Career Paths In Cybersecurity
Introductions

Rob Ashcraft
Sr. Technical Advisor

- 26-yrs in Information Technology
- 14-yrs in Information Security
- Held positions as Technician, IT Management, IT Sales
- Double Major: Computer Science / Mathematics
Work Hard, Play Hard!
Why Information Security?

1. **According to CIO Magazine**, “experts in cybersecurity are among the most sought-after professionals in the tech sector, with demand for workers in that field outpacing other IT jobs by a wide margin.”

2. **Recent report cites** “The demand for Information Security professionals has grown 350% faster than any other position in IT.”

3. **There is a war going out there!** - The need for strong information security in organizations is paramount.

4. **Show me da money** - U.S. security professionals to be $116,000, or approximately $55 per hour. That's nearly three times the national median income for full-time wage and salary workers, according to the Bureau of Labor Statistics.
Why Information Security?

We turn this...

... into this!
Career Paths Within Information Security

1. Administration / Engineering
2. Audit / Risk Management
3. Forensics / Ethical Hacking
4. Management
5. Pre-Sales Engineering & Account Management
Security Administration & Engineering

Plans, coordinates, and monitors systems for the physical and electronic protection of data; Identifies and resolves security threats.

- Knowing how computers operate on the network
- Understanding the communication side of a network
- Computer Science & Security education / experience
- Network Admin / Engineering experience

Positions
- Security Specialist
- Information Security Analyst
- Data Security Analyst
- Cloud Engineers & Architects
Audit / Risk Management

Conducts methodical examinations of an organization’s systems, platforms, and operating procedures to determine the security of its technical, physical, and administrative controls for best practices and compliance – These are MANDATORY assessments

- Have gained specialized training
- HIPAA, PCI, GLBA, FERPA, NERC-SIP,
- Understanding of frameworks, COBIT, NIST, ISO 27001, HI-Trust
- How does an audit list contrast to controls and policies in place
- Data Governance - Policy Dev and Enforcement

Positions

IT Auditor / Internal Audit
Privacy Officer
Compliance Officer
PCI Assessor (QSA)
Forensics & Ethical Hacking

Proactively finding vulnerabilities to strengthen security posture and/or extracts computer information for prosecuting cyber crime and improving data security of an organization.

- Good understanding how data transmit over network
- How data is stored
- How data is processed
- Coding vulnerabilities
- Assessing damage from breach

Positions

Security Analysts / Consultant
Forensics Analysts / Consultant
Penetration Tester / Ethical Hacker
Incident Responder
Expert Witness
Security Management

Management
Oversees the development and supervision of controls required to ensure an organization is effectively managing digital risks
• Team Leads
• Multiple Projects and Multiple People at a time
• Understanding the needs of “client” and appropriating the proper resources

Positions
Team Lead / Supervisor
Project Lead
Project Manager
Security Officer / ISO
Director of Security
CISO
Pre-Sales Engineering & Account Management

A lucrative and challenging career in working with organizations to understand their needs for information security and compliance and ability to map your services and products to their needs

- Technical background
- Good people skills
- Good organizational skills
- Success driven

Positions
Pre-Sales Engineer
Account Manager
Account Executive
Sales Management
What Are Hiring Managers Looking For?

- Education / Certifications
- Technical Experience
- Real Knowledge / Aptitude
- Outside resources and personal initiatives to learn
- Communication Skills
- Written Skills
- Perceived Work Ethic
- Perceived Professionalism
- Perceived Dependability
- Passion
Getting The Gig

• First-Rate Resume(s)
• Online Job Boards
• Networking
• Research & Cold Call
• Follow-up
• Be Creative & Stand Out
• Practice Your Interview
Never Stop Learning!

- GIAC Penetration Tester (GPEN)
- GIAC Assessing and Auditing Wireless Networks (GAWN)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Certified Forensic Analyst (GCFA)
- Offensive Security Certified Professional (OSCP)
- GIAC Penetration Tester (GPEN)
- GIAC Web Application Penetration Tester (GWAPT)
- CREST Registered Penetration Tester (CRT Pen)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Penetration Tester (GPEN)
- ISFCE Certified Computer Examiner (CCE)
- GIAC Web Application Penetration Tester (GWAPT)
- Comptia Security +
- Comptia Network +
- Certified Virtualization Expert 4.1 (CVE 4.1)
- Payment Card Industry (PCI) Qualified Security Assessor (QSA)
- GIAC Security Essentials (GSEC)
- GIAC Certified Incident Handler (GCIH)
- Project Management Professional (PMP)
- (ISC)2 Certified Information Systems Security Professional (CISSP)
- (ISC)2 Health Care Information Security & Privacy Practitioner (HCISPP)
- Payment Card Industry Qualified Security Assessor (QSA)
- ISACA Certified Information Systems Manager (CISM)
- (ISC)2 Systems Security Certified Practitioner (SSCP)
- CWSP Certified Wireless Security Professional
- EC-Council Certified Ethical Hacker
- EC-Council Certified Security Analyst
Golden Rules

1. Work harder than everyone!
2. Show up early, stay late when needed
3. Enjoy a challenge & be flexible
4. Look for ways to improve (learn from failure)
5. Be teachable
6. Have a spirit of excellence
7. Have a optimistic & positive attitude
8. Align yourself with the Alphas (find good mentors)
9. Be grateful, not a complainer
10. Be a good negotiator
11. Continue Your Education (NEVER STOP LEARNING!)
Thank you for your time!