SMEA
經濟部中小企業處
Small and Medium Enterprise Administration
Ministry of Economic Affairs

Towards SME Digital Resilience

Unpacking the APEC Guidebook

Aslam Perwaiz,
Head, Disaster Risk Management Systems &
Team Leader,
***iPrepare Business* Facility of ADPC**

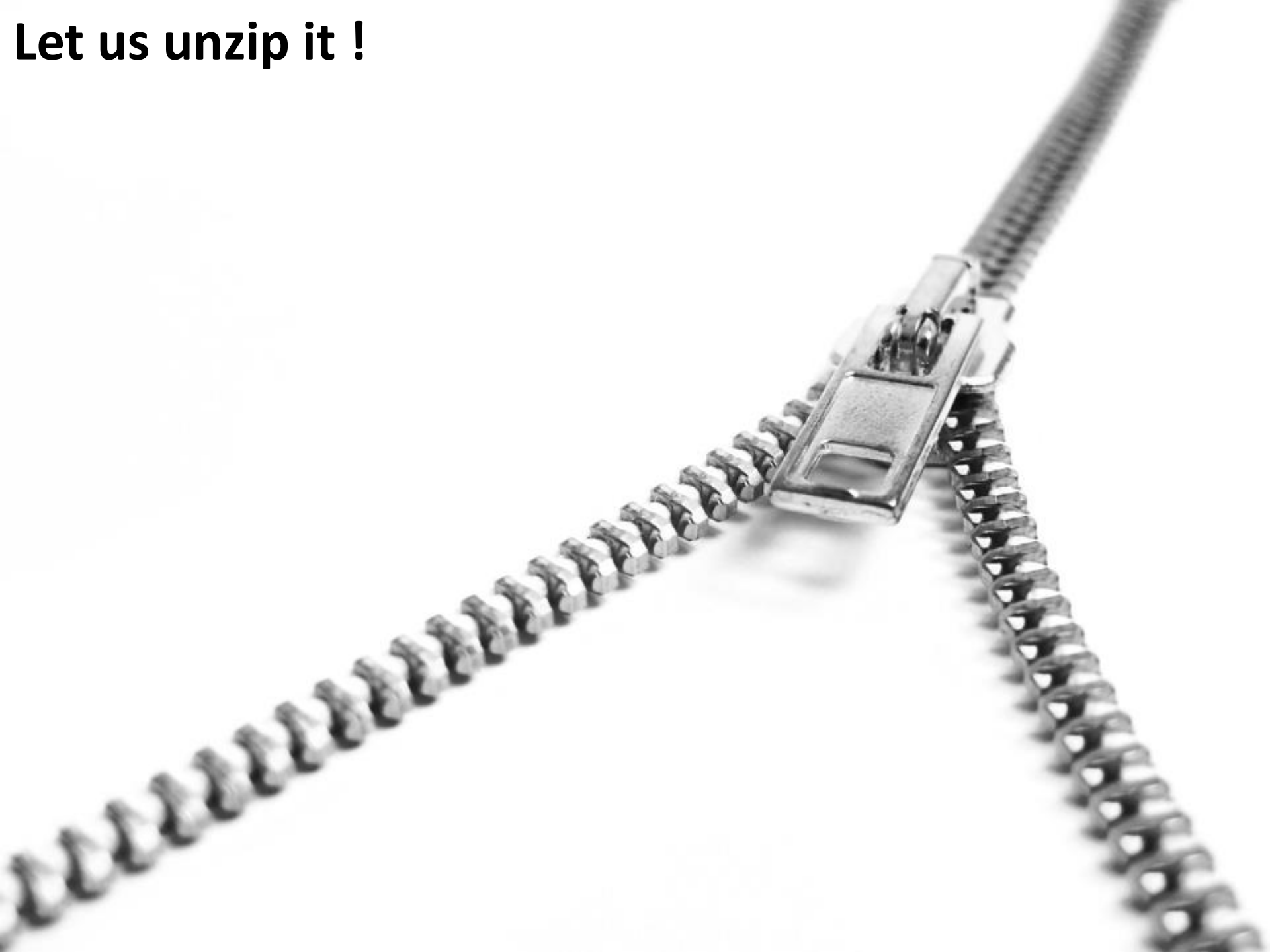
The term "digital resilience", therefore, refers to the capabilities of SMEs to respond to and recover from digital crises such as Internet security threats and cyber-attacks.

SMEs, cyber risk and resilience – to invest or not to invest?

How much do Small and Medium Sized Enterprises (SMEs) have to fear from cyber-attack?

74% of small businesses have suffered a cyber security breach, according to the PricewaterhouseCoopers 2015 Information Security Breaches survey . Of those affected, 38% suffered from viruses or malicious software while a further 16% were hit by a denial of service attack

Let us unzip it !



主辦單位
Host
經濟部中小企業處

合作夥伴
Partner
TREND MICRO 趨勢科技

執行單位
Organizer
台灣經濟研究院

Commissioned by the Small and Medium Enterprise Administration, Ministry of Economic Affairs, Chinese Taipei

Executed by the Industrial Technology Research Institute of Taiwan

APEC
Asia-Pacific Economic Cooperation

APEC
Guidebook on SME Digital Resilience

Key Steps

Step 1: Understanding your ISMS requirements and forming an ISMS team

Step 2: Determining ISMS policies and objectives

Step 3: Listing and categorizing information assets

Step 4: Identifying and evaluating information asset risk

Step 5: Assessing information asset risk

Step 6: Producing a risk treatment plan

Step 7: Selecting ISMS controls

Step 8: Establishing a business continuity plan

Step 9: Responding to and reporting information security incidents

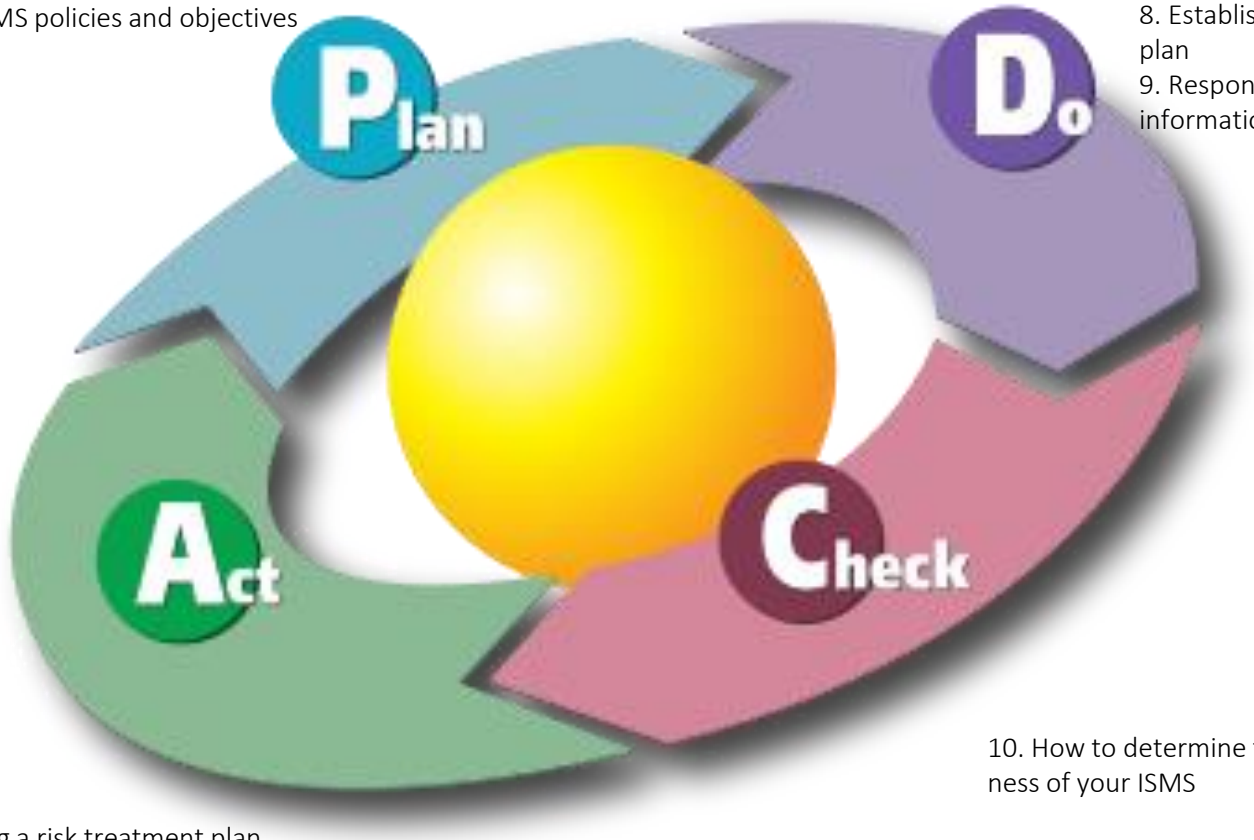
Step 10: How to determine the effectiveness of your ISMS

Step 11: Continuous ISMS improvement and problem follow-up

PDCA Cycle

1. Understanding your ISMS requirements and forming an ISMS team
2. Determining ISMS policies and objectives

3. Listing and categorizing information assets
4. Identifying and evaluating information asset risk
5. Assessing information asset risk
7. Selecting ISMS controls
8. Establishing a business continuity plan
9. Responding to and reporting information security incidents



10. How to determine the effective ness of your ISMS

6. Producing a risk treatment plan
11. Continuous ISMS improvement and problem follow-up

Key Words

1. ISMS requirements
2. ISMS team
3. ISMS policies and objectives
4. Information assets
5. Information asset risk
6. Risk treatment plan
7. ISMS controls
8. Business continuity plan
9. Information security incidents
10. ISMS effectiveness
11. ISMS Improvement

Questions

Aslam Perwaiz
Team Leader
iPrepare Business Facility of ADPC