DEVELOPING YOUR CYBER CAREER ACTION PLAN

PRESENTED BY TERESA ALLISON, PMP, CISSP, CISA, SECURITY+

PRESENTER

- **Teresa Allison** is an Independent Consultant with over 18 years of experience in the field of information technology consulting. She has served as a trusted advisor to CIOs and their staffs by providing them with solutions for addressing their management needs for multi-billion dollar federal information technology programs.

- She has supported Health & Human Services, Homeland Security, Transportation, Financial Regulatory, Veterans Affairs, Diplomacy & Foreign Affairs, and International Development & Foreign Assistance agencies.

- Teresa is certified IT professional who currently holds the PMP, CGEIT, CSM, ITIL, Security+, CISA, CISSP, and Lean Six Sigma certifications.

- She graduated from Carnegie Mellon University's H. John Heinz III College with a Master of Science in Public Policy and Management and minor in Management of Information Systems. She received her bachelor's degree in Political Science from Xavier University.

MY CYBER CAREER JOURNEY

Driving Factors

- To protect information
- Wanted more interesting work
- Change of scenery in the IT landscape
- Greater opportunities for advancement

Opportunities

- Free cybersecurity training
- Support from Training Instructors
- Carnegie Mellon University Alumni Mentors

Challenges

- Past Work History / Experience
- Salary

EXPLORE YOUR INTEREST IN CYBER

- Ask yourself why am I interested in a career in cybersecurity?
    - To protect information
    - More interesting work
    - Better Pay
    - Upward mobility

EXPLORE YOUR INTEREST IN CYBER

- Determine If you have the passion for a career in cybersecurity?
  - Listen to cybersecurity web casts
    - Bright Talk
      - ISC2
      - ISSA
      - Women's Society of Cyberjutsu
  - Take free online cybersecurity trainings
    - Cybrary
    - Professor Messer
  - Attend free/low cost events and workshops
    - Event Brite & Gov Events
    - Meet Up Groups
    - Cover6 Solutions
- Ask yourself if the cybersecurity topics/trainings are appealing and interesting to you?

EXPLORE YOUR INTEREST IN CYBER

- Network within the cybersecurity community to learn more about the field of cybersecurity
  - Join, attend, and volunteer with professional association events
    - ISC2
    - ISSA
    - ISACA
    - Women's Society of Cyberjutsu
    - International Consortium of Minority Cybersecurity Professionals (ICMCP)
  - Join & attend cybersecurity meet up groups
    - DC Cybersecurity Meet Up Group
    - NOVA Cyber IT Meet Up Group
    - Risk Management Framework LifeBoat Meet Up Group
    - CGI Meet Up Group
    - Breaking Into Cyber Meet Up Group
    - Splunk Meet Up Group

EXPLORE YOUR INTEREST IN CYBER

Cybersecurity Domains Mind Map

- **Security Architecture**
- **Career Development**
- **Framework & Standards**
- **Risk Assessment**
- **Security Operations**
- **Threat Intelligence**
- **Governance**

Henry Jiang – Cybersecurity Domains
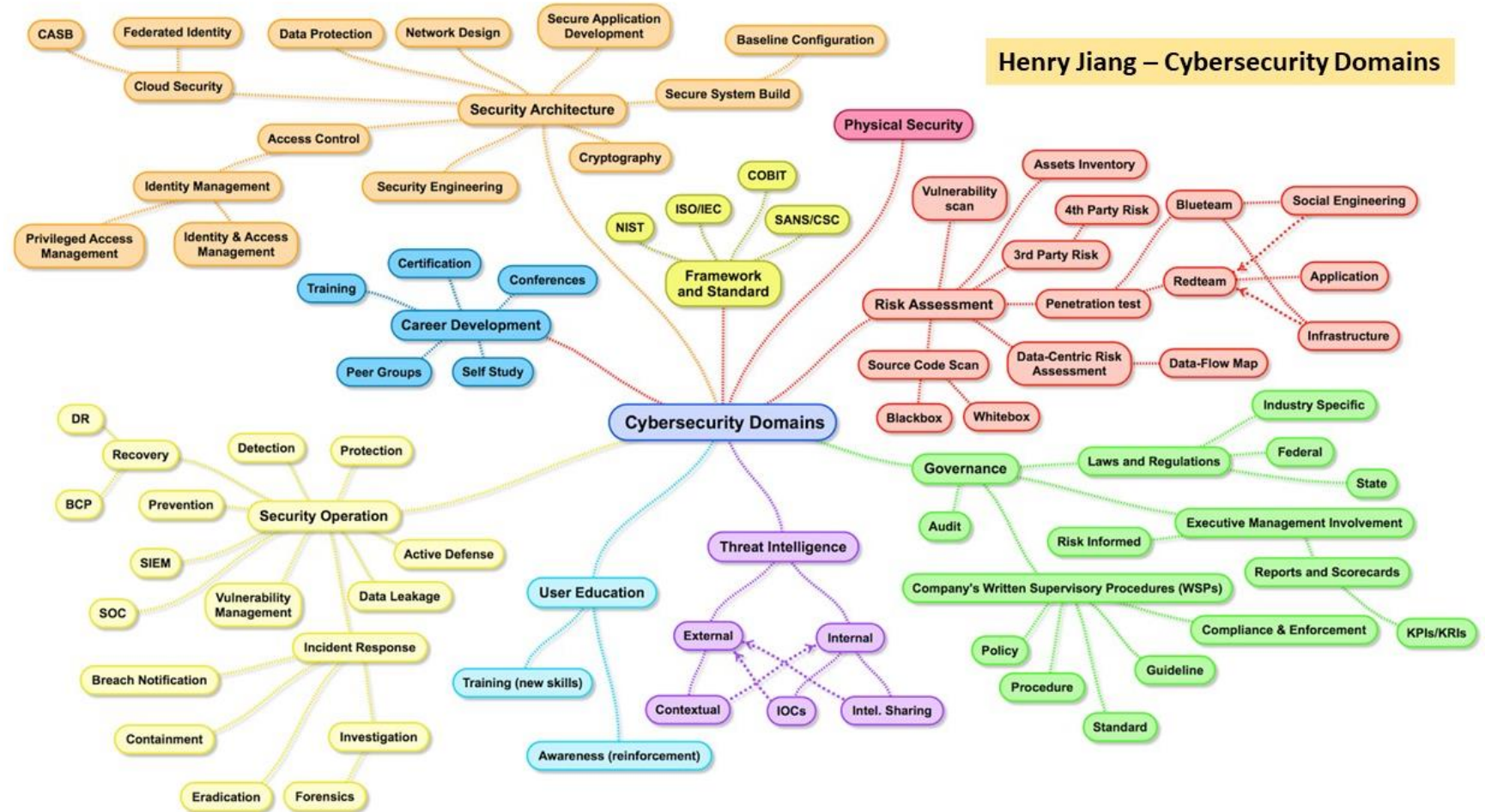
RESEARCH CYBER POSITIONS

- Research cyber jobs on the internet and review the requirements
  - Cyber Seek
    - www.cyberseek.org
  - NICE Cybersecurity Workforce Framework (NIST)
    - https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity
  - Job Search Websites
    - www.indeed.com
    - www.careerbuilder.com
    - www.dice.com
  - O*Net Online (US Bureau of Labor)
    - https://www.onetonline.org/
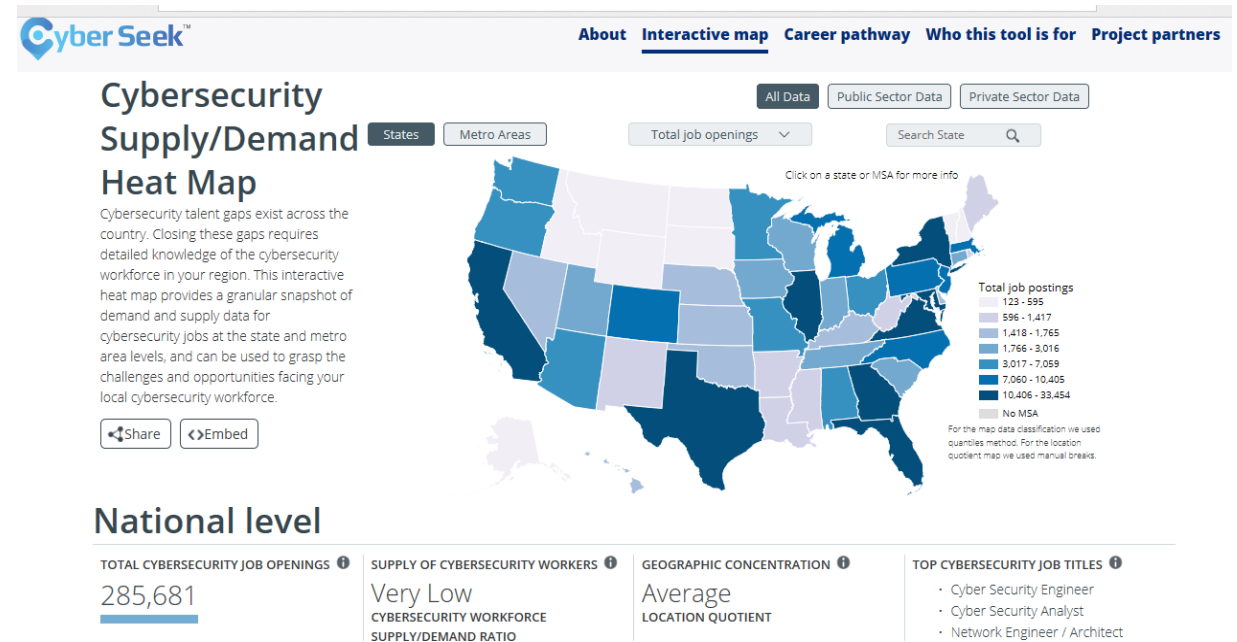
RESEARCH CYBER POSITIONS

- Identify six (6) Cybersecurity positions that you are interested in.

- Narrow it down to the three (3) positions that are the best fit for your interests and background.

RESEARCH CYBER POSITIONS

- Assess current work experience, training and education.

  - What are the gaps in your background that need to be addressed before you can meet the requirements for your ideal position?

    - Work Experience

    - Education

    - Training

    - Certifications

RESEARCH CYBER POSITIONS

Informational Interviews

Conduct informational interviews with people who currently work in the type of cybersecurity position that you are interested in.

- Ask them what the day to day work is like.
- Share your resume with them and ask for some feedback about it.
- Find out what next steps you need to take to make your cyber career a reality.
- Always send a thank you note!

RESEARCH CYBER POSITIONS

Mentoring

Find a mentor who can provide you with advice about pursuing a career in cybersecurity

- Look for someone who works in the field who can cheer you on.

- Meet with them on a regular basis to discuss progress towards career goals and obstacles.

- Always offer to support your mentor in their projects or provide assistance when you can.

- Thank them for taking the time to help you with your career.

RESEARCH CYBER POSITIONS

Career Coaching

If you have the means to afford it you can hire a cyber career coach that can help you figure out a plan for finding a job in cyber.

- Research the career coach's background and the services that she or he offers

- Gain an understanding of the fee structure; expect an hourly rate for a series of sessions

- Know what you want to achieve from career coaching sessions

LEARN CYBERSECURITY POLICIES & STANDARDS

Federal IT Security Policies

- FISMA - Federal Information Security Modernization Act of 2014

- FedRAMP - Federal Risk and Authorization Management Program

- OMB Circular A-11, Preparation, Submission and Execution of the Budget

- OMB Circular A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs

- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

- OMB Circular A-130, Managing Federal Information as a Strategic Resource

LEARN CYBERSECURITY POLICIES & STANDARDS

General IT Security Policies

- NIST SP 800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems

- NIST SP 800-30 – Risk Management Guide for Information Systems

- NIST SP 800-34 – Contingency Planning Guide for Information Systems

- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

- NIST PRISMA - Program Review for Information Security Management Assistance

- PCI DSS - Payment Card Industry Data Standard

- OWASP - Open Web Application Security Project

- ISO/IEC 27000 - Information Security Techniques

- ISO/IEC 15408 - Evaluation Criteria for IT Security

LEARN CYBERSECURITY POLICIES & STANDARDS

SANS CIS 20 Controls

https://www.cisecurity.org/controls/

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized & Unauthorized Software
3. Secure Configurations for Hardware & Software
4. Continuous Vulnerability Assessment & Remediation
5. Controlled Use of Administrative Privileges

6. Maintenance, Monitoring & Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation & Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection

LEARN CYBERSECURITY POLICIES & STANDARDS

SANS CIS 20 Controls

14. Controlled Access Based on the Need to Know

15. Wireless Access Control

16. Account Monitoring & Control

17. Security Skills Assessment & Appropriate Training to Fill Gaps

18. Application Software Security

19. Incident Response & Management

20. Penetration Tests & Red Team Exercises

https://www.cisecurity.org/controls/

LEARN CYBER TOOLS

IT Security Tools

- **Data & Traffic Analysis Tools -** OpenVAS, Elastic, LogStash, Retina CS, Kivana, Microsoft Baseline Analyzer, Alien Vault Ossim, Nmap, Splunk, Wireshark, Nessus, Metaploit, Snort, Intrusion Detection Systems, Intrusion Protection Systems

- **Security Operations Center (SOC) Tools –** ArcSight, Tenable, Nessus, RSA Archer, Big Fix, Cisco, Palo Alto, Splunk, McAfee, Symantec, Varonis, Exabeam, Tanium

- **Programming Languages –** Perl, Python

- **Operating Systems –** Linux and Unix
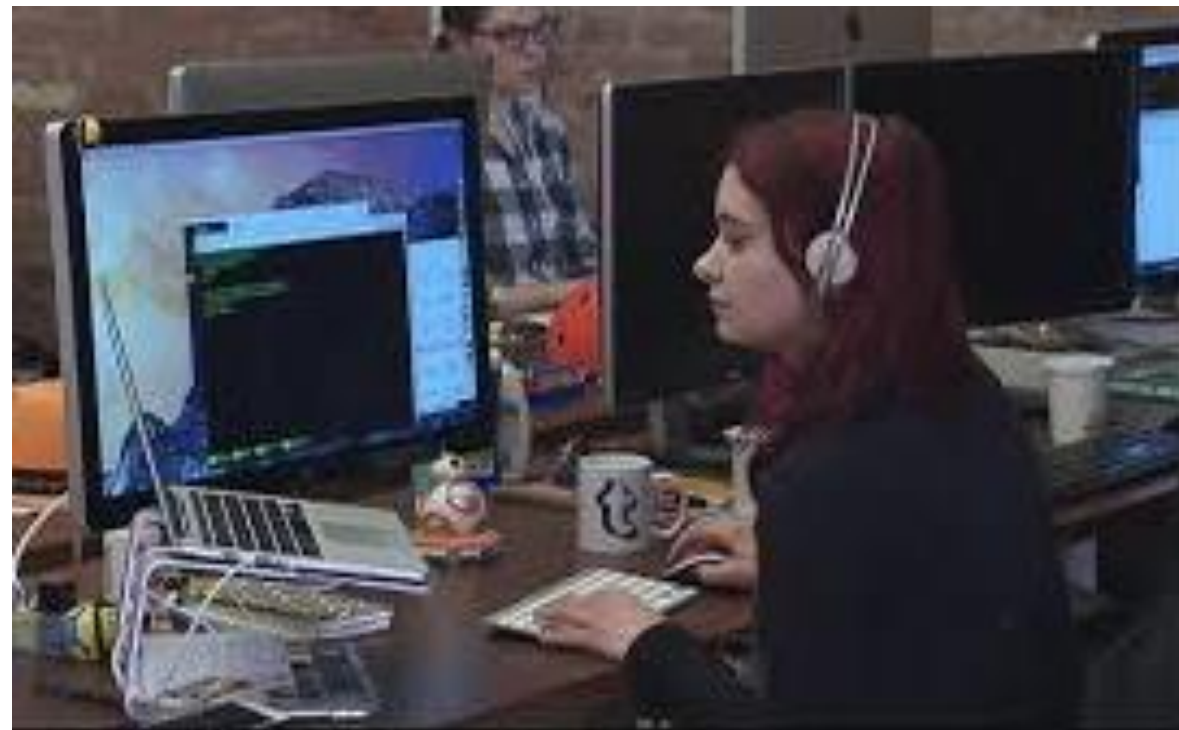
LEARN CYBER TOOLS

Build Your Own Home Cyber Lab

Create a safe place for you to play with cybersecurity technologies and build your skills. You can set up an environment with physical or virtual machines. IT allows you to work with:

- Firewalls

- Intrusion Detection Systems

- Windows, Unix and Linux OS

- IT Security Software

LEARN CYBER TOOLS

Open Source Tools

- **Nmap –** Network mapper

- **Wireshark –** Network protocol analysis

- **OpenVAS –** Vulnerability scanning and management

- **Metaploit Framework –** Penetration software

- **Kali Linux –** Pentesting tool

- **Snort** – Network Intrusion Detection System

- **OSSEC** – Host Intrusion Detection System

- **Nikto** – Web server scanner

LEARN CYBER TOOLS

Compete in Capture the Flag Competitions

Develop your cyber skills further by participating in Capture the Flag (CTF) competitions. This will help you to:

- Test your cybersecurity skills
- Network with cyber community
- Collaborate and work as a part of team
- Win prizes and awards
- Gain recognition for your cyber skills

LEARN CYBER TOOLS

Upcoming CTF Events

- **Women's Society of Cyberjutsu**
  - **CTF Practice – April 20 @ 7:00 PM**
  - https://womenscyberjutsu.org/events/EventDetails.aspx?id=1092561&group=

- **ISSA Mid-Altantic Conference**
  - **CTF Competition – June 1 @ 7:30 AM**
  - https://www.fbcinc.com/e/ISSA-ISC/ctf.aspx

LEARN CYBER TOOLS

Create Your Own Coding Portfolio in GitHub

Github is a software development platform that you can use to work on coding projects and build a coding portfolio to demonstrate your skills to interviewers. Include:

- Personal Page
- Side Projects
- Course Projects
- Open Source Projects

OBTAIN CYBER / IT CERTIFICATIONS

Cyber Certifications

- **CompTia:** Security+, CySA, CASP

- **ISACA:** CISA, CRISC, CGEIT, CISM

- **ISC2:** CISSP, SSCP, CCSP, CAP, CSSLP, HCISSP

- **EC-Council:** CND, CEH, ECSA, CHFI, CCISO, CSCU

IT Certifications

- **CompTia:** IT Fundamentals, A+, Network+, Linux+, Server+, Cloud+, Project+

- **PMI:** PMP, PMI-ACP, CAPM

- **AXELOS:** ITIL, PRINCE2

- **CISCO:** CCNA, CCNP

- **Microsoft:** MCSA, MCSE

- **Amazon:** AWS Cloud Architect

- **VMWare:** VCP-NV

OBTAIN CYBER / IT CERTIFICATIONS

Approved Baseline Certifications

IAT Level I
A+ CE
CCNA-Security
Network+ CE
SSCP

IAT Level II
CCNA Security
CySA+ **
GICSP
GSEC
Security+ CE
SSCP

IAT Level III
CASP CE
CCNP Security
CISA
CISSP (or Associate)
GCED
GCIH

IAM Level I
CAP
GSLC
Security+ CE

IAM Level II
CAP
CASP CE
CISM
CISSP (or Associate)
GSLC

IAM Level III
CISM
CISSP (or Associate)
GSLC

IASAE I
CASP CE
CISSP (or Associate)
CSSLP

IASAE II
CASP CE
CISSP (or Associate)
CSSLP

IASAE III
CISSP-ISSAP
CISSP-ISSEP

CSSP Analyst
CEH
CFR
CySA+ **
GCIA
GCIH
GICSP
SCYBER

CSSP Infrastructure Support
CEH
CySA+ **
GICSP
SSCP

CSSP Incident Responder
CEH
CFR
CySA+ **
GCFA
GCIH
SCYBER

CSSP Auditor
CEH
CySA+ **
CISA
GSNA

CSSP Manager
CISM
CISSP-ISSMP

DoD Approved 8570 Baseline Certifications

- **IA - Information Assurance**
  - **IAT - Technical**
  - **IAM - Management**
  - **IASAE - System Architects & Engineers**

- **CSSP - Cyber Security Service Provider**
  - **Analyst**
  - **Infrastructure Support**
  - **Incident Responder**
  - **Auditor**
  - **Manager**

- **Source:** https://iase.disa.mil/iawip/pages/iabaseline.aspx

OBTAIN CYBER / IT CERTIFICATIONS

Certification Planning Tips

- Research Cyber / IT certifications

- Compare training delivery options

- Develop a training budget for obtaining Cyber / IT certifications

- Search within work, volunteer, government and other organizations for funding and submit requests

- Set target dates for completing your certifications

OBTAIN CYBER / IT CERTIFICATIONS

Study Tips for Certifications

- Schedule your training

- Develop a study plan

- Identify study groups that you can participate in or create one

- Study, Study, Study!

- Celebrate passing exams

APPLY FOR CYBERSECURITY JOBS

Leveraging LinkedIn

The social media web site LinkedIn can be very useful in transitioning to a cyber career. It starts with creating a solid profile, then being active on social media to learn about cyber organizations, next making connections and leveraging them to identify cyber career opportunities.

APPLY FOR CYBERSECURITY JOBS

Perfecting Your Profile

- Add an interesting profile background
- Use a high quality professional picture
- Create a strong headline
- Generate a customized URL
- Write an interesting summary
- Utilize cyber key words where you can
- Add cyber certifications as you achieve them
- List cyber volunteer activities
- Create a portfolio that highlights your cyber expertise (i.e. presentations, articles, etc.)
- Share how people can best interact with you on LinkedIn

APPLY FOR CYBERSECURITY JOBS

Social Media Strategies

- Join cyber security interest groups to connect with other people who have an interest in cyber

- Invite cyber experts that you meet in person or on line to join your network and keep in contact with them

- Follow companies that you are interested in working for that do cyber work

- Connect with recruiters that are hiring for your target cyber jobs

- Post cybersecurity articles to share with the LinkedIn community

- Share presentations or other works that show-off your cyber expertise

APPLY FOR CYBERSECURITY JOBS

Cyber Resume Make Over

As a career changer, it is not always easy to create a cyber resume that attracts a recruiter's attention because you may still be building your cyber skills and experience so you will need focus on strengthening other sections of your resume to demonstrate your interest in a cyber career.

APPLY FOR CYBERSECURITY JOBS

Objective

- State clearly your interest in pursuing a career in cyber or reference a specific cyber position.

Technical Skills

- List IT skills or core competencies, IT methodologies, IT security policies, IT policies, software, applications, programming languages, and databases that you know.

Professional Credentials

- List cyber certifications, IT certifications and other professional credentials.

Volunteer Experience

- Add volunteer positions with cybersecurity organizations.
- Explain your roles and activities that you do to promote cyber and advance the profession.

Professional Conferences & Training

- Show your knowledge! List the cyber events and training classes that you have attended.

Professional Affiliations

- List your professional association memberships.

APPLY FOR CYBERSECURITY JOBS

Mary Jane Markowitz

Objective	To obtain a position as IT Specialist (Info Sec) with the Federal Government that involves ensuring the confidentiality, integrity, and availability of systems, networks, and data.
Technical Skills	IT Security Policies: FISMA, NIST SP 800-14, NIST SP 800-30, NIST SP 800-34, NIST SP 800-53 IT Security Tools: Nmap, Wireshark, Nessus, RSA Archer, Splunk, Kali Linux
Professional Credentials	2017| Certified Information Security Manager (CISM), ISACA, Rolling Meadows, IL 2018| Certified Information Security System Professional (CISSP), ISC2, Clearwater, FL 2016| Security + Certification, CompTIA, Downers Grove, IL
Volunteer Experience	2018 |Volunteer|Cyberjutsu Girls Academy|Conducted a wide range of STEM (science, technology, engineering and math) workshops for middle school-aged girls in the DC Metro area to increase their competency and confidence in STEM.
Professional Conferences & Training	2018	Privacy & Security Forum, Washington, DC 2017	ISC2 Secure Summit, Washington, DC 2016	ISSA Mid-Atlantic Conference, Rockville, MD
Professional Affiliations	2016 – Present	Member, ISACA, Washington, DC 2016 – Present	Member, Women's Society of Cyberjutsu, Washington, DC 2016 – Present	Member, ISSA, Washington, DC

APPLY FOR CYBERSECURITY JOBS

Ace the Cyber Technical Interview

You should expect interviewers who want to test your cybersecurity knowledge. It is highly likely that they are going to ask you some tough questions. Be ready!

- Refresh your memory on cyber concepts

- Get a list of technical questions from the internet and practice answering them

DEVELOP YOUR CYBERSECURITY ACTION PLAN

- Your goal is to have a career in cybersecurity.

- In order to achieve this goal it will take vision, strategy, determination, motivation and planning

- Specifically you need an action plan.

DEVELOP YOUR CYBERSECURITY ACTION PLAN

Actions speak louder than words! It's one thing to say that you want a career in cyber but it's another thing to put a plan in place to make it happen. To turn your dream into a reality you need to take some steps to make it happen:

- Sit down and make an action plan

- Check your progress on a monthly basis

- Hold yourself accountable

- Reward yourself for success

DEVELOP YOUR CYBERSECURITY ACTION PLAN

S Specific

M Measureable

A Attainable

R Relevant

T Time Based

When creating your action plan you need to make sure that the action items that you list are SMART.

In addition, you need to avoid the pitfalls that people often fall into when developing an action plan. For example:

- Failing to write action items down
- Listing too many action items
- Creating an action plan that is too complex

DEVELOP YOUR CYBERSECURITY ACTION PLAN

Mark Stanford's Story

- Mark graduated from a liberal arts college with a bachelor's degree in criminal justice with a minor in business two years ago.

- He has been working as a Background Investigator for a company that does work for the Office of Personnel Management since he graduated from college.

- Stanford is interested making a career change into cybersecurity, but is not sure what specialty area is the best fit for him.

DEVELOP YOUR CYBERSECURITY ACTION PLAN

Sample Cyber Career Action Plan

Name: Mark Stanford	Date: 01/01/2018

Cyber Career Vision	Cyber Career Objective	Cyber Career Strategy
My vision is to help organizations protect the confidentiality, integrity, and availability of data and information systems.	My objective is to explore career paths in the field of cyber security and identify 3 target positions that are of interest to me and are solid career options for me to pursue in the future.	My strategy is to research position descriptions online and then to conduct informational interviews with people who are doing the work that I am most interested in. I am also going to read, listen to webinars, and attend events to learn more about cybersecurity.

DEVELOP YOUR CYBERSECURITY ACTION PLAN

Action Area	Action	Target Date	Status
Explore Your Interest in Cyber	• Attend monthly ISSA meetings to learn more about cyber topics and network with cyber professionals	01/01/18	o Not Yet Started o In Progress o Completed
Research Cyber Positions	• Visit the Cyberseek web site and identify six jobs that are of interest to me	02/01/18	o Not Yet Started o In Progress o Completed
	• Conduct six informational interviews with cyber professionals	03/01/18	o Not Yet Started o In Progress o Completed
Learn Cyber Policies & Standards	• Read ISO/IEC 27000 - Information Security Techniques	01/01/18	o Not Yet Started o In Progress o Completed
Learn Cyber Tools	• Attend Splunk Users Meet Up Group	02/02/18	o Not Yet Started o In Progress o Completed
Obtain Cyber / IT Certifications	• Research the Security+ Certification	06/18/18	o Not Yet Started o In Progress o Completed
Apply for Cyber Jobs	• Follow companies on LinkedIn that do cyber work	02/18/18	o Not Yet Started o In Progress o Completed

DEVELOP YOUR CYBERSECURITY ACTION PLAN

Tammy William's Story

- Tammy graduated from a state university with a Bachelors degree in Management of Information Systems.

- She has been working as a IT consultant for a big four firm for five years and wants to make a shift from consulting to auditing.

- Williams has a friend in the firm who is an IT Auditor and she is very attracted to the types of client engagements that her friend works on.

DEVELOP YOUR CYBERSECURITY ACTION PLAN

Sample Cyber Career Action Plan

Name: Tammy Williams   **Date: 02/14/2018**

Cyber Career Vision	Cyber Career Objective	Cyber Career Strategy
My vision is to help organizations implement IT Security controls that can help them to avoid or reduce the effects of potential cyberattacks	My objective is to have a highly successful career as an IT Auditor with an accounting or consulting firm in the Washington, DC metropolitan area.	My strategy is to build on my existing IT experience and education to transition to a career in cyber. To improve my value proposition to IT Audit employers I will develop my IT auditing skills and obtaining an IT Audit certification.

DEVELOP YOUR CYBERSECURITY ACTION PLAN

Action Area	Action	Target Date	Status
Explore Your Interest in Cyber	• Attend monthly ISACA and IIA meetings to learn more about IT auditing and network with IT Audit professionals	01/01/18	○ Not Yet Started ○ In Progress ○ Completed
Research Cyber Positions	• Conduct four informational interviews with IT Audit professionals at large, small, private, non-profit and public organizations in the Washington DC metropolitan area	02/01/18	○ Not Yet Started ○ In Progress ○ Completed
Learn Cyber Policies & Standards	• Read NIST SP 800-30 – Risk Management Guide for Information Systems	03/01/18	○ Not Yet Started ○ In Progress ○ Completed
Learn Cyber Tools	• Set a home lab to teach myself open source IT security tools like Nmap, Wireshark and OpenVAS	03/01/18	○ Not Yet Started ○ In Progress ○ Completed
Obtain Cyber / IT Certifications	• Obtain the Certified Information System Auditor (CISA) Certification	06/30/18	○ Not Yet Started ○ In Progress ○ Completed
Apply for Cyber Jobs	• Follow IT auditing companies EY, Deloitte, Morgan Franklin and Cotton & Company on LinkedIn	01/01/18	○ Not Yet Started ○ In Progress ○ Completed

DEVELOPING YOUR CYBERSECURITY ACTION PLAN

CONTACT INFORMATION

Teresa Allison, VP of Strategic Relations

Information System Security Association, DC Chapter

E-mail: vp_strategic_relations@issa-dc.org