Certification and Training

CSE 4471: Information Security
Instructor: Adam C. Champion, Ph.D.

Based on slides by Sam Jeyandran
(former student in Info. Sec. course)
Outline

• Organizational information security personnel
  – In general
  – At OSU

• Professional information security certification
Information Security Personnel (1)

Figure 11.2. Positions in Information Security (redrawn)
Information Security Personnel (2)

- Chief security officer (CSO): Head of security, reports to CIO and execs
  - Manages org’s info. sec. program and policies
  - Works on strategic, tactical, operational plans
  - Handles security budgeting, personnel
  - Usually needs college degree and CISSP
- Security manager: handles org’s info. sec. program on a daily basis
  - Develops/implements policies under CSO’s guidance
  - Monitors progress of organization’s info. sec. program
  - Handles incident response, disaster recovery, risk assessment
  - Usually needs college degree, CISSP
- Security technician: deploys/manages firewalls, IDSs, etc. under security manager’s guidance
OSU Information Security Personnel
Org Chart

Source: https://orgchart.osu.edu/organization/ocioodee
Professional Certifications

- Information System Audit and Control Association (ISACA)
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
- Int’l. Information Systems Security Certification Consortium (ISC)$^2$
  - Certified Information System Security Professional (CISSP)
  - System Security Certified Practitioner (SSCP)
- Int’l. Information System Forensics Association (IISFA)
  - Certified Information Forensics Investigator (CIFI)
- Many require candidates have professional security experience/college degree, no criminal record
Other Certifying Organizations

- System Administration, Networking, and Security Institute (SANS)
- Global Information Assurance Certification (GIAC)
- Information System Security Association (ISSA)
- American National Standards Institute (ANSI)
- Computer Professional for Social Responsibility (CPSR)
- Companies: Microsoft, Cisco, etc. (vendor-specific)
- Int’l. Society of Forensic Computer Examiners (ISFCE)
- CompTIA: A+ certs (vendor-neutral)
CISSP Concentrations

- Information System Security Architecture Professional (ISSAP): Concentration in Architecture
- Information System Security Engineering Professional (ISSEP): Concentration in Engineering
- Information System Security Architecture Professional (ISSMP): Concentration in Management
CISA Exam Content Areas

- CISA Exam (Six Domains)
  - IS Audit Process (10%)
  - IT Governance (15%)
  - Systems and Infrastructure Life Cycle (16%)
  - IT Service Delivery and Support (14%)
  - Protection of Information Assets (31%)
  - Business Continuity and Disaster Recovery (14%)
CISM Exam Content Area

• CISM Exam (Five Domains)
  – Information Security Governance (21%)
  – Risk Management (21%)
  – Information Security Program Management (21%)
  – Information Security Management (24%)
  – Response Management (13%)
CISSP Exam Content Area (1)

- CISSP Exam (10 Domains)
  - Access Control Systems and Methodology
  - Applications and Systems Development Security
  - Business Continuity Planning (BCP), Disaster Recovery Planning (DRP)
  - Cryptography
  - Law, Investigation and Ethics
  - Operations Security
  - Physical Security
  - Security Architecture and Models
  - Security Management Practices
  - Telecommunications and Network Security
SSCP Exam Content Area

• SSCP Exam (7 Domains)
  – Access Control
  – Administration
  – Audit and Monitoring
  – Cryptography
  – Data Communications
  – Malicious Code/Malware
  – Risk, Response and Recovery
CIFI Exam Content Area

- CIFI Exam (6 Domains)
  - Auditing
  - Incident Response
  - Law and Investigation
  - Tools and Techniques
  - Traceback
  - Countermeasures
Training, Seminars and Conferences

- http://www.issa.org/
- http://www.isaca.org/
- https://www.isc2.org
- http://www.ansi.org/
- http://www.sans.org/
- http://www.giac.org/
- http://www.infoforensics.org
Professional Publications

• ISACA: *Information Systems Control Journal*

• (ISC)$^2$: *The (ISC)$^2$ Journal (Information Systems Security)*

• ISSA: *The ISSA Journal*
Chapters and Membership

• Chapters: local and worldwide
• Membership
  – ISACA is a leading information technology organization representing more than 50,000 individual members in more than 140 countries.
  – ISSA has over 13,000 members worldwide
Summary

• Infosec personnel generally include CSO, security manager, and technicians
• Real-world org charts may vary
• Professional organizations offer infosec certs
• Recommendations:
  – CIS/CSE Majors:
    • CISSP (most prestigious)
    • SSCP
  – MIS (College of Business)
    • CISA
    • CISM