



The Value of Information Security Certifications

Ed Zeitler, CISSP
Executive Director, (ISC)²

www.isc2.org



(ISC)²



SECURITY TRANSCENDS TECHNOLOGYSM

- Why professional certificate for information security?
- About (ISC)² and its credentials
- Number of (ISC)² members worldwide & in Asia-Pacific

Ed Zeitler, CISSP

What does this stand for?

Chester Soong, CISSP-ISSAP, ISSMP

What do these stand for?

Why a certificate for information security?

- In an era of increasingly complex global security risks, the skills and knowledge of security professionals become central to every risk mitigation strategy.
- The quality of security solutions depends on the ability of security professionals to stay up-to-date, fully trained, and to collaborate with their fellow professionals around the world.
- Like in other industries, such as the CPA for accounting, credentials provide employers an additional measure of confidence in the knowledge, expertise and ethics of the professional with a credential
- Information security certifications provide organizations with the assurance that its staff has been tested on understanding industry best practices and possess a broad knowledge of the field as well as sound professional judgment.



Professional Certification – The Characteristics

- **International** – Accredited against some international standard that is recognized worldwide, such as ISO standard
- **Examination** – Rigorous exam to assure knowledge of a taxonomy of information security topics - CBK®
- **Independent** – Not product or service specific – Tests habitual knowledge
- **Endorsement** – Strict endorsement and audit process to verify candidate assertions
- **Ethics** – Comprehensive set of behavioral guidelines – Professional judgment
- **Experience** – Practical application of the CBK is acquired through experience
- **Re-certification** – Continuing education to maintain credential
- **Maturity** – Wide acceptance as the true measure of competency

...to the Enterprise

- Solutions orientation, not specialization
- Broad understanding of Taxonomy of information security topics
- The rigor and regimen adds to credibility
- A business and technology orientation to risk management

...to the Professional

- Career differentiator
- Confirms knowledge of a broad range of information security topics
- Networking with experts globally
- Part of an elite group of professionals
- Member of an organization offering career resources and support

(ISC)² Certifications & Membership



SECURITY TRANSCENDS TECHNOLOGYSM



- Established in 1989 - Non-profit consortium of industry leaders
- Global leaders in certifying and educating information security professionals with the CISSP[®] and related concentrations, CAP^{CM} & SSCP[®]
- Global standard for information security – (ISC)² CBK[®], a taxonomy of information security topics
- Nearly 50,000 certified professionals in 129 countries
- Produce the only global study of the information security workforce

Credential Offerings



Credentials – The *Gold Standards* in information security certification

- Certified Information Systems Security Professional (CISSP®)
- Certification and Accreditation (CAP^{CM})
- System Security Certified Practitioner (SSCP®)

CISSP Concentrations – In-depth, specialized enhancements to the CISSP

- Information Systems Security Architecture Professional (ISSAP®)
- Information Systems Security Engineering Professional (ISSEP®)
- Information Systems Security Management Professional (ISSMP®)



Meant for professionals who:

- Are experienced professionals who manage and enforce information security policies
- Have minimum 4 years cumulative work experience in (ISC)² CISSP CBK® domains, or 3 years and either Master's degree in information security or undergraduate degree
- Subscribe to (ISC)² Code of Ethics
- Are endorsed by another CISSP, qualified professional with knowledge of information systems or an officer of the candidate's corporation
- Pass a rigorous exam to assess their knowledge, skills and abilities relevant to the (ISC)² CISSP CBK®
- Earn 120 hours of Continuing Professional Education (CPE) every 3 years for recertification
- May pursue specialized concentrations available in several areas of the (ISC)² CISSP CBK



- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security





- Access Control Systems and Methodology
- Telecommunications and Network Security
- Cryptography
- Requirements Analysis and Security Standards/Guidelines Criteria
- Technology Related Business Continuity Planning (BCP) & Disaster recovery Planning (DRP) & Continuity of Operations Planning (COOP)
- Physical Security Integration



- Systems Security Engineering
- Certification & Accreditation
- Technical Management
- U.S. Government Information Assurance (IA) Regulations





- Enterprise Security Management Practices
- Enterprise-Wide Systems Development Security
- Overseeing Compliance of Operations Security
- Understand Business Continuity Planning (BCP) & Disaster recovery Planning (DRP) & Continuity of Operations Planning (COOP)
- Law, Investigations, Forensics and Ethics

Meant for professionals who:

- Formalize processes used to assess risk and established security requirements
- Ensure information systems possess security commensurate with the level of exposure to potential risk
- Possess at least 2 cumulative years of relevant certification and accreditation work experience as evidenced by the responsibilities included in the previous and current positions held within their organization(s)
- Subscribe to the (ISC)² Code of Ethics
- Pass the CAP certification examination based on the requirements of knowledge, skills and abilities identified
- Earn 65 hours of CPE credits every 3 years





- Understanding the Purpose of Certification
- Initiation of the System Authorization Process
- Certification Phase
- Accreditation Phase
- Continuous Monitoring Phase

Systems Security Certified Practitioner (SSCP®)

Meant for professionals who:

- Are systems and network security administration professionals
- Possess a minimum 1 year cumulative professional experience in (ISC)² SSCP CBK® domains
- Subscribe to (ISC)² Code of Ethics
- Earn 60 hours of CPE credits every 3 years





- Access Control
- Administration
- Audit and Monitoring
- Risk, Response and Recovery
- Cryptography
- Data Communications
- Malicious Code/Malware

- Program to

- Provide early support for information security careers
- Set new entrants on the right path early in their careers
- Encourage early commitment to the profession
- Accelerate the growth of professionals worldwide

- Designed for candidates who

- Pass the CISSP® or SSCP® examination
- Lack professional experience required for certification
- Are willing to subscribe to the (ISC)² Code of Ethics

- Indicates a candidate

- Possesses an independent and objective measure of competence via understanding of the (ISC)² CBK®
- Aspires to adhere to the rigors and ethics of the profession through association with (ISC)²
- Is required to complete the necessary professional experience and the subsequent endorsement process within 5 years

- Provides access to suite of (ISC)² career support programs

- Official (ISC)² communications (bi-monthly newsletter)
- Peer networking

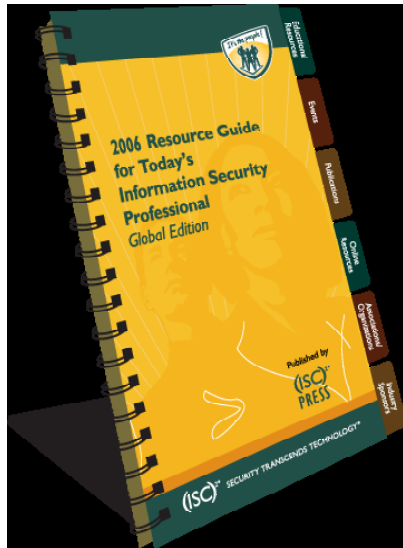


Voted “Best Professional Training Program” by SC Magazine in 2006 & 2007

- Providers of only (ISC)²-authorized CBK Review Seminars for CISSP, SSCP and CAP through the (ISC)² Institute and dozens of authorized academic affiliates around the world
- eLearning and instructor-led course options
- (ISC)² Academic Program – Education affiliates
- Continuing education for (ISC)² certified members
 - (ISC)² Security Leadership Series
 - (ISC)² members discounts to conferences held by IPEvents, RSA, MISTI, CSI and many other globally renowned providers



Supporting the Professional



- **Annual (ISC)² Information Security Scholarship Program – US\$100,000**
- **Research**
 - **Annual (ISC)² Global Information Security Workforce Study**
 - **Management and communication practices (with Auburn University)**
- **Free materials**
 - **(ISC)² Resource Guide for Today's Information Security Professional**
 - **(ISC)² Career Guide: Decoding the Information Security Profession**



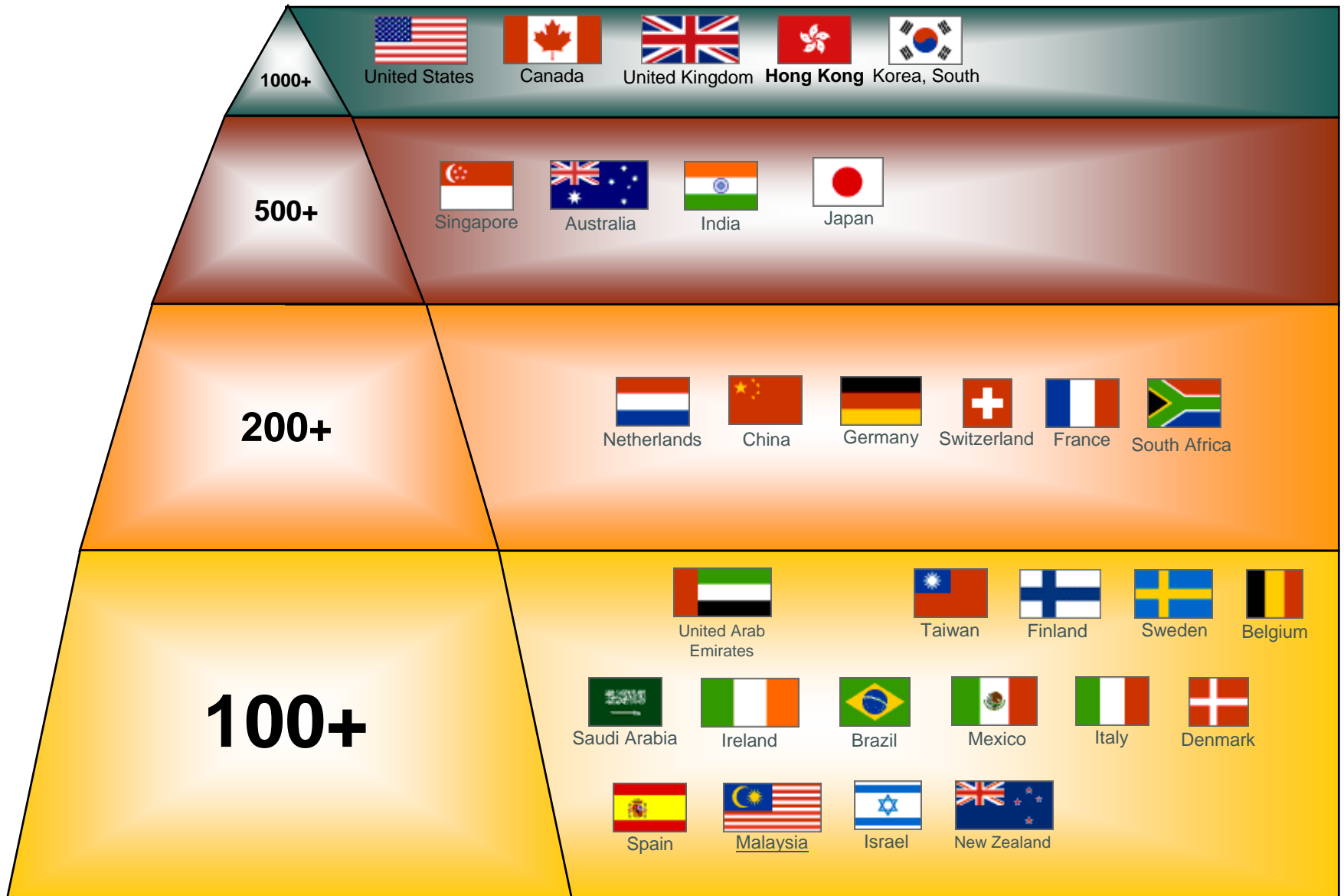


48,818 (ISC)² Members Worldwide*:

- CISSP 47,945
 - ISSAP 755
 - ISSEP 302
 - ISSMP 656
- CAP 287
- SSCP 586
- Associate of (ISC)² 610

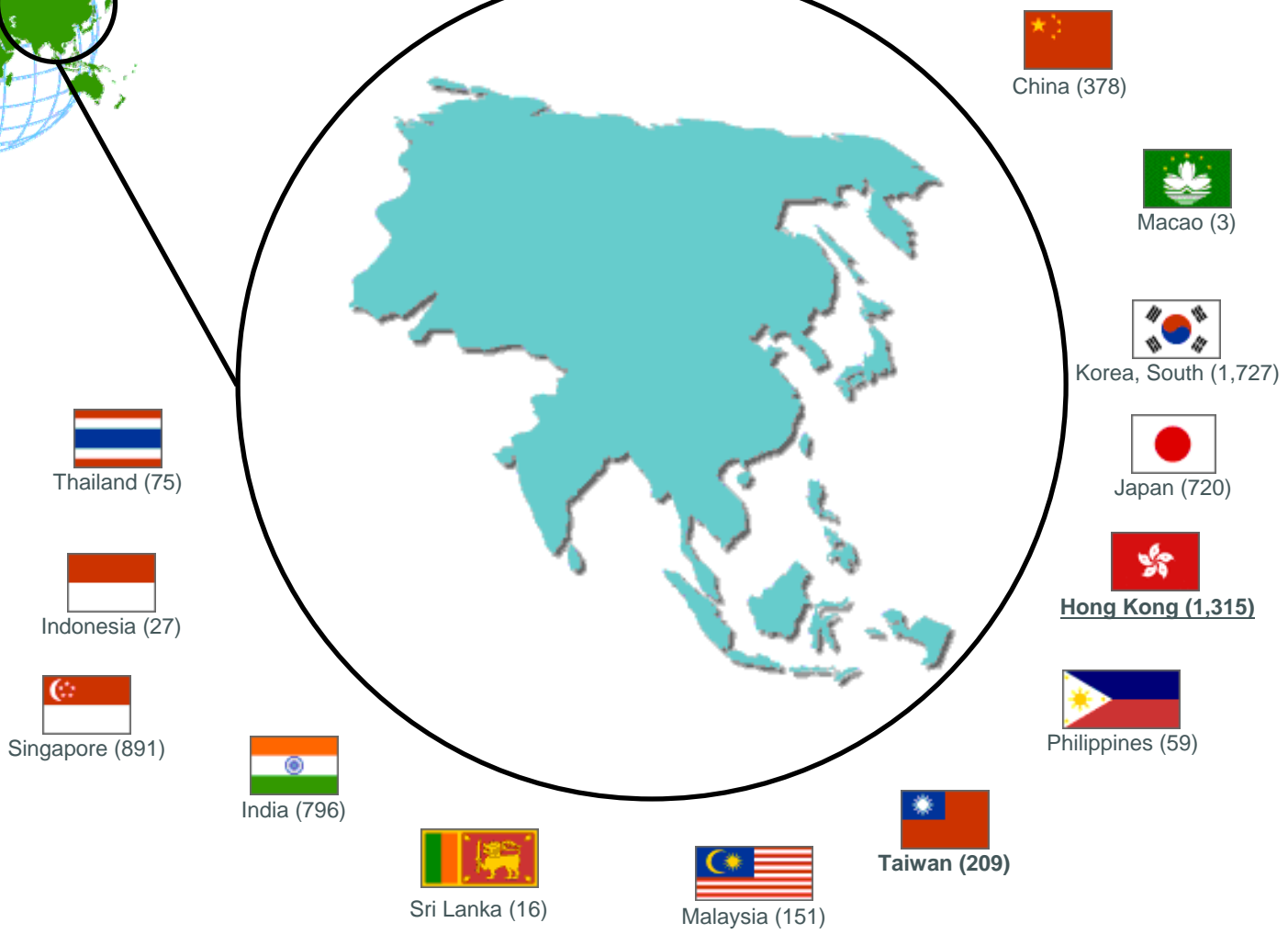
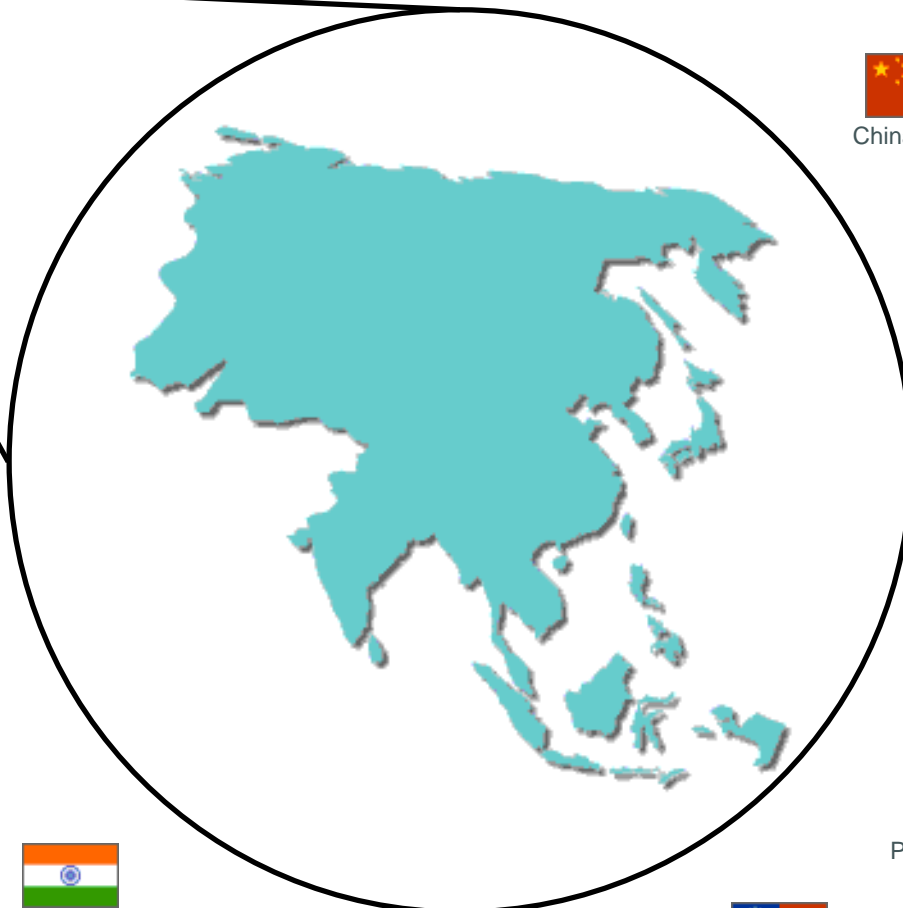
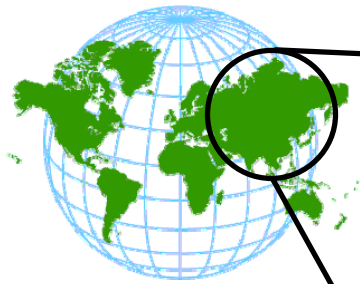
**As of 2/28/07*

(ISC)² Honor Roll



Members in Asia-Pacific

As of: 14/Feb/07



People Are the Key

For more information about us, please visit www.isc2.org



(ISC)²[®]

SECURITY TRANSCENDS TECHNOLOGYSM