How to Have a Career in InfoSec – Meet ISC2 and learn about becoming a CISSP

(ISC)2®
SECURITY TRANSCENDS TECHNOLOGY®

Agenda

- A Brief Introduction
- What is Information Security?
- What is ISC2?
- A Look into the CISSP and the Security Domains
- Questions

A Brief Introduction

- Christopher Robinson aka CRob
- Sr. Technical Account Manager for Red Hat, Inc.
- Education Chair for Cleveland ISC2 Chapter
- 18 years Enterprise Engineering/Operations Management and Strategic Planning experience
- Worked for several Fortune 500 companies
- Leader, artist, mentor, writer, strategerist, brewer, teacher, vintner, father, consultant, teacher, gamer, Security-ologist

What is ISC2 and what's a CISSP?

- International Information Systems Security Certification Consortium
  - A global non-profit recognized as a leader in educating and certifying security professionals
- Certified Information Systems Security Professional
  - The recognized "Gold Standard" for confirming security experience and knowledge
  - Cert-holders have either 5 years of direct experience with multiple security domains or 4 years with a college degree or other approved credential and be endorsed by a current CISSP

(ISC)²
SECURITY TRANSCENDS TECHNOLOGY

Maintaining your CISSP

CPEs yearly – reviewed every 3 years

$85/annually

InfoSec Headlines

Why does security matter?

- Private customer data must be protected from unauthorized use/access (Identity Theft)
- Trade Secrets and the like must be protected from competitors (Industrial Espionage)
- Company Reputation/Brand must be protected (Character/Brand Defamation)
- Financial Transactions must be guaranteed authentic (Theft, Fraud, Money Laundering, etc.)
- Business Continuity must be ensured (Natural/Political Disasters – Hurricane Katrina, Japan's 2011 Tsunami, September 11th, 2001)
- And dozens of other reasons....

Interesting 2012 stats

- 2012 saw the rapid rise of Mobile Malware and Mobile Botnets
- Over 1.1mil identities were exposed worldwide via breech in 2011
- A 2010 study found that 46% of stolen laptops contained confidential data
- Total number of records containing sensitive personal information involved in security breaches in the U.S. is 562,943,732 in 3,241 data breaches since January 2005.
- The average total cost per company that reported a breach in 2011 was $5.5 million.
- Malicious or criminal attacks are the most expensive cause of data breaches and are on the rise. In 2011, 37 percent of data breach cases involved malicious attacks and averaged $222 per record. Negligence accounted for 39 percent of reported breaches.

- http://www.indefenseofdata.com/data-breach-trends-stats/

General InfoSec Concepts

- CIA – Confidentiality, Integrity, Availability
- Separation of Duties
- Principle of Least Privilege
- Principle of Due Care
- Compensating Controls
- Defense in Depth/Layered Defense
- At the end of the day Security is all about managing Risk.

The 10 Domains of InfoSec

- Access Control
- Telecommunications & Network Security
- InfoSec Governance & Risk Management
- Software Development Security
- Cryptography
- Security Architecture & Design
- Operations Security
- Business Continuity & Disaster Recovery
- Legal, Regulations, Investigations & Compliance
- Physical Security

Cleveland ISC2 Chapter

- Our Goal – To Educate, Inform, and Entertain
  - We meet the last Tuesday of every* month at 5:30pm at varying locations (generally in/near Independence, Ohio)
  - Great guest speakers from Security, Business, Education and other fields.
  - Excellent peer-to-peer conversations on relevant InfoSec issues.

Visit http://www.isc2chapter-cleveland.us/

for more details!

*every month, mostly

(ISC)² SECURITY TRANSCENDS TECHNOLOGY

Why Security Matters

DR scenario walk-through

Policy 4 guidance and potential legal action

Add security to ensure business can continue running

it’s the legal, ethical and moral thing to do

Questions

The 10 Domains of Security

Access Control

- This Domain focuses on Access and Privileges within IT systems.
  - Who, what, when, where, why?
  - Authentication – validating the identity of a user to a system (via something you know, something you have, something you are, and/or somewhere you are)
  - Authorization – defines what a user can they do once they are identified
- Areas of Interest
  - Access Models, User Provisioning, Biometrics, Privileged Account review, Auditing/logging, Passwords, Kerberos SSO, & more!

Telecommunications and Network Security

- This Domain focuses on networking, network devices, protocols and security measures
  - The OSI & TCP/IP Models
  - Network topologies
  - Network Hardware
  - Packets & Protocols
- Areas of Interest
  - Wireless Networking, Network Design, Security-focused network devices, communications and connectivity

Information Security Governance & Risk Management

- This Domain focuses on Information Assets of an Organization and creating policies to ensure these are protected.
  - Control Frameworks
  - Legislative and Regulatory Compliance
  - Policy, Roles & Responsibilities
  - Due Care
- Areas of Interest – data classification, risk assessments, threat identification, policy development

Software Development Security

- This Domain focuses on the Software Development Lifecycle (SDLC)
  - SDLC & Maturity Models
  - Security Controls and Security Issues related to development
  - Stresses that security is most effective when implemented throughout the **entire** life cycle
- Areas of Interest – Programming languages, application controls, common software threats & vulnerabilities, project methodologies

Cryptography

- This Domain is concerned with the principles and methods of applying mathematical algorithms to data to ensure its protection
  - History of Cryptography
  - Encryption concepts – symetric/asymetric encryption, hybrid cryptography, hashing, etc
  - Understanding cryptographic attacks
  - Public Key Infrastructure certificates
  - Understanding cryptanalytic attacks
- Areas of Interest – Data at Rest/Data in Transit, Key Management, PKI, algorithms and math

Security Architecture & Design

- This Domain focuses on design architectural principles, physical component identification, and security models
  - Security evaluation models
  - Industry security implementation guidelines (PCI-DSS, ISO)
  - Understanding software & system vulnerabilities
- Areas of Interest – Single-points of failure, SOA, Defense in-depth, countermeasures

Operations Security

- This Domain focuses on controls over media, hardware and privileged access
  - Need-to-know/least privilege
  - Separation of duties
  - Privileged entity monitoring and controls
- Areas of Interest – Patch & Vulnerability management, configuration management, fault tolerance/system resiliency, Incident Response

Business Continuity & Disaster Recovery

- This Domain focuses on the preservation of the business in the face of major disruptions.
  - BCP – Business Continuity Planning
  - DRP – Disaster Recovery Planning
  - BIA – Business Impact Analysis
- Areas of Interest – understanding business continuity requirements, conducting business impact analysis, developing and testing a DR plan

Legal, Regulations, Investigations & Compliance

- This Domain focuses on common types of laws and how the law is critical during incident response
  - Investigative measures and techniques that can be used to gather evidence
  - Legal issues that pertain to information security nationally & internationally
  - Rules of Evidence
  - Incident Response
- Areas of Interest – data forensics, criminal & civil law, Regulation, Privacy

Physical Security

- This Domain addresses the threats, vulnerabilities and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information.
    - Site & Facility Design
    - Operational physical security
    - Understanding personal privacy and safety
- Areas of Interest – safety safety safety, internal and perimeter controls