Panel: From Cyber Resilience to Confidence

Moderator: Phoram Mehta, President (ISACA Singapore Chapter)

Panelists: Koh Suat Hong(PDPC), Joshua McCloud (Cisco Systems), Lim Thian Chin (Cyber Security Agency of Singapore), Joe Weiss (Applied Control Solutions), John Yong (SATA CommHealth)

GTACS 2020
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA
Singapore Chapter

The Breach Goes On

Joshua McCloud
National Cybersecurity Officer, Cisco

Current Event Lures

Growth in percentage of attacks leveraging COVID-19, racial injustice, etc

Malware & Phishing

COVID-19 (PoetRat)
Public health notices with RAT infection

Black Lives Matter (Trickbot)
Social campaign with banking trojan

Organizations & Critical Infrastructure

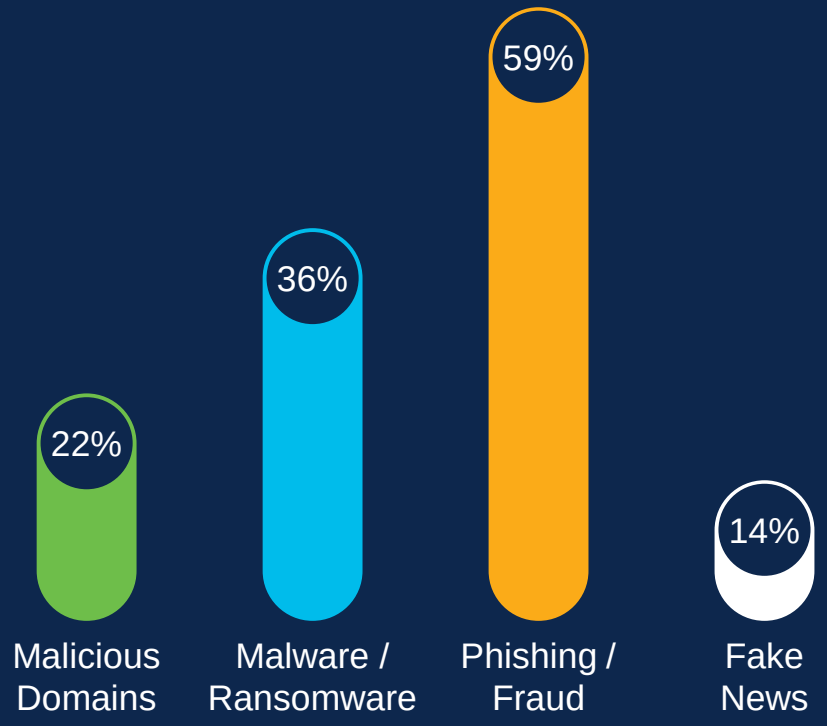
Healthcare (Kwampirs)
Supply chain attack on hospital ICS management

Critical Infrastructure (DDoS, Ransomware, Vulnerabilities)
Remote access attacks – VPN, RDP
Video conferencing vulnerabilities

Source: Cisco Talos

INTERPOL Report

Cybercrime: COVID-19 Impact



Main Treats Identified

Asia Regional Trends

COVID-19 related fraud and phishing campaigns

Illegal online sale of fake medical supplies, drugs, PPE

Fake news and misinformation related to COVID-19

Lack of cybersecurity awareness and ‘hygiene’

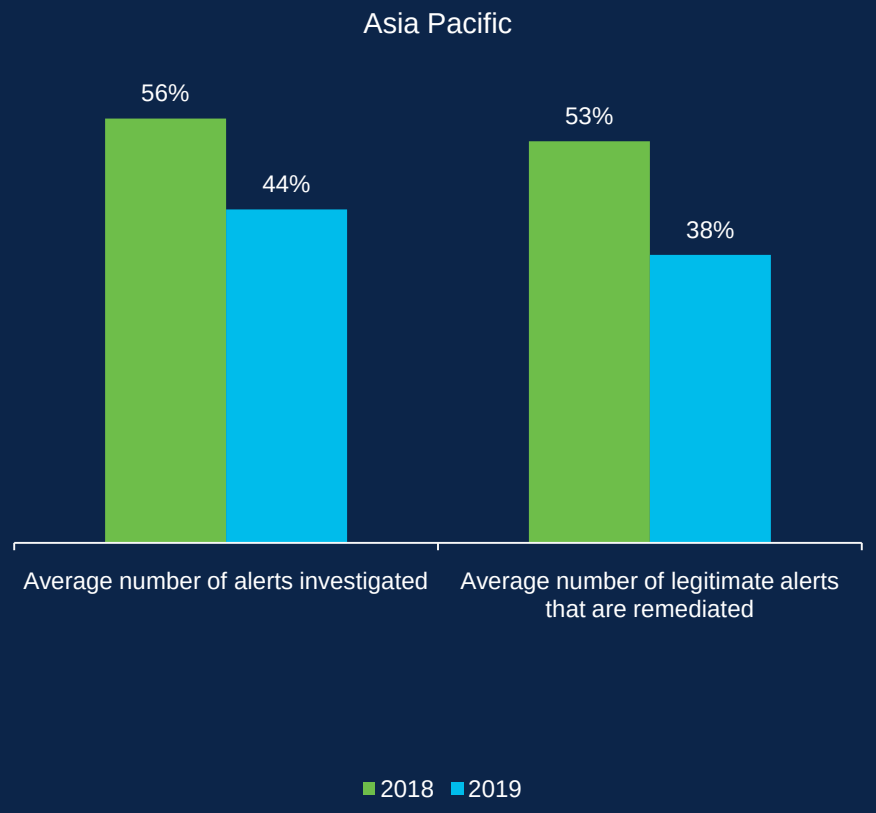
Source: INTERPOL

Security practitioners in Asia Pacific are being kept busier than their global counterparts

Percentage of organizations that reported receiving more than 10,000 alerts a day

Source: Cisco 2019 Asia Pacific CISO Benchmark Study
http://cs.co/APACbenchmark

Organizations in Asia Pacific continue to struggle to cope with security



Hackers are no longer just targeting IT infrastructure

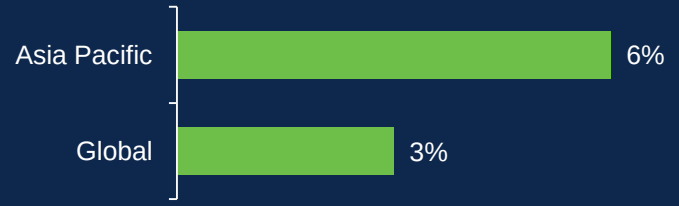
In Asia Pacific **VS** **Global**

25%	of organizations had already experienced an OT attack	21%
73%	expected this trend to increase in the next year	64%

Security practitioners in Asia Pacific are finding it challenging to orchestrate alerts

Organizations in Asia Pacific are managing slightly more vendors per company than their global counterparts.

>10 vendors

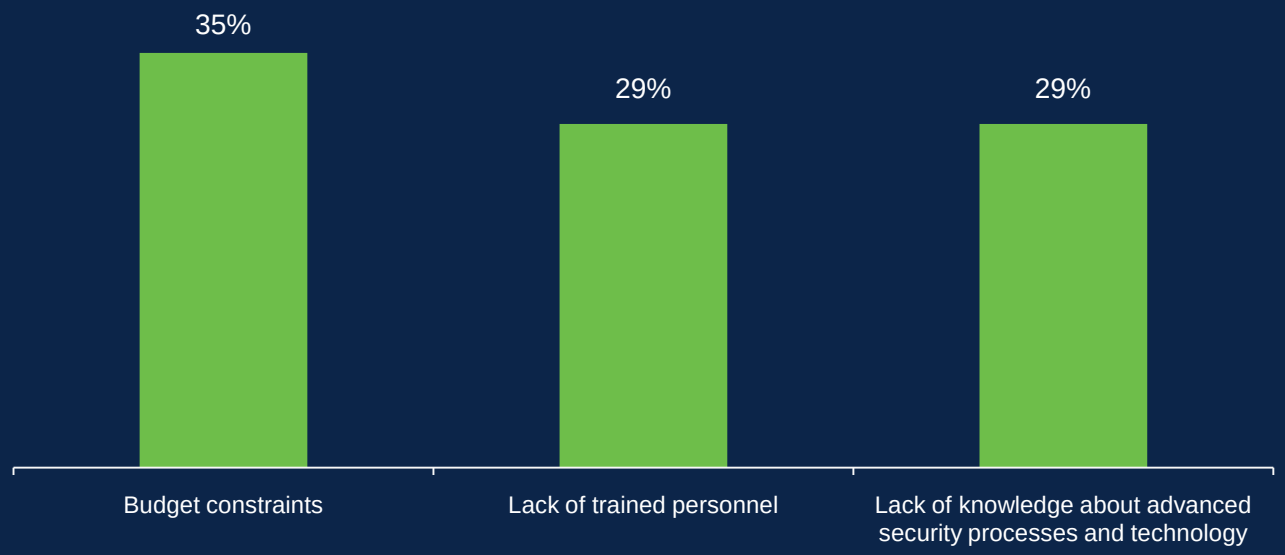


>50 vendors

Companies in Asia Pacific are finding it more challenging to manage a multi-vendor environment.

Constraints are not helping the cause...

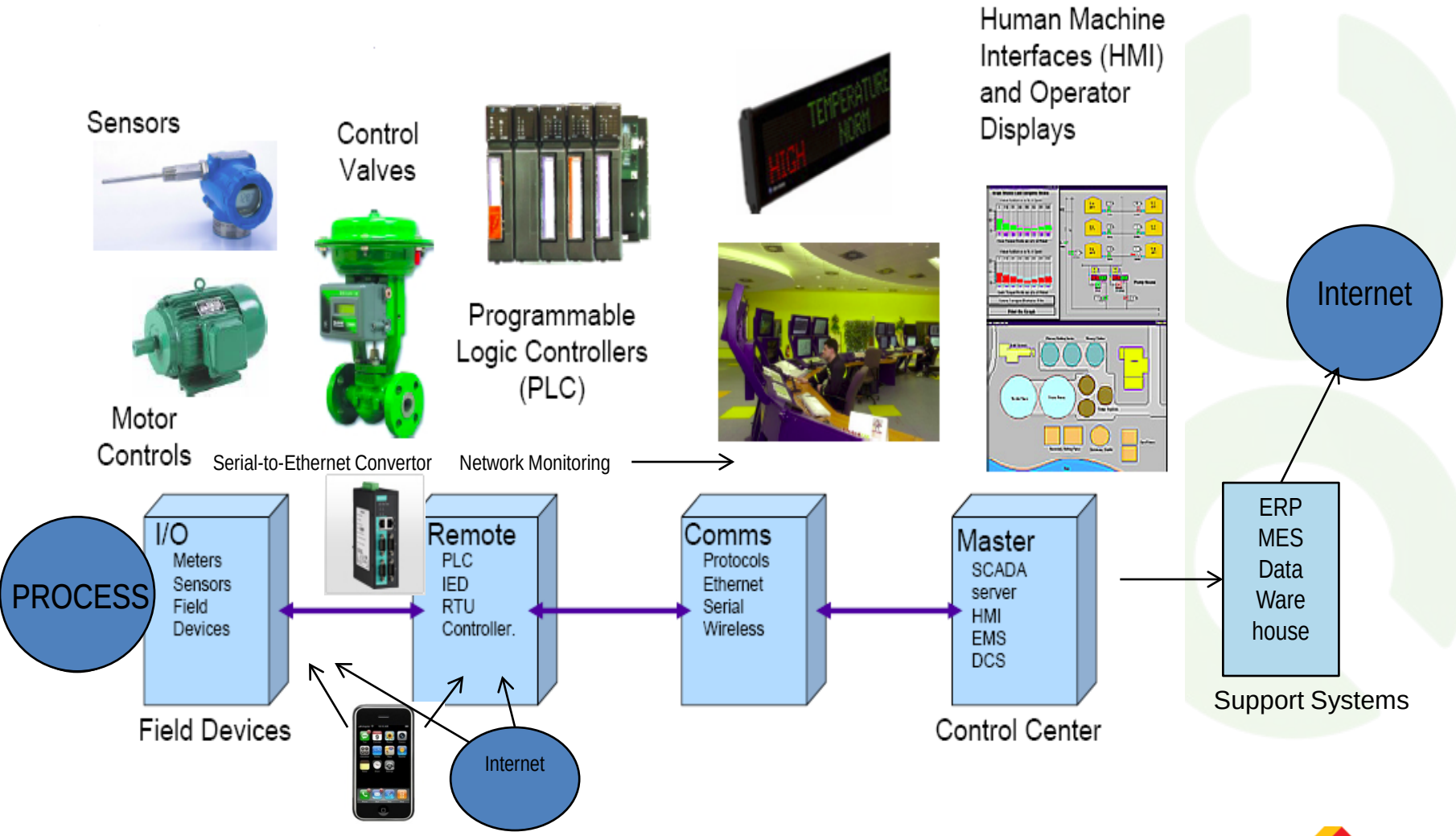
The top three barriers for adopting advanced security technologies in Asia Pacific



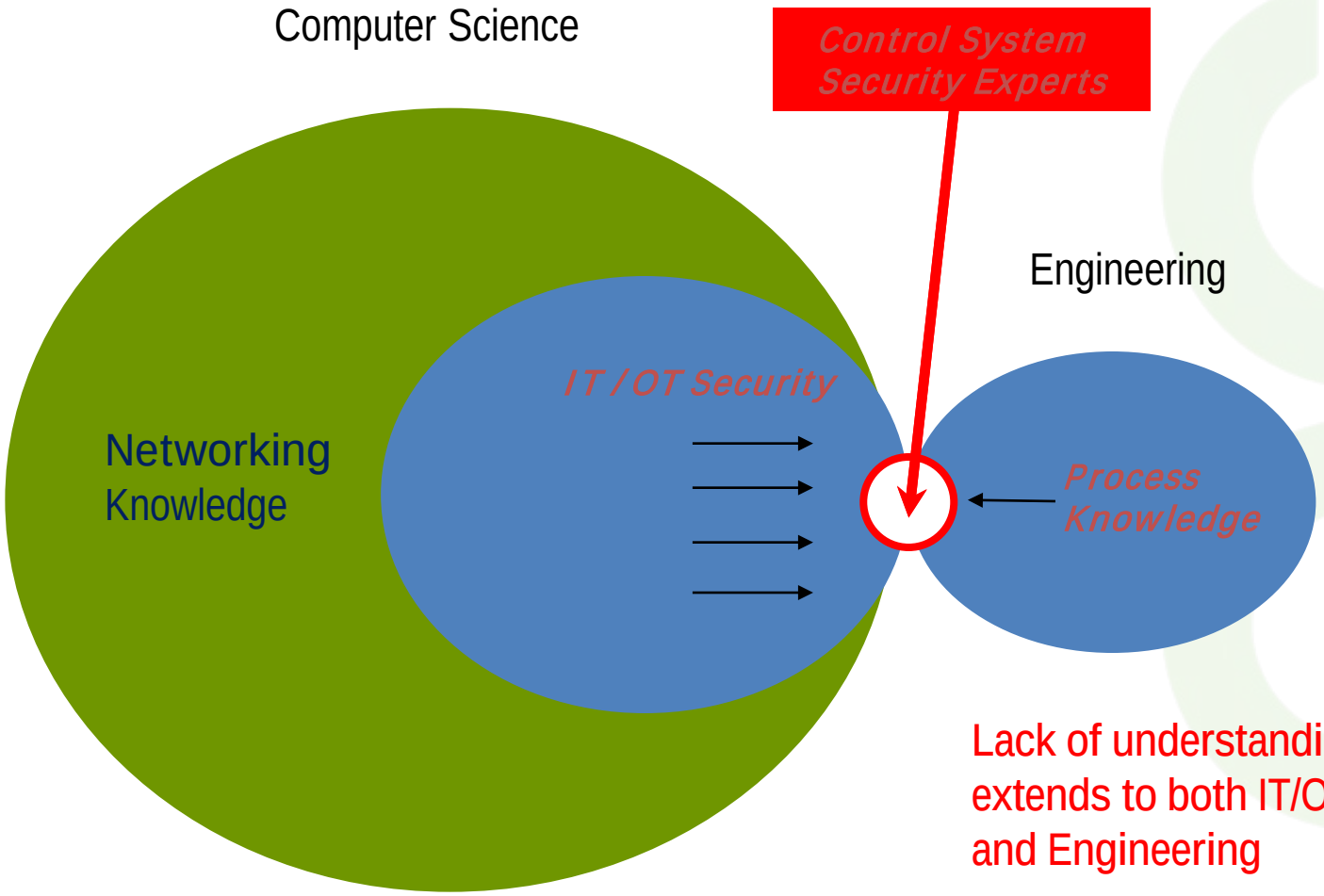
APAC Benchmark Study

http://cs.co/APACbenchmark

Control systems basics



IT/OT vs Engineering - Packets vs Process



Lack of understanding extends to both IT/OT and Engineering

Koh Suat Hong's Key Messages - Seven Principles of DPbD

Panel: From Cyber Resilience to Confidence

- **Proactive and Preventive -** Assess, identify, manage and prevent any data protection risks before any data breach occurs
- **Data Protection as the Default -** Integrate data protection measures into processes and features of the systems
- **End-to-End Security -** Security measures to be built into in the entire Software Development Lifecycle ("SDLC")
- **Data Minimisation -** Collect, store and use personal data that is relevant and necessary for the intended purpose
- **User-Centric -** Develop and implement ICT systems with individuals in mind while protecting their personal data
- **Transparency -** Take an active role in informing individuals on what data is collected from them and how it is being used
- **Risk Management -** Systematically identify and mitigate risks through design and implementation

John Yong's Key Messages

Panel: From Cyber Resilience to Confidence

1. Chief security and Chief audit must be Board ready

2. Accountability on cyber security responsibility need to be clearly defined, and sufficient allocation of time/budget need to be consider, in one of the senior management staff member.

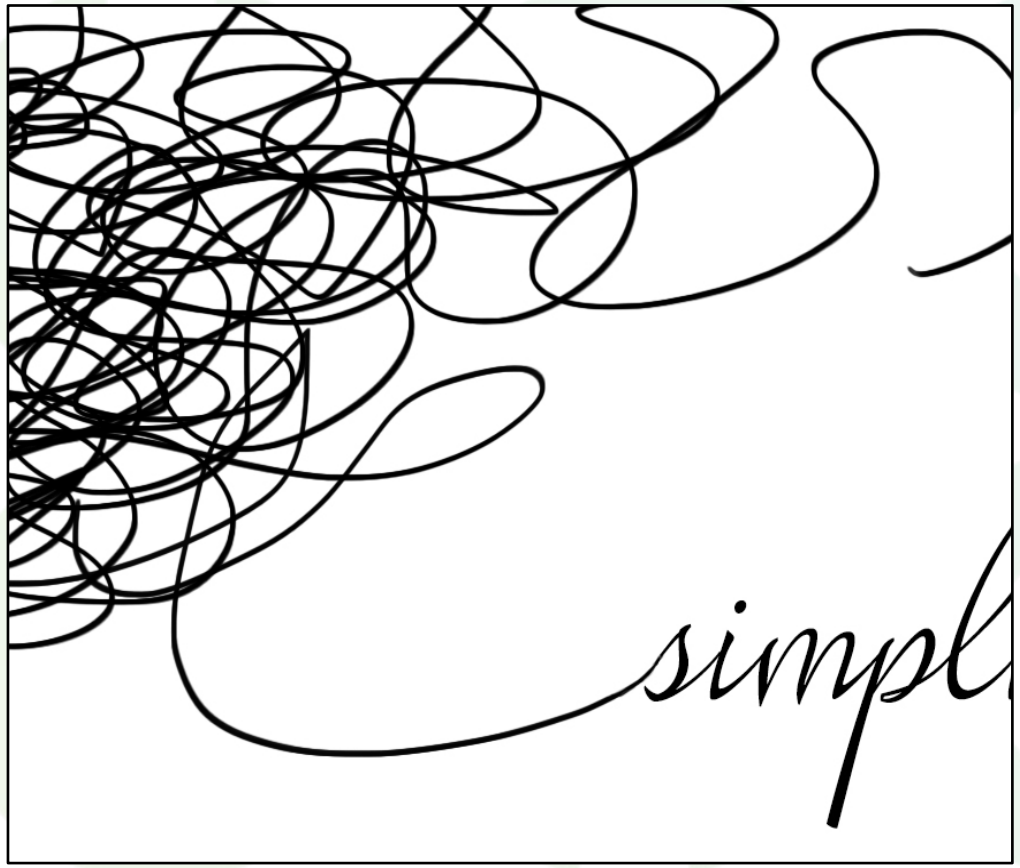
3. Cyber definition, may need to be redefined. This is to include risks such as privacy, mis-information, physical, ICS and ICT

Lim Thian Chin's Key Messages

Panel: From Cyber Resilience to Confidence

- Immediate
  - Knock down hot spots
  - Mop up operations
  - Consolidate security gains

- Under new norms
  - Secured workforce
  - Secured stakeholders/customers
  - Re-look at supply chain / 3P risk
  - Increased sectoral collaboration



Joshua McCloud's Key Messages

Panel: From Cyber Resilience to Confidence

- Drive security discussion at board level to better fund initiatives
- Move towards adopting a zero trust architecture to reduce attack surface
- Workforce, Workload, Workplace
- Reduce fatigue levels by investing in automation and orchestration
- Build a cyber resilience plan to reduce downtime
- Identify critical components, Assign roles & responsibilities
- Increase security awareness amongst employees
- Attack simulations, simplified & engaging training

GTACS 2020

GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA®

Singapore Chapter