Getting Started in Cybersecurity: How to Hone Your Hacking Skills

Dr. Davina Pruitt-Mentle

CyberWatch K12

Ed Tech Policy, Research and Outreach
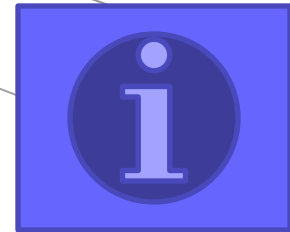
What do you know about Cybersecurity?

The Net --- Eagle Eye

THE NET
Suspense

THEY CONTROL YOU

What is Cybersecurity?

What is Information Assurance?

What Jobs/Careers are there in Cybersecurity?

CyberSecurity: Which Job is for Me?

CyberWatch W12

Computer Programmer/ Engineer/ Software Developer/ Web Designer
Description: Analyzes user needs to design, build, test, and maintain software applications and systems.

Penetration Tester/Systems/Networks / Vulnerability Researcher/ Exploit Developer
Description: Think like a hacker to identify flaws and vulnerabilities which jeopardize the safety and security of the data and communications of businesses and organizations.

Information Security Engineer / Architect / Analyst/ Compliance Manager
Description: Assists Information Security professionals in designing plans, evaluating organizational weaknesses, and implementing procedures to protect the information assets of an institution or company.

Malware Analyst/ Expert
Description: Examines malicious code to understand the type of damage it can do and how it replicates and spreads. Determines methods for detecting and deleting malware from systems. These professionals also investigate the source of the malware.

Network Security/ Engineer
Description: Protects the data and information of an organization's information and communication technology from damage or unauthorized access.

Cryptographer
Description: Uses math, logic, and computer science to turn readable text into an unreadable form. Cryptographers also analyze encrypted (unreadable text) to turn it into a readable form.

Computer Forensics / InfoSec Crime Investigator/ Forensics Expert/Analyst / Computer Crime Investigator
Description: Investigates digital media for data stored or encrypted. Test information security systems. Analyzes security breaches. These professionals often work in the law enforcement or military and defense fields.
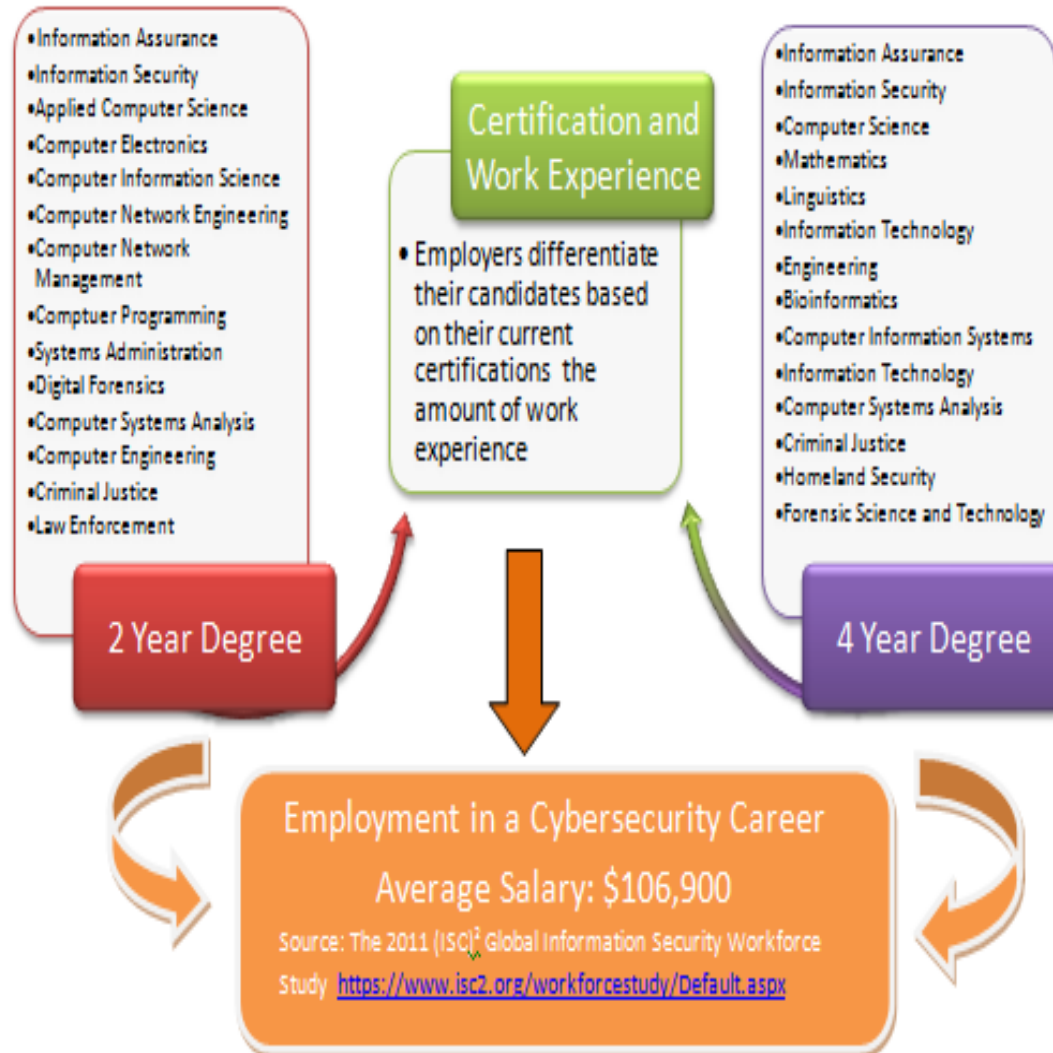
Incident Responder/Disaster Recovery / Business Continuity Analyst/ Manager
Description: Recognizes, analyzes, and responds to incidents which have caused damage to information, data, and information and communication technologies. This includes recovering from all types of threats-- natural (tornados, hurricanes), human (hackers) and technical (malware, equipment failure)

Programming
Hardware
Networks
Languages
Intellegence
Engineering
Math
Emergency Management
Ethical Hacking
Law Enforcement

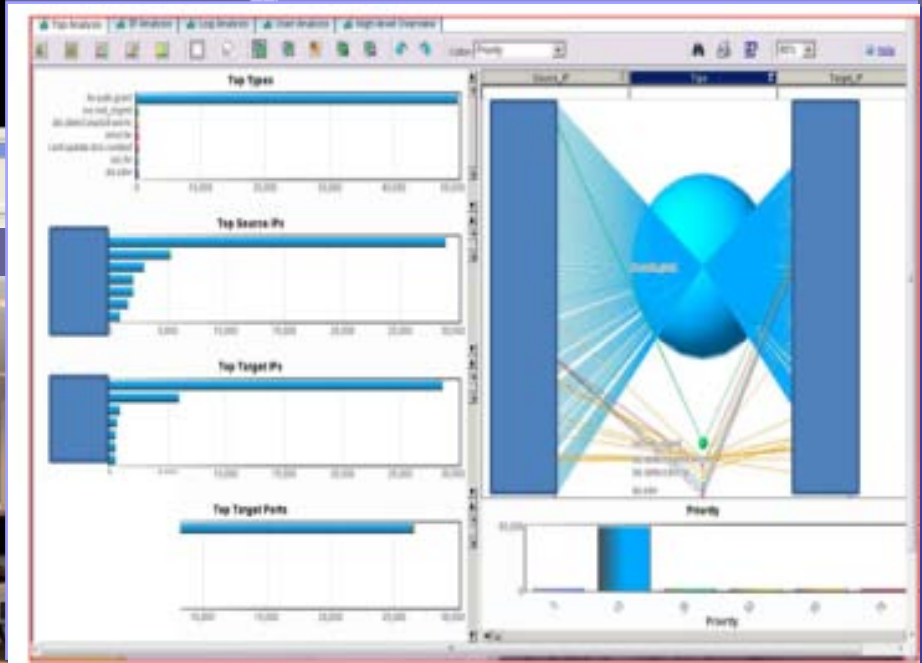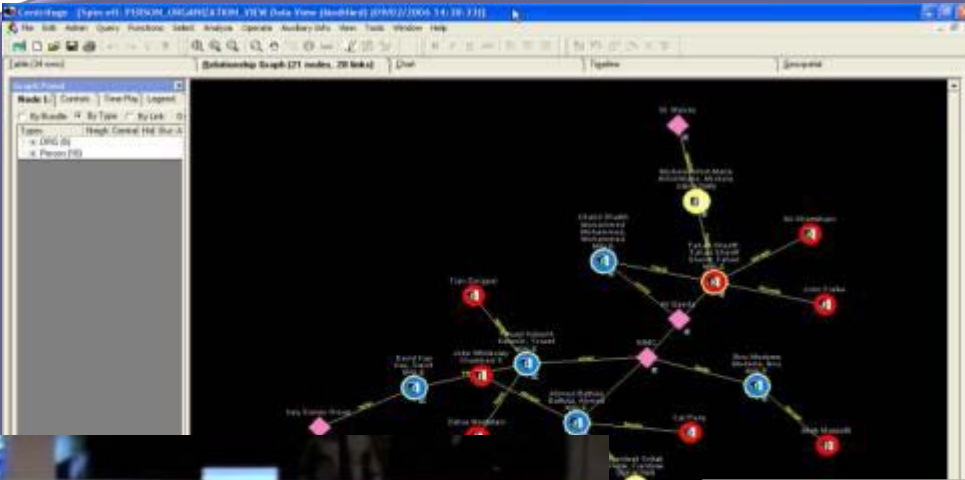CyberSecurity
What are you interests?

Pathways to Cybersecurity Careers

Employers want graduates who understand that technical as well as human interventions provide for effective defenses. In addition to technical competence, IA professionals need to exhibit creative problem solving, organizational awareness, patience, self-management and teamwork skills.

2 Year Degree

- Information Assurance
- Information Security
- Applied Computer Science
- Computer Electronics
- Computer Information Science
- Computer Network Engineering
- Computer Network Management
- Comptuer Programming
- Systems Administration
- Digital Forensics
- Computer Systems Analysis
- Computer Engineering
- Criminal Justice
- Law Enforcement

Certification and Work Experience

- Employers differentiate their candidates based on their current certifications the amount of work experience

4 Year Degree

- Information Assurance
- Information Security
- Computer Science
- Mathematics
- Linguistics
- Information Technology
- Engineering
- Bioinformatics
- Computer Information Systems
- Information Technology
- Computer Systems Analysis
- Criminal Justice
- Homeland Security
- Forensic Science and Technology

Employment in a Cybersecurity Career

Average Salary: $106,900

Source: The 2011 (ISC)² Global Information Security Workforce Study https://www.isc2.org/workforcestudy/Default.aspx

Cybersecurity a Growing Field?

Cybersecurity:
A National Growth Career
Occupations Projected to Grow Fastest, 2006-2016

Network Systems and Data Communications Analysts

Personal and Home Care Aides

Home Health Aides

Computer Software Engineers, Applications

Veterinary Technologists and Technicians

Personal Finance Advisors

Makeup Artists, Theatrical and Performance

Medical A

Veterinarians

Substance Abuse and Behavioral Disorder Counselors

Skin Care Specialists

Financial Analysts

Social and Human Service Assistants

Gaming Surveillance Officers and Gaming Investigators

Physical Therapist Assistants

Pharmacy Technicians

Forensic Science Technicians

Dental Hygienists

Mental Health Counselors

Mental Health and Substance Abuse Social Workers

US Dept of Labor

Table 3. The 10 industries with the largest wage and salary employment growth, 2008-18 (1)
(In thousands)

Industry	Sector	Employment 2008	Employment 2018	Change Number	Change Percent
Management, scientific, and technical consulting services	Professional and business services	1,009	1,844	835	82.8
Offices of physicians	Health care and social assistance	2,266	3,038	772	34.1
Computer systems design and related services	Professional and business services	1,450	2,107	656	45.3
Other general merchandise stores	Retail trade	1,490	2,097	607	40.7
Employment services	Professional and business services	3,144	3,744	600	19.1
Local government, excluding education and hospitals	Government	5,819	6,306	487	8.4
Home health care services	Health care and social assistance	958	1,399	441	46.1
Services for the elderly and persons with disabilities	Health care and social assistance	585	1,016	431	73.8
Nursing care facilities	Health care and social assistance	1,614	2,007	394	24.4
Full-service restaurants	Accommodation and food services	4,598	4,942	343	7.5

1 Data are from the National Employment Matrix.

Table 1.6 Occupational Employment and Job Openings Data, 2008—18, and worker characteristics, 2008
(Numbers in thousands)

2008 National Employment Matrix title and code		Employment		Change, 2008-18		Job openings due to growth and replacement needs (in thousands)	Median annual wages	Median annual wage quartile	Most significant source of education and training category
		2008	2018	Number	Percent				
Financial examiners	13-2061	27.0	38.1	11.1	41.16	16.0	$70,930	VH	Bachelor's degree
Computer software engineers	15-1030	909.6	1,204.8	295.2	32.46	371.7	-	-	-
Computer software engineers, applications	15-1031	514.8	689.9	175.1	34.01	218.4	$85,430	VH	Bachelor's degree
Computer software engineers, systems software	15-1032	394.8	515.0	120.2	30.44	153.4	$92,430	VH	Bachelor's degree
Network systems and data communications analysts	15-1081	292.0	447.8	155.8	53.36	208.3	$71,100	VH	Bachelor's degree
Biomedical engineers	17-2031	16.0	27.6	11.6	72.02	14.9	$77,400	VH	Bachelor's degree
Environmental science and protection technicians, including health	19-4091	35.0	45.2	10.1	28.91	25.2	$40,230	H	Associate degree
Self-enrichment education teachers	25-3021	253.6	334.9	81.3	32.05	120.3	$35,720	H	related occupation
Physician assistants	29-1071	74.8	103.9	29.2	38.99	42.8	$81,230	VH	Master's degree
Surgical technologists	29-2055	91.5	114.7	23.2	25.32	46.3	$38,740	H	award
Veterinary technologists and technicians	29-2056	79.6	108.1	28.5	35.77	48.5	$28,900	L	Associate degree
Home health aides	31-1011	921.7	1,382.6	460.9	50.01	552.7	$20,460	VL	training
Dental assistants	31-9091	295.3	400.9	105.6	35.75	161.0	$32,380	L	training
Personal and home care aides	39-9021	817.2	1,193.0	375.8	45.99	477.8	$19,180	VL	training

Source: Employment Projections Program, U.S. Department of Labor, U.S. Bureau of Labor Statistics

Computers & Information Technology Cybersecurity Specialist
Source: http://www.geteducated.com/career-center/

Outlook & Growth

- **34 percent—faster** than normal
- **An increase** in computer security jobs is expected as technology continues to advance and become more affordable.
- More businesses will **add computers** and will need specialists to make their networks secure.
- In addition, **use of the Internet** by businesses should increase the demand for computer security specialists.
- Some specialists will work inside consulting firms dedicated exclusively to computer security issues.

Salary & Wages

- Those in executive roles—with titles such as chief information security officer, chief security officer or security **manager—earned $106,326 on average**.
- Those in more technical roles (security engineer, security penetration tester or web security manager) **earned an average of $75,275.**

Computers & Information Technology Cybersecurity Specialist
Source: http://www.geteducated.com/career-center/

What is a Cybersecurity Specialist?

- Work with companies to build secure computer systems.
- Question managers and staff about their current security methods.
- Find out what information the company wants to protect.
- Determine what information employees should be able to access.
- Plan the security system.
- Train staff on how to use security software and properly use computers to prevent any problems.
- Write rules and procedures for employees to follow.
- Evaluate security breaks and determine if there are problems or errors.
- Track where the break came from and shut off the access point.

Education & Degree Path

- AS or AAS or BS degree in
  - computer science,
  - engineering,
  - information systems
  - information assurance
- Another route is to major in your area of interest and minor in one of these degrees.
- Many programs offered online

Cybersecurity:
A National Growth Career
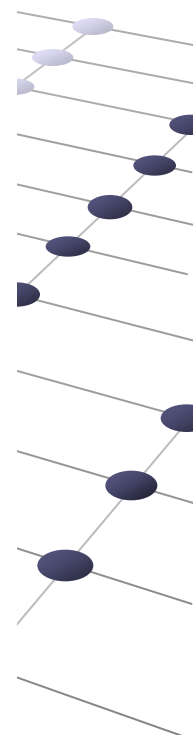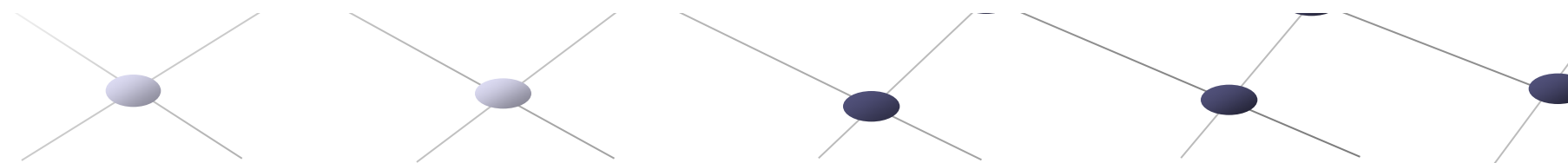
Maryland wants to be cybersecurity epicenter
By Ben Bain; Jan 12, 2010
http://fcw.com/articles/2010/01/12/web-cybersecurity-center-maryland.aspx

Gov. O'Malley's report, titled *CyberMaryland*
- Maryland is positioned to be the hub for federal, academic and private-sector cybersecurity efforts
- Maryland is already home to the National Institute of Standards and Technology, the National Security Agency, the Intelligence Advanced Research Projects Activity — the soon-to-be home of the Defense Information Systems

✓ Maryland's IT employment rate rose by 3.3 percent between 2001 and 2008, while nationwide it fell by 17.1 percent during that same time period

Very interesting…. but how does this apply to me?

Ft Meade, Maryland

US Cyber Command
USCYBERCOM: is a sub-unified command, subordinate to U.S. Strategic Command
•protecting DoD networks
from cyber attacks and will manage cyber warfare activity.

The Defense Information Systems Agency (DISA)
The Colocation of Defense/Military Adjudication Activities
Defense Media Activity (DMA)
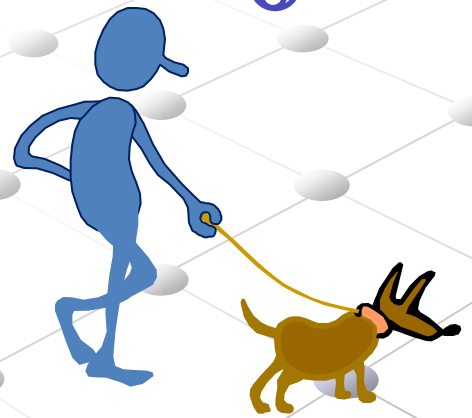
How to Get There?

CyberWatch

www.Cyberwatchcenter.org

Centers of Academic Excellence

CAE   CAE2Y   CAER

Certificates

- PMI PMP
- PMI CAPM
- ITIL v2 Foundations
- CISSP
- Cisco CCIE Routing & Switching
- Cisco CCVP

- ITIL v3 Master
- MCSD
- CCNP
- Red Hat Certified Engineer

UPCOMING PROGRAMS IN CYBERSECURITY

CW K12 CyberWatch

Expanding Knowledge in Cyberawareness and Careers in Cybersecurity

MD SUMMER CYBERWARRIOR CAMPS

- Cryptography
- Building Games/Simulations
- Digital Forensics
- Computer Security
- Cyberethics, safety and security
- Field Trips and Guest Speakers

ASK ABOUT DATES AND LOCATIONS

USCC US CYBER CHALLENGE

2 MARYLAND LOCATIONS
JULY 11-15, 2011 CCBC or
JULY 18-22, 2011 UMCP
5 days of training
- Intrusion Detection in Depth
- Hacker Techniques
- Web Application Pen Testing & Hacking
- Programming
- Computer Forensics

SAVE THE DATES
- HS Networking Security Competition
- MD US Cyber Camps
- MD Cyberwarrior Camps
- Sept 22, 2011 Careers in Cybersecurity GC Workshop
- Oct 6-7, 2011 10th Annual Cyberethics, safety and security Conference
- Oct 18, 2011 Cool Careers in Cybersecurity for Girls Summit

HS Networking Security Competition
Cool Careers in CyberSecurity 4 Girls Summit   US Cyber Challenge Camps
After School Cyberwarrior Programs   Careers in Cybersecurity for Guidance Counselors
SECURE IT Program   Annual Cyberethics Safety Security Conference

VISIT: http://www.edtechpolicy.org/cyberk12/

Contact person: Davina Pruitt-Mentle, Ph.D.

410 531 3910

dpruitt@umd.edu

CW K12 CyberWatch

Questions
Thank You

Careers in IS/IA & Digital Forensics

- Handout for Labor Stats and Career Paths
- http://www.careeronestop.org/

Computer Programmer/ Engineer/ Software Developer/ Web Designer

- Analyzes user needs to
  - design,
  - build,
  - test, and
  - maintain software applications and systems
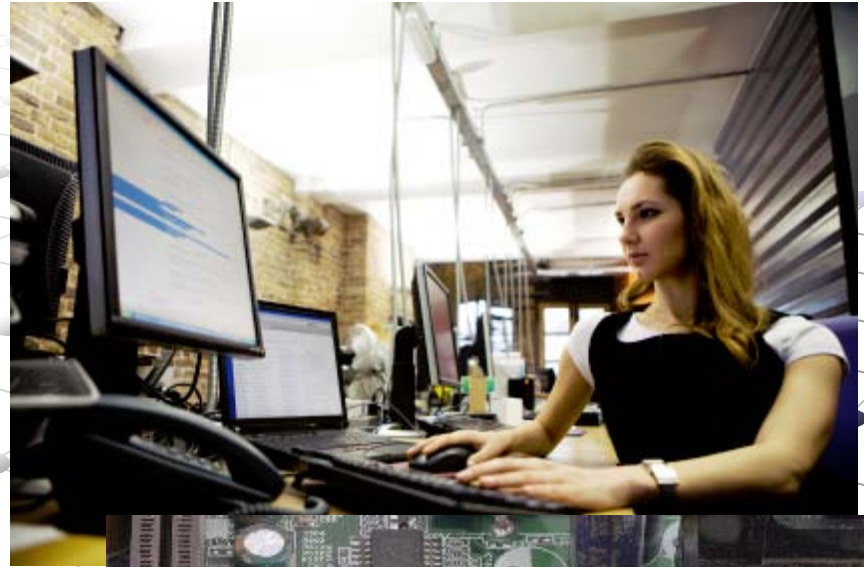
Penetration Tester/Systems/Networks / Vulnerability Researcher/ Exploit Developer

- **Think like a hacker to**
  - identify flaws and
  - vulnerabilities which jeopardize the safety and security of the data and communications of businesses and organizations
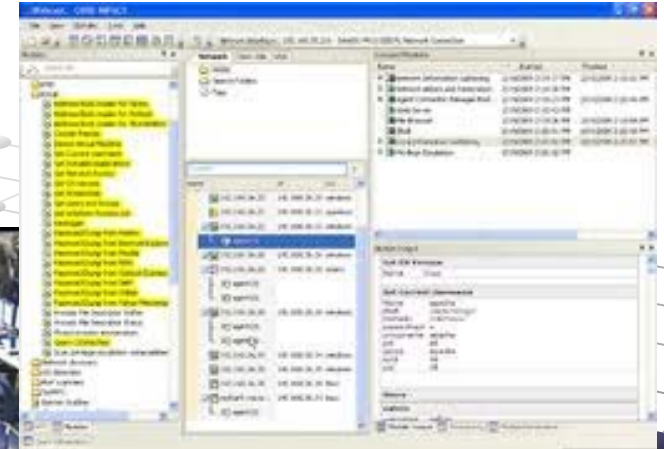
Information Security Engineer / Architect / Analyst/ Compliance Manager

- Assists Information Security professionals in

    - designing plans,

    - evaluating organizational weaknesses, and

    - implementing procedures to protect the information assets of an institution or company

Malware Analyst/ Expert

- Examines malicious code to understand the type of damage it can do and how it replicates and spreads.

- Determines methods for detecting and deleting malware from systems.

- These professionals also investigate the source of the malware.
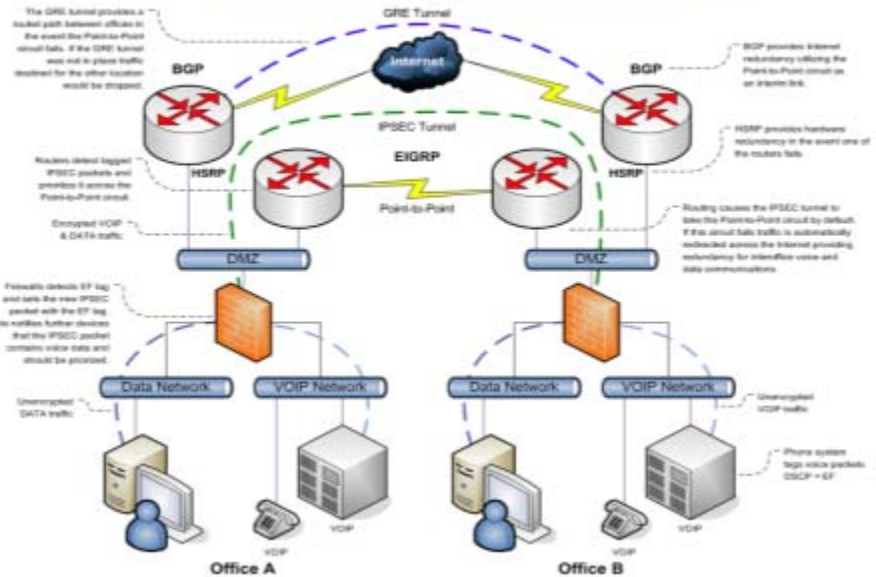
Network Security/ Engineer

- Protects the data and information of an organization's information and communication technology from damage or unauthorized access
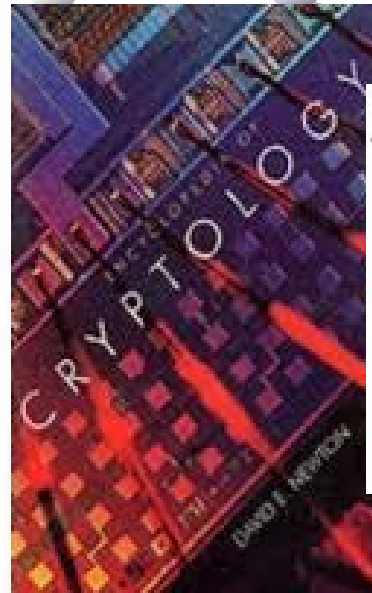
Cryptographer

- Uses math, logic, and / or computer science to turn readable text into an unreadable form.

- Cryptographers also analyze encrypted (unreadable text) to turn it into a readable form.
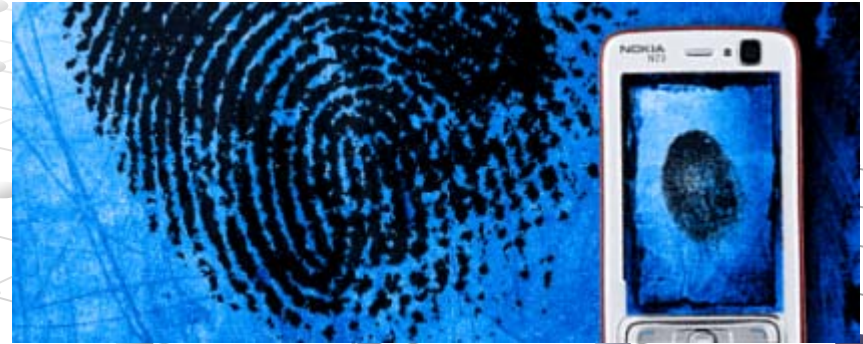
CODE TABLE

Computer Forensics / InfoSec Crime Investigator/ Forensics Expert/Analyst / Computer Crime Investigator

- Investigates digital media for data stored or encrypted.
- Tests information security systems.
- Analyzes security breaches.
- These professionals often work in the law enforcement or military and defense fields.

Incident Responder/Disaster Recovery / Business Continuity Analyst/ Manager

- **Recognizes, analyzes, and responds to incidents which have caused damage to information, data, and information and communication technologies.**

- **This includes recovering from all types of threats-- natural (tornados, hurricanes), human (hackers) and technical (malware, equipment failure)**

NOAA's Command Center

Defining CyberSecurity?

- CyberSecurity focuses on the technical aspects of computer defense
  - the safety of computers and computer systems in a networked environment, while Information Assurance focuses on confidentiality, integrity, availability and validation of data, and therefore CyberSecurity is a subset of Information Assurance.

- Information Assurance (DOD)
  - is a subset of CyberSecurity , and CyberSecurity includes management of the risks associated with computers and networks and mission assurance.

The Center for Strategic and International Studies (CSIS) Commission on CyberSecurity

- for the 44th Presidency suggests the term *"cyber security services"*

  - the development, implementation, operation and administration of measures and/or activities intended to prevent, detect, recover from and/or respond to intentional or inadvertent compromises of the confidentiality, integrity and availability of information technology including but not limited to intrusion detection, computer forensics, configuration management, and system development.

CyberSecurity involves protecting that information by…

- **Preventing**
- **Detecting**
- **and Responding to attacks**

- In the fields of:
  - management science
  - systems engineering
  - criminology
  - security engineering
  - computer science
  - robotics

In the fields of:
- data and communications
- accounting
- forensic science
- law enforcement
- bioengineering
- intelligence

Everything relies on computers and the internet now

- communication (email, cellphones)
- entertainment (digital cable, mp3s)
- transportation (car engine systems, airplane navigation)
- shopping (online stores, credit cards)
- medicine (equipment, medical records
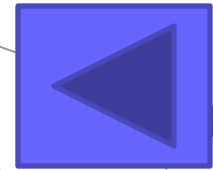- and the list goes on.

How much of your daily life relies on computers?
How much of your personal information is stored either on your own computer or on someone else's system?

The Defense Information Systems Agency (DISA)

- **DISA**, is responsible for DoD computer and automated information systems and networks.

Defense Media Activity (DMA)

- **DMA,** is the Department of Defense's direct line of communication for news and information to U.S. forces worldwide.

- The agency presents news, information and entertainment on a variety of media platforms.

The Colocation of Defense/Military Adjudication Activities

- DoD's place for workers from three military services and other defense activities to 'adjudicate' or determine who should receive security clearances after proper background investigations.

- More than 750 people from 10 different agencies will work in the new 150,000 square feet facility.

What is IA?

- **CyberWATCH Video**
  - **http://www.cyberwatchcenter.org/CyberWATCH/**
- **Fox Video—Cyber challenge**
- **Sneakers**
  - **http://www.imdb.com/video/screenplay/vi2448753433/**
- **The Net**
  - **http://www.imdb.com/video/screenplay/vi2046230809/**
- **Staying Safe Online: The Need for Cybersecurity**
- **NATO Brief**
- **Obama Need for Cybersecurity**

- **National Collegiate Cyber Defense Competition**
- **The Duhs of Security**
- **Hacker**
  - **http://www.youtube.com/watch?v=2efhrCxl4J0**
- **NSA Commercial**
  - **http://www.nsa.gov/careers/Media_Center/index.shtml**

What is IA (cont)?

- Theory and Practice of Cryptography
  - http://www.youtube.com/watch?v=IzVCrSrZIX8
- There May be a Shortage of Cybersecurity Professionals
  - http://www.youtube.com/watch?v=MUPIMT2Mjyk
- Lockheed Martin_ HOW Cyber Security
  - http://www.youtube.com/watch?v=fhjFsWGcUm4&feature=related
- Whoa, That's Awkward_ (EDUCAUSE WINNER)
  - http://www.youtube.com/watch?v=gtSIDpoX0r0&feature=related
- Northrop Grumman Battlespace Command
  - http://www.youtube.com/watch?v=WsWW6HskcWg&feature=related
- NSA spy techniques (good background--bias messaging)
  - http://www.youtube.com/watch?v=48dRrNCjLus&feature=related
- Lockheed Martin Security Intelligence Center
  - http://www.youtube.com/watch?v=uSSBjpIjvOA&feature=related
- United States Air Force-Cyberspace Domain
  - http://www.youtube.com/watch?v=xeWnZRZrpaY&feature=related

Other Videos

Robotics

- Lockheed Martin HULC Exoskeleton
  - http://www.youtube.com/watch?v=kat8I5UM_Vs&feature=related

Remove Cyber Security Removal Video

How to remove bad videos/bots
  - http://www.youtube.com/watch?v=pM8bU0MHVEI&feature=related

Humorous October is cybersecurity awareness month--good example of what to do

- Cyber Security Awareness - Missouri S&T
  http://www.youtube.com/watch?v=XSMuaaWjnJ8&feature=related

- CyberChallenge
  - http://www.uscyberchallenge.org/

Careers in IS/IA & Digital Forensics

- Handout for Labor Stats and Career Paths
- http://www.careeronestop.org/

IT Security EBK:
A Competency and Functional Framework for IT Security Workforce Development

Functional Perspectives
- M – Manage
- D – Design
- I – Implement
- E – Evaluate

IT Security Roles

IT Security Competency Areas	Executive			Functional				Corollary		
	Chief Information Officer	Information Security Officer / Chief Security Officer	IT Security Compliance Officer	Digital Forensics Professional	IT Security Engineer	IT Security Operations and Maintenance Professional	IT Security Professional	Physical Security Professional	Privacy Professional	Procurement Professional
1 Data Security	M	M D / E	E		D / E	I / E	M D / E		D / E	
2 Digital Forensics		M D / E		M D / I E		I				
3 Enterprise Continuity	M	M / E	E			D / I	E	D / I		
4 Incident Management	M	M D / E	E	I		D / I E	D / E	I	M D / I E	
5 IT Security Training and Awareness	M	M / E	E			I	D / E		D / E	
6 IT Systems Operations and Maintenance			E	D / I	D / E	M D / I E	I			
7 Network Security and Telecommunications			E	I	D / I	D / I	M D / E			
8 Personnel Security			E				D / E	E	D / I	
9 Physical and Environmental Security	M	M / E	E				D / E	M D / I E		
10 Procurement	M D	M D / E	E		E	E		E		M D / I E
11 Regulatory and Standards Compliance	M / E	M D / E	D / I E				I		M D / I E	
12 Risk Management	M / E	M D / E	I / E	I	I	I	D / I E	I	M D / I E	
13 Strategic Management	M D / E	M D / I E	D / E							
14 System and Application Security	M	M / E	E		D / I E	I				

Mapping Professional Specialist Groups to Career Levels

Professional Specialist Group Model						
		Management	**Technology**	**Architecture**	**Assurance**	**Risk Management**
Senior Executive	CISO	CTO	CIO	COO	CAO	CRO
Manager/Director	ISM,ISD, Mgr Dir, Ops Mgr/Dir, Consulting Mgr/DIR	Development Manager Systems and Infrastructure			Head of Internal Audit	Information Risk Mgr/Dir Consulting Mgr/Dir
Expert	Principal Consultant	Senior Dev Engineer	Senior Architect	Senior Architect	Senior Security Auditor	Principal Consultant
Sepecialist Managerial	Product/Program manager, Team Leaders, Account Sales managers					
Specialist Technical	Security Consultant Business Analyst	Security Product Manager	Security Designer	Security Designer	Security Auditor	Information Risk Consultant
Entrant	Analyst	Deverloper	Security Designer Trainee	Security Designer Trainee	Security Auditor Trainee	Information Risk Trainee

Career Levels and Traditional Paths
Senior Executive
CIO; CISO; CTO; CRO; COO

EXPERT

Principal Consultant;
Senior/Chief Architect;
Senior Security Auditor; Etc.

Specialist (Technical/Business)
Security Consultant; Security
Designer/Architect; Security Auditor;
Information Risk Consultant; Security
Product Manager; Business Analyst

MANAGER/DIRECTOR

Consulting Manager/Director; Information
Security Manager/Director; Head of
Security Audit; Information Risk
Manager/Director; Operations
Manager/Director

Specialist (Management) Project Manager;
Program Manager; Team Leader;
Account Manager; Sales Manager;
Marketing Manager

ENTRANT

Security Analyst; Security Developer; Security Administrator; Trainee
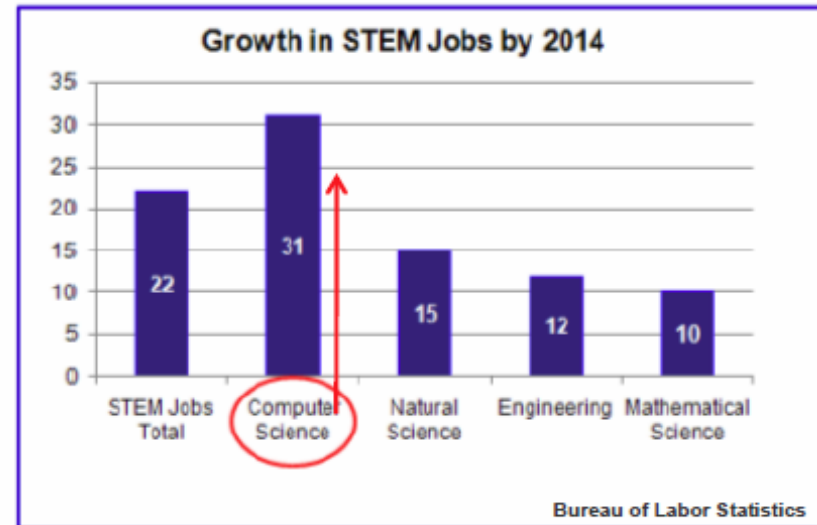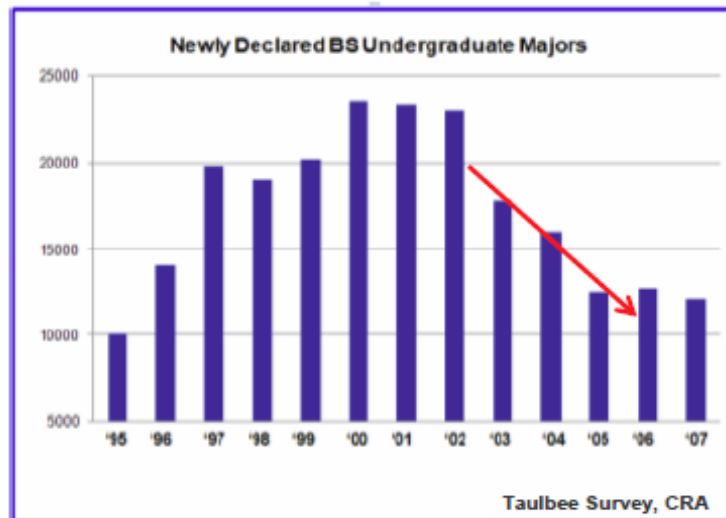Information Risk Consultant; Security Product Sales; Etc.

Years of experience & ability

Our Education Problem

Problem: The U.S. is not producing enough computer scientists and CS degrees

- CS/CE enrollments are down 50% from 5 years ago[1]
- CS jobs are growing faster than the national average[2]

Newly Declared BS Undergraduate Majors

Taulbee Survey, CRA

Growth in STEM Jobs by 2014

Bureau of Labor Statistics

- **National Collegiate Cyber Defense Competition (NCCDC)**
  - Provides a controlled, competitive environment to assess a student's depth of understanding and operational competency.
- **U.S. Cyber Challenge (High School)**
  - DC3 Digital Forensics Challenge, CyberPatriot Defense Competition, Netwars Capture-the-Flag Competition

Homeland Security