



INDUSTRY FOCUS:

ICT SYSTEM SECURITY



Prepared by:
Lynette Lee
Syed Mohamad Bukhari Syed Bakeri

SMEBank-EconomicResearch@smebank.com.my

(603) 2615 2020



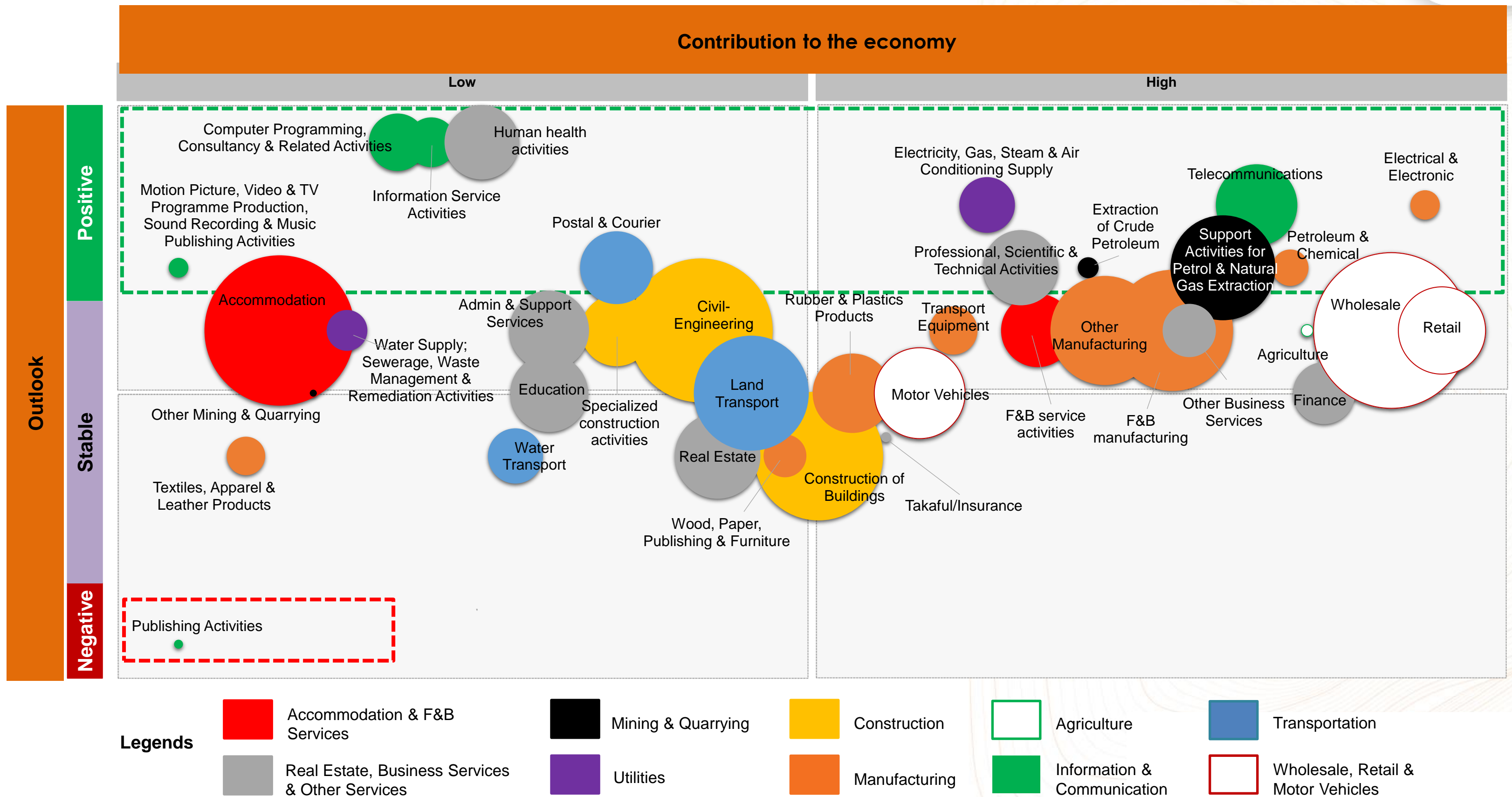
A decorative graphic consisting of a solid red circle with the number "1" inside, and a thick orange arc that curves around the left side of the circle.

1

Industry Focus: ICT system security

Industry Focus: Outlook of 39 sub-sectors

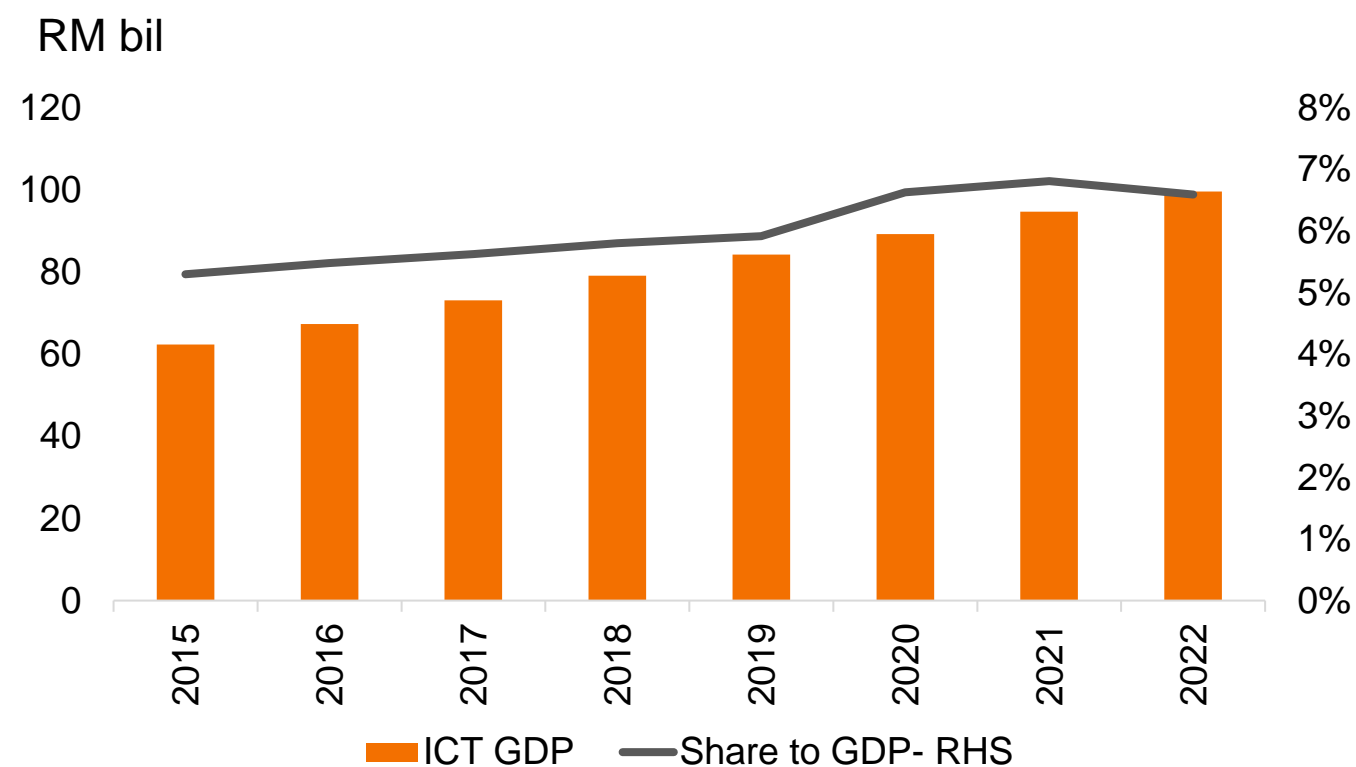
Computer Programming, Consultancy & Related Activities



Malaysia's cybersecurity compounded annual growth rate is forecasted to clock in at **16.8% between 2023 - 2028 > global at 11.4%**, thanks to rapid digitalisation, technology upcycle, and higher internet penetration. Furthermore, the government is targeting **the digital economy** to contribute >25.5% of national GDP by 2025 (2021: 23.2%; 2010: 16.5%).

Sub-Sector	Outlook
ICT system security	Positive

Resilient performance of the ICT sector



- + **Rising digitalisation** in government and private sectors in Malaysia may **expose them to cyber dangers**. Devices or systems that are **connected to computer networks through internet** can be vulnerable to threats (e.g. malware, ransomware).
 - Growing internet connectivity and related activities, **including expanding e-commerce, IoT, cashless payment trends, cloud services, mobile applications, smart appliances, and automations** could expose businesses to the risk of cyberattacks.
 - Although Malaysia has the 2nd lowest ransomware detected in ASEAN, after Singapore, increasing cyberattack (eg: Malware, Ransomware, Phishing etc) in Malaysia could prompt **rising demand for cybersecurity** especially from businesses/organisations. Breach/leaking of data can **damage the IT system** and **company reputation**. An average of 84 mil cyberattacks were recorded in 4Q 2022 (1Q 2022: 57.8 mil).
- + **45% of businesses** choose to **outsource cybersecurity** which signals opportunity to players in this sector. Nonetheless, it is estimated that there are only around 400 cybersecurity players (0.04% of services business) in Malaysia.
- + Sectors which are **highly regulated such as the financial services sectors** are required by BNM to protect from failures/breaches of IT systems, applications, platforms or infrastructure.
- **Competition with large players and MNC, lack of skilled labour, and high cost (e.g training, software, licenses)** are among the key challenges for this sector.

Definition

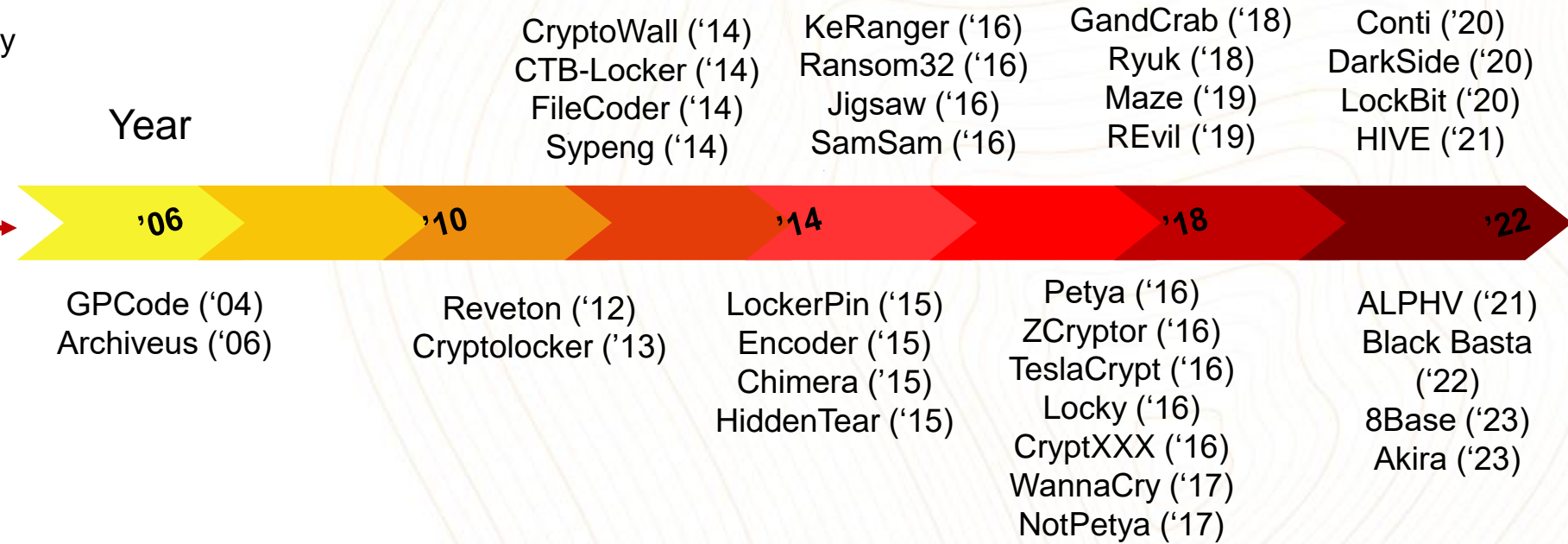
- Cybersecurity is the practice of **defending** computers, servers, mobile devices, electronic systems, networks, and data from **malicious attacks**.

Type of cybersecurity

- IoT Security
- Mobile Security
- Application Security
- Operational Security
- Network Security
- Cloud Security
- Endpoint Security

Common cyber threat

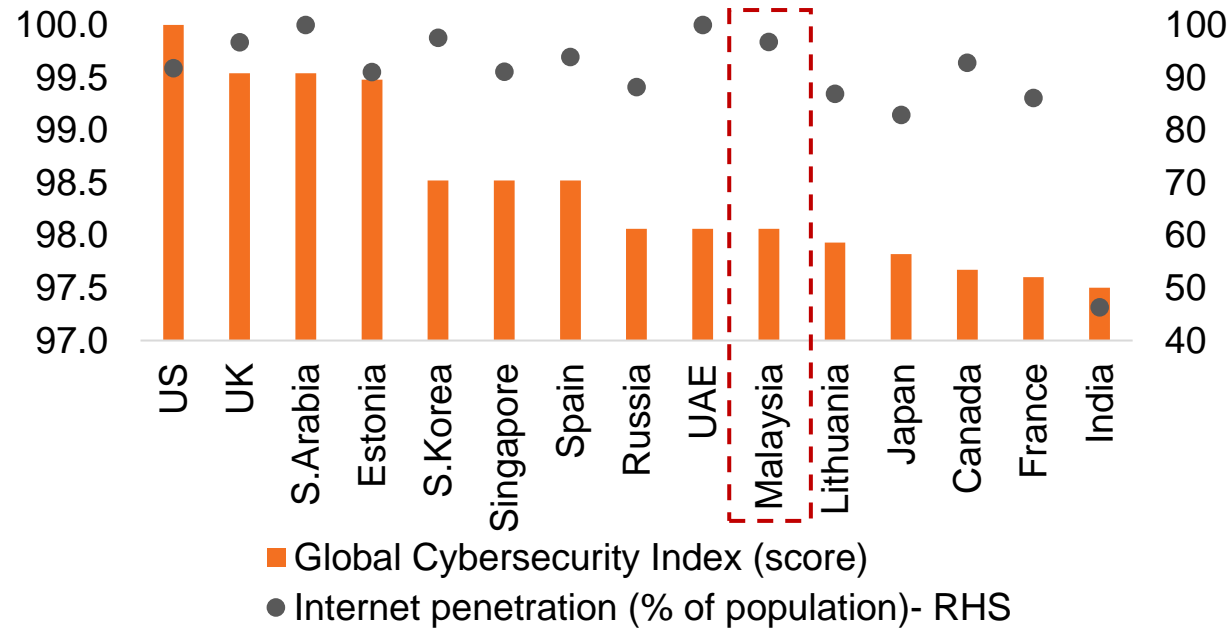
- Malware
- Ransomware**
- Phishing / social engineering
- Insider threats
- Distributed denial-of-service (DDoS) attacks
- Advanced persistent threats (APTs)
- Man-in-the-middle attacks



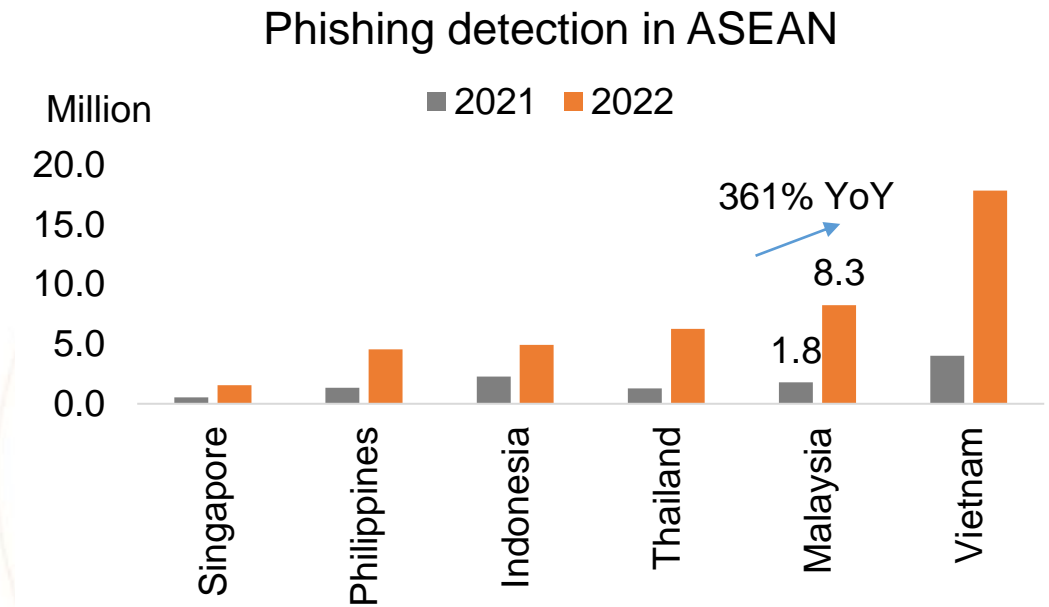
Preventing is important

- Cybercrime and cyber insecurity** are listed as **Top 10 global risks** for the short and long-term by World Economic Forum.
- Malicious attacks** could contribute to **potential monetary losses** to individual/organization, especially with **growing unethical hacker business model** such as **Ransomware as a service**.
- Businesses which stores their data** (customers information, inventory, financial records etc) **in computers** could be exposed to cyber breaches even by clicking on unsecure links, email and website.
- Ransomware cost** the world USD20 bil in 2021. That number is **expected to rise** to USD265 bil by 2031, **up by 12 times**.
- In 2021, 37% of all businesses and organizations globally were hit by ransomware. Businesses spent **USD1.85 mil on average** due to ransomware but was only able to **recover ~65% of their data (35% permanently loss)**.
- Cybersecurity adoption is not just an option but a necessity now** for most of businesses. **Preventing** through **strong cybersecurity** is important especially in this digitalisation era, to **protect businesses from losing data and monetary loss**.

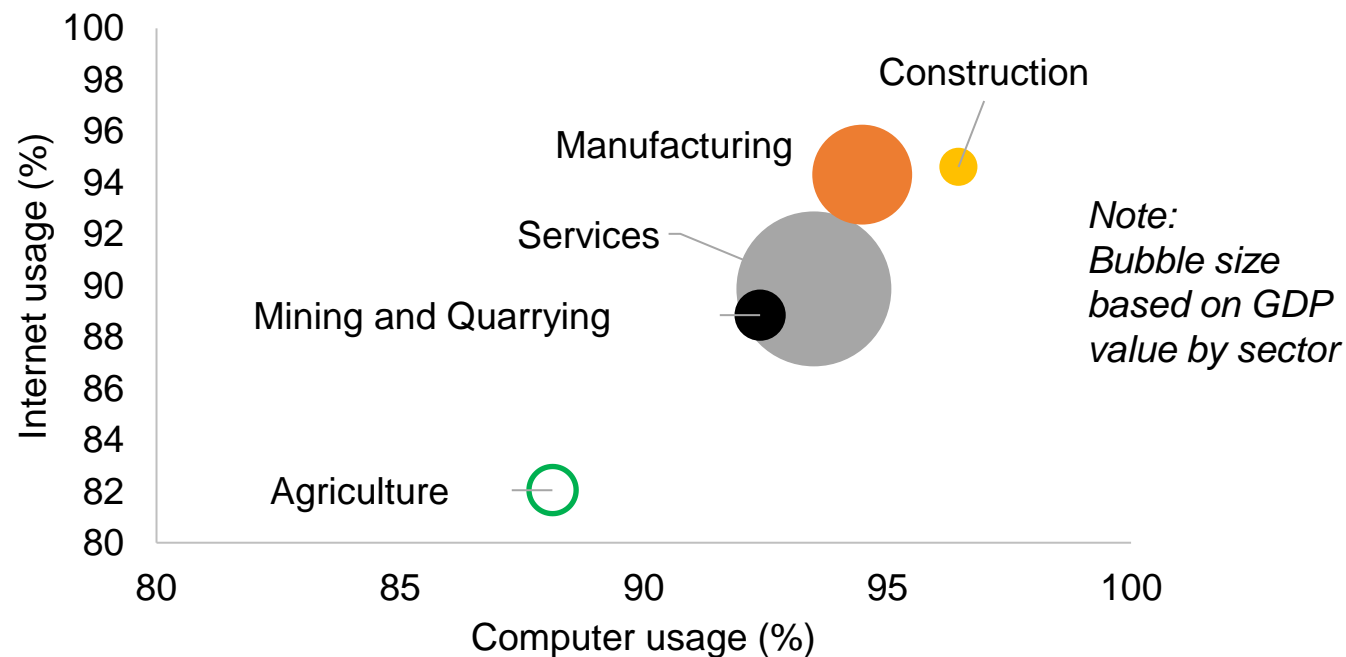
Malaysia ranked **Top 10** globally in cybersecurity, above many developed countries



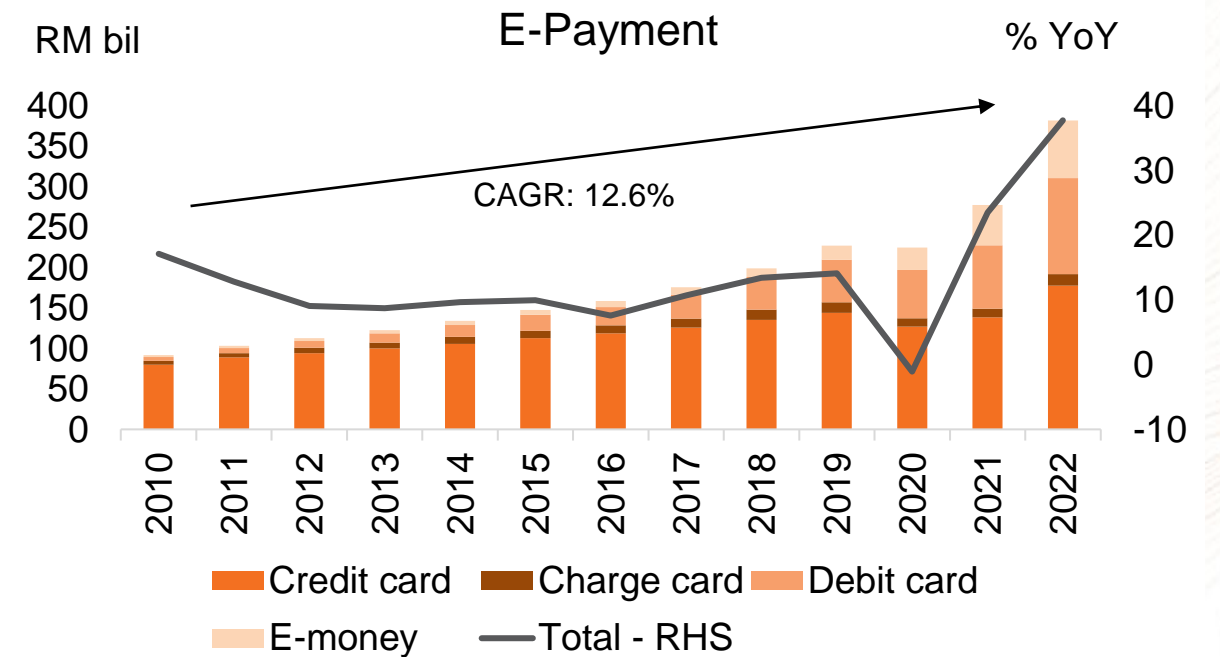
Malaysia has the **2nd highest phishing** detected in ASEAN, after Vietnam



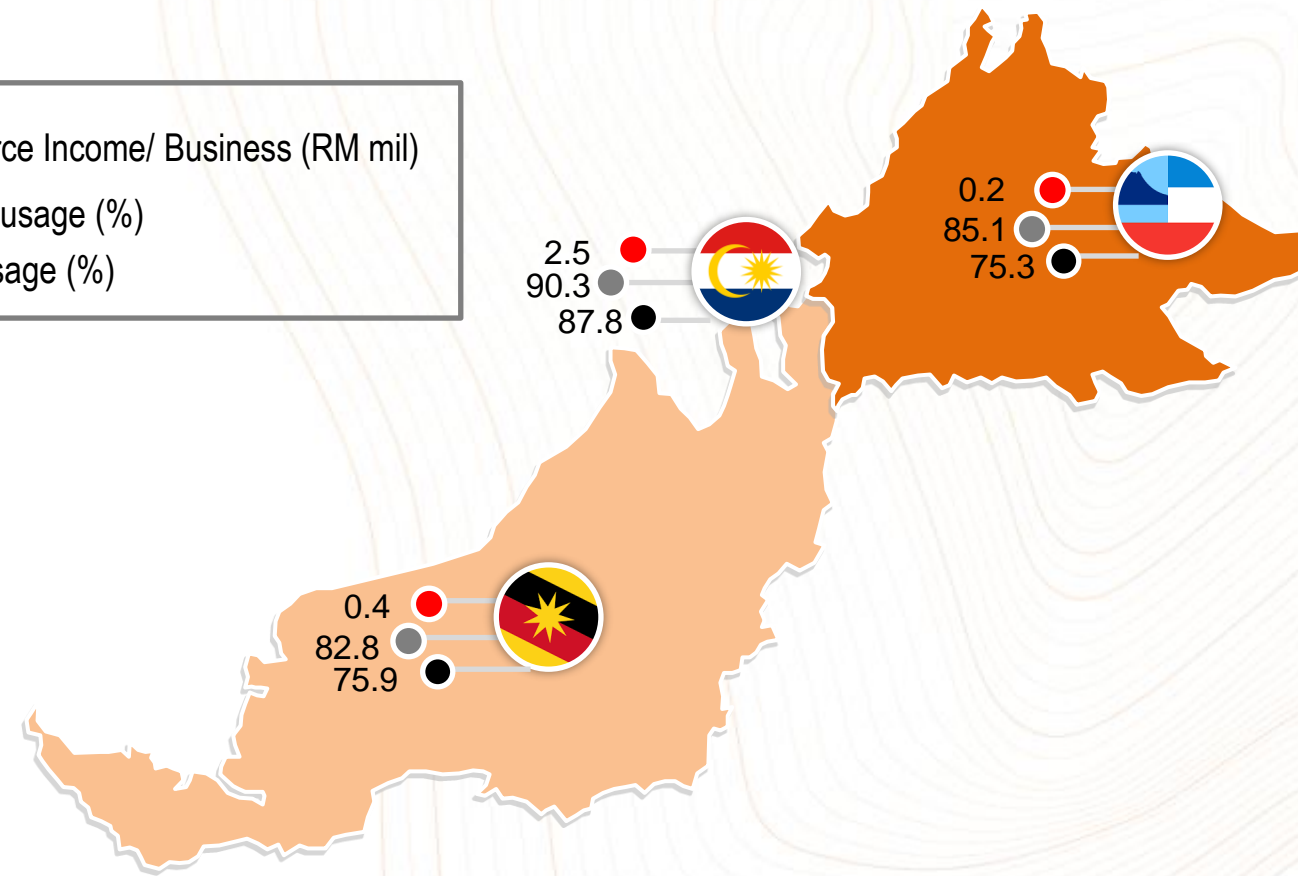
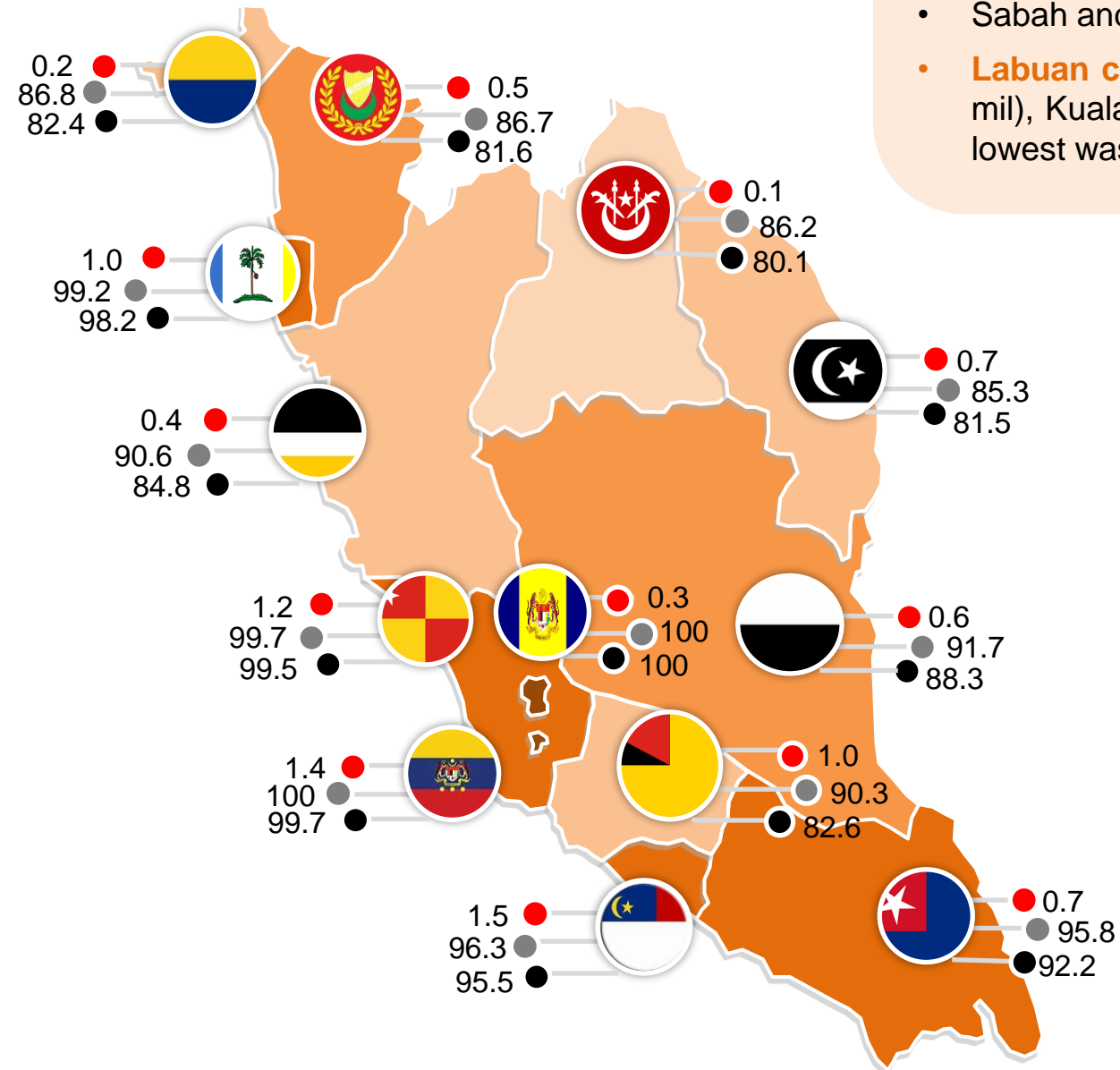
High usage of computer & internet by sectors in Malaysia, increasing exposure to cyber threat



Cybersecurity is crucial amid **rising cashless** payment trend

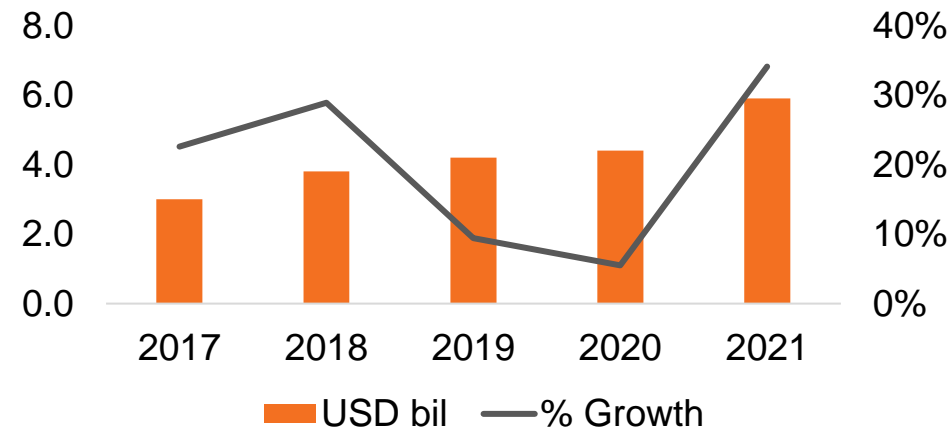


- **Majority of businesses** in Malaysia use computers (>82%) and internet (>75%), **exposing them to cyber threat**. Hence, this could be a push/ rising demand for cybersecurity services.
- In 2021, the **highest usage of computers among businesses** was recorded in **Kuala Lumpur (100%), Putrajaya (100%)** and **Selangor (99.7%)**.
- In terms of **internet penetration**, **Putrajaya was the highest** at 100%, followed by **Kuala Lumpur (99.7%)** and **Selangor (99.5%)**,
- Sabah and Sarawak was at the lowest for both computer usage and internet penetration nationwide.
- **Labuan charted the highest e-commerce income per business of RM2.5 mil** followed by Melaka (RM1.5 mil), Kuala Lumpur (RM1.4 mil), Selangor (RM1.2 mil), and Pulau Pinang (RM1.0 mil). On the other hand, the lowest was Kelantan (RM113k/business), Perlis (RM175k,) and Sabah (RM246k).



Cybersecurity for new inventions

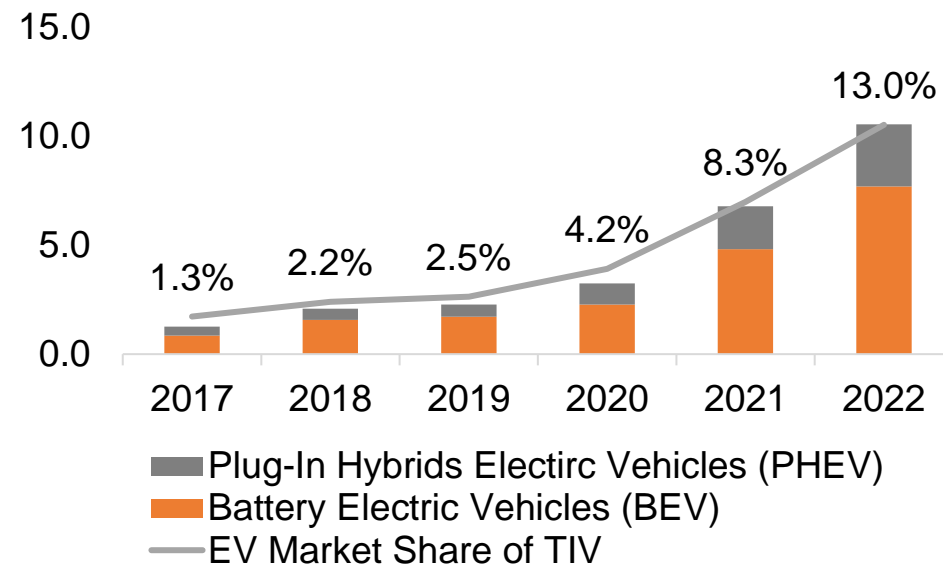
Global Drones Market Value



Rising Autonomous Navigation Features especially Drones

- **Global Drones market** has enjoyed a rapid growth, **expanding by 34.1% in 2021** (2020: 5.5%; average 2017-2019: 20.3%).
- **Global drone payload market** grew by **9.2% in 2021** (2020: 9.1%). A resilient growth in 2020 was seen despite global growth contracting by 3.1%, likely due to increase in digitalisation and automation adoption.
- **Drones' adoption is seen across various sectors.** Global Unmanned traffic management market in 2022 saw an increase particularly in **agriculture & forestry (22% YoY), logistics & transportation (22%), surveillance & monitoring (20%),**
- Drones can be hacked since they are radio wave and internet connected devices, making it possible for unauthorised access, system corruption (due to malware), and stealing of information (e.g. video and images).

Global BEV & PHEV sales (mil)



Electric Vehicle gaining traction

- EV is the future, in line with efforts to reduce climate change risks. **CAGR of 24.5% between 2022 - 2028.**
- The systems built into electric cars perform critical **duties over the Internet**, including **remote monitoring, software updates & customer billing**, as do a growing number of **internet-enabled EV charging stations.**
- For further information on EV, kindly refer to our [Thematic: Electric Vehicle](#) report.

Autonomous mobile robot

- The global autonomous mobile robots (AMR) is expected to expand at a **CAGR of 16.4%** from 2022 to 2032.
- AMRs can be found in various applications such as **warehousing, logistics, manufacturing, and healthcare.**
- In 2021, Malaysia's largest home improvement retailer, MR.DIY has launched their robotic e-commerce warehouse.
- As robots are connected to computer system, any **breach in network can result in system downtime.** This could **delay the operations** which could translate to **additional cost to the businesses.**



Regulatory requirement

Policy and plans



Personal Data Protection Act 2010

- PDPA is an Act that regulates the processing of personal data in regards to commercial transactions.
- **Users need to be protected** to prevent any form of abuse against **the storage or processing of personal data** of individuals, public and private sectors.



BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Risk Management in Technology (RMiT) 2020 policy

- This policy document sets out **BNM's requirements** with regards to financial institutions' management of technology risk.
- All entities under BNM supervision needs to **comply with the policy** which includes **protection from failures or breaches of IT systems, applications, platforms or infrastructure.**



Suruhanjaya Sekuriti
Securities Commission
Malaysia

Guidelines on management of cyber risk (2016) policy

- The entity under SC's supervision must have in **place clear and comprehensive cyber policies** and procedures, which commensurate with its risk profile.

Cyber Security Strategy 2020 - 2024

- In 2020, the government rolled out a medium-term action plan, Malaysia Cyber Security Strategy, with an allocation of RM1.8 billion.
- The 5 important strategic pillars concerning cyber security for enhanced planning and implementation are as follows:
 1. Effective Governance and Management
 2. Strengthening Legislative Framework and Enforcement
 3. Catalysing World Class Innovation, Technology, R&D, and Industry
 4. Enhancing Capacity and Capability Building, Awareness, and Education
 5. Strengthening Global Collaboration
- Government is in the midst of drafting **a new law** to bolster the country's resilience and response to cyber threats dubbed the **Cyber Security Bill.**

National Cyber Security Agency (NACSA)

- Established in February 2017 as the national lead agency for cyber security matters, with the objective of securing and strengthening Malaysia's resilience in facing the threats of cyber attacks, by co-ordinating and consolidating the nation's best experts and resources in the field of cybersecurity.

National Cyber Security Policy (NCSP) 2006

- The NCSP provides the perspective of how cybersecurity should be implemented in an integrated manner.

Key Challenges

1

Competition with large and MNC players which have more resources and expertise.
Key Cybersecurity players;

- LGMS
- Wizlynx Group
- Securemetric
- Akati Sekurity
- IBM Corporation
- Kaspersky
- Cisco System Inc
- Fortinet

2

Shortage of skilled labour for Cybersecurity

- **27k cyber security experts** are needed **by 2025** according to Ministry of Communication.
- Currently, the sector has 15,248 workers, which means an additional 12k workers are required/in shortage.

3

Higher cost and capital

- Businesses need to bear the **high cost to provide cybersecurity services** such as paying for **cybersecurity software licensing**. Depreciation of the Ringgit may also increase costs for imported softwares.
- **Higher cost for certification & training.** A certified cyber security expert needs to be up to date with current information and trend amid evolving cyber threat such as malware, ransomware etc.
- **Constant need for updating and upgrading to the newest versions.**

Opportunities

1

Rising e-commerce and cashless payment trend will require cyber protection

- E-commerce grew 6% YoY to RM1.1 tri or 73% of national GDP, up 2x from 34% of GDP in 2015.
- Electronic payment grew 37.7% YoY in 2022 (2021: 23.5%)

2

Cybersecurity will compliment government digitalisation agenda, providing opportunities to providers

- Nasional Digital ID
- Border system
- Cloud services
- Cashless payment
- Central Database hub (PADU)
- Online transaction (LHDN, Immigration, JPN, etc)

3

“Bring Your Own Device” approach

- Strong cybersecurity is needed to make sure office devices are not infected when connected with **outside device**. Lack of protection may expose to malware, etc

4

Digitalisation and automation trend exposes businesses/organisations to cyberattack including using robots, drones, RFID, internet of things, 5G, cloud database, etc

ICT Sector

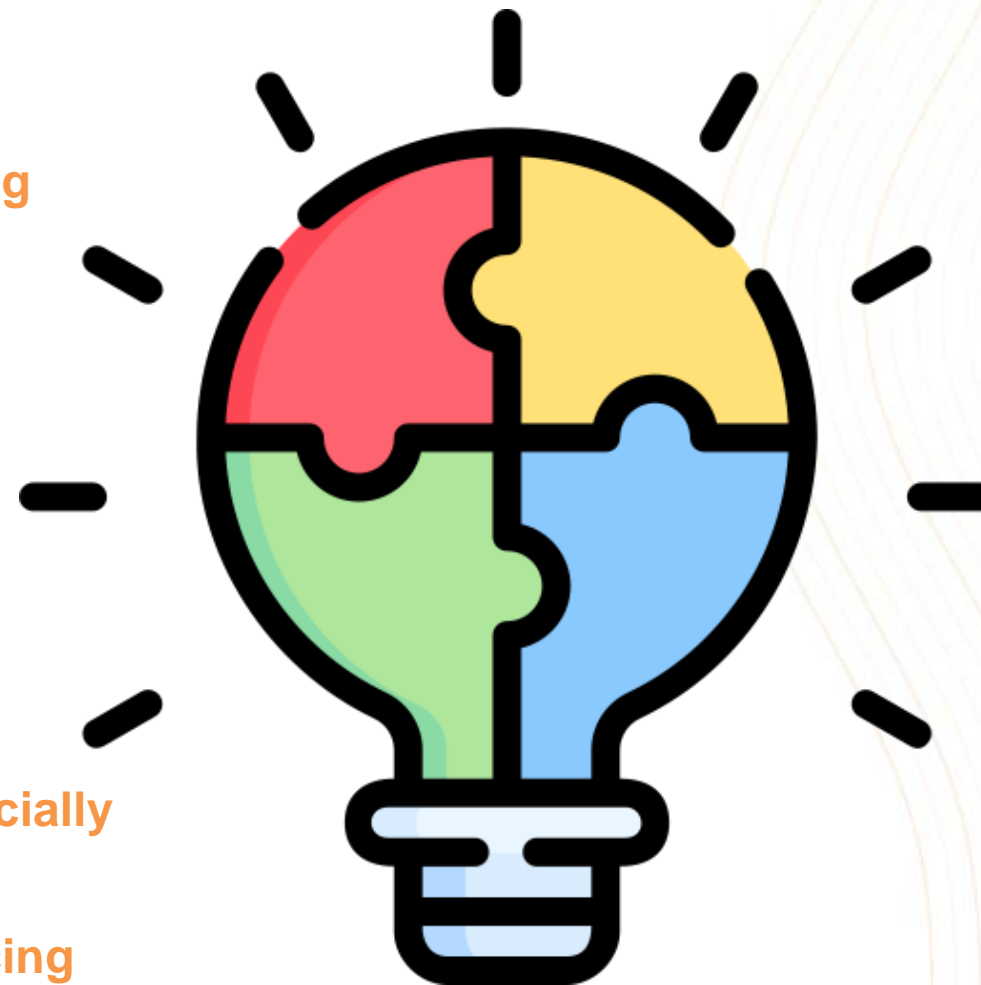
4.7% of total respondents from 1H 2023 SME Sentiment Index

67% foresee their **profit to increase**
(led by Small-sized enterprises)

even though **79%** expect **cost of doing business to be higher**

76% want to **hire more employees** but **mostly** prefer on **contract/ part time** basis

55% can only **sustain less than a year, financially**
(mainly Micro-sized enterprises)
hence **97%** are looking for **additional financing**



All Sector

72% of **all MSMEs** will focus on digital transformation over the next 6-12 months

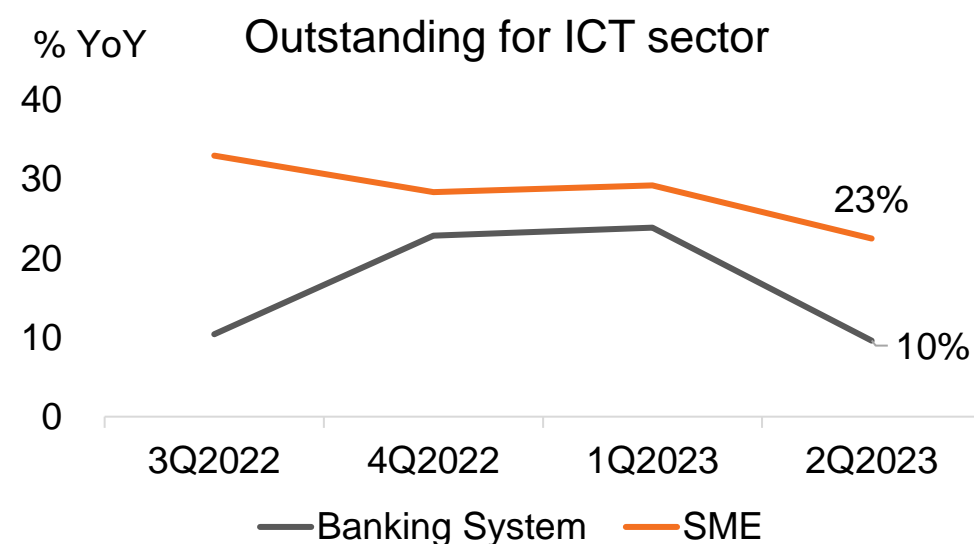
68% agree that **digital transformation is impactful** to their business performance
(particularly Micro-sized enterprises)

58% plan to **invest in automation** to sustain their business during an economic slowdown
(led by Large-sized enterprises)

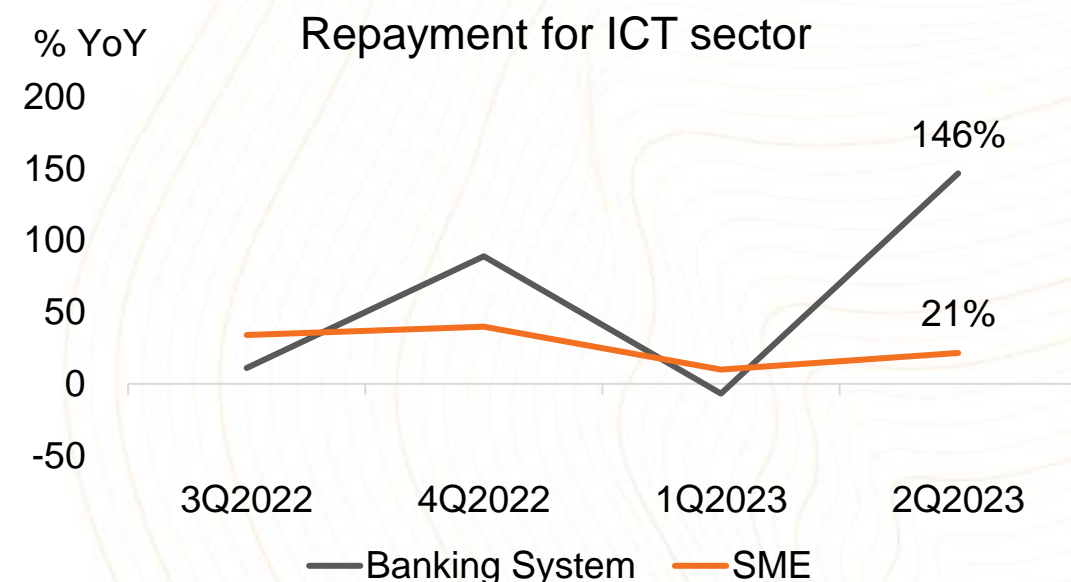
SME SENTIMENT INDEX
1H 2023

Financing Performance in Banking sector and SME segment

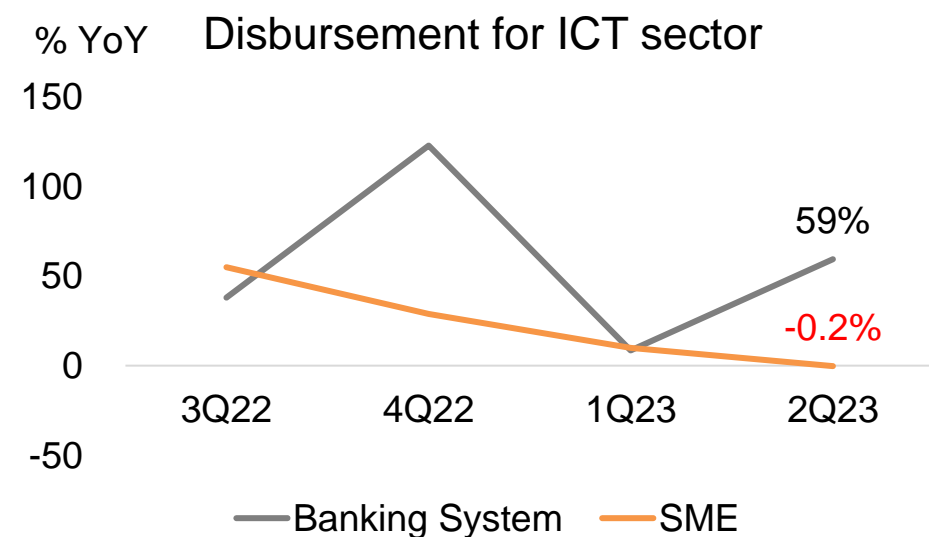
Financing growth in ICT sector remained resilient, where SME financing makes up 25% of total banking system outstanding in the ICT sector



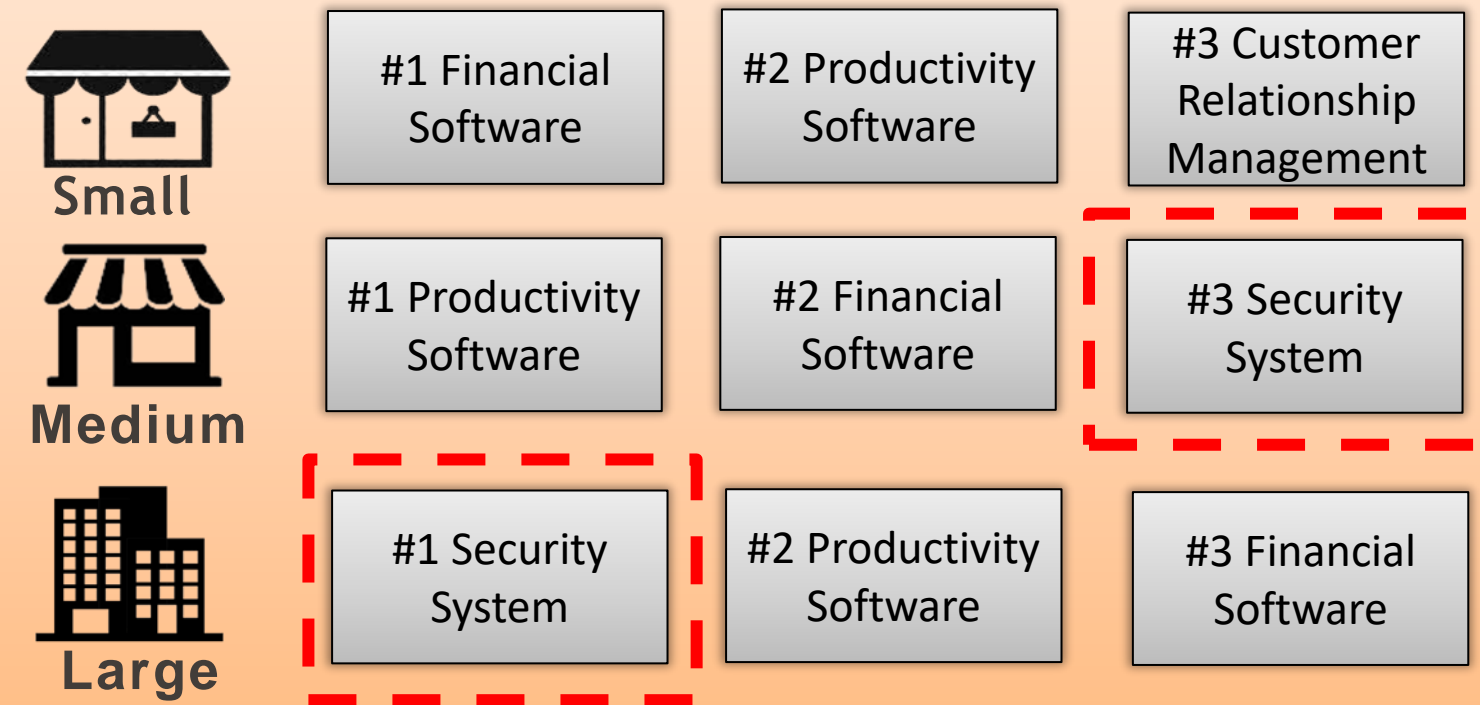
Businesses' repayment stays healthy for ICT sector



Disbursement for banking system accelerated while SMEs slowed



SPENDING PRIORITIES BY BUSINESS SIZE



DISCLAIMER

SME BANK has exclusive proprietary rights in the data or information provided herein. This document is the property of SME BANK and is protected by Malaysian and international copyright laws and conventions. The data and information shall only be used for intended purposes and not for any improper or unauthorised purpose. All information contained herein shall not be copied or otherwise reproduced, repackaged, transmitted, transferred, disseminated, redistributed or resold for any purpose, in whole or in part, in any form or manner, or by any means or person without SME BANK's prior written consent.

This research report provides general information only. Neither the information nor any opinion expressed constitutes an offer or an invitation to make an offer, to buy or sell any securities or other investment or any options, futures or derivatives related to such securities or investments. It is not intended to provide personal investment advice and it does not take into account the specific investment objectives, financial situation and the particular needs of any specific person who may receive this report. Investors should seek financial advice regarding the appropriateness of investing in any securities, other investment or investment strategies discussed or recommended in this report and should understand that statements regarding future prospects may not be realised. Investors should note that income from such securities or other investments, if any, may fluctuate and that price or value of such securities and investments may rise or fall. Accordingly, investors may receive back less than originally invested. Past performance is not necessarily a guide to future performance. Any information relating to the tax status of financial instruments discussed herein is not intended to provide tax advice or to be used by anyone to provide tax advice. Investors are urged to seek tax advice based on their particular circumstances from an independent tax professional.

Any opinion, analysis, observation, commentary and/or statement made by SME BANK are solely statements of opinion based on information obtained from sources which SME BANK believes to be reliable and therefore, shall not be taken as a statement of fact under any circumstance. SME BANK does not and is in no position to independently audit or verify the truth and accuracy of the information contained in the document and shall not be responsible for any error or omission or for the loss or damage caused by, resulting from or relating to the use of such information. Analysts based in SME BANK offices produce research on macroeconomics, equities, fixed income, currencies, commodities and portfoliostrategy.

SME BANK and its affiliates, subsidiaries and employees shall not be liable for any damage or loss arising from the use of and/or reliance on documents produced by SME BANK or any information contained therein. Anyone using and/or relying on SME BANK document and information contained therein solely assumes the risk in making use of and/or relying on such document and all information contained therein and acknowledges that this disclaimer has been read and understood, and agrees to be bounded by it.



Small Medium Enterprise Development Bank Malaysia Berhad 49572-H

Menara SME Bank, Jalan Sultan Ismail, 50250 Kuala Lumpur

Tel: 03-2615 2020 **Faks:** 03-2698 1748



 www.smebank.com.my

 [smebankmalaysia](https://www.linkedin.com/company/smebankmalaysia)

 [smebankmalaysia](https://www.facebook.com/smebankmalaysia)

 [@SME Bank](https://twitter.com/SME_Bank)

 [smebank_malaysia](https://www.instagram.com/smebank_malaysia)

 [smebank](https://www.tiktok.com/smebank)

