

Cultivating Information Security Expertise

Jason Riddle, CISSP
Knoxville Utilities Board
jriddle@kub.org

Why In-house Expertise is Needed

- Legal liability
- Security is a process, not a product
- Salespersons work on commission
- Managed security providers need a good point of contact

Where Can Expertise Be Found?

- Few colleges offer bachelors degrees in information security
- Security professionals often come from other areas
 - Systems/network administrators
 - Military/government
 - Audit

Methods of Cultivating Expertise

- I. Professional certification programs
- II. Formal education
- III. Self study & OJT
- IV. Industry involvement

I. Professional Certifications

- Different paradigm than formal education
- How do you determine value?
- Are there any specifically for security professionals?

Certifications vs. Formal Education

- Formal education stresses learning with testing to reinforce and assess knowledge
- Professional training is often tuition driven
- Certification attempts to fill the gap by assessing knowledge retained from training

Determining Value

- The ability to do the work should always be valued above certification
- Not every expert is certified; not all those certified are experts

Security Certifications

- CISSP – Certified Information Systems Security Professional
- CISA – Certified Information Systems Auditor
- CPP – Certified Protection Professional

Security Certifications (continued)

- GIAC – Global Incident Analysis Center (SANS)
- ICSA
 - ICSA (ICSA Certified Security Associate)
 - ICSE (ICSA Certified Security Expert)
 - ICSP (ICSA Certified Security Practitioner)

CISSP

- (ISC)2 – International Information Systems Security Certification Consortium
 - <http://www.isc2.org>
- Concentrates on concepts and theory
- Most useful for managers and policy makers

CISSP Ten Domains of Knowledge

- Access Control Systems and Methodology
- Telecommunications and Network Security
- Security Management Practices
- Applications and Systems Development Security
- Cryptography
- Security Architecture and Models
- Operations Security
- Business Continuity & Disaster Recovery Planning
- Physical Security
- Law, Investigations, & Ethics

CISSP Requirements

- Three years of experience in at least one of the ten domains
- Passing score on written exam
- Adhere to the (ISC)2 code of ethics

CISA

- Information Systems Audit & Control Association
 - <http://www.isaca.org>
- Most valuable for audit personnel
- Test covers many of the same areas of knowledge as CISSP exam

CISA Areas of Knowledge

- Management, Planning, and Organization of IS
- Technical Infrastructure & Operational Practices
- Protection of Information Assets
- Disaster Recovery & Business Continuity
- Business Application System Development, Acquisition
- Implementation & Maintenance
- Business Process Evaluation & Risk Management

CISA Requirements

- Passing score on written exam
- At least five years professional Information Systems auditing, control, or security work experience
- Subscribe to the Code of Professional Ethics
- Adhere to the Continuing Education Policy

CPP

- American Society for Industrial Security
 - <http://www.asisonline.org>
- Emphasis on security management concepts and physical security
- Most valuable for enterprise security managers

CPP Areas of Knowledge

- Security Management
- Investigations
- Legal Aspects
- Personnel Security
- Physical Security
- Protection of Sensitive Information
- Emergency Management

CPP Requirements

- Extensive security experience
 - Nine years experience or a bachelors degree and seven years experience
- Successful completion of exam

GIAC

- Global Incident Analysis Center
 - <http://www.incidents.org>
 - <http://www.sans.org>
- Emphasis on hands-on technical knowledge
- Provides maximum value for information security analysts/administrators

GIAC Requirements

- Course materials delivered at seminars or online
- Passing score on exam
- Completion of a practical assignment which demonstrates that candidates can apply what they have learned

GIAC Certifications

- Security Essentials
- Securing Windows
- Securing Unix
- Intrusion Detection
- Advanced Incident Handling and Hacker Exploits
- Firewalls, Perimeter Protection, & VPNs

ICSA (under development)

- Trusecure Corporation
 - www.trusecure.com
 - Home of ICSA Labs
 - Publisher of Information Security Magazine
- Will offer three certifications that focus primarily on network security
- Two upper level certifications provide divergent paths for technical personnel and managers/academics

ICSA Certifications

- **ICSA (ICSA Certified Security Associate)**
 - Network or system administrator responsible for enterprise security administration
- **ICSE (ICSA Certified Security Expert)**
 - Senior network engineers
 - Already ICSA certified
- **ICSP (ICSA Certified Security Practitioner)**
 - Supervisors and/or instructors

ICSA Requirements

- Still under development
- All levels will require:
 - passing a written exam
 - Adhering to ICSA code of ethics
 - Meeting minimum experience requirements

Other Valuable Certifications

- Microsoft
- Unix
- Cisco
- Additional vendor certifications

Microsoft Certifications

- MCSE (Microsoft Certified Systems Engineer)
 - <http://www.microsoft.com/trainingandservices/>
 - Seven exams covering the Windows 2000 operating system
- MCP (Microsoft Certified Professional)
 - Pass one of the core exams

Unix Certifications

- Solaris Certified Network/System Administrator
 - <http://suned.sun.com>
- IBM Certified Specialist – AIX Administration
 - <http://www-1.ibm.com/servers/aix/support/aixcert/>
- Red Hat Certified Engineer
 - <http://www.redhat.com/training/rhce/courses/>

Cisco Certifications

- CCIE (Cisco Certified Internetwork Expert)
 - <http://www.cisco.com/warp/public/10/wwtraining/certprog/>
 - CCNA
 - Single exam
 - CCNP
 - Four exams
 - CCIE
 - Qualification exam and two day lab

Vendor Certifications

- Almost every major vendor offers a certification associated with their product
- An example:
 - Check Point Software
 - CCSA (Check Point Certified Security Administrator)
 - CCSE (Check Point Certified Security Engineer)

II. Formal Education

- While still relatively rare, graduate degree and certificate programs in Information Security are available through traditional classroom instruction as well as distance learning

National INFOSEC Education and Training Program

<http://www.nsa.gov/isso/index.html>

- Sponsored by the NSA
 - Certifies centers of excellence in information assurance education
 - Currently 23 universities have been certified
 - Goal of program:
“Reduce vulnerabilities in our national information infrastructure by promoting higher education in information assurance...”

Centers of Excellence in Southeast

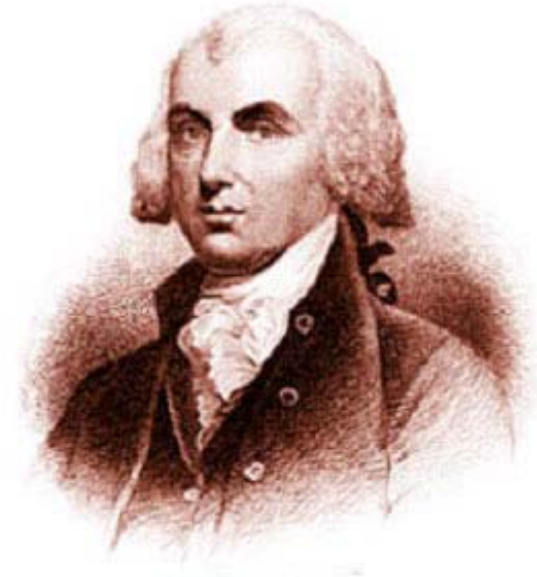
- Georgia Tech
 - <http://www.oit.gatech.edu/>
- Florida State
 - <http://www.cs.fsu.edu/infosec.html>
- Mississippi State
 - <http://www.cs.msstate.edu/~iids/index.htm>

Distance Learning

- **James Madison University**
- **George Mason University**

James Madison University

- MS in Computer Science with concentration in infosec
- Two year program
- Travel to campus once per semester
- www.infosec.jmu.edu



George Mason University

- Certificate in Information Systems Security
- Several MS programs with concentrations in infosec
- www.issc.gmu.edu/~csis



III. Self Study & OJT

- Information on security is abundant on the internet. Finding the right place to look can be tricky.
- There is no substitute for practical experience.

Security Resources on the Web

- Ron Rivest's Security Links
 - <http://theory.lcs.mit.edu/~rivest/crypto-security.html>
- Sword & Shield Security Links
 - <http://www.sses.net/resources/secsites.htm>
- Security Focus
 - www.securityfocus.com

Self Study Resources

- SmartForce (formerly CBT Systems)
 - <http://www.smartforce.com/corp/marketing/>
 - Offer computer based training on information security
- InfosecU
 - <https://infosecu.com/index.asp>
 - Offer online self-study courses for many security related subjects

On the Job Training

- Get in there and do it!
- Practical experience is often the best teacher
- Ask consultants to conduct a knowledge transfer instead of performing work and leaving



IV. Industry Involvement

- Become active in professional organizations
- Subscribe to information security periodicals
- Contribute to online security forums

Professional Organizations

- ISSA – Information Systems Security Association
- CSI – Computer Security Institute
- InfraGard

ISSA

- “The Information Systems Security Association (ISSA)[®] is a not-for-profit international organization of information security professionals and practitioners. It provides education forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.”

<http://www.issa.org/>

CSI

- **“Computer Security Institute (CSI) is the world's leading membership organization specifically dedicated to serving and training the information, computer and network security professional.”**

<http://www.gocsi.com/>



InfraGard

- “InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures.”

<http://www.infragard.net/>

Information Security Periodicals

- Information Security Magazine
 - <http://www.infosecuritymag.com/>
- Security Advisor Magazine
 - <http://www.advisor.com/www/SecurityAdvisor>
- Security Management
 - <http://www.securitymanagement.com/>

Summary

Methods of Cultivating Expertise

- I. Professional certification programs
- II. Formal education
- III. Self study & OJT
- IV. Industry involvement

Questions



Contact Information

Jason Riddle, CISSP
Knoxville Utilities Board

Jriddle@kub.org

Ph. 865-558-2056

Presentation available online at: www.kub.org/infragard