

# SPIRITS

- ▶ A Commitment to Global Cyber Resilience



2017 December

# SPIRITS

- ▶ **S**ervice **P**rovider **I**nterconnection, **R**outing and **I**nformation **S**ecurity **B**est **P**ractices **S** (SPIRITS)
- ▶ A Compilation of Generally Accepted Best Practices of the Global Internet

# Organizers

- ▶ Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)
- ▶ Hong Kong Internet Exchange (HKIX)
- ▶ Hong Kong Internet Registration Corporation Limited (HKIRC)
- ▶ Hong Kong Internet Service Providers Association (HKISPA)
- ▶ Hong Kong Network Operator Group (HKNOG)



# The Problem

- ▶ Cyber security attacks are becoming more prominent today and caused extensive disruption to network services.
- ▶ Some of these attacks are taking advantage of existing deficiencies in protocols and the vulnerabilities of the devices connected to the Internet.
  - ▶ 2008 Pakistan local blocking of Youtube caused worldwide Youtube blackout
  - ▶ 2015 Route leak causing UK traffic routed through Ukraine
  - ▶ 2014+ Large scale DDoS attacks are now exploiting amplification of DNS, NTP protocols, spoofing of UDP traffic
  - ▶ 2016+ Large scale DDoS attack by Mirai IoT botnet (weak password) followed by IoT Reaper botnet on vulnerability exploits

# The Problem

- ▶ Some attacks are abusing the Internet infrastructure services
  - ▶ 2009- Domain Generation Algorithm used by botnets and malware [HKCERT + HKIRC]
  - ▶ 2015 Brute Force Campaign of Hee Thai Limited (ASN 63854) [HKCERT + APNIC]
    - ▶ [https://www.hkcert.org/my\\_url/en/blog/15042901](https://www.hkcert.org/my_url/en/blog/15042901)

# The Solution

Problem	Possible Solution
Route Hijacks and Leaks	Good Routing Practice Use BGPsec and RPKI
Attacks Using Spoofed Traffic	Filter Spoofed Traffic Use TCP instead of UDP protocol
Amplified Attack	Harden Internet Services
Securing your own network is necessary but not sufficient to bring you security	Build a secure culture and norm of network hygiene → others also do their security
Abuse of Internet Infrastructure	Collaborated response to Security Incidents

Effort : BCP38 RFC2827 (Year 2000)

## BCP38 (Network Ingress Filtering)

- ▶ Defeating Denial of Service Attacks which employ IP Source Address Spoofing

# APNIC Security Practices



- ▶ **Source Address Validation Everywhere (SAVE) or Best Current Practice (BCP) 38**
  - ▶ Filter spoofed IP addresses used by Distributed Denial of Service (DDoS) attacks.
- ▶ **Resource Public Key Infrastructure (RPKI)**
  - ▶ Allows IP address holders to specify which Autonomous Systems are authorized to originate their IP address prefixes.
- ▶ **Domain Name Security Extensions (DNSSEC)**
  - ▶ Help prevent attacks that hijack the process of looking up a website.
- ▶ **Updated Incidence Response Team (IRT) reference in APNIC Whois**
  - ▶ Ensure network admin be reached easily
  - ▶ Combat network abuse



# MANRS



















## Mutually Agreed Norms for Routing Security

- ▶ Initiated by Internet Society
- ▶ Objective
  - ▶ Improving Security and Reliability of Global Internet Routing System based on collaboration and shared responsibility
- ▶ Expected Actions
  1. Prevent propagation of incorrect routing information.
  2. Prevent traffic with spoofed source IP addresses.
  3. Facilitate global operational communication and coordination
  4. Facilitate validation of routing information on a global scale



# MANRS Participant Directory

- 55 global network providers shown

	Country	ASNs	<u>Filtering</u>	<u>Anti-spoofing</u>	<u>Coordination</u>	<u>Global Validation</u>
<a href="#">NTT</a>	US	2914				
<a href="#">ClaraNet</a>	UK	8426				
<a href="#">SURFnet</a>	NL	1103				
<a href="#">LACNIC</a>	UY	28000, 28001, 28002				
<a href="#">TransIP B.V.</a>	NL	20857				

<http://www.manrs.org/participants>

# What the Early Participants of MANRS said?

Jason Livingood, Vice President, Internet Services, **Comcast**

- ▶ *Comcast is committed to helping drive improvements to the reliability of the Internet ecosystem. We are thrilled to be engaged with other infrastructure participants across the spectrum and around the globe in pursuit of these goals.*

Dale Drew, Senior Vice President, Chief Security Officer, **Level 3 Communications**

- ▶ *As one of the most connected Internet providers in the world, security of the Internet is top-of-mind at Level 3 Communications.*
- ▶ *We are dedicated to supporting and protecting the Internet ecosystem and work each day to safeguard customers' critical communications. The Internet is a shared responsibility, and only through these important collaborative efforts can we continue to ensure the protection of this collective infrastructure. -*

# What the Early Participants of MANRS said?

## Xing Li, Deputy Director, CERNET

- ▶ *CERNET believes the security, stability, and resiliency of the Internet operation can be improved via distributed and shared responsibilities as documented in MANRS. As one of the largest academic networks in the world, CERNET is committed to the MANRS actions. - Xing Li, Deputy Director*

# SPIRITS

- an introduction

# Timeline of the Birth of SPIRITS

## ▶ 2016

- ▶ **Sep** "Challenges to Cyber Resilience (for Internet Infrastructure Providers)" Symposium
  - ▶ Organized by HKCERT, HKISPA and HKNOG

## ▶ 2017

- ▶ **May** 5-party Meeting @ HKCERT
- ▶ **Sep** First Draft of SPIRITS
- ▶ **Nov** Second Draft of SPIRITS
- ▶ **Dec** HKISPA Symposium

# Background

- ▶ Internet infrastructure providers (ISPs and network providers) and cyber security watchdog in Hong Kong are taking the initiative to help safeguard the resilience and security of the Internet.
- ▶ SPIRITS is a baseline of actionable recommendation for ISPs and hosting service providers to apply. It is also a visible commitment to the community to promote collaborative security.

# Objectives of SPIRITS

- ▶ Promote the **culture of shared responsibility by service providers** for security and resilience of the Internet
- ▶ Provide **accepted standards and best practices** in a summarized benchmark
- ▶ Encourage **commitment to good practice standards in the industry**
- ▶ Educate end users the **security metrics** to look for when procuring Internet services



# 6 Voluntary Subscribed Actions

## 1. Coordination

- ▶ Maintain globally accessible up-to-date contact information
- ▶ Participate in information sharing and security incident response

## 2. Anti-spoofing Routing

- ▶ Enable source address validation in the infrastructure

## 3. Network Route Filtering

- ▶ Manage routing and prevent propagation of incorrect routing information

## 4. Internet Services Protection

- ▶ Ensure a secure Internet exchange peering
- ▶ Ensure authenticity, security and prevent abuse in key Internet services including Mail, DNS and NTP

## 5. Operation Security Best Practice

- ▶ Ensure accountability and trust in policy and logging
- ▶ Comply with local law and regulations

## 6. Global Validation

- ▶ Publish data and commitment to the best practices for public validation

# Comparison

	<b>SPIRITS</b>	<b>MANRS</b>	<b>APNIC Best Practice</b>	<b>BCP38</b>
1.	Coordination	Coordination	WHOIS IRT Contacts	
2.	Anti-spoofing Routing	Anti-spoofing	SAVE (Anti-spoofing)	Anti-spoofing
3.	Network Route Filtering	Filtering	RPKI	
4.	Internet Services Protection		DNSSEC	
5.	Operation Security Best Practice			
6.	Global Validation	Global Validation		

# Deliverables



- ▶ A set of up-to-date best practices with checklist

- ▶ Web directory displaying service providers who declared commitment to the best practices
- ▶ Public has the visibility on the applicable best practices adopted by each listed service provider.

# MANRS Project Study Report

## August 2017

- ▶ While MANRS itself is not well known by enterprises, its attributes are highly valued.
- ▶ Enterprises have high expectations for MANRS efforts.
- ▶ Enterprise perceptions of MANRS can translate into increased revenue for service providers.
- ▶ Existing MANRS actions cover a reasonable set of controls.
- ▶ There are options to extend the MANRS actions for some providers.

BLACK & WHITE PAPER

451 Research | Advisory

## MANRS Project Study Report

AUGUST 2017

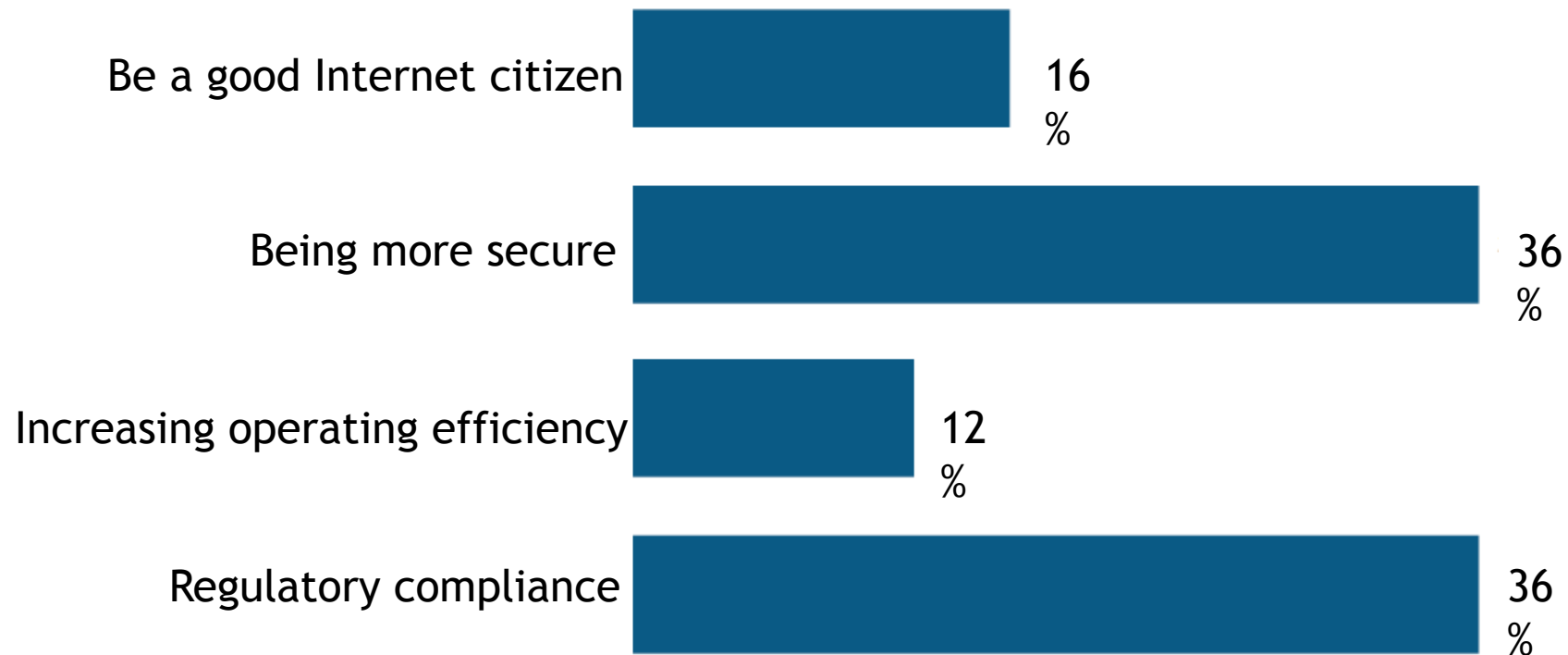
COMMISSIONED BY



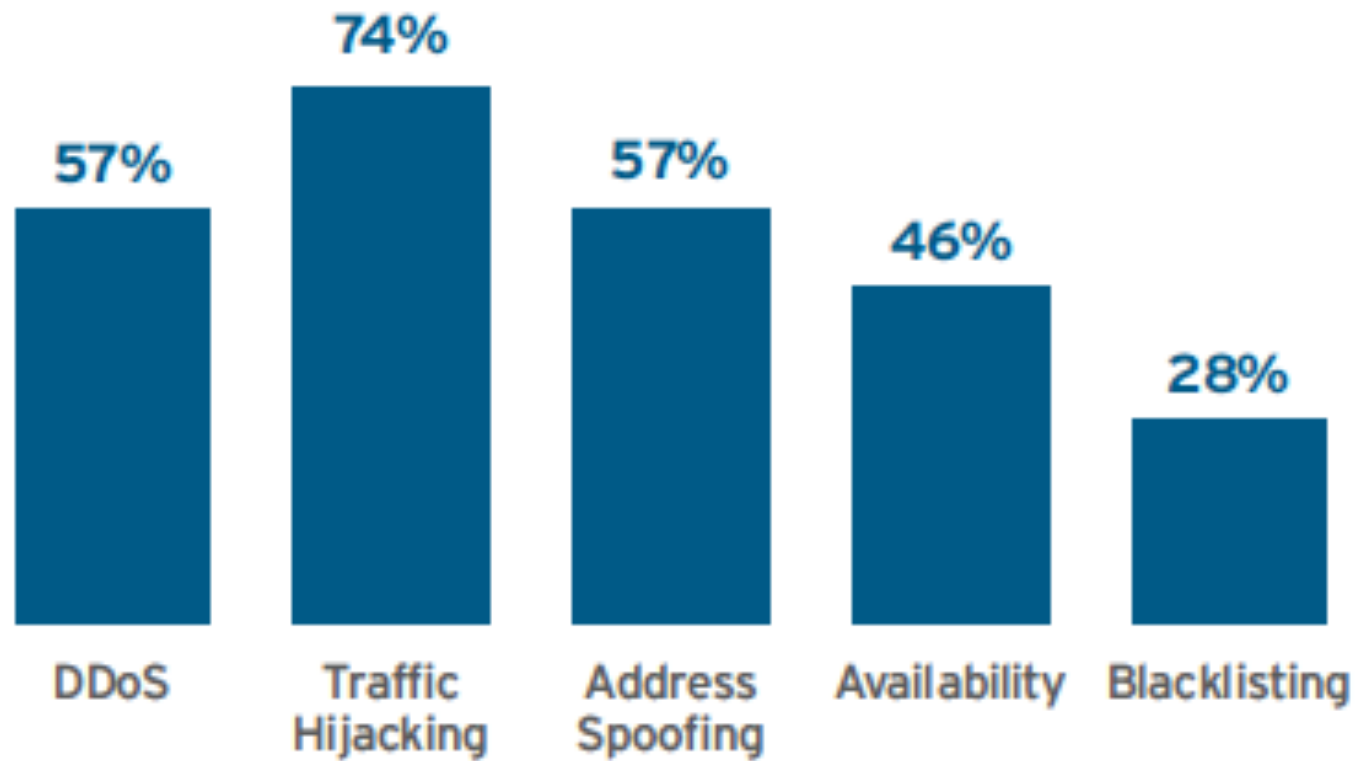
©COPYRIGHT 2017 451 RESEARCH. ALL RIGHTS RESERVED.

# Service Provider Study: Reason for implementing MANRS

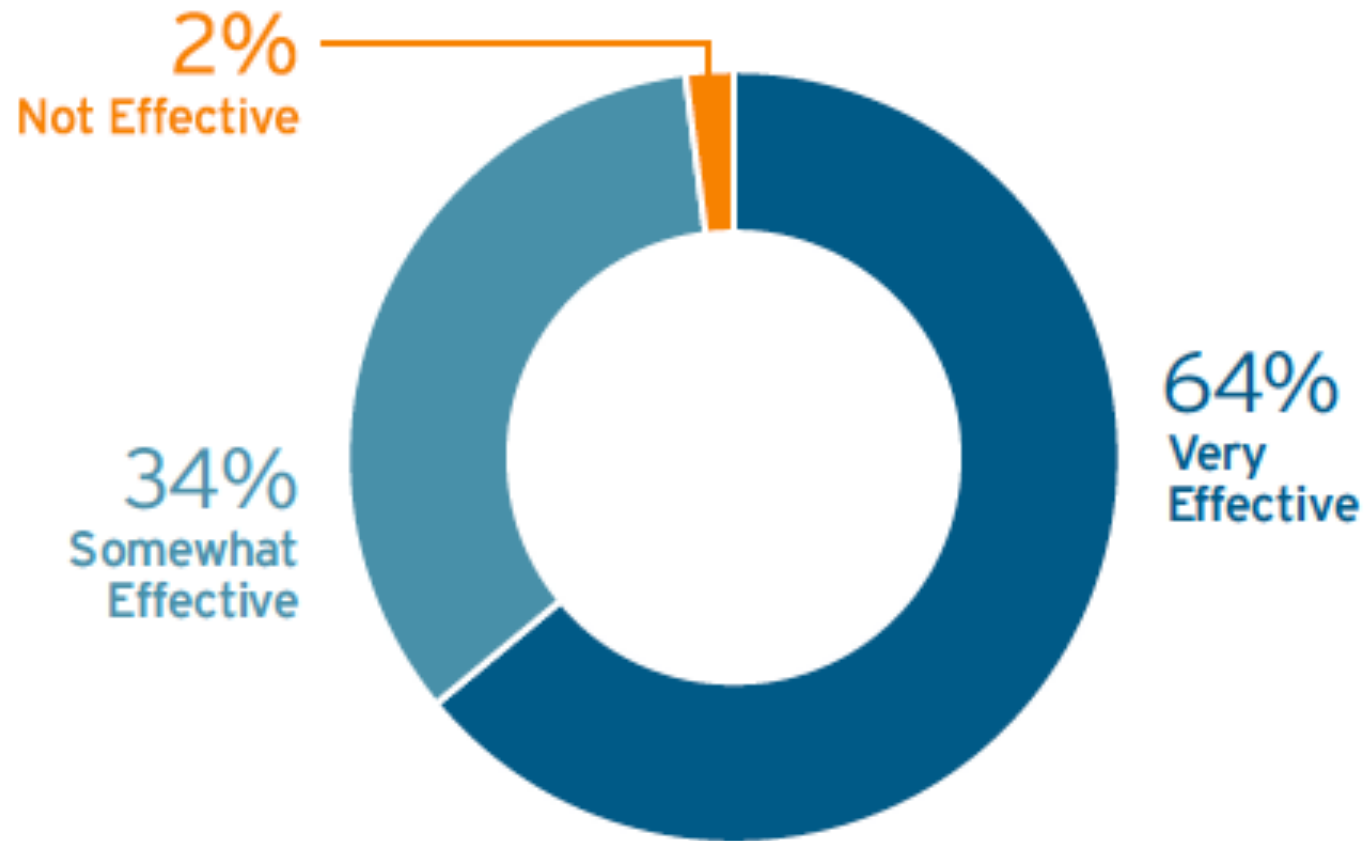
- ▶ Near two-thirds heard about MANRS
- ▶ Cautious enthusiasm for MANRS in the service-provider community



# Enterprise Study: Internet Security Concerns

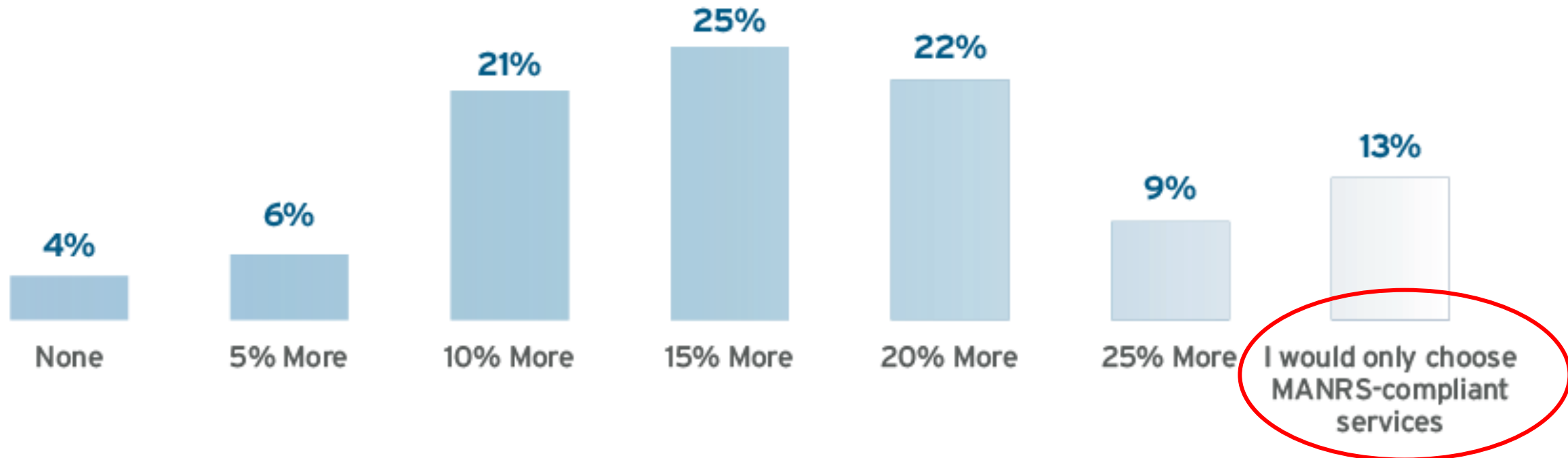


# Enterprise Study: MANRS Effectiveness



# Enterprise Study: Pricing Premium for MANRS

- ▶ Enterprises willing to pay more for MANRS compliance, the median value was 15%





# Incentive for Best Practices / SPIRITS

- ▶ Regulation
- ▶ Operational benefits of good neighbourhood
- ▶ Better Security
- ▶ Service Provider: Differentiation; Competitive Value
- ▶ Consumers: need certainty on performance, security and interoperability, and last of all free from provider locking

# Right time for SPIRITS

- ▶ Maturity of Internet services competition
  - ▶ More value to add to service
- ▶ Cloud computing catalyzes the need of service provider transparency in
  - ▶ Security and Privacy Protection Capability (ISO27017, 27018)
  - ▶ Security-as-a-Service
- ▶ Growing Global Regulation on Security and Privacy
  - ▶ GDPR
  - ▶ NIST Cyber Security Framework

# Next Step

## ▶ 2017

- ▶ **Dec** Circulate Version 1 of Framework (Voluntary Participation and Listing) for comment

## ▶ 2018

- ▶ **Mar** Website published
- ▶ **Apr** Deadline for Consultation Inputs
- ▶ **May** Version 2 published
- ▶ **Jun** Publication of Initially Committed Service Providers

# Questions for you and us

- ▶ How can SPIRITS be made to help the industry?
- ▶ What are your concern with SPIRITS ?
- ▶ Will you like to contribute to SPIRITS?
- ▶ What are the future features that we need to consider?
  - ▶ Training ?
  - ▶ Validation ?

The background features abstract, overlapping green geometric shapes in various shades of green, creating a modern and dynamic look. The shapes are primarily triangles and polygons, some with thin white outlines, set against a white background.

# Thank You

S.C. Leung

Centre Manager

HKCERT

Email: [scleung@hkcert.org](mailto:scleung@hkcert.org)