RSAConference2018

Singapore | 25–27 July | Marina Bay Sands

#RSAC

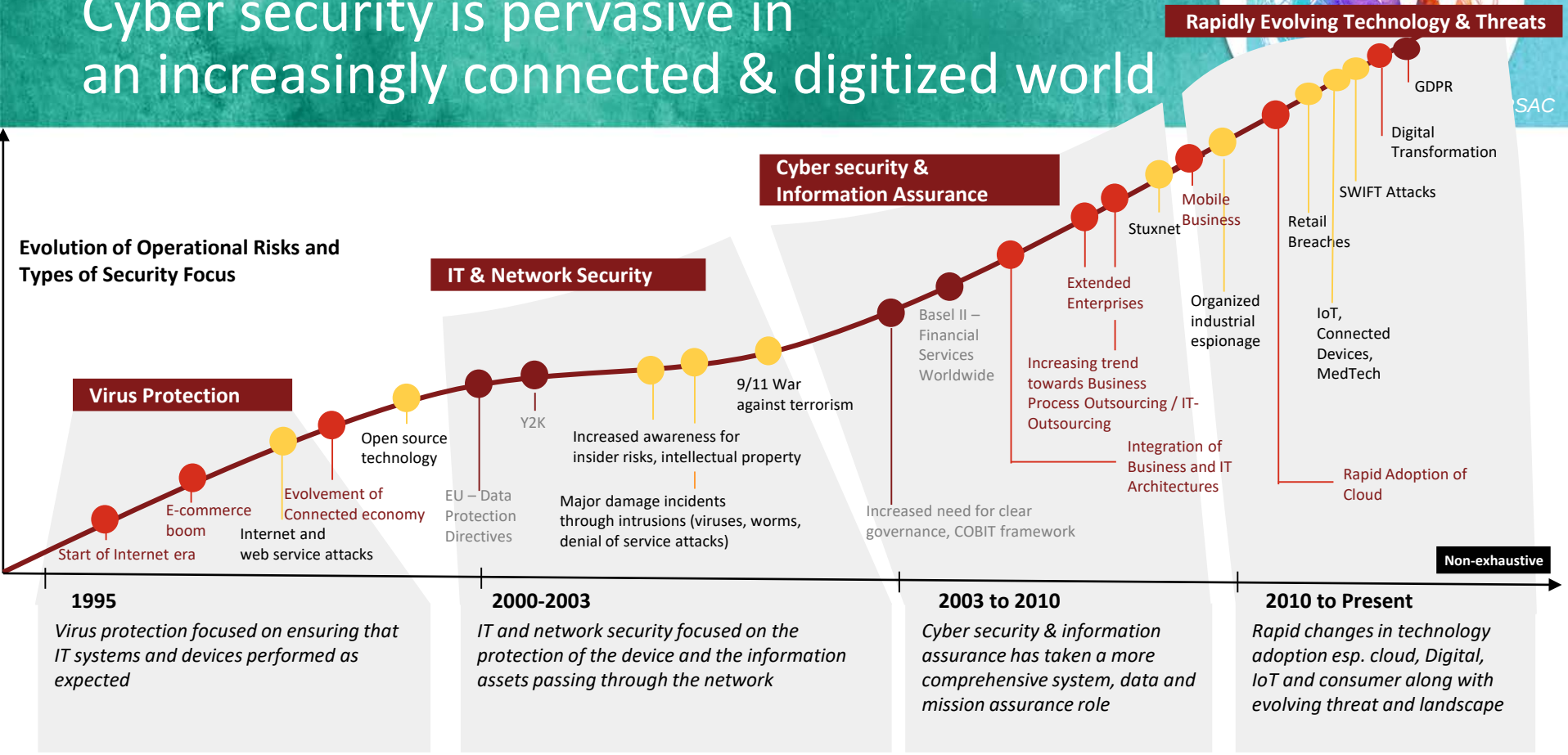
SESSION ID:

# THE CISO … IN A BOX

**Urooj Burney**

APJ Cybersecurity & Privacy Impact Center Leader
PwC South East Asia Consulting

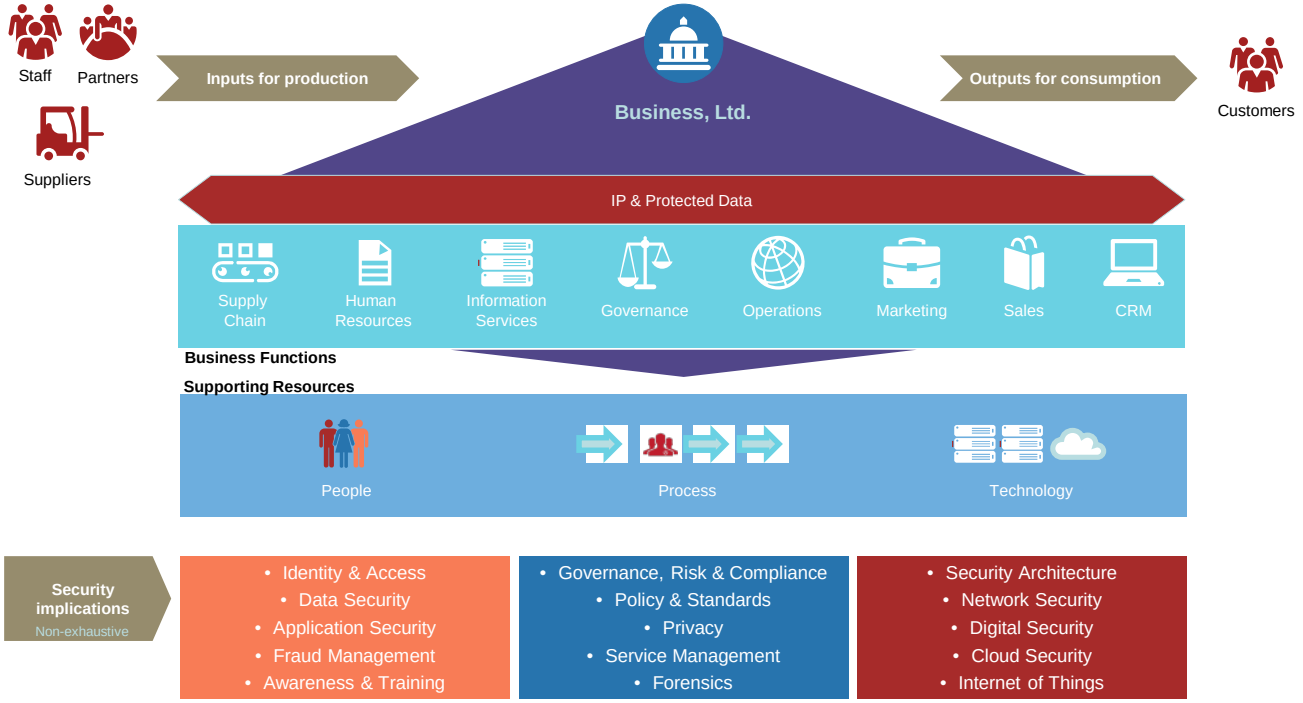
# Cyber security is pervasive in an increasingly connected & digitized world




pwc

RSAConference2018 Asia Pacific & Japan

# The genesis of cyber security…



# …from static to persistent



**Traditional Information Security**

- The people, process, and technology measures to support information and systems confidentiality, integrity, and availability.

**Cyber Security**

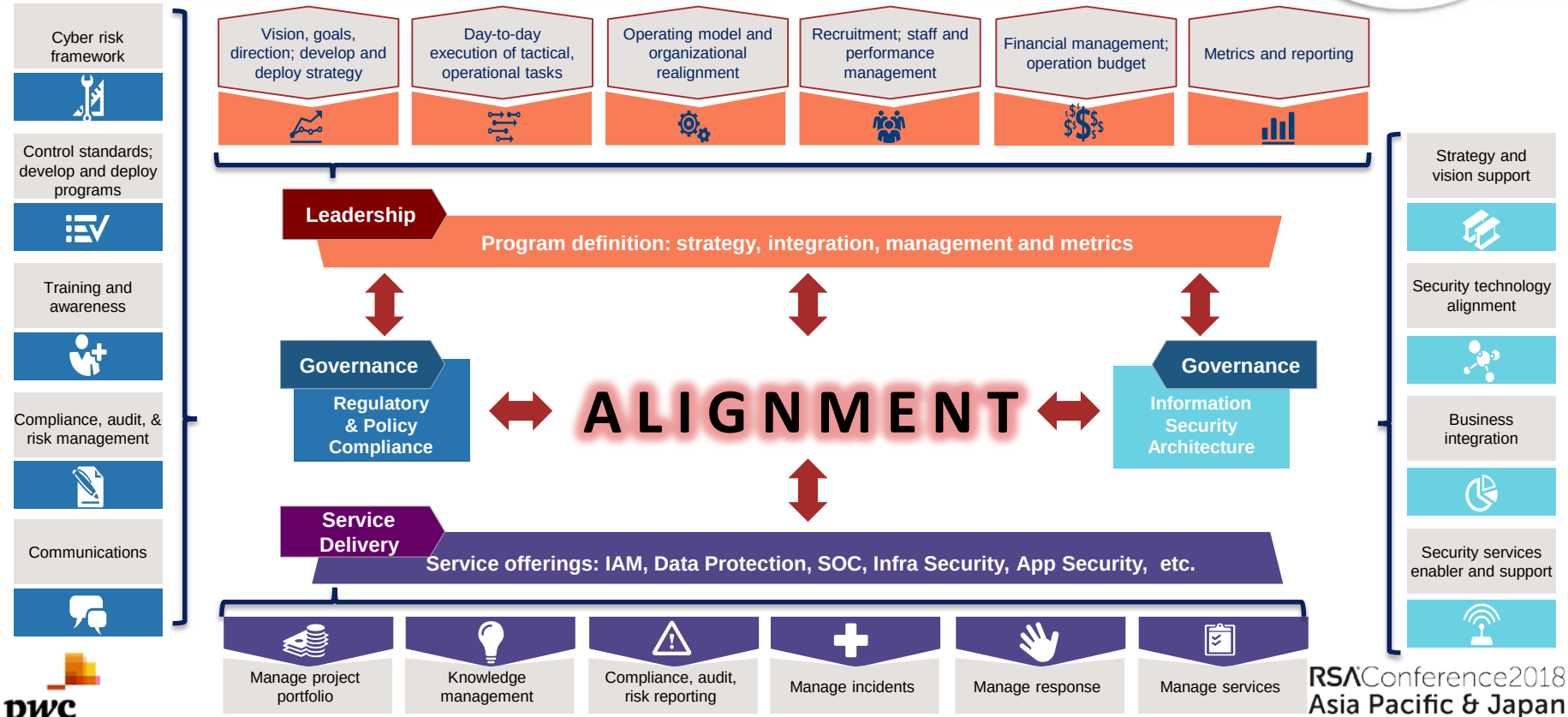
- Assumed state of compromise. The term has evolved to take on new meaning and seriousness today given the characteristics of the threats and impact of compromise.

## *Characteristics of cybersecurity perpetrators*

| | | |
|---|---|---|
| 1 | *Use sophisticated and persistent methods of attack* | Breach analysis shows criminals perform considerable reconnaissance and adopt both high and low tech tactics to achieve access into a network. |
| 2 | *Target information for long term strategic gain* | Attackers are seeking valuable corporate intellectual property; terrorist activities against governments, and defacement of corporate brand/organizational reputation. |
| 3 | *Are global and multi-national* | Many of the largest attacks have come from Eastern Europe, China, Russia, and South America, with many groups having a multi-national component. |
| 4 | *Are Organized* | Cybercrime syndicates (“hacktivists”), such as Anonymous, coordinate attacks through their thousands of members across the globe. |

# The evolving role of the CISO, and their teams, has followed this change






pwc

# The CISO's success is driven by how the company has positioned the CISO role



## The Business Enabler

- Reports to:
  - The CEO or the board
  - Business focused senior executive
- Board understands the need and importance of cyber and manages risk
- Security by design and security aware culture

## Security as IT

- Reports to:
  - CIO/CTO
  - Senior Management
- Technical expert
- Uses technology to address and solve issues
- Lacks required business acumen
- Accomplished in their own right

## Security as Compliance

- Middle Management
- Limited technical background
- Compliance is used to drive the cyber agenda
- Generally underfunded but not aware of impacts

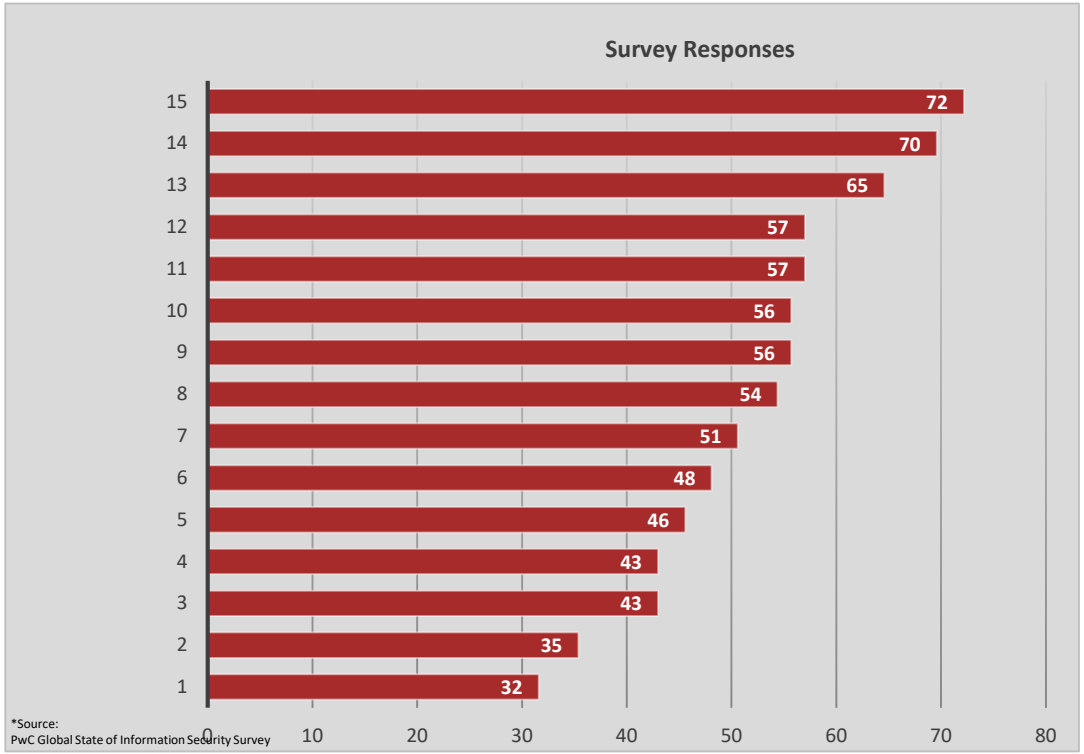
## Security as a Cost Centre

- Low-to-mid Management
- Not called CISO
- Technical background
- Function is understaffed and under-funded
- Cyber is not a company priority
- Board awareness is limited

Source: Synopsys - 2018 CISO Report

# The CISO's reporting structure evidences how companies value security

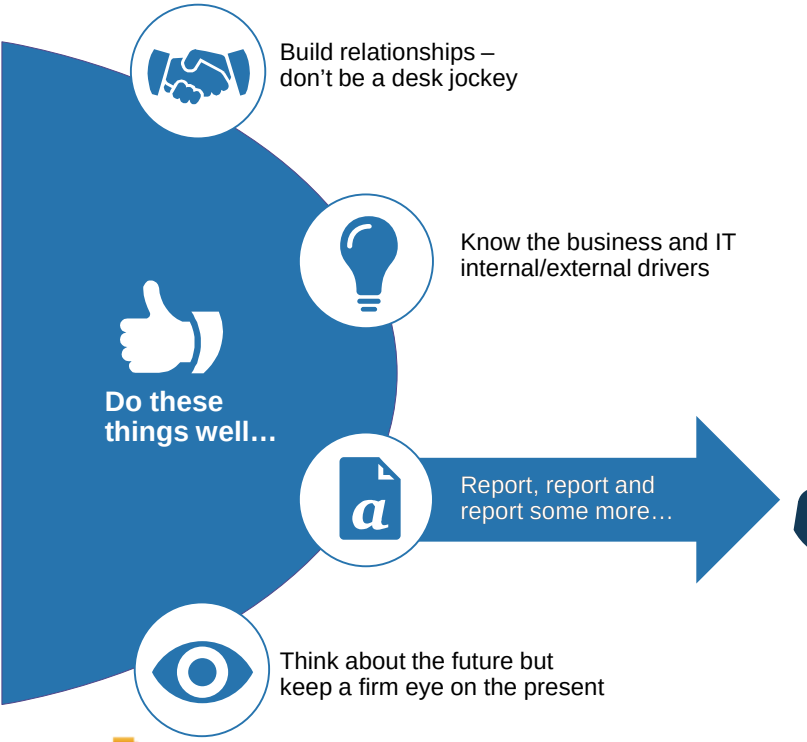





Regardless of the organizational structure, the CISO needs to be ***"UNBOXED"*** and have an enterprise role, reach and influence.

# The route to ‘Good’ is the same for all





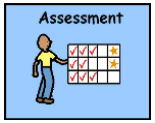

- Organization review and alignment to cyber priorities
- Governance processes and oversight mechanisms
- Help define measures for “Cyber Risk”
- Review of cyber risks and the related remediation plans
- Learning and awareness
- Establish metrics to define success/failure

**What leadership owes the CISO**

# Operating to *“enable the business”* should be “business as usual”



| Business Mission | Client/Partner On-Boarding | Design, Development Deployment | Production |
|---|---|---|---|



Compliance
Security Awareness & Training
Security Workshops

Client Evaluation Input
Contract/Negotiations Input
Partner & Client Risk Review
Gap Identification & Remediation Planning

Security Architecture Review
Application Code Reviews
Vulnerability Assessments & Pen Testing

On-going Risk Management
Audit Support
Federated Access
Security Assessments (Application & Infrastructure)
Security Management
Incident Management & Response


**Security Program**

**Information Security Expertise**


**Service Catalog**

Non-exhaustive

pwc

RSAConference2018 Asia Pacific & Japan

# Where the CISO reports, dictates their ability to "own" the security discussion or be owned by it

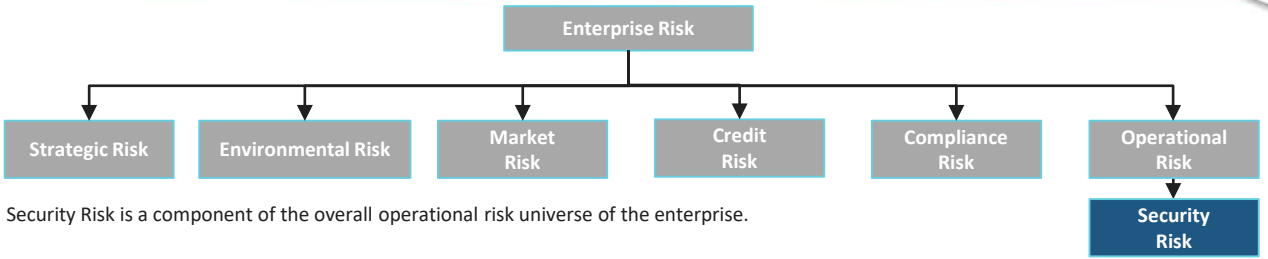


- Regulatory and Compliance Penalties (GDPR, PDPA, MAS IB TRM …)
- Break-ins and stolen IP, staff and/or customer data, monies
- Insider threats
- Increased costs of people and technology
- Escalating costs of response and recovery

# The CISO role continues to change as the business landscape evolves

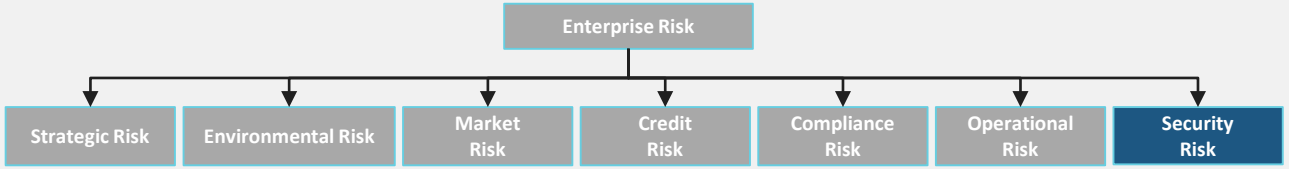


**Past:**




Security Risk is a component of the overall operational risk universe of the enterprise.

**Industry trend:**




As a result of the above trends, materiality of security risk has been elevated.

Increased dependency on technology, increased technology related attacks and fraud and increased regulatory attention to technology drive changes in the industry. Additional complexity - every risk category has a technology-component to it. For example:

- Strategic Risk – Technology is the key enabler of new business initiatives
- Credit Risk – Poor information security can lead to lower credit ratings

**Today and ahead:**


Select highly-innovative and very risk averse organizations established roles such as Chief Cyber-Security Risk Officer responsible for cyber risk management at the same level as a CRO and CIO and with direct access to the Board.




# THANK YOU