



# Security in Today's Insecure World *for SecureTokyo*

David Shearer  
(ISC)<sup>2</sup> Chief Executive Officer

[dshearer@isc2.org](mailto:dshearer@isc2.org) | [www.isc2.org](http://www.isc2.org)

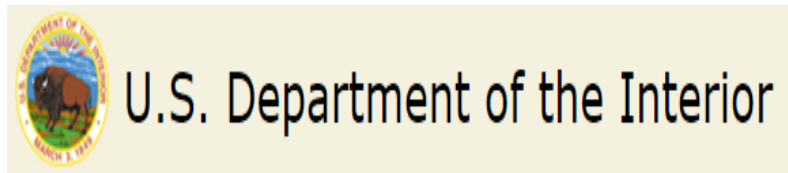
# I'm Influenced by a Mission Driven Background



- U.S. Maritime Transportation System Security
- Search and Rescue
- U.S. Maritime Law Enforcement



- International Intellectual Property Protection
- Canadian, European, Japanese Patent Office Collaboration and the World Intellectual Property Organization



- Federal lands law enforcement
- Wildland fire fighting
- Bureaus covering oil and gas, geological science, dams and critical infrastructure, etc.



- Food safety
- Wildland fire fighting
- Agricultural research, land sciences

# Dave, some days at the office





# Maybe this is a closer resemblance



# Below the Cybersecurity Waterline?



“...there are **known knowns**; there are things we know we know. We also know there are **known unknowns**; that is to say we know there are some things we do not know. But there are also **unknown unknowns** – the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.”

Source: Former U.S. Secretary of Defense Rumsfeld Speech: [https://en.wikipedia.org/wiki/There\\_are\\_known\\_knowns](https://en.wikipedia.org/wiki/There_are_known_knowns)



# Workforce Skills and Capacity Issues

- We have an aging global cybersecurity workforce.
  - Less than 6% of the 13,930 respondents to the 2015 (ISC)<sup>2</sup> Global Information Security Workforce Study (GISWS) are below the age of 30.
- Lack of qualified candidates is exacerbating an already stressed workforce.
- Without adequate staffing levels, the workforce is often addressing day-to-day incidents without work cycles to address cybersecurity programmatically.



## Key Known, Knowns

We face a global cybersecurity challenge that requires a well-orchestrated and sustained global response.

- The challenge cannot be solved locally based on our interconnectedness.
- Trying to go it on your own will no longer suffice.
- Information sharing about attacks is increasingly important among private-to-private, private-to-public and public-to-public sectors.
- Globalization means systemic failures have a ripple effect across business sectors and countries.



## Additional Key Known, Knowns

Organizations are frequently inherently challenged to execute against core strategies.

- If cybersecurity is not seen as a core corporate strategy, there's limited chance for success.
- Organizational structure and culture can contribute or hinder the cybersecurity program.





## Additional Key Known, Knowns

- Workforce studies and other types of research can help the private and public sectors enhance security posture strategies.
  - Identify trends.
  - Identify future challenges and proactively seek mitigation strategies.
  - Assess what other industries are doing to gauge global risks.
  - Look for cross-sector collaboration opportunities.

# Center for Cyber Safety and Education

## Growth of Respondent Pool

**2011** = 10,413 Respondents

**2013** = 12,393 Respondents

**2015** = 13,930 Respondents

11,208 Members

2,722 Non-members

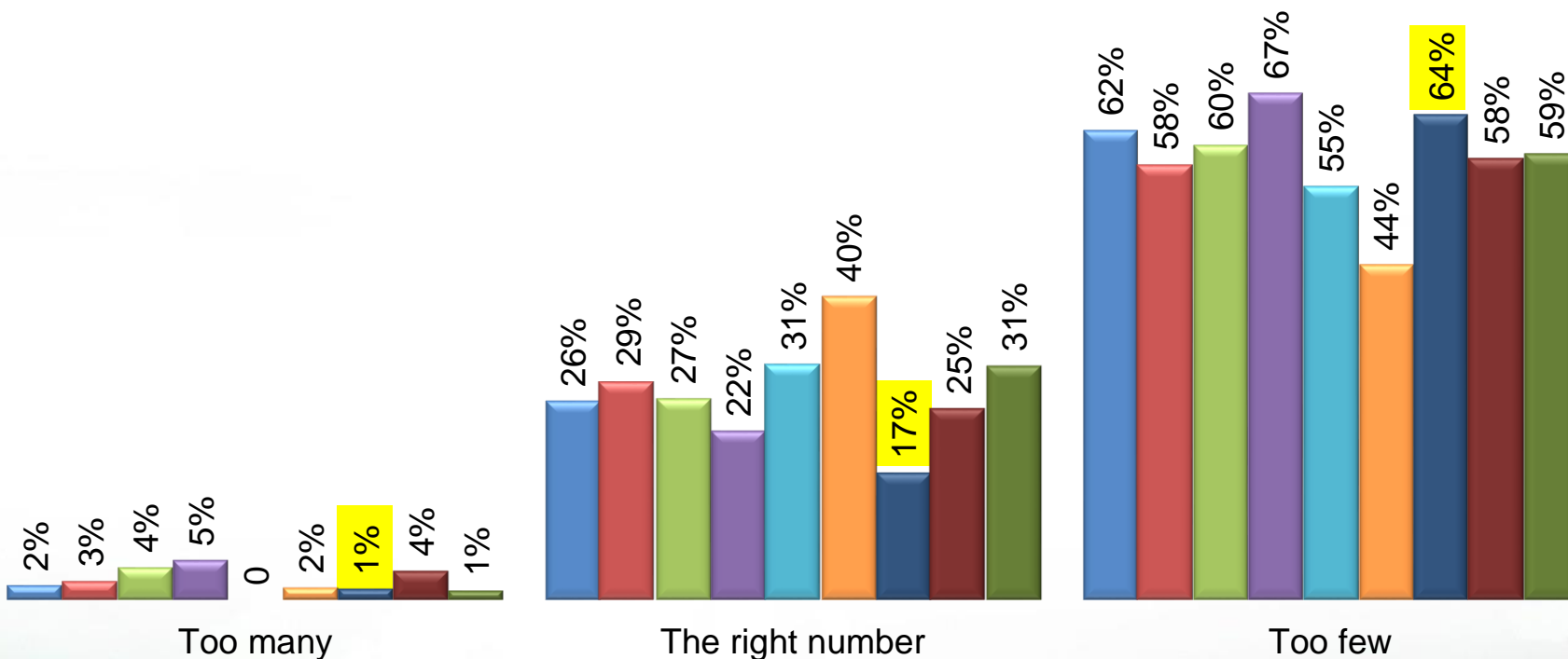


<https://www.isc2cares.org/IndustryResearch/GISWS/>

# Number of Security Workers – Enough?

A majority from APAC countries, including Japan, indicate that there are too few security workers in their organization.

■ Worldwide 
 ■ APAC 
 ■ Australia 
 ■ China 
 ■ Hong Kong 
 ■ India 
 ■ Japan 
 ■ Singapore 
 ■ South Korea

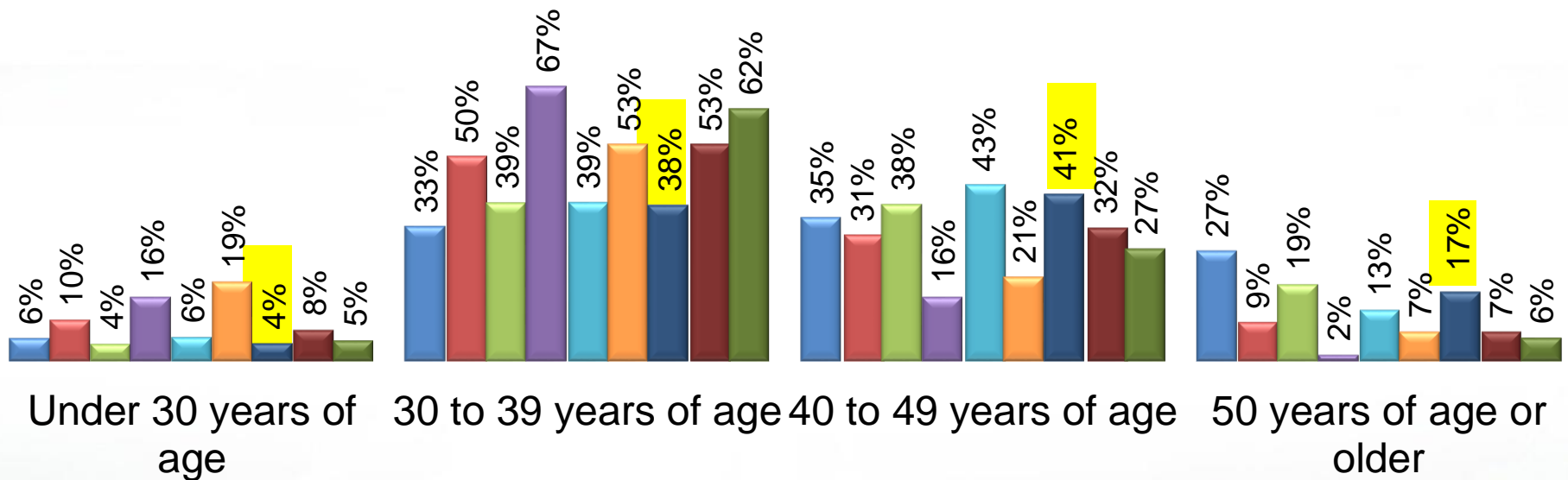


Base: Filtered respondents (n=7,985)

# Age

The global average age within the profession is 42 – we need to attract more young entrants to the profession. Japan professionals are relatively older than their counterparts in APAC.

■ Worldwide ■ APAC ■ Australia ■ China ■ Hong Kong ■ India ■ Japan ■ Singapore ■ South Korea

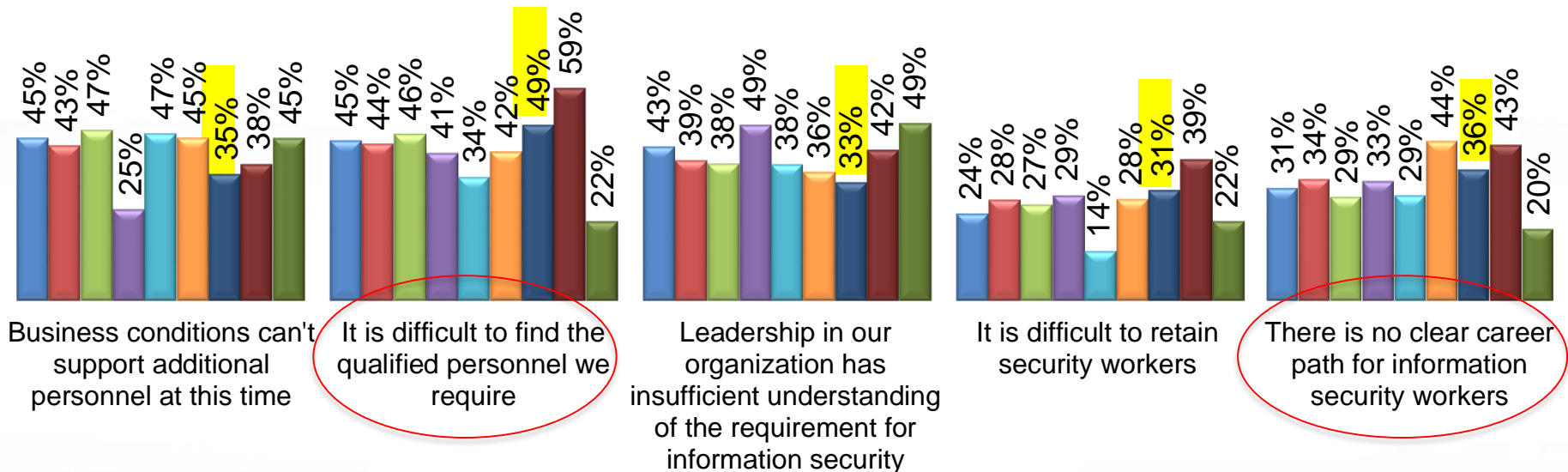


Base: All 2015 worldwide respondents (n=13,930)


# Reasons for Worker Shortage

Most often, businesses cannot support additional personnel, leadership has insufficient understanding or report that it is difficult to find qualified personnel.

■ Worldwide 
 ■ APAC 
 ■ Australia 
 ■ China 
 ■ Hong Kong 
 ■ India 
 ■ Japan 
 ■ Singapore 
 ■ South Korea



Base: Filtered respondents (n=4,969)



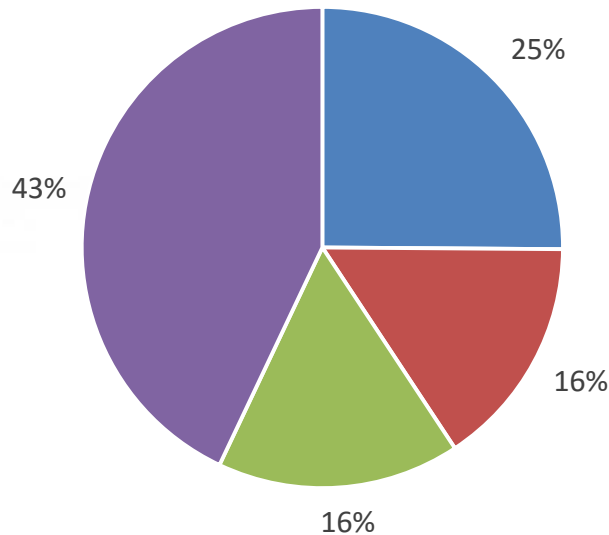
# Combined (ISC)<sup>2</sup> Members and Non-Members

## Country Profile—Japan

- **Gender Composition of Workforce**
  - 95% male and 5% female
- **Education**
  - 53% have degrees and an additional 37% have advanced degrees
- **Average Salary**
  - US\$85,800/ year
- **Average Years of Experience**
  - 13
- **Management Responsibility**
  - 24% have mostly security consulting responsibilities and 17 % have mostly architectural responsibilities
- **Reporting Structure**
  - 20% report to IT Department and 20% to Executive Management

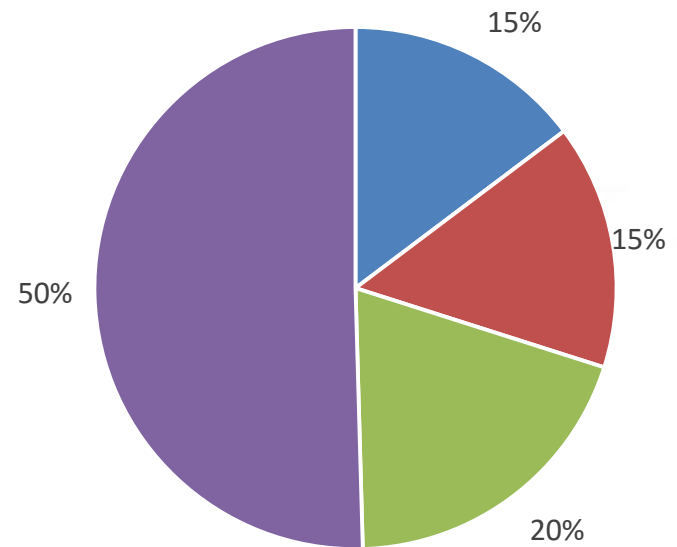
# Combined (ISC)<sup>2</sup> Members and Non-Members Global vs Japan—Organizational Size

### Number of Employees (Global)



- 1 to 499 employees
- 500 - 2,499 employees
- 2,500 - 9,999 employees
- 10,000 or more

### Number of Employees (Japan)

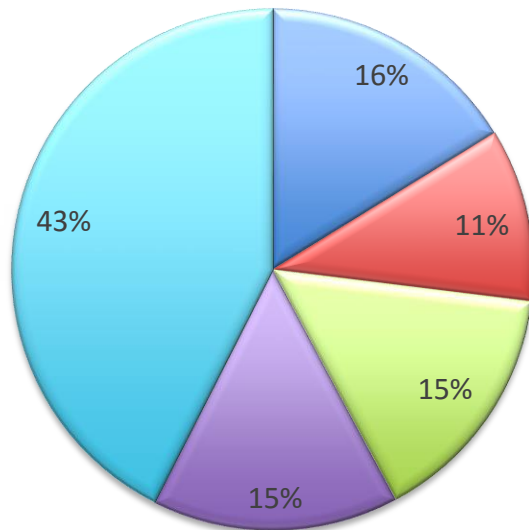


- One to 499 employees
- 500 to 2,499 employees
- 2,500 to 9,999 employees
- 10,000 employees or more

Base: All member and non-member respondents (n=10413).

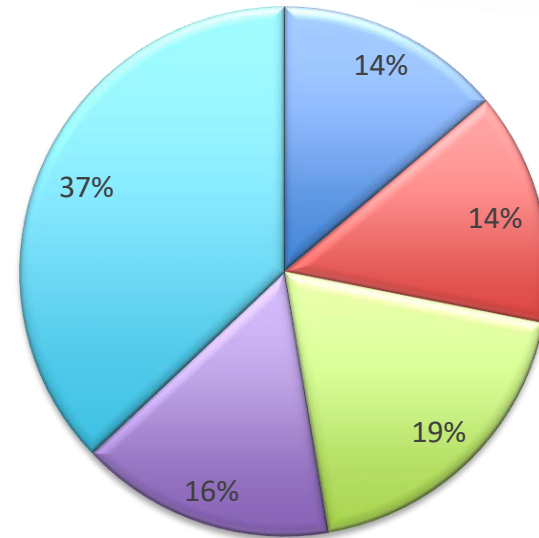
# Combined (ISC)<sup>2</sup> Members and Non-Members Global vs Japan—Organizational Revenue

## Annual Revenue (Global)



- Less than \$50 million
- \$50 to less than \$500 million
- \$500 million to less than \$10 billion
- \$10 billion or more
- Unable to provide

## Annual Revenue (Japan)

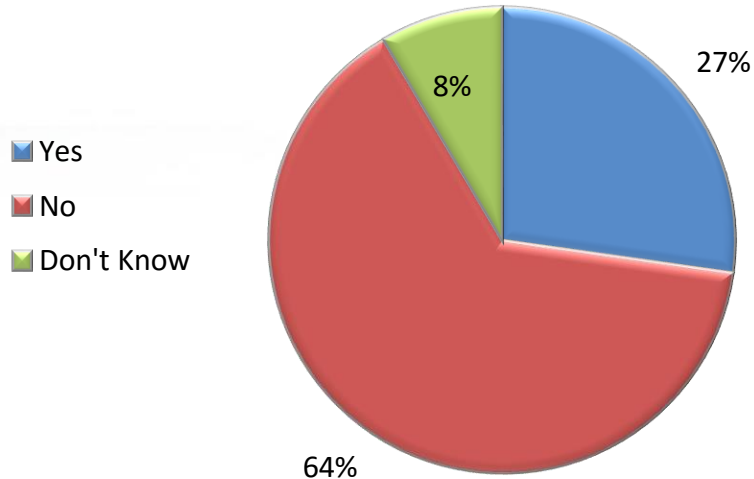


- Less than \$50 million
- \$50 to less than \$500 million
- \$500 million to less than \$10 billion
- \$10 billion or more
- Unable to provide

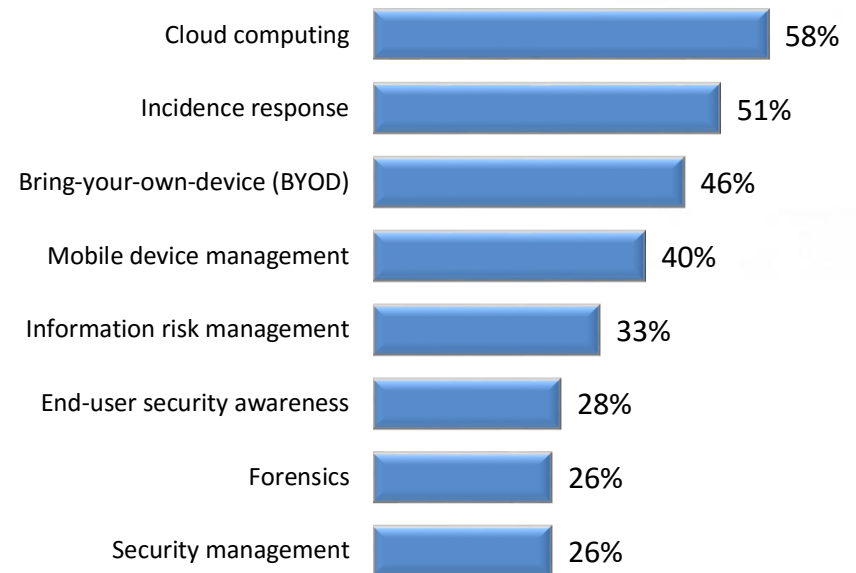


# Combined (ISC)<sup>2</sup> Members and Non-Members Country Profile—Japan

## Require Security Certifications



## Top Demands for Training





# How to tackle the workforce shortage?

- Encourage new entrants
- Clearer career path for CISO

# What (ISC)<sup>2</sup> has done to tackle the shortage?

- Associate Program of (ISC)<sup>2</sup>
  - Allows those just starting out in the information security workforce to demonstrate their competence in the field.
  - Associates have passed a rigorous (ISC)<sup>2</sup> certification exam, proving their cybersecurity knowledge, and maintaining their continuing professional education (CPE) requirements while working toward completing the experience requirements to become fully certified as a (ISC)<sup>2</sup> Member --CISSP, SSCP or CCSP, etc.
- (ISC)<sup>2</sup> Center for Cyber Safety and Education Scholarship Program to invest in the education of future cybersecurity professionals with the goal of helping to fill the cybersecurity professional pipeline of tomorrow.
- Introduction of International Academic Program (IAP) (previously known as GAP)



# U.S. Experience: Cybersecurity National Action Plan (CNAP)



- » Announced in Feb 2016 by President Obama
  - Call to increase federal cybersecurity spending by 35% to modernize IT and address skills shortage, IoT
  - US\$4 trillion budget bill to the Congress -- US\$62 million in cybersecurity personnel
- » Creation of a Federal Chief Information Security Officer (CISO)
  - To drive cybersecurity policy, planning, and implementation across the federal government
  - The position reports to the administrator of the Office of E-Government and Information Technology. The advertised annual salary range is US\$123,175 to \$185,100



## CNAP (continued)

- » (ISC)<sup>2</sup> and KPMG survey federal cybersecurity executives on the state of cybersecurity in the federal government – ‘The 2016 State of Cybersecurity from the Federal Cyber Executive Perspective’ to be released in May 2016



# Singapore Experience: National Infocomm Competency Framework (NICF)

- » The National Infocomm Competency Framework (NICF) developed by Infocomm Development Authority of Singapore (iDA) and Singapore Workforce Development Agency (WDA)
- » The NICF Overview Map is a snapshot of the Infocomm sector
- » Serves as a reference for career progression and corresponding training pathways leading to NICF qualifications
- » Similar to U.S. DoD 8140 model

# Job description of a CISO

- Contribute to the development of a strategy plan
- Select new technology models for business
- Develop a budget
- Develop strategic and action plans
- Align the IT needs with the strategic direction of the enterprise
- Identify and implement business innovation
- Maximise business value of IT investments
- Review and plan for risk to business solution providers
- Implement change management process
- Determine appropriate IT strategies and solutions
- Manage project costs
- Manage project risk
- Direct projects
- Manage stakeholders for project success
- Understand and apply compliance standards
- Develop business case that support information security program investments
- Formulate information security goals and objectives
- Manage overall information security risk

Source: *National Infocomm Competency Framework (NICF), IDA, Singapore*

# Infocomm Security Career Path proposed by NICF

Security Engineering	Security Management	Security Operations	Security Services
<ul style="list-style-type: none"> <li>• Chief Information Security Officer</li> </ul> $\Delta X \Theta$	<ul style="list-style-type: none"> <li>• Chief Information Security Officer</li> </ul> $\Delta X \Theta$	<ul style="list-style-type: none"> <li>• Chief Information Security Officer</li> </ul> $\Delta X \Theta$	<ul style="list-style-type: none"> <li>• Information Security Services Director</li> <li>• Head of IS Audit</li> </ul> $\Delta X \Theta$
<ul style="list-style-type: none"> <li>• Chief Security Architect</li> </ul> $\Delta X \Theta$	<ul style="list-style-type: none"> <li>• Information Security Manager</li> <li>• IT Compliance Manager</li> <li>• IT Risk Manager</li> </ul> $\Delta X \Theta$	<ul style="list-style-type: none"> <li>• Information Security Manager</li> <li>• IT Risk Manager</li> </ul> $\Delta X \Theta$	<ul style="list-style-type: none"> <li>• Information Security Services Manager</li> <li>• Digital Forensic Investigation Manager</li> <li>• IS Audit Manager</li> </ul> $\diamond \Delta X \Theta$
<ul style="list-style-type: none"> <li>• Security Engineer</li> </ul> $\Delta X$	<ul style="list-style-type: none"> <li>• Senior Information Security Officer</li> </ul> $\Sigma \Delta X$	<ul style="list-style-type: none"> <li>• Security Administrator</li> <li>• System Security Administrator</li> <li>• Network Security Administrator</li> <li>• Database Security Administrator</li> </ul> $\Delta X$	<ul style="list-style-type: none"> <li>• Information Security Consultant</li> <li>• Digital Forensic Investigator</li> <li>• IS Auditor</li> </ul>
<ul style="list-style-type: none"> <li>• Associate Security Engineer</li> </ul>	<ul style="list-style-type: none"> <li>• Information Security Officer</li> </ul> $=$	<ul style="list-style-type: none"> <li>• Associate Security Administrator</li> <li>• Associate Network Security Administrator</li> <li>• Associate Database Administrator</li> </ul> $\Sigma \Theta$	<ul style="list-style-type: none"> <li>• Associate Information Security Consultant</li> <li>• Associate Digital Forensic Investigator</li> <li>• Associate IS Auditor</li> </ul>

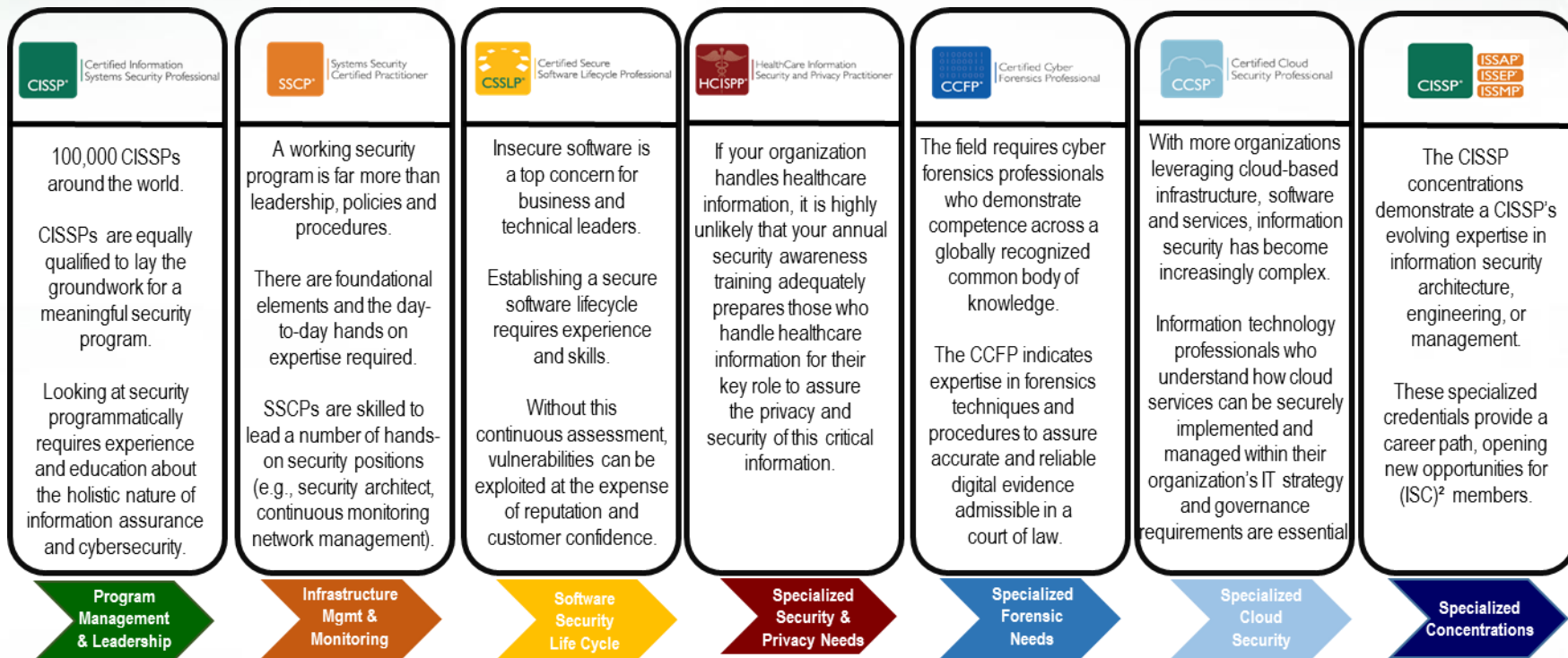


LEGEND for NICF course providers

$\diamond$  Ngee Ann Polytechnic  
  $\Sigma$  Singapore Polytechnic  
  $\Delta$  Strategic Technology Management Institute  
  $X$  Institute of Systems Science  
  $\Theta$  Litan Hall Academy



# (ISC)<sup>2</sup> Credentials





(ISC)<sup>2</sup><sup>®</sup>

INSPIRING A SAFE AND SECURE CYBER WORLD.

