers to fundamental cybersecurity **best practices** that an organization's security practitioners and users can undertake.

SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE		1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS		2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY		3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW		4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION		5. USE A PASSWORD MANAGER

Practice Great Cyber Hygiene - Cyber Risk Opportunities

OTHER CYBERSECURITY MEASURES FOR ORGANISATIONS

- Defence-in-depth
- Zero trust approach.
- Firewall, anti-malware software and patch management.
- Proper cybersecurity awareness and training.
- Implementing good security policy.
- Have a Bring Your Own Device (BYOD) policy
- Regularly back up all data.
- Be alert and cautious. Look and think before you click.



Cyber Resilience – so much more than Cybersecurity

No matter how secure is an organization, there is **no such thing as 100% secure**

It is no longer the question of **how to secure oneself** from being attack

It's just a **matter of time** that a cyber-attack can occur to an organization. Similarly, human error can also affect a business's operations and render it incapable of serving its customers.

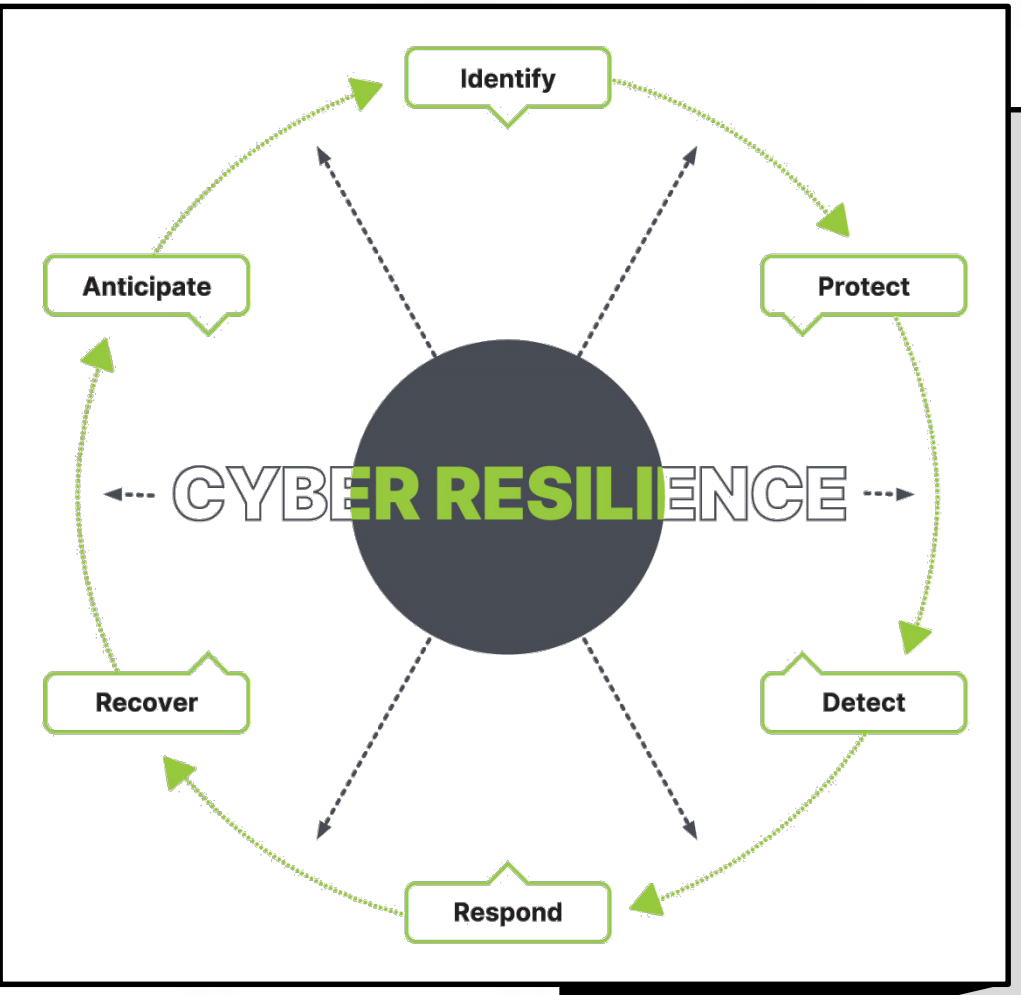
Hence, what is more important is that the organisation try their **best to strategize** in order to lessen the impact due to cyber-attacks. It is crucial to know **how to act and recover or bounce back once being attacked**

CYBERSECURITY VS CYBER RESILIENCE

CYBERSECURITY	CYBER RESILIENCE
Definition: **procedures followed**, or measures taken to **ensure the safety** of a state or organisation	**Definition**: the capacity to **recover quickly** from difficulties; **toughness**
Technologies and processes are **designed to protect** an organisation from **cybercrime**	Technologies and processes designed to **keep delivering intended services** in spite of **cyber incidents**
Works to **reduce the risk of cyber-attacks** and to **protect the organisation** from **cyber theft/ espionage**	Works to ensure **continuity on a wider scope**, **comprising cybersecurity** and **business requirements**
Can work effectively without **compromising** the usability of **other systems**	Requires **organisation-wide culture shift** that normalises and embeds **security best practices**
Includes a **business plan** to **resume operation** in the event of a **successful attack**	Requires the organisation to become **agile and adaptable** in the **face of cyber-attacks and incidents**

Action/plan/program in reducing risk and implementing security approach	**Action/plan/program upon occurred incidents and what to do next**

Cyber Resilience



– so much more than Cybersecurity

- Traditional security measures are no longer enough to protect a company's data and network security.
- Improve security system, internal process and work culture.
- It provides many benefit to an organization such as to increase their security posture and reducing the risk of exposure to their infrastructure.
- Helps reduce financial loss and reputational damage.
- Inspires trusts in its clients and customers.

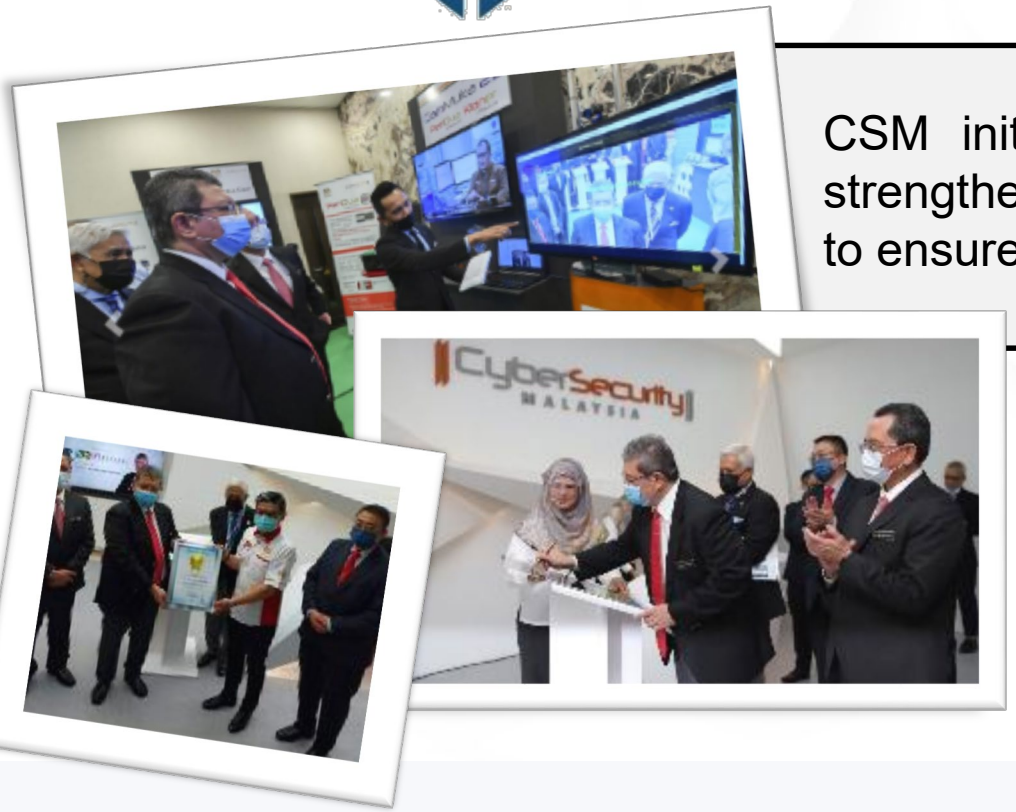
TO BE MORE CYBER RESILIENT

- Keep your cybersecurity systems updated with all the necessary SOPs active
- Have proper policies, guidelines such as Business Continuity Policy, Incidence Response, Disaster Recovery, Risk Assessments, etc.
- Use modern and security-rich network infrastructures by trusted manufacturers
- Make sure your IT team is leveraging the latest threat intelligence methodologies to monitor malicious activities
- You must onboard the right talent and cybersecurity tools to address the evolving cybersecurity threats
- Outsource an experienced cybersecurity firm to deal with cyber threats effectively.
- Make cybersecurity a culture.

CyberSecurity Malaysia's Initiatives

SiberKASA

OFFICIAL LAUNCH ON 23 MARCH 2021



CSM initiatives aimed at developing, empowering, sustaining and strengthening cybersecurity infrastructure and ecosystem in Malaysia to ensure network security preparedness.

CYBERSECURITY MALAYSIA'S INITIATIVES

HOLISTIC APPROACH

Adoption of holistic approach that **identifies potential threats** to organization and **impacts to the national security & public well-being ; and**

To develop the nation to become **cyber resilience** having the **capability to safeguard the interests** of its **stakeholders, reputation, brand and value creating activities.**

SiberKASA

(Program PemerKASAan Keselamatan Siber)

Objective: Empowering, strengthening and preserving the cyber security infrastructure and ecosystem in Malaysia so that it is always sustainable, protected and resilient.

HUMAN	PROCESS	TECHNOLOGY
Covers aspects of skills, knowledge, ethics, behavior and talent	Covers aspects of policy development, strategy, Standard Operating Procedure (SOP), recognition of international standards	Involves technology in particular matters related to minimizing vulnerabilities, digital forensic analysis, malicious code (malware) and data

PRODUCT AND SERVICE

PRODUCTS AND SERVICES

HUMAN	PROCESS	TECHNOLOGY
1. Global Accredited Cybersecurity Education (ACE)Scheme 2. CyberSAFE L.I.V.E Gallery 3. Cybersecurity Competency Training (CyberGuru)	1. Information Security Governance, Risk & Compliance Health Check Assessment (ISGRiC) 2. ISMS Guidance Series 3. Information Security Management System(ISMS)	1. Crypto Random Test Tool 2. X-Forensics Tools 3. PenDua Tool 4. Coordinated Malware, Eradication, and Remediation Platform (CMERP) 5. LebahNet 6. CamMuka (Facial Recognition)
1. CyberDrill Exercise 2. Behavioral Competency Assessment (BCA) 3. Cyber Safety Awareness for Everyone (CyberSAFE) 4. CyberSecurity Malaysia Awards, Conference & Exhibition (CSM-ACE)	1. Business Continuity Management System (BCMS) Certification 2. Digital Forensics (DF) Case Management 3. Incident Handling Case Management 4. Cyber Discovery 5. MyTrustSEAL 6. Penetration Testing Service Provider(PTSP) Certification 7. Technology Security Assurance (TSA) 8. ICT Product Security Assessment (IPSA) 9. Security Posture Assessment (SPA) 10. SCADA Security Assessment (SSA) 11. PHP Secure Code Assessment (PSCA) 12. Malaysian Common Criteria Scheme (MyCC) 13. Cybersecurity Strategic and Technical Advisory	1. MyCyberSecurity Clinic (MyCSC)- Data Recovery and Data Sanitization Services 2. Lab Quality Management 3. Cybersecurity Lab Services 4. CyberSecurity Malaysia Cryptographic Evaluation Lab (MyCEL) 5. CCTV Forensics Service 6. Cyber Threat Intelligence Service 7. Cloud Security Compliance Audit 8. Cloud Security Assessment Audit 9. Cloud Security Audit for ISMS 10. Security Operation Centre Service 11. Red Teaming Service

CONCLUSION AND WAY FORWARD

- There is no such thing as 100% security. There is still much improvement to be made. We need to increase and strengthen our cybersecurity manpower and professional skills.

- There is a need to ensure for a secure, resilient and trusted cyber environment in order to sustain progression and prosperity. In this regard, a more innovative and proactive adaptive security approach is required to address such situations. Adaptive cybersecurity encompasses predictive, detective, responsive and corrective capabilities.

- In addition, our approach also has to be adaptive, dynamic and innovative covering people, process and technology.

- Strengthening Public-Private-Academia Partnership and national, bilateral, regional and International Collaboration.

- Malaysia should gear itself towards cyber resilience as the threat of a global cybersecurity breach continues to pose a major risk.

MINISTRY OF
COMMMUNICATIONS AND DIGITAL

CyberSecurity MALAYSIA

THANK YOU

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

T +603 8800 7999 | **F** +603 8008 7000 | **H** +61 300 88 2999

www.cybersecurity.my | info@cybersecurity.my

CyberSecurityMalaysia | cybersecuritymy | cybersecuritymy | CyberSecurity Malaysia | cybersecurity_my

JUBLI PERAK 1997 - 2022 CyberSecurity MALAYSIA

SIBER MADANI
Sentiasa Bijak ▪ Sentiasa Selamat

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : ISMS 00114

ACB ISMS 02
SAMM 456

MSC MALAYSIA Status Company

WSIS PRIZES 2020 WINNER www.wsis.org

THE MALAYSIA BOOK of RECORDS