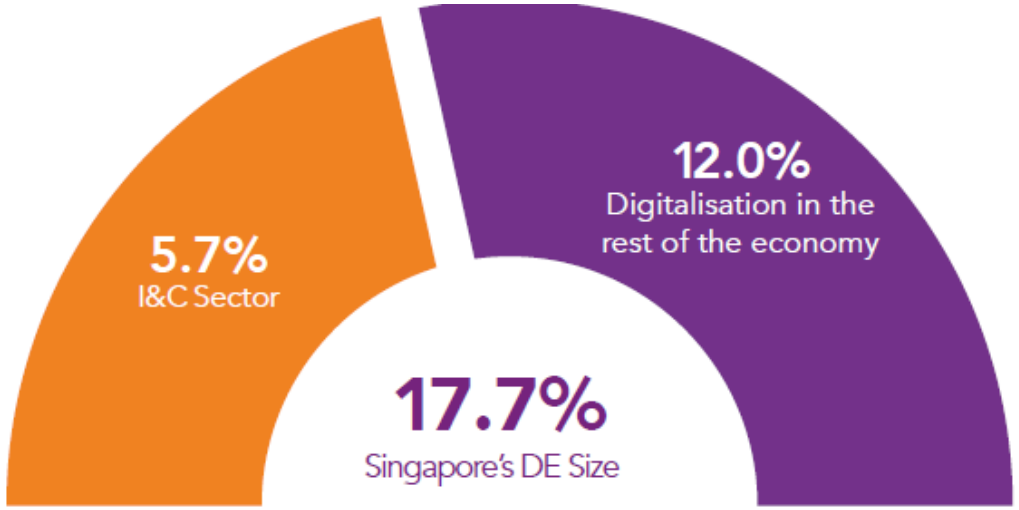
FROM RISK TO RESILIENCE

FORTIFYING YOUR ORGANISATION AND MAKING CYBERSECURITY YOUR COMPETITIVE ADVANTAGE

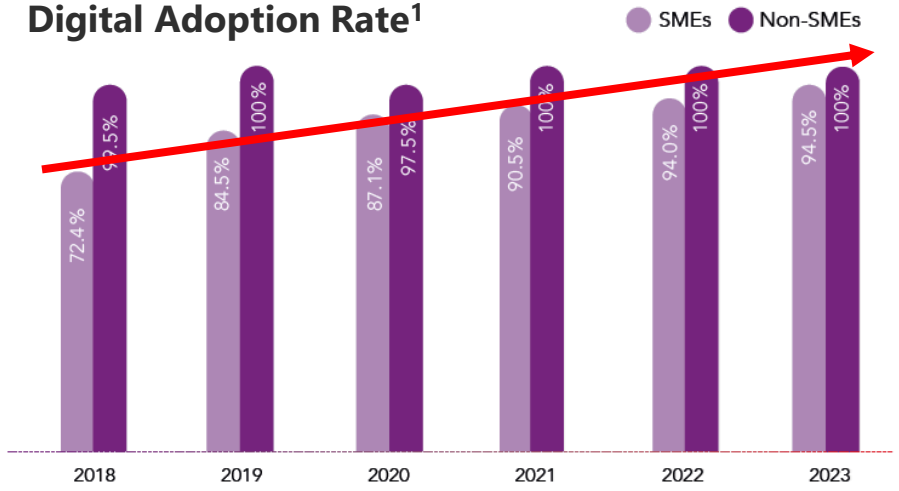
Safer Cyberspace Division
Cyber Security Agency of Singapore

The digital economy opens a range of new opportunities for organisations in Singapore

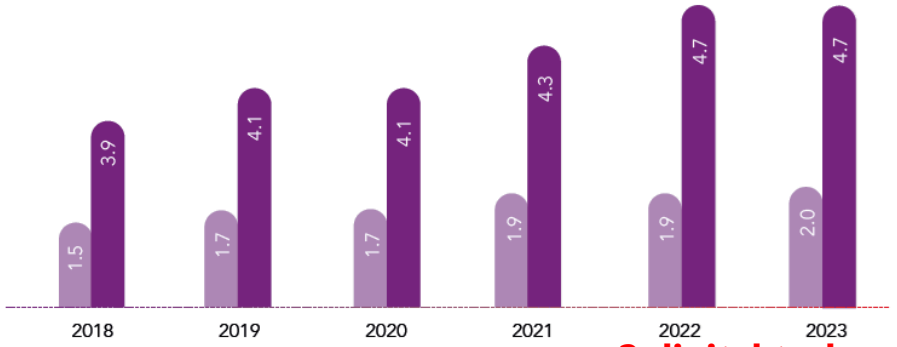
Composition of Singapore's digital economy size (% of GDP), 2023



Digital Adoption Rate[1]



Digital Adoption Intensity[2]



4.7 digital tech
Non-SME

2 digital tech
SME

1 - Percentage of firms adopting at least 1 digital technology

2 - Average no of digital technologies adopted per firm

Source – IMDA, 2024, "Singapore Digital Economy Report 2024"

Chemical industry leaders are increasingly implementing digitalisation to achieve business growth and sustainability goals[1]

Digital adoption intensity by sector

Source – IMDA, 2024, "Singapore Digital Economy Report 2024"

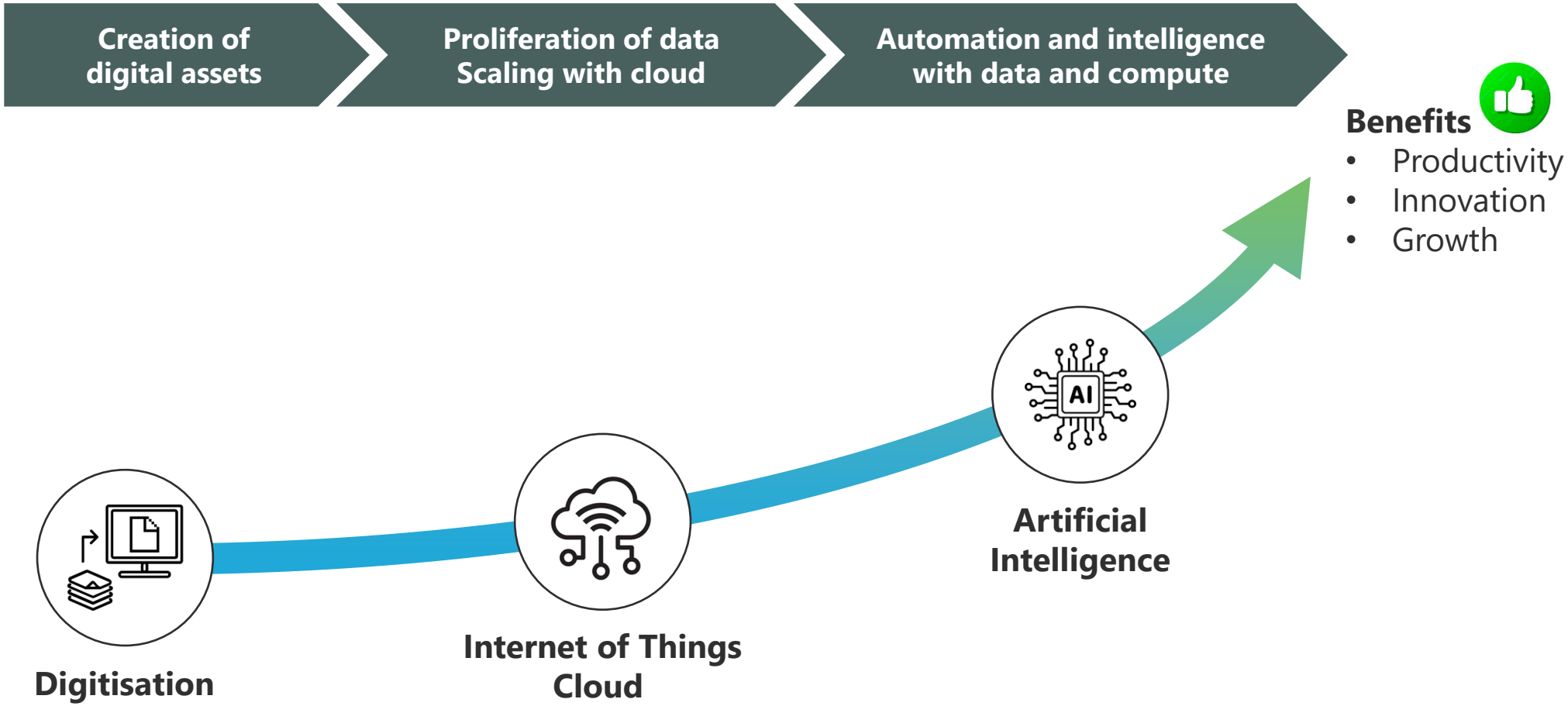
Digitalisation in chemical industry

56% *Speed of acceleration of digitalisation post-pandemic*

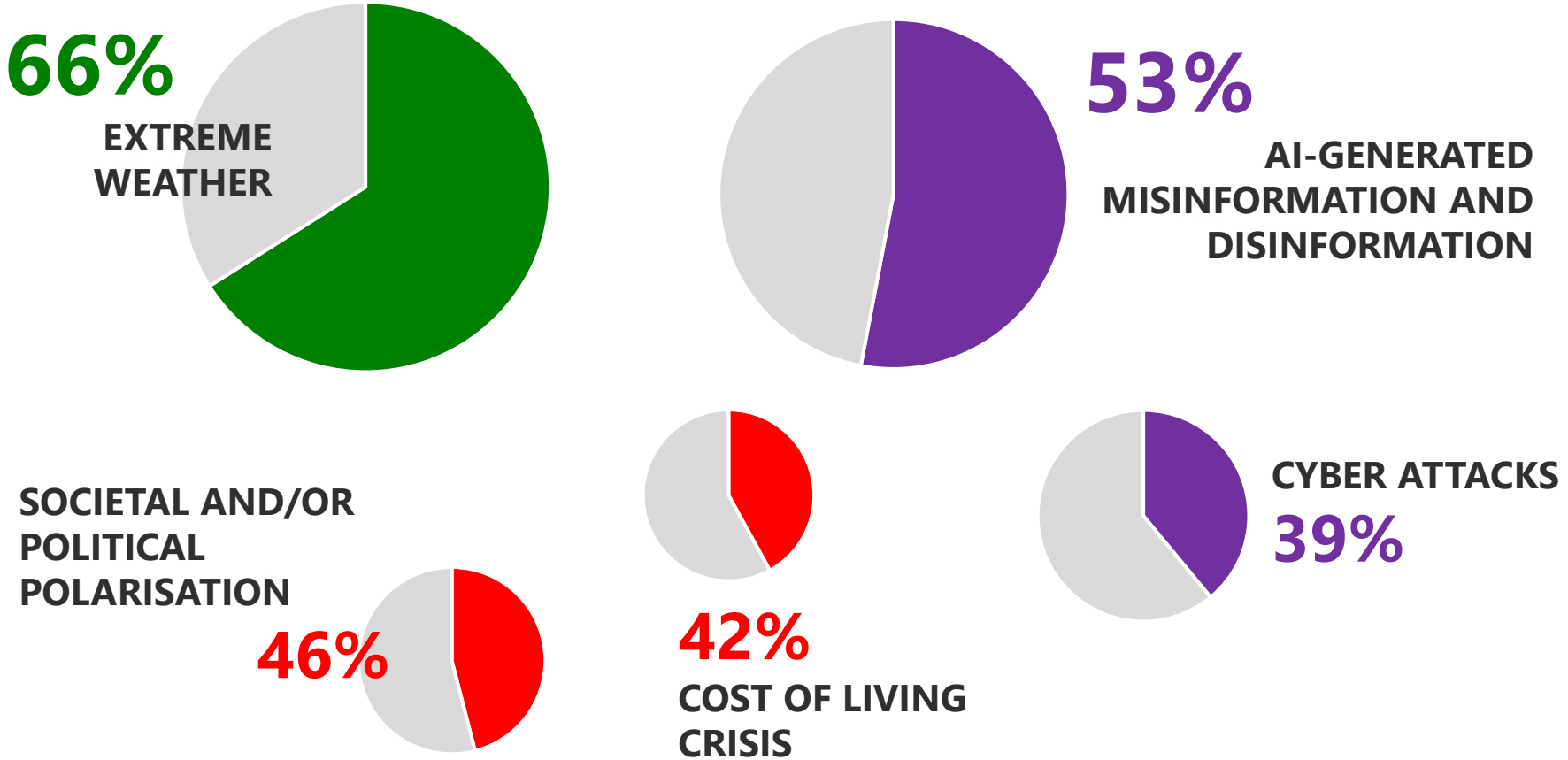
40% *of chemical businesses emphasize digitalisation to fulfill sustainability goals*

Source – Deloitte, 2022, "Why the chemical industry is prioritizing digitalisation"

Typical digital transformation journey for many organisations – reshaped by new/emerging technologies



AI- and cybersecurity-related risks are amongst the key tech risks at the top of business leaders' minds

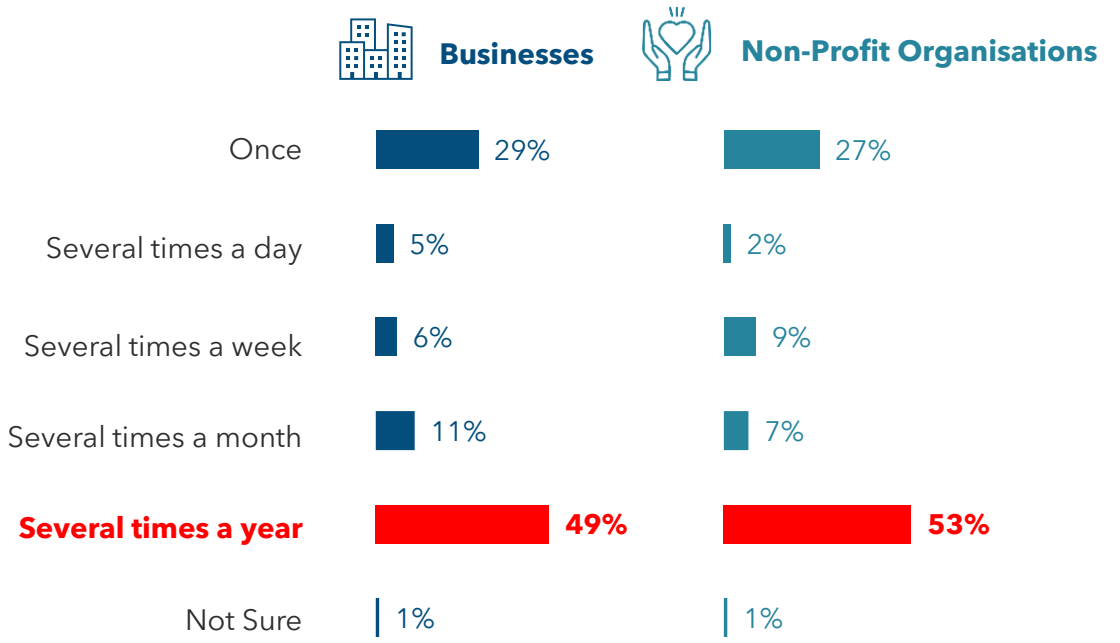


Source – World Economic Forum, 2024, "Global Risks Report 2024"

How vulnerable are organisations in Singapore to cybersecurity incidents? What are the key vulnerabilities?

OVER 8 IN 10 organisations have encountered a cybersecurity incident in a year

Frequency of Incidents



Top 5 Incidents

	Businesses	Non-Profit Organisations
1	Ransomware	Ransomware
2	Social Engineering	Social Engineering
3	Exploitation of cloud misconfiguration	Denial of Service (DOS) attack
4	Software / Zero-day vulnerabilities	Exploitation of cloud misconfiguration
5	Denial of Service (DOS) attack	Web application attacks

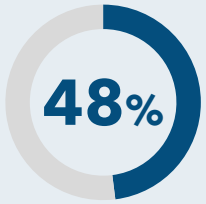
Source – CSA, Singapore Cybersecurity Health Report 2023

How does cybersecurity incidents impact your business?

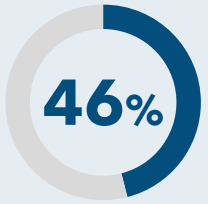
99% of these organisations suffered a business impact

Businesses

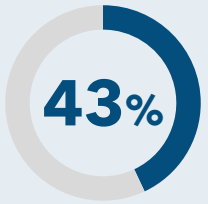
Business Disruption



Data Loss



Reputation Damage



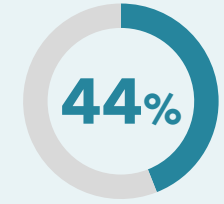
31%	Financial loss
27%	Incident response cost
26%	Regulatory implications

Non-Profit Organisations

Data Loss

Business Disruption

Reputation Damage



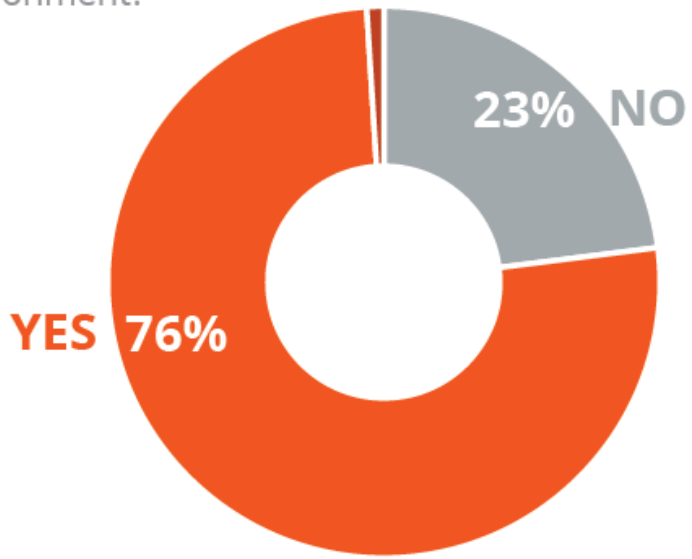
34%	Financial loss
25%	IP and/or Trade Secret loss
24%	Incident Response cost

Source – CSA, Singapore Cybersecurity Health Report 2023

Frequency and types of attacks in the industrial sector

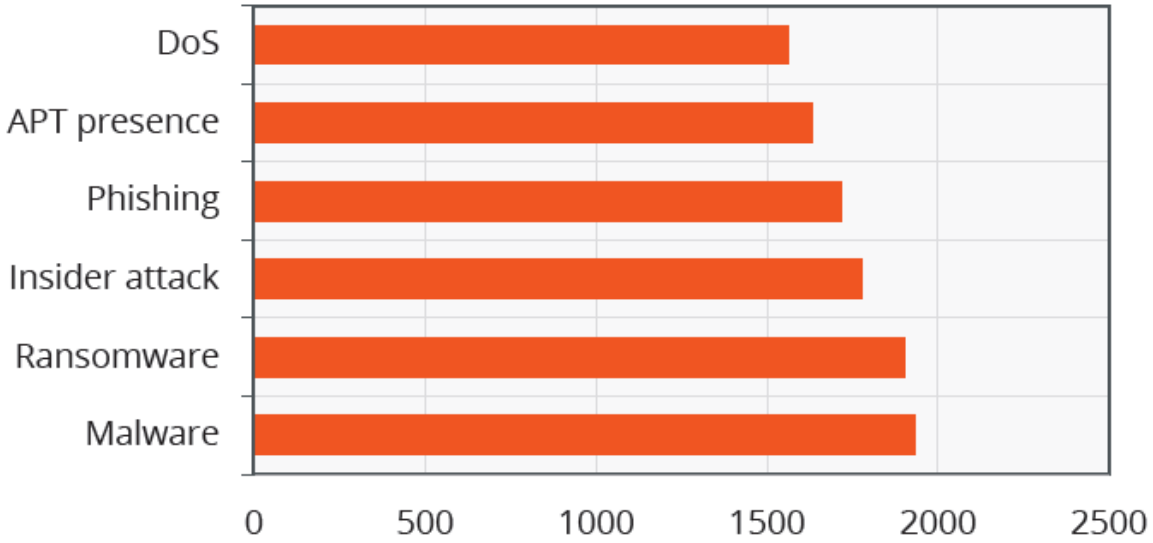
More than 76% of respondents have experienced a cyberattack in their OT environment

Has your organization ever experienced a cyberattack (s) in your OT environment?



Top Most Feared Attacks

What types of OT cyberattacks do you fear the most?



Ransomware particularly prominent

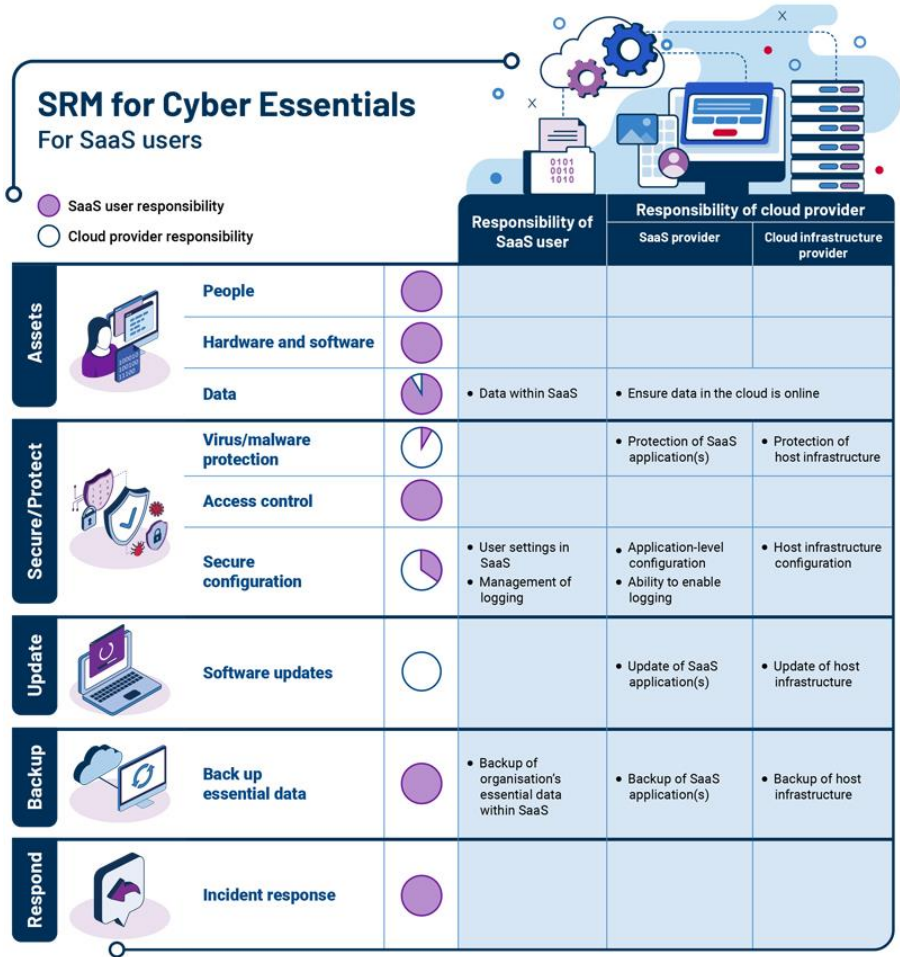
Syndicates such as DarkSide, BlackCat, and Ryuk having successfully breached the IT-OT gap to target OT environments - High success rate in utilities and the energy sector

Source – Palo Alto, Mar 2024, "The State of OT Security: A Comprehensive Guide to Trends, Risks and Cyber Resilience"

Cybersecurity is not static and evolves with new tech adoption

Intersections with cloud security

Cloud Shared Responsibility Model (SRM)



Source - CSA, Cloud Security for Organisations

67% *of respondents found shared responsibility model of SaaS most confusing[1] (IaaS - 59% , PaaS – 63%)*

Biggest Security Threats in Public Cloud[2]

59% Misconfiguration of the cloud platform/wrong setup

51% Exfiltration of sensitive data

51% Insecure interfaces/APIs

49% Unauthorized access

1 – "Demystifying the Cloud Shared Responsibility Security Model" Volume 2, Oracle and KPMG, 2020
2 – Checkpoint, 2023, Cloud Security Report

Cybersecurity is not static and evolves with new tech adoption

Intersections with AI security

88%

of prompt injection challenge participants ***successfully tricked GenAI bot*** *into* ***giving away sensitive info***

Source – Immersive Labs, May 2024

AI AS A THREAT

All organisations
AI-enabled attacks by adversaries

AI AS A TARGET

Organisations using AI
Expected to rise as more embrace AI

AI AS A TOOL

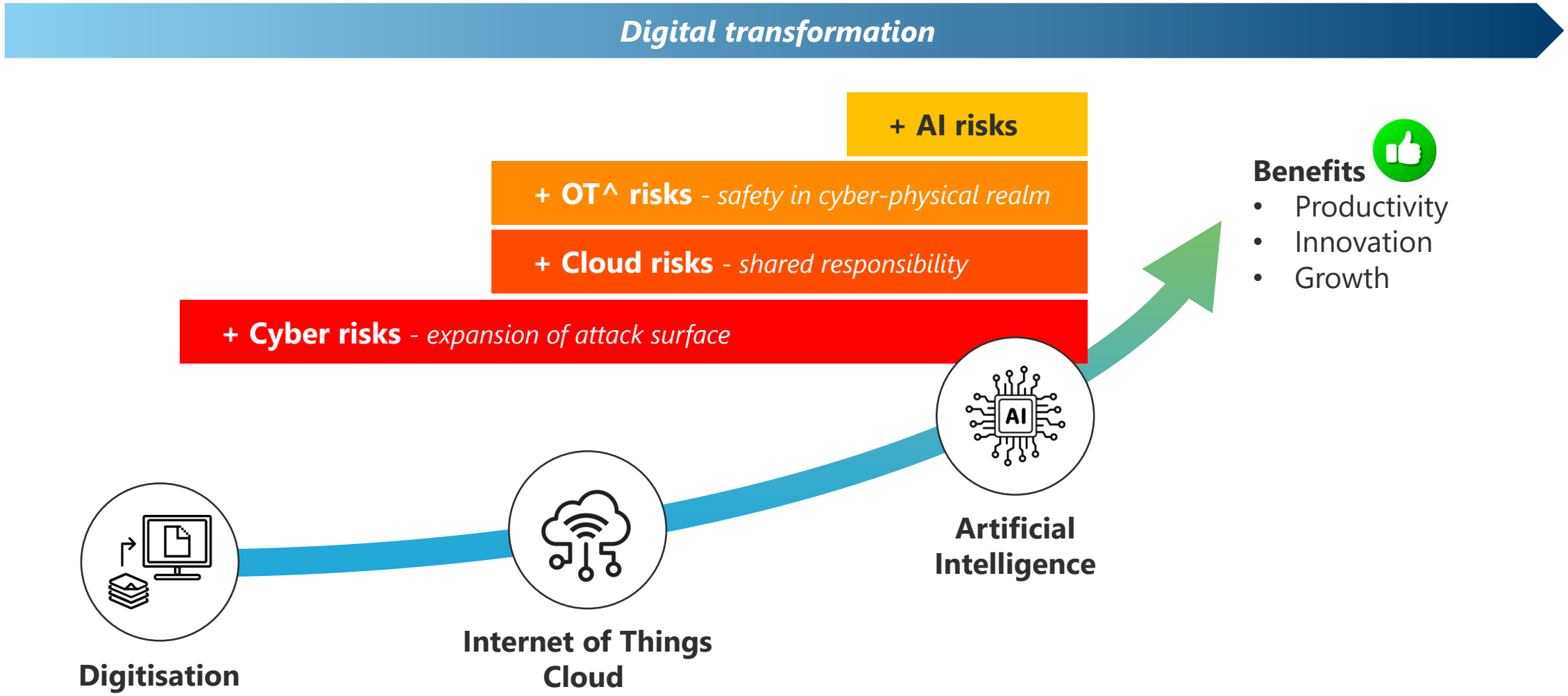
Use of AI to enable or support cybersecurity implementation in the organisation

Forbes

A Voice Deepfake Was Used to Scam a CEO Out Of $243,000

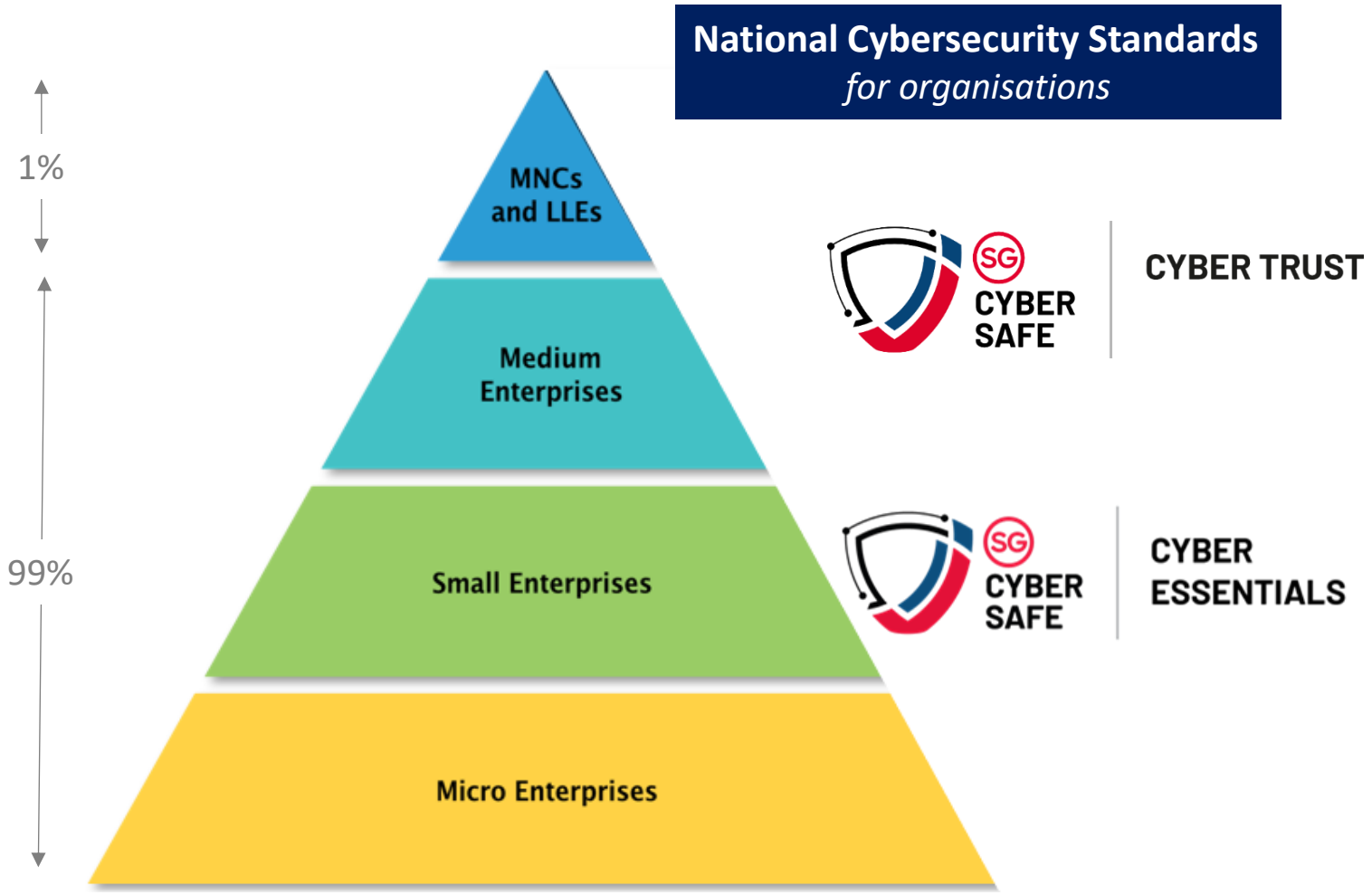
Source – Forbes, Sep 2019

Put in place strong cybersecurity foundation, and incrementally manage emerging tech risks with adoption



^ Operational Technology

Cyber Essentials and Cyber Trust help organisations to put in place good foundation for cybersecurity



For organisations that have gone beyond cyber hygiene

- Helps organisations take a risk-based approach to cybersecurity
- Provides guided risk assessment for organisations to match their risk level to their cybersecurity implementation

For organisations embarking in cybersecurity

- Helps organisations prioritise the cyber hygiene measures to implement first
- Equips organisations against common cyber attacks

Your organisation – Prevention is better than cure

Build a strong cyber foundation with Cyber Essentials

FOR ORGANISATIONS THAT ARE EMBARKING ON THEIR CYBERSECURITY JOURNEY

- Recognition of **good cyber hygiene** for **protection from common cyber attacks**
- Simplifies cybersecurity by **prioritising the measures** to focus on first

ASSETS

SECURE/ PROTECT

UPDATE

BACKUP

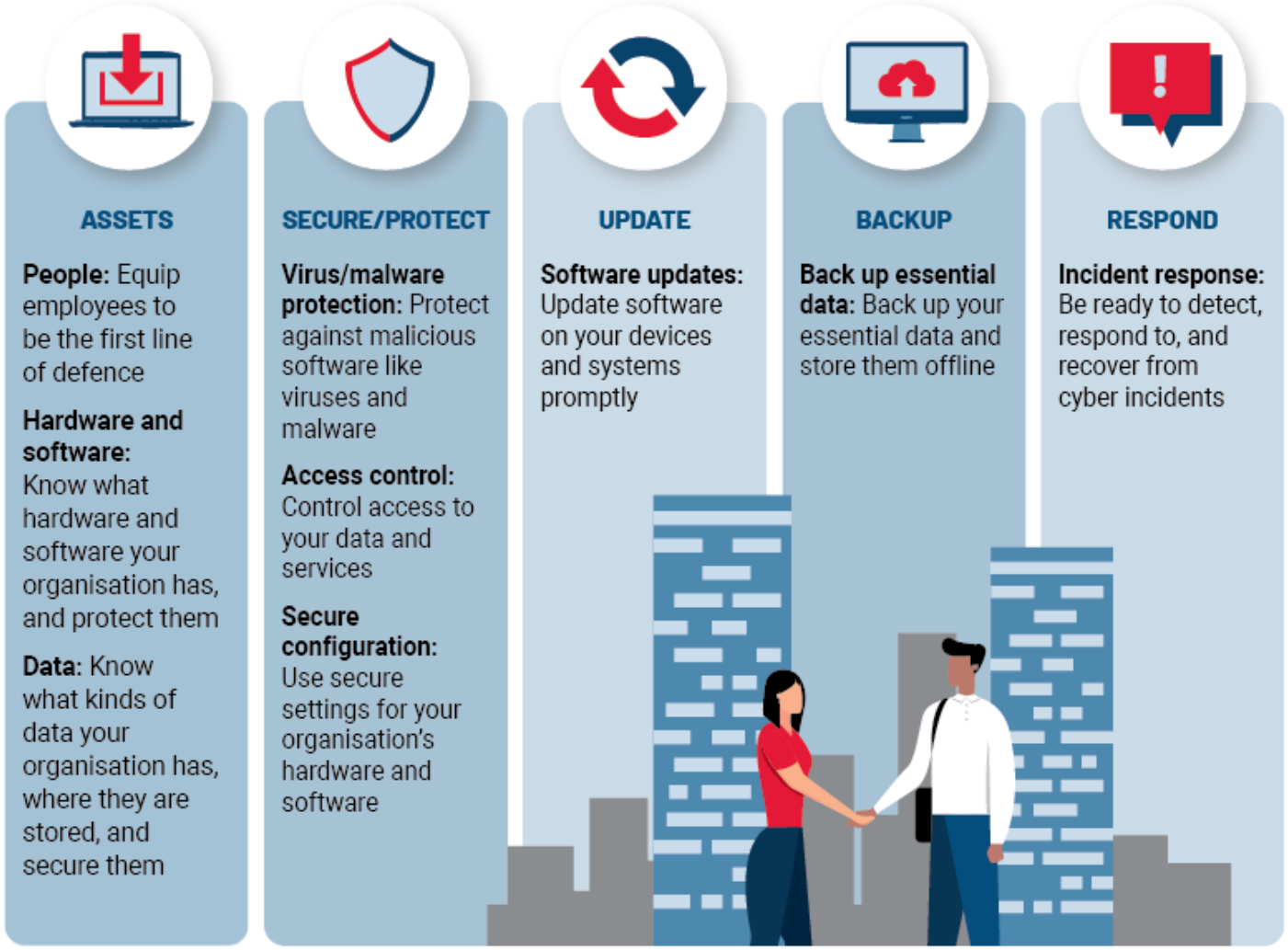
RESPOND

Certification Validity	**2** years
Assessment Mode *By independent assessor*	Desktop assessment

www.csa.gov.sg/cyber-essentials/

Your organisation – Prevention is better than cure

Cyber Essentials provides protection from common cyber attacks



ASSETS

People: Equip employees to be the first line of defence

Hardware and software: Know what hardware and software your organisation has, and protect them

Data: Know what kinds of data your organisation has, where they are stored, and secure them

SECURE/PROTECT

Virus/malware protection: Protect against malicious software like viruses and malware

Access control: Control access to your data and services

Secure configuration: Use secure settings for your organisation's hardware and software

UPDATE

Software updates: Update software on your devices and systems promptly

BACKUP

Back up essential data: Back up your essential data and store them offline

RESPOND

Incident response: Be ready to detect, respond to, and recover from cyber incidents

SG CYBER SAFE | CYBER ESSENTIALS

Your organisation – Prevention is better than cure

Cyber Trust mark helps organisations to take a risk-based approach to cybersecurity

MARK OF DISTINCTION FOR ORGANISATIONS WITH MORE EXTENSIVE DIGITALISATION

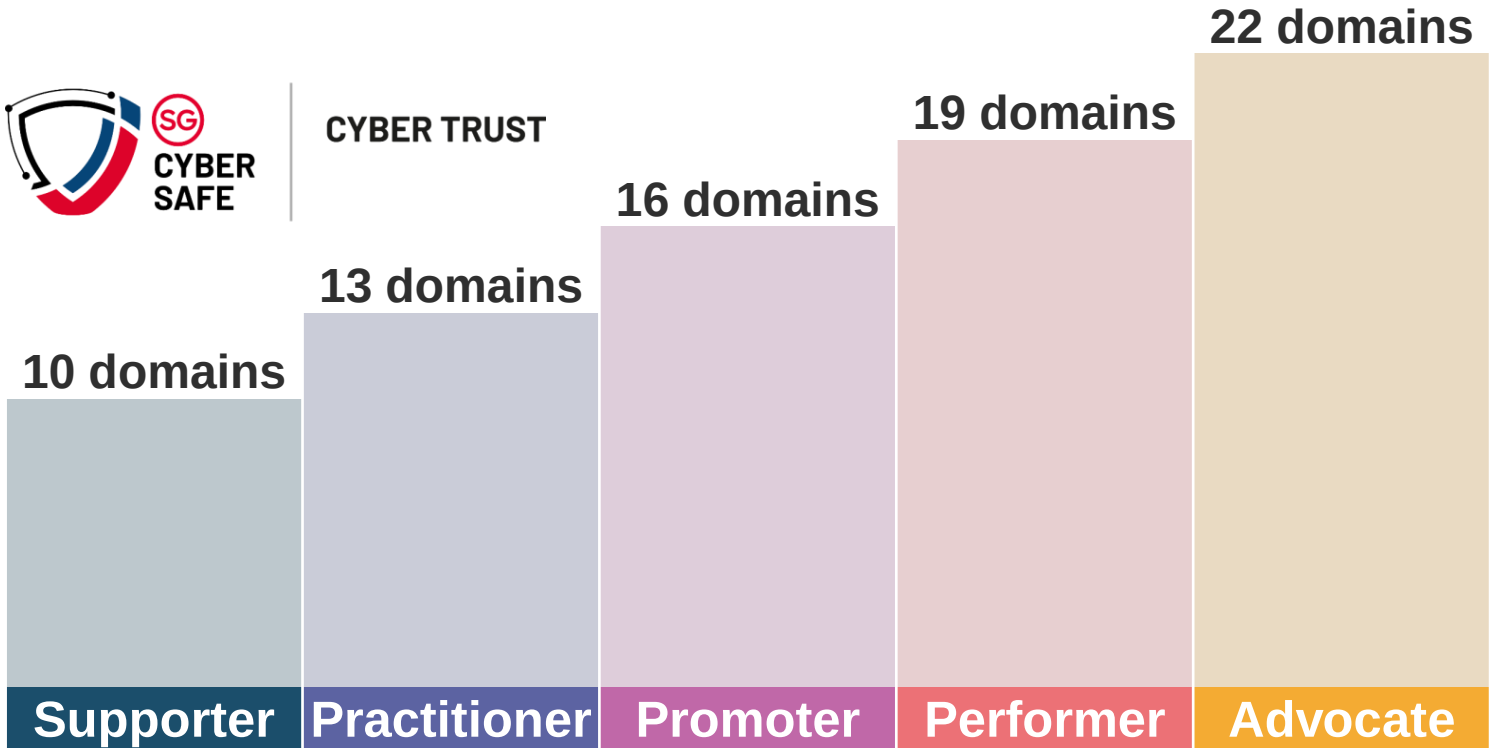
- Recognise organisations as **trusted partners** with robust cybersecurity
- Takes on **risk-based approach** to meet your organisation needs without over-investing

Certification Validity

3 years

Assessment Mode
By independent assessor

1. Documentation
2. Implementation and effectiveness



www.csa.gov.sg/cyber-trust/

Layer on security for digital technologies to achieve more holistic coverage of digital security risks

Cloud

Scope –
Cloud setup in orgn

Shared Responsibility Model

Operational Technology (OT)

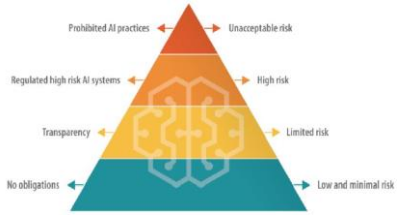
Scope –
OT setup in orgn

Safety

AI

Scope –
AI systems in orgn

Safety and AI risk mgmt



. . .

Cybersecurity - Risk-based approach

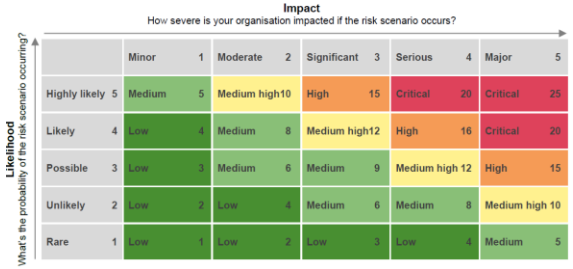
Scope - Organisation-Level

CYBER SAFE | CYBER ESSENTIALS

Cyber hygiene

CYBER SAFE | CYBER TRUST

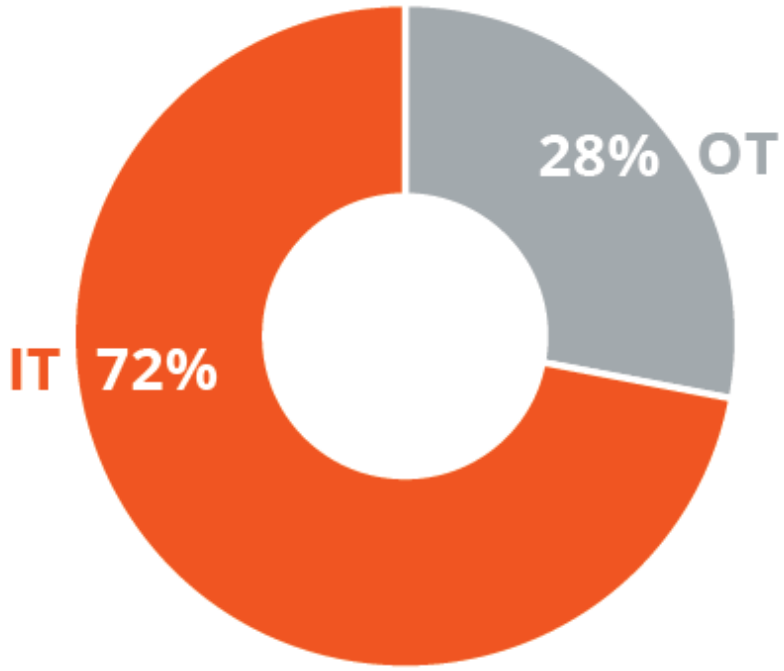
Risk management



Strategies for organisations deploying OT

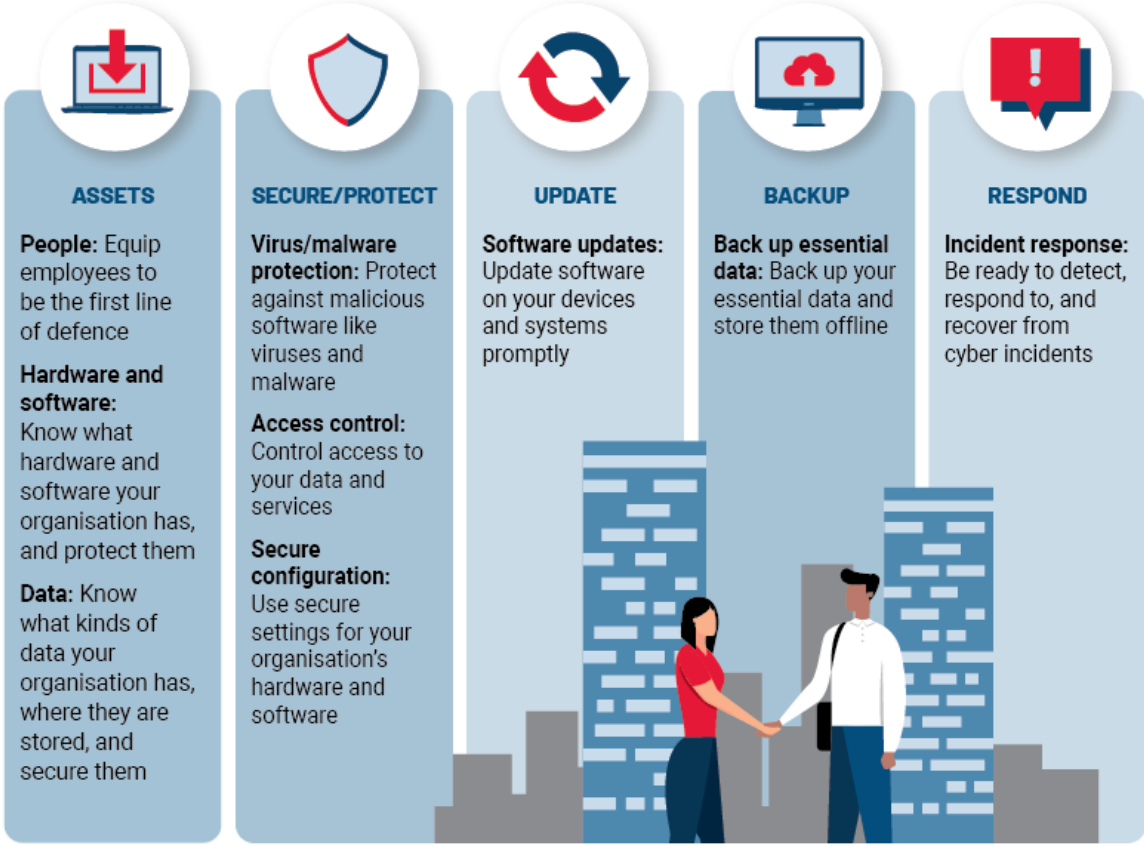
IT is the most popular attack entry point

Where did the attack originate?



Cyber Essentials

√ Classical cybersecurity



Source – Palo Alto, Mar 2024, "The State of OT Security: A Comprehensive Guide to Trends, Risks and Cyber Resilience"

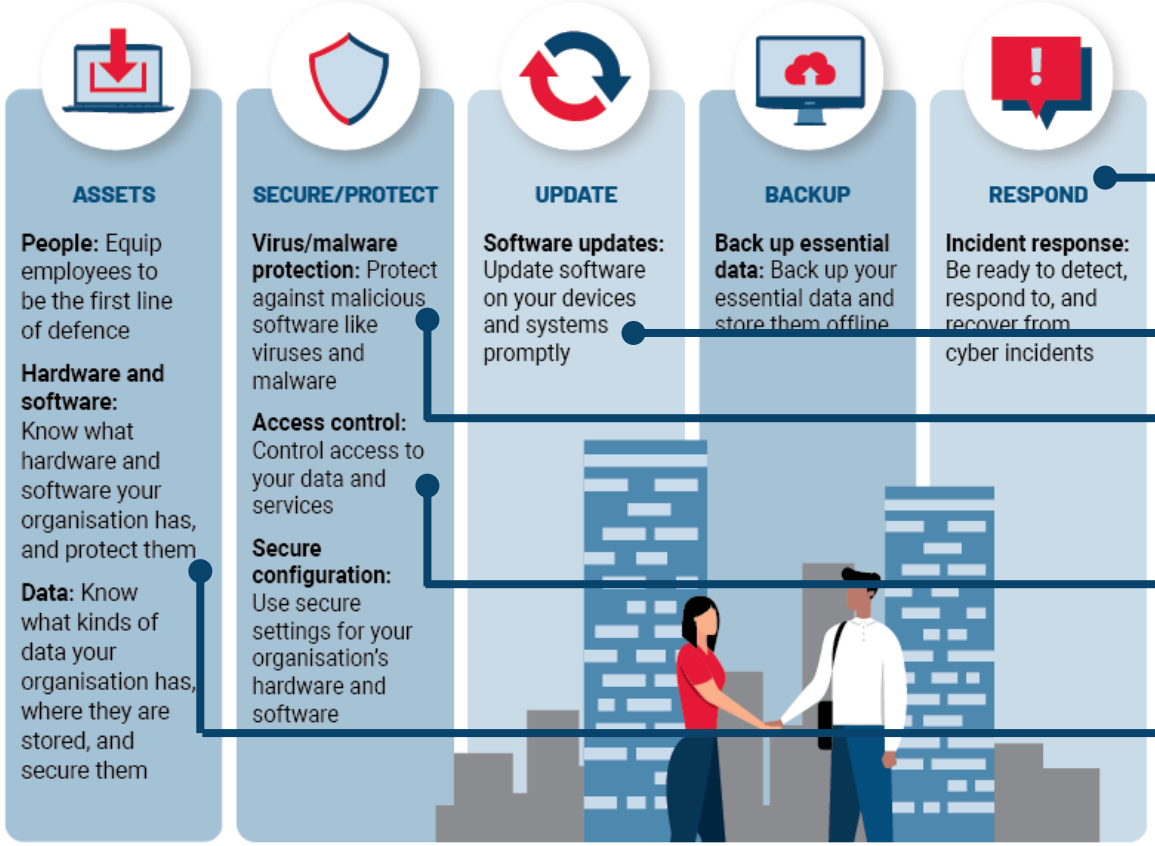
Strategies for organisations deploying OT

Protection for OT

Cyber Essentials

√ Classical cybersecurity

√ OT security



ICS incident response plan – Designed for OT environment

Risk-based vulnerability mgmt – Prioritise patching based on potential impact

Deploy segmentation – Minimize attack surface, reduce potential impact of incidents

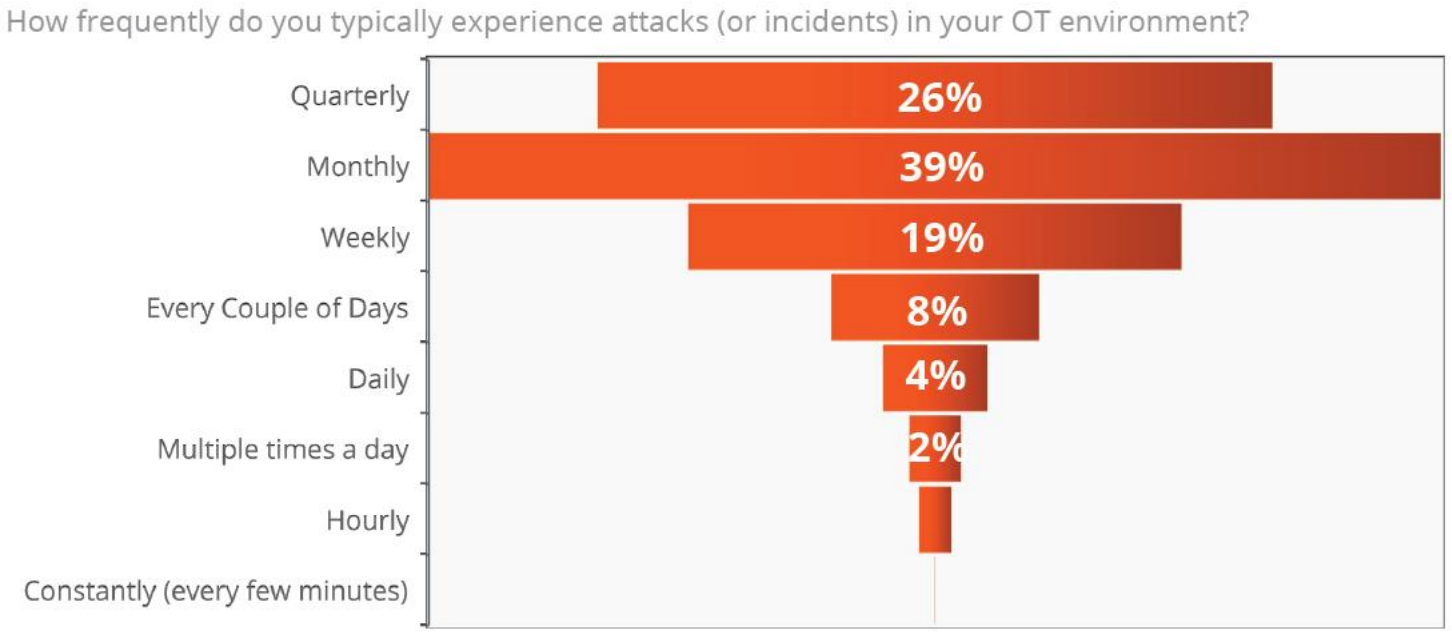
Secure remote access

Establish **visibility** and **compensating controls** for OT assets

Your suppliers

How secure are your 3rd party providers? Will your organisation be impacted as a result of an insecure provider?

Frequency of attacks (or incidents) in OT environment



An overwhelming 75% of respondents reported frequent attacks/incidents, often monthly, but also weekly and daily

Supply chain attacks

- ***Increasingly problematic*** threat, used successfully to target a greater number of organizations
- With industrial operators using *more commercial off-the-shelf solutions* in their OT, the *blast radius can be significant* and highly damaging

Timely to equip vendors so that this does not become the 'weak link'

Source – Palo Alto, Mar 2024, "The State of OT Security: A Comprehensive Guide to Trends, Risks and Cyber Resilience"

SG Cyber Safe programme provides guided approach to help organisations in their cybersecurity journey

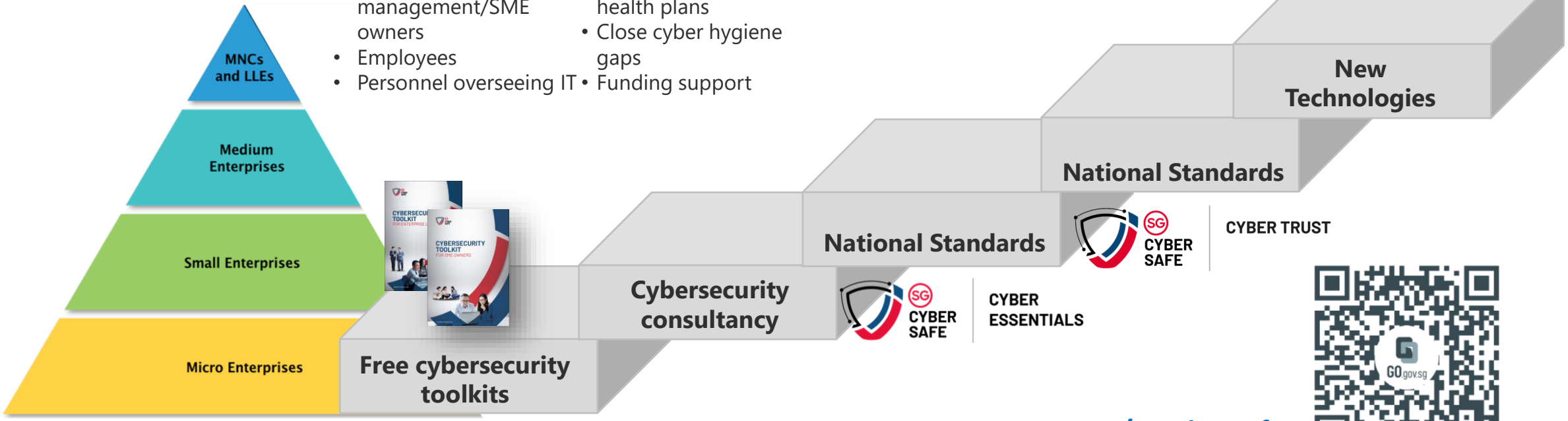
SG CYBER SAFE

Goal

Generate awareness → **Enable action** → **Help orgs attain minimum or appropriate level of cybersecurity** → **Manage digital security risks holistically**

For different roles in organisation:
- Senior management/SME owners
- Employees
- Personnel overseeing IT

Onboard consultants to help orgs with
- Tailored cybersecurity health plans
- Close cyber hygiene gaps
- Funding support



www.csa.gov.sg/sgcybersafe

Summary of cybersecurity resources and initiatives for organisations

SG CYBER SAFE

Self-Help

Cybersecurity Toolkits

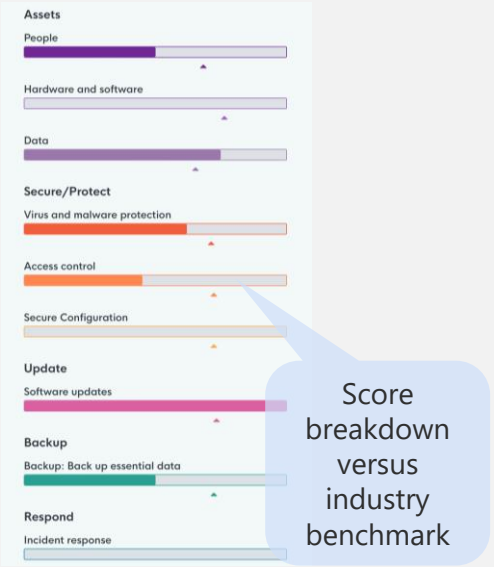
Business leaders or SME owners (link)

Employees (link)

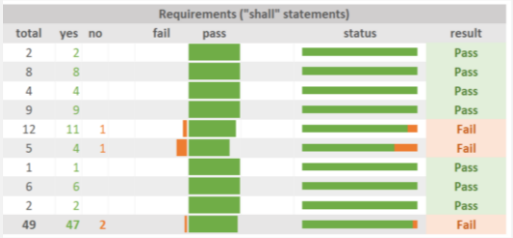
Personnel handling cybersecurity, e.g. templates (link)

Cybersecurity Health Check *(link)*

You are a Cyber Explorer 41/100



Cyber Essentials Self-Assessment *(link)*



- Conduct self-assessment before approaching certification body
- **Funding support for certification fees** available for eligible organisations

Outsource

Cybersecurity Health Plan with CISOaaS *(link)*

- Cybersecurity consultants onboarded by CSA
- Scope of service aligned to Cyber Essentials
- Consultants help you with cybersecurity health plan to identify cyber hygiene gaps and close gaps
- **Up to 70% funding support** available for eligible organisations

www.csa.gov.sg/sgcybersafe

THANK YOU

www.csa.gov.sg

CSAsingapore

CSA SINGAPORE