(ISC)^2 Update

(“Trust is the Ultimate Firewall”)

Dow A. Williamson, CISSP

Director of Communications

dwilliamson@isc2.org

www.isc2.org

(ISC)^2®

SECURITY TRANSCENDS TECHNOLOGY℠

Overview

- **(ISC)²** – *About Us*
- **Trust** – *The Ultimate Firewall*
- **Career Path** – *Cradle-to-Grave for INFOSEC Professionals*
- **Associate of (ISC)²** – *Professionalism and Ethics Upfront*
- **Professional Certifications** – *The Gold Standards*
- **CISSPs/SSCPs** – *Around the World*
- **Next Steps**

(ISC)²®

Overview

- **(ISC)²** – *About Us*
- **Trust** – *The Ultimate Firewall*
- **Career Path** – *Cradle-to-Grave for INFOSEC Professionals*
- **Associate of (ISC)²** – *Professionalism and Ethics Upfront*
- **Professional Certifications** – *The Gold Standards*
- **CISSPs/SSCPs** – *Around the World*
- **Next Steps**

(ISC)²®

(ISC)² - About Us

- Established in 1989
- Global Standard for Information Security – (ISC)² CBK™, a compendium of industry “best practices”
- Non-profit consortium of industry leaders
- Dedicated to training, educating, qualifying, and certifying information security professionals worldwide
- Approximately 20,000 constituents in 90 countries
- Board of Directors -- Top INFOSEC professionals -- worldwide

(ISC)²®

“Defense in Depth Strategy” – Where Does (ISC)^2 Fit?

(ISC)^2{

People

- Training/Awareness
- Certification
- Physical Security
- Personnel Security
- Information System Security Administration

Technology

- Technology Layering
- Security Criteria
- IT/IA Acquisition
- Risk Assessments
- Certification & Accreditation

Operations

- Assessments
- Monitoring
- Intrusion Detection
- Warning
- Response
- Recovery

Overlapping Approaches & Layers of Protection

Overview

- **(ISC)²** – *About Us*
- **Trust** – *The Ultimate Firewall*
- **Career Path** – *Cradle-to-Grave for INFOSEC Professionals*
- **Associate of (ISC)²** – *Professionalism and Ethics Upfront*
- **Professional Certifications** – *The Gold Standards*
- **CISSPs/SSCPs** – *Around the World*
- **Next Steps**

(ISC)²®

Security Evolving to "Trust"

*We chose the term "**Trust**" carefully because it is the **real essence of relationships in the networked world**.*

- ***Security*** is primarily defensive and inward looking
- ***Control*** is a process to achieve it

But…"***Trust***" is an ***ongoing and outgoing interaction*** that establishes and maintains ***mutual confidence*** among ***many entities***.

"Trust" is crucial to the 21st century world!

(ISC)²®

"Trust"

- Requires ***security*** and ***control***…but, it goes beyond them…
- Depends on ***technology*** and ***protective mechanisms***…but, not solely…
- Involves ***professionalism***, ***reputation***, ***contracts***, ***law***, ***openness***, ***familiarity***, ***fair business practices and ethics***, ***quality***, ***timeliness***, and a host of other relationship characteristics…

"Trust" is the (ISC)² Ethical Code requirement!

(ISC)²®

The Basis of “Trust”

- The development of mutual ***“Trust”*** is based on each player’s ***willingness and ability to continuously demonstrate*** to all the other players’ satisfaction that the ***game is honest, open, following the rules and properly controlled***.

- This has some ***profound implications*** for security and control technologies, processes, relationships, policies, standards, organizations and professionals.

(ISC)²®

21st Century "Trust" Characteristics

- ***Reciprocity*** - the willingness of all the players to extend protection not only to all the other players but also to the network-based environment itself - the common cause. This does not mean equal protection for all. It means appropriate protection for all.
- ***Clarity*** of Responsibility and Liability
- ***Standardization*** of Processes, Interfaces and Technologies
- ***External*** Demonstrability

(ISC)²®

21st Century “Trust”

Components

- Authentication
- Authorization
- Availability
- Confidentiality
- Privacy
- Accountability
- Path Integrity
- Non-repudiation
- Auditability
- Process Integrity
- Data Integrity

But…
In Far Riskier, More Complex, Higher Stakes, Higher Speed, Rapidly Evolving, Larger, Widely Variable, and *Interdependent* Environments.

Guidance/ Documentation

- Organization Policies (multi-level)
- Strategies
- Architectures
- Procedures
- Standards
- Designs and Specifications
- Awareness and Training Documents
- Public Statements and Releases

Technologies

- Digital Certificates/PKI structure
- Certificate/Registration Authorities
- Integrated Authorization
- Digital Notaries & Time Stamping
- Directory Services
- Single Sign-on
- File Encryption
- Message Encryption
- Path Encryption (VPN’s)
- Network Security (Firewalls, etc.)
- Two/Three Factor Authentication
- Biometrics
- Smart Cards
- Platform Security (Trusted O/S)
- Anti-Virus Protection
- Disaster Recovery
- High Availability Monitoring
- Enterprise Application Security
- Data Base Security
- Access Control Facilities
- Intrusion Detection/Response
- ……and More

(ISC)²®

Overview

- **(ISC)²** – *About Us*
- **Trust** – *The Ultimate Firewall*
- **Career Path** – *Cradle-to-Grave for INFOSEC Professionals*
- **Associate of (ISC)²** – *Professionalism and Ethics Upfront*
- **Professional Certifications** – *The Gold Standards*
- **CISSPs/SSCPs** – *Around the World*
- **Next Steps**

(ISC)²®

Implications for (ISC)^2

- ***Our Offerings*** of Training, Credentials, Concentrations, Publications, and Services…
- ***MUST anticipate and support the needs of***…
- A widening range of ***Individual Professionals***, their ***Employers***, the ***Profession*** itself, and the larger ***Information Community***.

(ISC)^2®

(ISC)² is Evolving to Anticipate and Support…

- ***<u>Trusted Professionals</u>*** -- Individual career needs and aspirations
- ***<u>Employers</u>*** -- Strategic and tactical needs
- ***<u>Profession</u>*** -- The changing nature
- ***<u>Information Community</u>***

(ISC)²®

…In These Key “Trust” Roles and Organizations

- CISO/CSO - including policy
- Business Security Strategy and Architecture
- Technical Security Strategy and Architecture
- Application/User Security (Design, Development, Deployment and Maintenance)
- Infrastructure Security (Design, Development, Deployment and Maintenance)
- Network and Directory Services Management
- Monitoring, Control, Reporting, and Audit
- Intrusion Detection, Attack & Penetration, and Incident Response
- Access, Authorization and Accountability Management
- Classification and Data Management
- Regulatory and “Dictates” Compliance
- Training, Education, Awareness, and Professionalism
- Employee, Partner, Stakeholder, Government, and Public Relations

(ISC)²®

Professional Offerings - Credentials

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL · CISSP®

SYSTEMS SECURITY CERTIFIED PRACTITIONER · SSCP®

- ***Credentials*** – The *"Gold Standards"*
  - Certified Information Systems Security Professional (CISSP®)
  - System Security Certified Practitioner (SSCP®)
- ***Concentrations*** – in depth specialized credential enhancements
  - CISSP
    - NEW! Information Systems Security Architecture Professional (ISSAP^{CM}) — CISSP ARCHITECTURE CONCENTRATION
    - NEW! Information Systems Security Engineering Professional (ISSEP^{CM}) — CISSP ENGINEERING CONCENTRATION
    - NEW! Information Systems Security Management Professional (ISSMP^{CM}) — CISSP MANAGEMENT CONCENTRATION
  - SSCP – As required

(ISC)²®

Professional Offerings - Training

- Pre-Exam or Stand Alone
  - Certified Information Systems Security Professional (CISSP®)
  - System Security Certified Practitioner (SSCP®)
- CISSP Concentrations
  - Information Systems Security Architecture Professional (ISSAP^{CM}) NEW!
  - Information Systems Security Engineering Professional (ISSEP^{CM}) NEW!
  - Information Systems Security Management Professional (ISSMP^{CM}) NEW!
- SSCP Concentrations (As required)
- Associate of (ISC)² - pre-certification training/education NEW!

(ISC)^2®

Professional Offerings – Industry Support

(ISC)² Government Advisory Board for Cyber Security

- Industry Advisory Groups NEW!
  - Government Advisory Board for Cyber Security (GABCS)
- Planning Support for Employers and Groups
- Special Packaging of Training and Credentials
- Special Credentials and Exams
  - CISSP ISSEP Concentration (developed in conjunction with U.S. National Security Agency) CISSP ENGINEERING CONCENTRATION
  - Others (TBD)
- Tailored Training

(ISC)²®

Professional Offerings – Academia/Constituents

(ISC)² Newsletter

(ISC)² Website

- Constituent Services
- Contributions to the Profession and Professional Affiliations (including other Certifications)

INFORMATION SECURITY FORUM

ISSA™ Information Systems Security Association

- Publications, Forums and Communications
- Academic Affiliations

Royal Holloway University of London

PURDUE UNIVERSITY

IDAHO STATE UNIVERSITY

- Constituent Advancement and Support
- Associate of (ISC)²

(ISC)²®

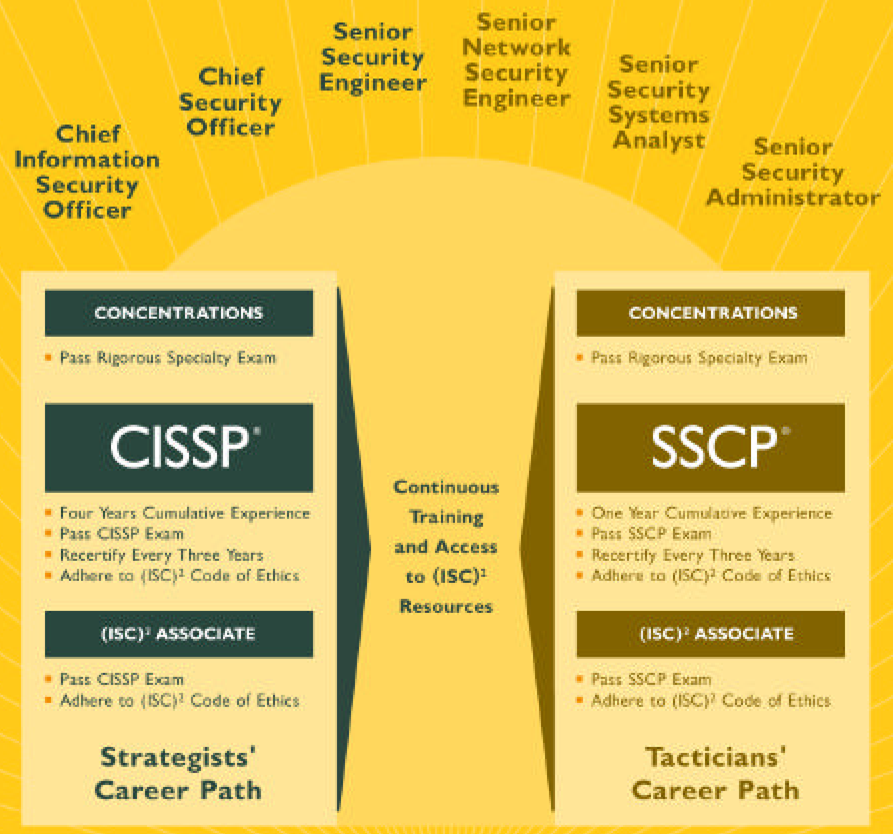
Sorting It Out – Roles, Credentials, Training

- The Diagram that follows maps what we believe are the most appropriate but by no means only (ISC)² offerings for some of the roles outlined earlier.
- These are intended as guides, not mandates.
- Development of specially designed credential/training programs for specific industries, enterprises, agencies, institutions and geo-political entities are a major strategic priority for (ISC)².
- Our strategy is to carefully monitor marketplace and professional demands and to modify and enhance our offerings as appropriate in response to them.

(ISC)²®

Career Path - Overview

Whether you’re a CISO or just starting your Information Security career, there’s an (ISC)^2 career path for you.



Chief Information Security Officer

Chief Security Officer

Senior Security Engineer

Senior Network Security Engineer

Senior Security Systems Analyst

Senior Security Administrator

CONCENTRATIONS

- Pass Rigorous Specialty Exam

CISSP®

- Four Years Cumulative Experience
- Pass CISSP Exam
- Recertify Every Three Years
- Adhere to (ISC)^2 Code of Ethics

(ISC)^2 ASSOCIATE

- Pass CISSP Exam
- Adhere to (ISC)^2 Code of Ethics

Strategists' Career Path

Continuous Training and Access to (ISC)^2 Resources

CONCENTRATIONS

- Pass Rigorous Specialty Exam

SSCP®

- One Year Cumulative Experience
- Pass SSCP Exam
- Recertify Every Three Years
- Adhere to (ISC)^2 Code of Ethics

(ISC)^2 ASSOCIATE

- Pass SSCP Exam
- Adhere to (ISC)^2 Code of Ethics

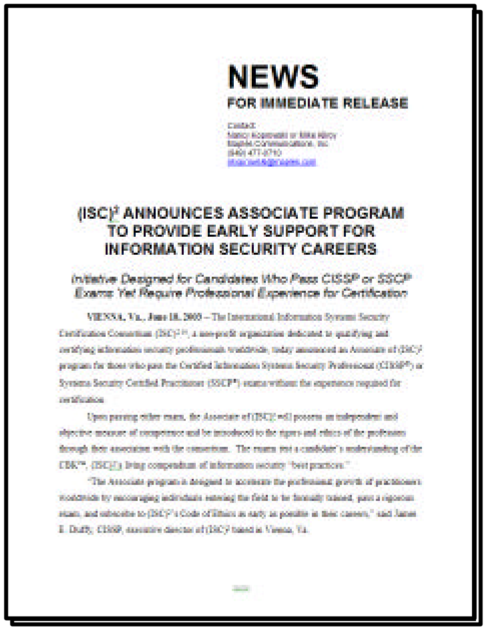
Tacticians' Career Path

Overview

- **(ISC)²** – *About Us*
- **Trust** – *The Ultimate Firewall*
- **Career Path** – *Cradle-to-Grave for INFOSEC Professionals*
- **Associate of (ISC)²** – *Professionalism and Ethics Upfront*
- **Professional Certifications** – *The Gold Standards*
- **CISSPs/SSCPs** – *Around the World*
- **Next Steps**

(ISC)²®

Associate of (ISC)²



NEWS

FOR IMMEDIATE RELEASE

Contact:
Nancy Kosmalski or Mike Kilroy
Maples Communications, Inc.
(949) 477-9710
[illegible]

(ISC)² ANNOUNCES ASSOCIATE PROGRAM TO PROVIDE EARLY SUPPORT FOR INFORMATION SECURITY CAREERS

Initiative Designed for Candidates Who Pass CISSP or SSCP Exams Yet Require Professional Experience for Certification

VIENNA, Va., June 18, 2003 – The International Information Systems Security Certification Consortium (ISC)²™, a non-profit organization dedicated to qualifying and certifying information security professionals worldwide, today announced an Associate of (ISC)² program for those who pass the Certified Information Systems Security Professional (CISSP®) or Systems Security Certified Practitioner (SSCP®) exams without the experience required for certification.

Upon passing either exam, the Associate of (ISC)² will possess an independent and objective measure of competence and be introduced to the rigors and ethics of the profession through their association with the consortium. The exams test a candidate's understanding of the CBK™, (ISC)²'s living compendium of information security "best practices."

"The Associate program is designed to accelerate the professional growth of practitioners worldwide by encouraging individuals entering the field to be formally trained, pass a rigorous exam, and subscribe to (ISC)²'s Code of Ethics as early as possible in their careers," said James E. Duffy, CISSP, executive director of (ISC)² based in Vienna, Va.

- ***Program to***…
  - Provide early support for Information Security careers
  - Accelerate the professional growth of practitioners worldwide
- ***Designed for candidates who***…
  - Pass the CISSP® or SSCP® examination
  - Lack professional experience required for formal certification
- ***Indicates a candidate***…
  - Possesses an independent and objective measure of competence via understanding of (ISC)² CBK™
  - Aspires to adhere to the rigors and ethics of the profession through association with (ISC)²
- ***Provides access to suite of (ISC)² career support programs***…
  - Specialized forums
  - Communications
  - Peer networking

Overview

- **(ISC)²** – *About Us*
- **Trust** – *The Ultimate Firewall*
- **Career Path** – *Cradle-to-Grave for INFOSEC Professionals*
- **Associate of (ISC)²** – *Professionalism and Ethics Upfront*
- **Professional Certifications** – *The Gold Standards*
- **CISSPs/SSCPs** – *Around the World*
- **Next Steps**

(ISC)²®

Characteristics of a Professional Certification

- ***International*** – based upon international compendium of industry “best practices” – (i.e., (ISC)^2’s CBK™)
- ***Examination*** – Rigorous exam to assure knowledge of 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/training to maintain credential
- ***Maturity*** – Wide acceptance as the true measure of competency

(ISC)^2®

Benefits of Certification…

…to the Enterprise

- Solutions orientation, not specialization
- Broad understanding of the CBK™
- The rigor and regimen adds to credibility
- A business and technology orientation to risk management

…to the Professional

- Career differentiator
- Confirms knowledge of information security
- Networking with global and domain experts
- Member of a “family” concerned about your career

(ISC)²®

(ISC)² Certifications

“Security Transcends Technology”

(ISC)²®

(ISC)² Certified Information Systems Security Professional

- Tailored for experienced information security professionals
- Minimum four years cumulative experience in CBK domains
- Undergraduate degree required for one year experience abatement
- Subscribe to (ISC)² Code of Ethics
- Endorsed by another CISSP or senior management
- Certification maintained through continuing education

CISSP® CBK™ Domains

- Security Management Practices
- Law, Investigation & Ethics
- Physical Security
- Operations Security
- Business Continuity & Disaster Recovery Planning
- Computer, System & Security Architecture
- Access Control Systems & Methodology
- Cryptography
- Telecommunications & Network Security
- Application Program Security

(ISC)^2®

(ISC)² Systems Security Certified Practitioner

SYSTEMS SECURITY • CERTIFIED PRACTITIONER •

SSCP®

- Tailored for systems and network security administration professionals
- Minimum one year cumulative experience in CBK domains
- Subscribe to (ISC)² Code of Ethics
- Certification maintained through continuing education

SSCP® CBK™ Domains

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

(ISC)^2®

(ISC)^2 Certification Concentrations

CISSP ARCHITECTURE CONCENTRATION

CISSP ENGINEERING CONCENTRATION

CISSP MANAGEMENT CONCENTRATION

- CISSP® Concentrations
  - Information Systems Security Architecture Professional (ISSAP^{CM})
  - Information Systems Security Engineering Professional (ISSEP^{CM})
  - Information Systems Security Management Professional (ISSMP^{CM})
  - Others (TBD)
- SSCP® Concentrations (TBD)

(ISC)^2®

(ISC)² Certification Examination Process

- ***<u>Managed Independent of (ISC)²</u>***
  - Schroeder Measurement Technology, Inc.
  - Measurement professionals oversee all aspects
- ***<u>Based on CBK™</u>*** – international compendium of industry “best practices”
- ***<u>Content Outline</u>*** – Evaluated and written by Subject Matter Experts
- ***<u>Job Analysis Study</u>*** – Used to continually update exam material
- ***<u>Test Development and Administration</u>***
  - Exams meet specifications of Content Outline
  - Exams have the same proportion of items from a given domain
  - Stringent “industry standards” are used to administer the exam
- ***<u>Scoring/Equating</u>***
  - Modern measurement models (Item Response Theory) are used to equate the exams
  - IRT allows the implementation of a “passing score” once the exam is developed

(ISC)²®

(ISC)² Certification Examinations

- ***Format***
  - 250/125 multiple choice questions (CISSP®/SSCP®)
  - Ample time to complete -- No trick questions
- ***Flexible Scheduling***
  - Major INFOSEC conferences
  - CBK™ Review seminar locations
  - Special “hosted” events
- ***Conceptual/Independent*** – Product independent…test knowledge of fundamentals
- ***Peer driven*** – Test questions written by previously certified constituents
- ***Rigorous endorsement process*** – Validated by CISSP/SSCP

(ISC)²®

(ISC)² Code of Ethics

Certification is granted or revoked at the sole discretion of the (ISC)² Board of Directors. Conscientious observance of the following code of conduct is a binding condition of credentials granted by (ISC)².

Code of Ethics Preamble

- **Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.**
- **Therefore, strict adherence to this code is a condition of certification.**

Code of Ethics Canons

- **Protect society, the commonwealth, and the infrastructure.**
- **Act honorably, honestly, justly, responsibly, and legally.**
- **Provide diligent and competent service to principals.**
- **Advance and protect the profession.**

"Trust is the Ultimate Firewall"

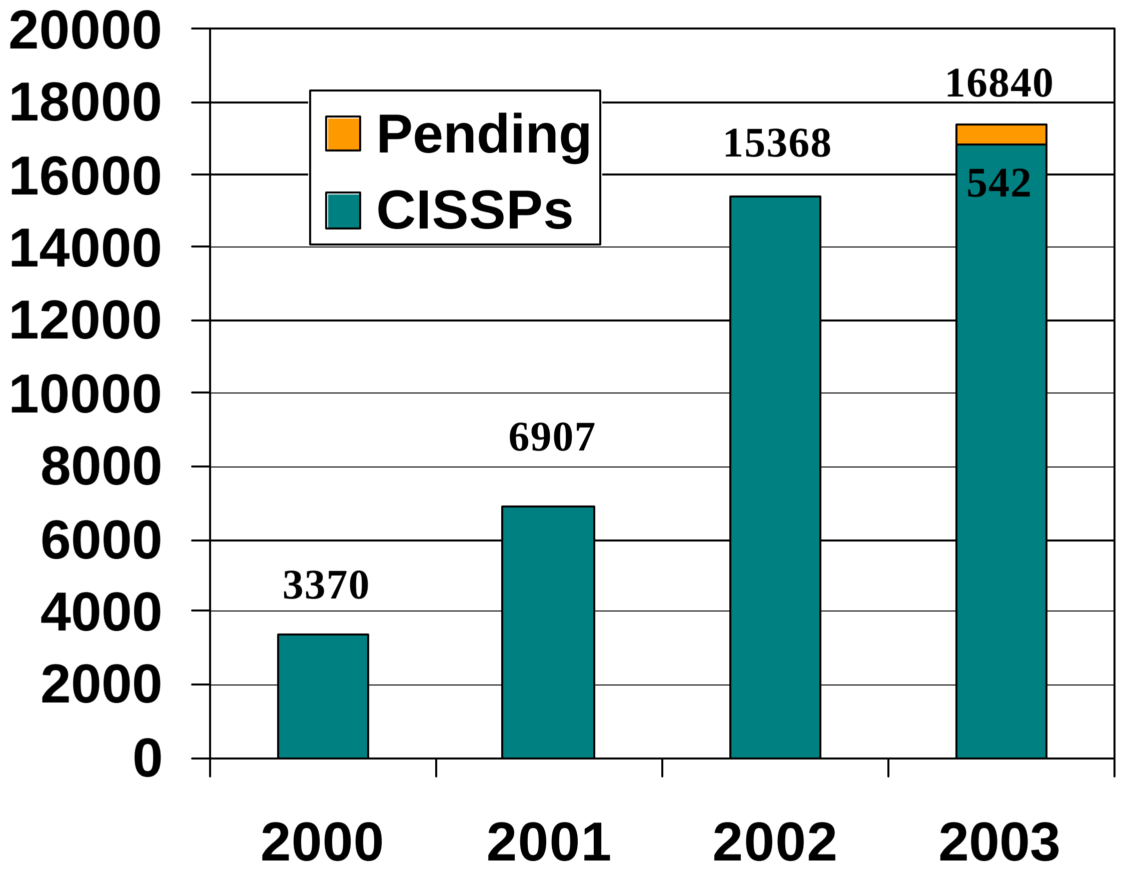
(ISC)²®

Overview

- **(ISC)²** – *About Us*
- **Trust** – *The Ultimate Firewall*
- **Career Path** – *Cradle-to-Grave for INFOSEC Professionals*
- **Associate of (ISC)²** – *Professionalism and Ethics Upfront*
- **Professional Certifications** – *The Gold Standards*
- **CISSPs/SSCPs** – *Around the World*
- **Next Steps**

(ISC)²®

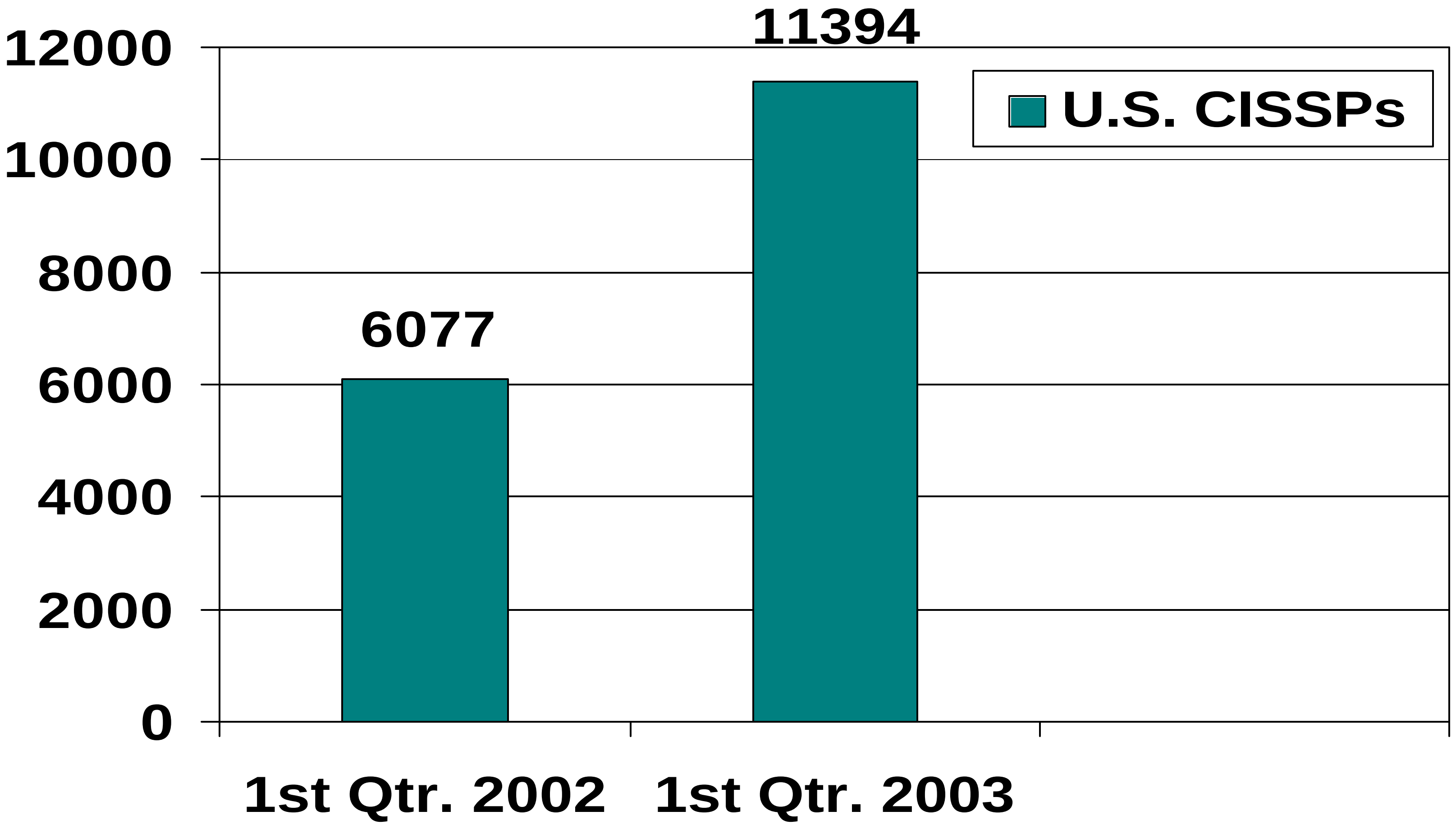
Growth in CISSPs - Worldwide



3/31

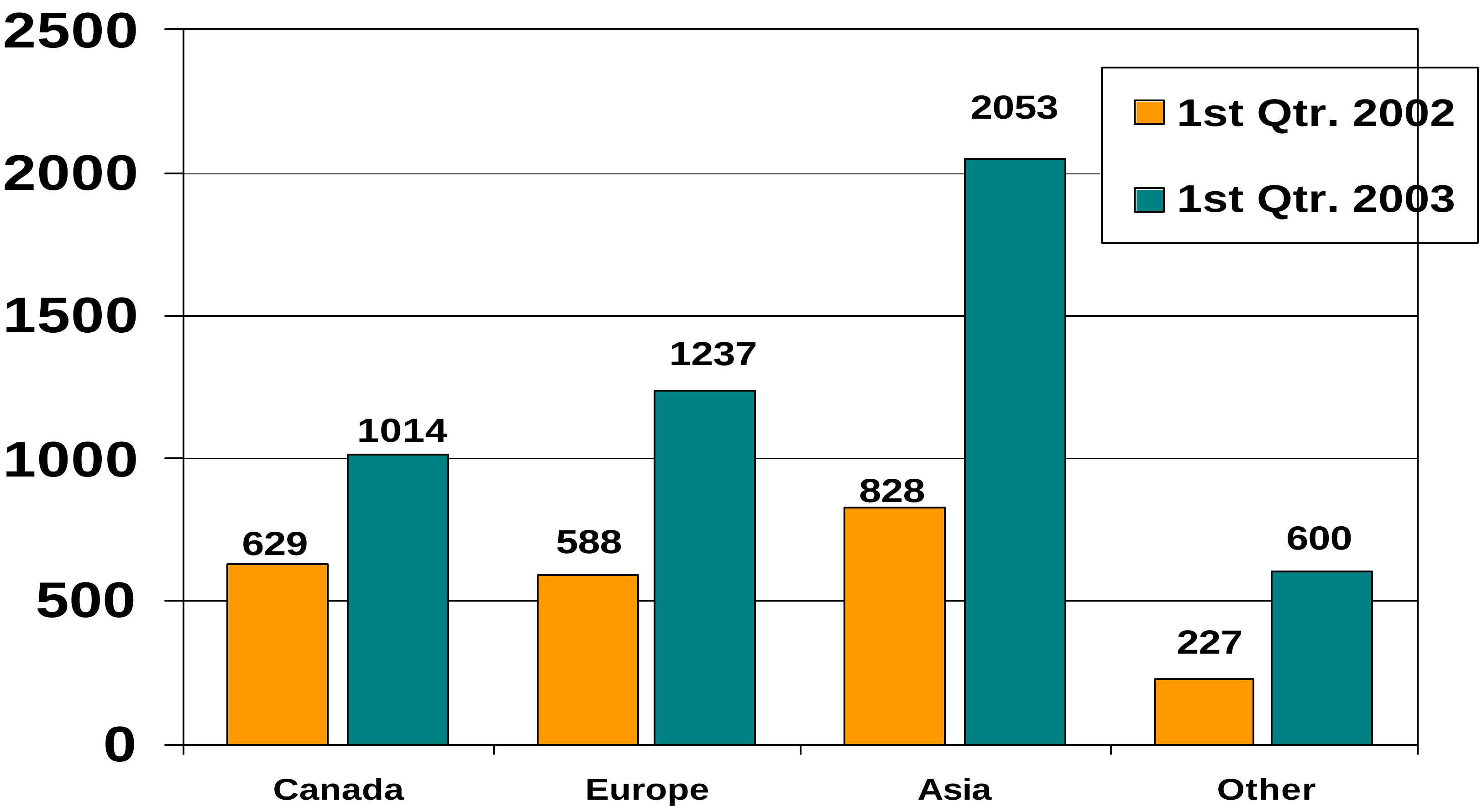
(ISC)²®

Growth in CISSPs – United States



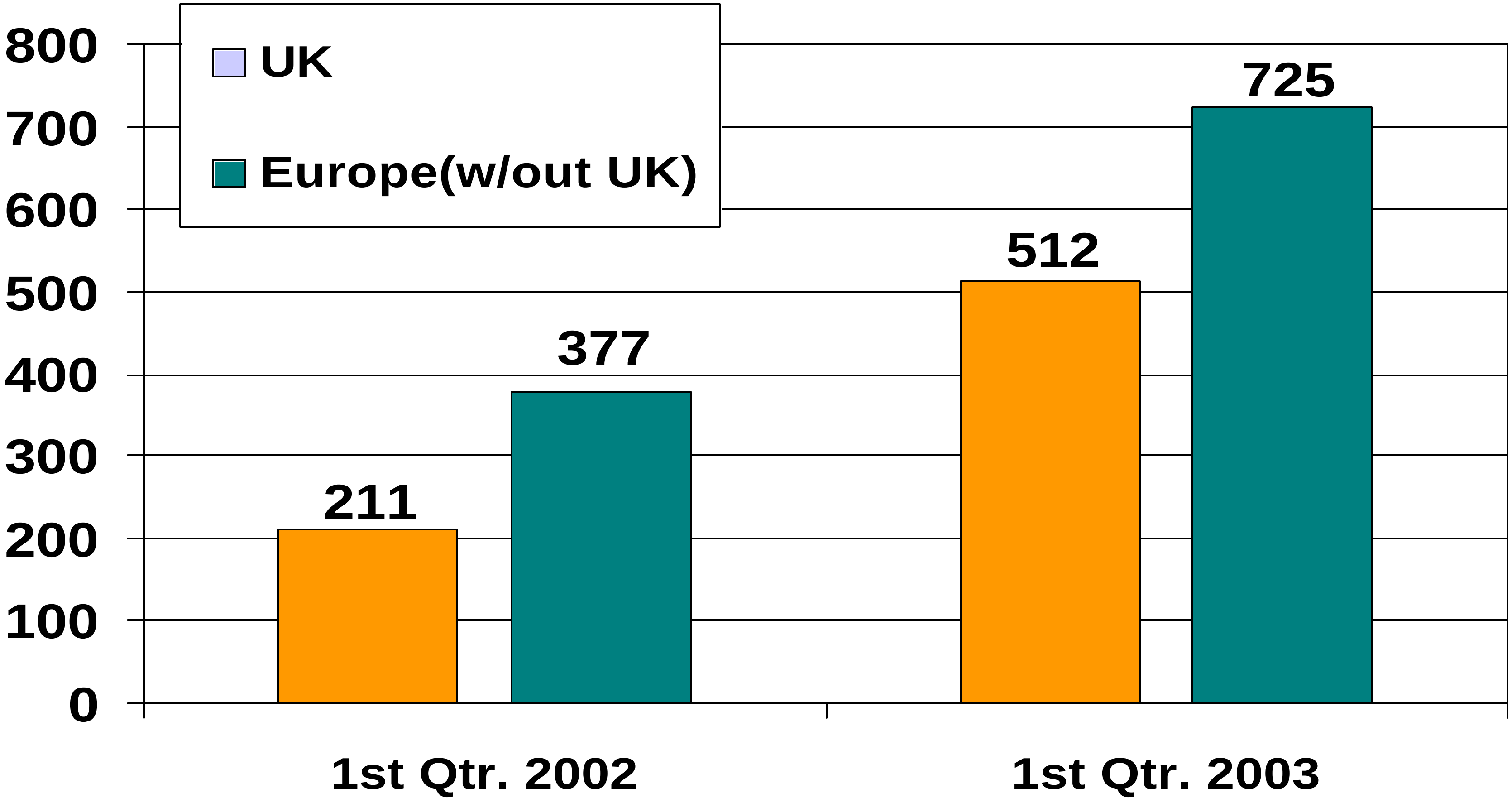
(ISC)²®

Growth in CISSPs - International



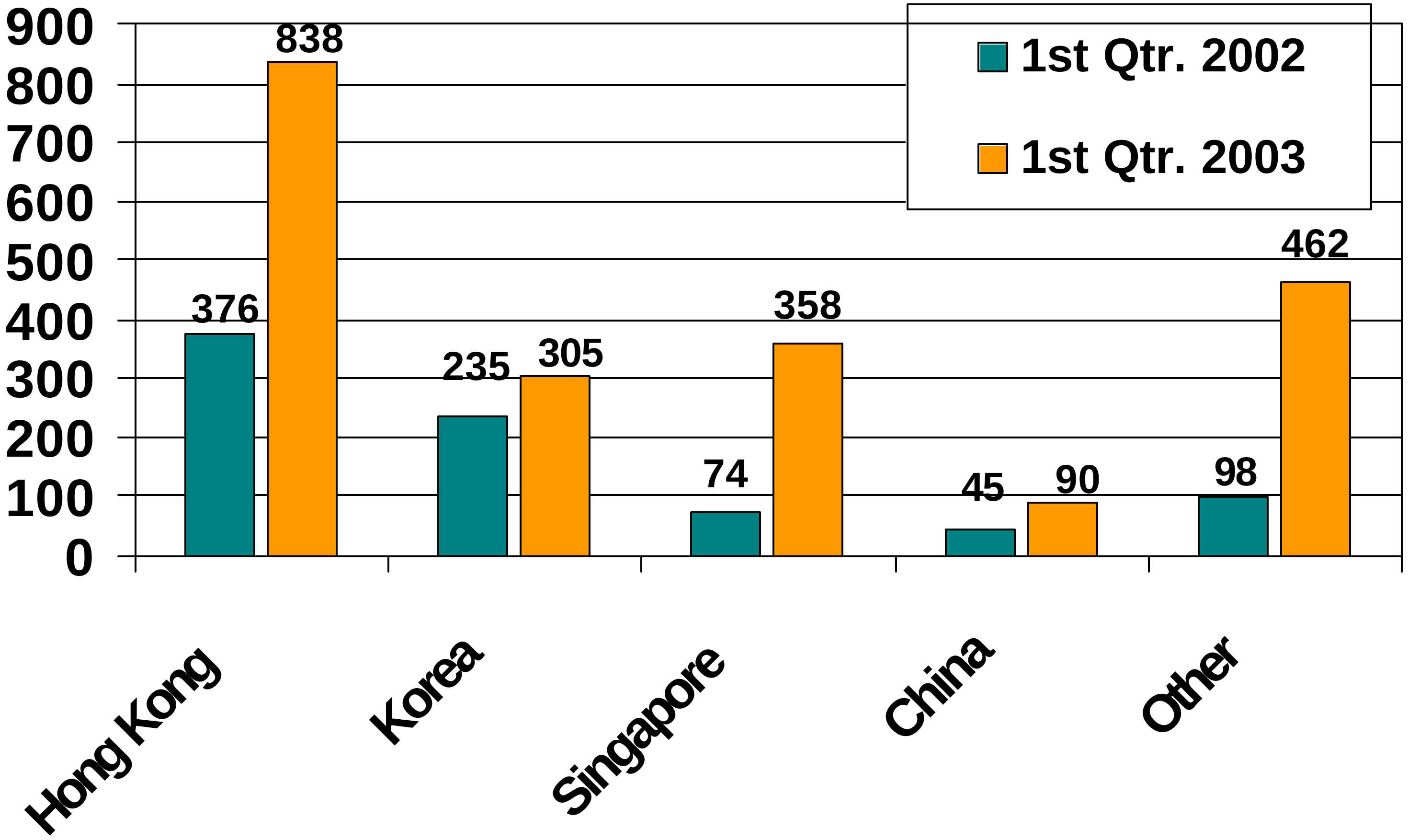
(ISC)²®

Growth in CISSPs - Europe



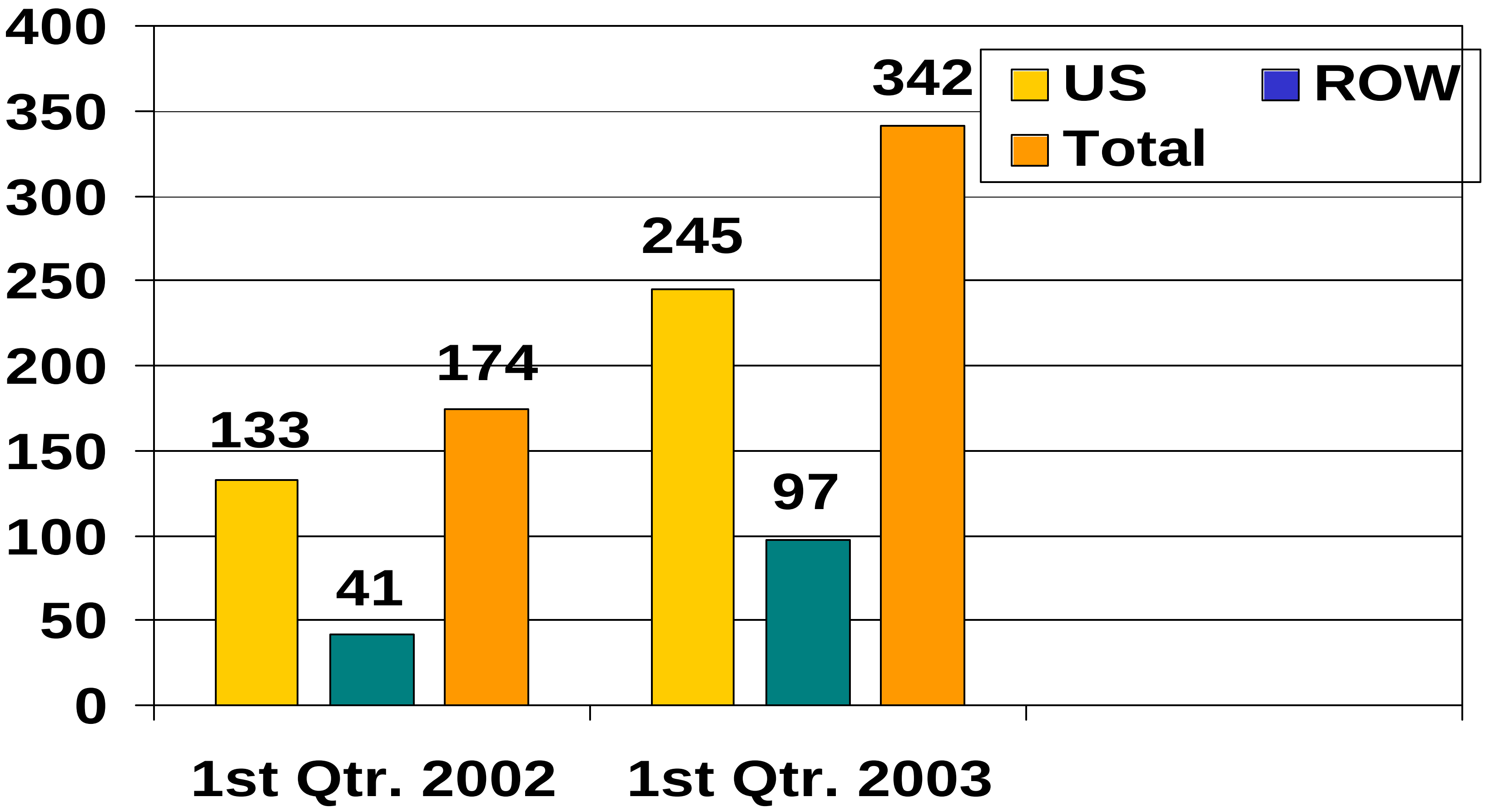
(ISC)²®

Growth in CISSPs - Asia



(ISC)²®

Growth in SSCPs - Worldwide



(ISC)²®

Overview

- **(ISC)²** – *About Us*
- **Trust** – *The Ultimate Firewall*
- **Career Path** – *Cradle-to-Grave for INFOSEC Professionals*
- **Associate of (ISC)²** – *Professionalism and Ethics Upfront*
- **Professional Certifications** – *The Gold Standards*
- **CISSPs/SSCPs** – *Around the World*
- **Next Steps**

(ISC)²®

Next Steps

- Continue to develop services for…
  - Constituents
  - Employers
  - Profession
  - Information Community
- Continue to develop concentrations for CISSP®/SSCP®
- Grow Associate of (ISC)² program worldwide
- Grow (ISC)² community from 20,000 to 100,000 constituents

(ISC)²®

“Trust is the UltimateFirewall”

(ISC)²®

SECURITY TRANSCENDS TECHNOLOGY℠