Cyber Security Career Guide

A RESOURCE FOR STUDENTS AND PROFESSIONALS

ISSUE 1 - 2016

The Virginia Cyber Security Partnership

Cyber Security Career Guide

A RESOURCE FOR STUDENTS AND PROFESSIONALS

PREFACE

Answer this question. How many electronic devices are digitally connected in your home? Chances are you don't actually know. You're not alone.

As a society we have a tendency to adopt new technology faster than we can digest the risks they create. Technological advancements have created enormous opportunities for businesses and individuals to do things that were once only considered science fiction. These same advancements, however, have changed the risk landscape and also created new opportunities for system exploitation. A different type of opportunity has been created with these risks, --an opportunity to protect the interests of our country and society through the cyber security profession. If you're interested in learning more about a rewarding career that is high in demand, then this guide is for you.

Over the last 10 years, few professions have grown as fast as cyber security. The demand for skilled and experienced talent has increased exponentially as new, complex, and more sophisticated threats emerge. As a result of a shortage in qualified professionals, the average cyber security professional currently earns over $100,000. To help put that in perspective, according to 2014 U.S. Census Bureau data, the average cyber security professional individually earns more than 75% of the combined household incomes in the United States.

Due to the continued growth in demand for skilled cyber security professionals, the pipeline of security professionals has not been able to keep up. By the year 2020 according to the 2015 (ISC)2 Global Information Security Workforce Study, the shortage of professionals is expected to reach 1.5 million. In Virginia alone, the number of cyber security related jobs is expected to increase by 25% through 2022. In 2014 Governor McAuliffe signed an Executive Order Launching “Cyber Virginia” and the Virginia Cyber Security Commission to correct this shortage.

The purpose of this guide is to help navigate the cyber security profession by providing useful insights and resources for anyone interested in entering the field of cyber security.

ABOUT THE VIRGINIA CYBER SECURITY PARTNERSHIP

The Virginia Cyber Security Partnership (VCSP) was founded in 2012 through a strategic collaboration with the Federal Bureau of Investigation (FBI) and cyber security leaders within the industry.

The Partnership works with the FBI and the Commonwealth of Virginia to promote mutually beneficial information sharing, foster professional development, and conduct community outreach.

The mission of the VCSP is to address the cyber security risks facing Virginia and our nation by establishing and maintaining a trusted community of public and private sector cyber professionals.

Members of the VCSP include representatives from many of Virginia's most respected organizations which enables cross industry insights for enhanced collaboration.

The VCSP achieves its mission through the delivery of three primary mission objectives:

- **Skill Enhancement,** providing opportunities to sharpen existing skillsets and develop new skills within cyber security.
- **Outreach and Pipeline Development**, enhancing the awareness of cyber security, and sharing opportunities within the cyber profession to expand the pipeline of skilled professionals to support the increased demand of cyber security programs.
- **Collaboration,** fostering a community and strengthening the overall program by creating opportunities for members to collaborate on threat intelligence, best practices, and other cyber related activities.

PART 1 | CAREERS IN CYBER SECURITY

INFORMATION ASSURANCE

Information assurance is the practice of managing information-related risks. More specifically, IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These goals are relevant whether the information is in storage, processing, or transit, and whether threatened by malice or accident. In other words, IA is the process of ensuring that authorized users have access to authorized information at the authorized time.

EXAMPLE ROLES WITHIN INFORMATION ASSURANCE

Information Assurance Analysts apply current technologies to the design, development, evaluation and integration of computer information systems and networks to maintain system security. These analysts are responsible for ensuring the protection of company data against unauthorized disclosure, accidental or intentional loss of data, or unauthorized modification.

Information Assurance Engineers oversee the storing and processing of information within a company, making sure that it is secure. The engineer should also conduct period risk assessments, allowing them to detect any potential risks that are present in order to minimize potential data breaches.

Incident Responders are cyber firefighters, rapidly addressing security incidents and threats within an organization as they occur. Using a wide range of computer forensic tools, they discover the problem, mitigate the damages, and take detailed notes throughout the entire process. Prior experience in computer investigations or general computer forensics is often necessary. The ability to obtain security clearance is sometimes also a requirement.

SECURITY OPERATIONS

Security Operations includes all of those functions required to ensure that a wide variety of technical security controls are effectively and efficiently implemented, configured and maintained. Hands on design, selection, and administration of capabilities such as malware protection, web content filtering, network firewalls, remote access, mail filtering, network packet capture, security information and event management, digital forensics, and whitelisting are typically included in security operations.

EXAMPLE ROLES WITHIN SECURITY OPERATIONS

Security Administrators are responsible for installing, administering, and troubleshooting an organization's security solutions, and are the point person for cyber security systems.

Security Architects design, build, and oversee the implementation of network and computer security for an organization.

Security Engineers sometimes called Network Engineers, build and maintain IT security solutions for an organization.

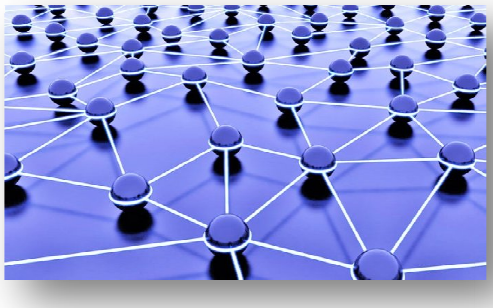
Security Operations Center (SOC) Analysts are part of the

team that performs the day-to-day monitoring of an environment, analyzing and responding to events as necessary, and providing technical support.

Vulnerability Assessors also known as Vulnerability Assessment Analysts, scan applications and systems to identify vulnerabilities.

INTELLIGENCE ANALYSIS

Intelligence analysis is the process of taking known information about situations and entities of strategic, operational, or tactical importance, with appropriate statements of probability, assessing and characterizing future actions in those situations and by those entities. The descriptions are drawn from what may only be available in the form of deliberately deceptive information; the analyst must correlate the similarities among deceptions and extract a common truth.



EXAMPLE ROLES WITHIN INTELLIGENCE ANALYSIS

Intelligence Analysts work for a variety of organizations, including federal government agencies, such as the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Central Intelligence Agency (CIA), public sector organizations such as the Virginia Fusion Center, the Virginia Information Technology Agency, as well as private sector companies. The tasks involved in this line of work entail extensive research and collecting information from many sources. Intelligence analysts then sort, target, and identify relevant data, which is reported to key officials.

Tactical Analysts provide up-to-the-minute information about the specific threats that have already matured or are on the operational horizon. These analysts are often embedded with active investigations and provide information on the impending mission. They may assist in preparation for a mission as well as the gathering of data following successful operations, which may involve interrogations, technology analysis, and crime scene investigations.

Collection and Reporting Analysts are handlers of raw intelligence. They manage intelligence gathering methodologies with the intent of improving accuracy and efficient collection. They often utilize linguists and decryption technologies to decipher high priority intelligence that may help others better prepare for a mission or more quickly and effectively achieve success.

Strategic Analysts assist in threat analysis, policy formulation, and strategic resource application. These analysts often use the processed information of others in order to generate comprehensive strategies that address and eliminate threats. These analysts use a big picture approach to organizational management, which enhances intelligence, criminal investigations, and national security operational performance.

Security Analysts, also known as threat analysts, detect and prevent cyber threats to an organization. Their responsibilities are continually expanding as the number of cyberattacks increases.

RISK MANAGEMENT, AUDIT & COMPLIANCE

Risk Management is the practice of identifying, assessing and managing risks to an organization's most important assets. Risks manifest themselves in many forms and may come from external threats, internal threats, or pre-existing vulnerabilities that have the potential to impact the confidentiality, integrity or availability of company data and information systems. Risk analysis is used to determine the probability of these risks impacting business operations and whether or not the consequences are tolerable. When the probability and consequences represent an unacceptable risk to the company, risk management methods are used to define and implement cyber security controls to mitigate those risks to an acceptable level.

Risk management may also include functions designed to ensure compliance with mandatory cyber security regulatory requirements or voluntarily adopted industry standards. These functions establish information security policies and design other managerial, technical and operational controls. These controls in turn address specific performance-based objectives typically meant to secure a specific group of assets, either within an industry segment or across government organizations. Once controls are established, audits are performed to validate that those controls are designed and implemented consistent with their intended purpose.

EXAMPLE ROLES WITHIN RISK MANAGEMENT, AUDIT & COMPLIANCE

Security Auditors assess the design and effectiveness of computer policies and programs and their related security components typically against recognized standards or best practices.

Security Software Developers (Programmers) develop software used in the prevention or detection of cyber incidents. They also play a role with the integration of security into applications software during the course of design and development

Risk Analysts evaluate how a company/organization operates its business to identify the physical assets (i.e., facilities and equipment), and information assets (i.e., intellectual property and privacy information) it considers most important. Wherever the assets are vulnerable to specific threats, they develop a plan to effectively manage and prudently invest in security measures that will mitigate the identified risk to the company. Risks mitigation becomes part of an overall strategic plan.

STRATEGIC PLANNING

Strategic planning is an organization's process of defining its strategy, or direction, and making decisions on allocating its resources to pursue this strategy. It may also extend to control mechanisms for guiding the implementation of the strategy. Strategy has many definitions, but generally involves setting goals, determining actions to achieve the goals, and mobilizing resources to execute these actions. A strategy describes how the ends (goals) will be achieved by the means (resources). In cyber security, the process of strategic planning involves development of strategies to manage information technology related

risks that fall outside the organization's risk appetite.

EXAMPLE ROLES IN STRATEGIC PLANNING

Security Managers, sometimes called Security Directors, are expected to manage an organization's IT security in every sense of the word – from devising imaginative security solutions to implementing policies and training procedures.

Security Officers, like a Chief Information Security Officer (CISO), oversee all operations and staff in any IT security department.

Security Managers and Officers are expected to have degrees in an associated field as well as extensive experience in information security and proven management skills.

DIGITAL FORENSICS

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science, which encompasses the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil (as part of the electronic discovery process) courts. Forensics may also be used by private sector companies; such as during internal corporate investigations or intrusion investigation (a probe into the nature and extent of an unauthorized network intrusion).

EXAMPLE ROLES IN DIGITAL FORENSICS

Computer forensics investigators may provide many services, from investigating computer systems and data in order to present information for legal cases to determining how an unauthorized user hacked into a system to gathering digital information that will assist in the termination of an employee. During the course of these tasks, the digital forensics investigator protects the computer system, recovers all files (including those that were deleted or password-protected), analyzes all data found on various disks, and provides reports, feedback, and even testimony, when required.

Forensics Experts, also known as computer forensic analysts or investigators, are digital detectives, harvesting and analyzing evidence from computers, networks and other forms of data storage devices.

Cryptanalysts analyze encrypted information to break the code/cipher or to determine the purpose of malicious software.

Cryptographers, also known as cryptologists, use encryption to secure information or to build security software. They also work as researchers to develop stronger encryption algorithms

PART 2 | CRITICAL TRAITS OF A CYBER PROFESSIONAL

Information security professionals are responsible for helping business leaders understand cybersecurity risk and how to properly mitigate such risk. In addition to understanding the multiple threats that face organizations today, an information security professional must also understand the business of their organization. They need to differentiate and prioritize the risks of threats in relation to the sensitivity of their organization's data. Ultimately they have to act as translators, being able to explain cyber threats and risks in non-technical terms that can help business leaders make decisions to protect one of their most important assets, data.

INTEGRITY

Integrity is the quality of being honest and having strong moral principles. It is generally a personal choice to hold oneself to consistent moral and ethical standards. Honesty and truthfulness of one's actions make up the integrity of an information security professional.

TRUSTWORTHINESS

Character is a function of all aspects of a person's behavior and attitudes. Trustworthiness is one character trait that is an essential foundation for any cyber security job. When employers and coworkers assess trustworthiness, they base their assessment on competence and credibility. As an example of trustworthiness, an information security professional may be charged with safeguarding highly sensitive information involving an organization's data breach or an investigation of data theft and misuse by internal employees. Competence requires an ability to execute assigned tasks in such a way that allows them to trust that you'll correctly and efficiently perform the task. Credibility means that you can be counted on to complete your assignments while also maintaining strict confidentiality. Demonstrating you are competent and credible helps to build trust.

TEAM COMMITTMENT

Teamwork is fundamental to confronting the cyber security risks facing private and public sector organizations. Strong collaboration within and between these organizations is essential to mounting a meaningful response to growing and evolving cyber threats.

Because cyber threats are sophisticated and complex, defending and mitigating these threats requires a variety of skills and functions. Each must work together towards a common objective. Information security professionals must work for collaboration and cooperation with teams in both technology and the business.

Cyber security professionals must also build strong relationships within their organization and with a wide

variety of industry and government partners in order to have a head start against cyber threats.

PERSEVERANCE

The practice of information security is hard. Systems and software being protected change frequently. Threats often evolve faster than new controls can be implemented to mitigate those threats. Cyber threat analysis can be tedious and take time to determine the right solution to combat threats against your organization. In addition, security policies viewed as necessary by a cyber security professional may be seen as obstacles to the mission of their colleagues across organization and are sometimes met with resistance. These are just a few of the many difficulties associated with mitigating security risks. Cyber security professionals must always be steadfast in their efforts to achieve and maintain a strong security posture, in spite of the many challenges they will face along the way.

EFFECTIVE COMMUNICATIONS

Information security isn't about being in control. It's about helping business leaders make wise decisions based on their knowledge of the business environment and market forces. Information security professionals who understand this and provide value to their business leadership through effective communications are worth their weight in gold. The most effective communicators demonstrate good listening skills, are concise and convincing when articulating their message, and are adept at written forms of communication as well as oral communications and presentation skills.

PART 3 | CAREER DEVELOPMENT

VALUE-BASED CAREER DECISIONS

All career development should start with a good understanding of your values. While it may not be intuitive, career decisions can at times involve difficult choices. This could include deciding whether to change job locations and move away from friends or family; switch departments or companies; participate in a new project; take on a leadership or management role; or shift your career path entirely. When faced with those choices, it's important to be clear about the personal values that are the foundation for career decision-making. Consider the things that motivate you or give you pride in your work and workplace such as sense of achievement, contribution to the community, intellectual stimulation and growth, ethical behavior, respect for others or financial security. Values are qualities considered to be the most important guiding principles that help set priorities in your career and life. They are highly personal and define what is purposeful and meaningful to you. Though values may change in response to life circumstances, they are generally thought to be enduring and provide a compass for setting goals and making decisions.

3 DIMENSIONS OF DEVELOPMENT

Once you've assessed and arrived at the values most important to you, it's time to think about the development process itself. Think of the skills and competencies you have as well as your weaknesses. Be willing to recognize where you may have blind spots about your strengths and weaknesses and get input from others who can give you a more objective perspective. Mentors are good sources of objective feedback. Remember too that career development is not only about the job you're in, it's also about the job you want. The specific development activities you choose should include steps to improve yourself along three dimensions; technical knowledge (proficiency in your craft), business awareness (understanding how you fit into the big picture and how your company operates), and soft skills (e.g., communication skills, negotiations and influence, leadership, conflict resolution, etc.). The breadth and depth of development for each of these vectors should vary based on your overall development needs.

DEVELOPMENT METHODS

Often career development is thought of as training. You think of a course you can take that will teach you the skills or competencies you're trying to improve and that becomes your development. In reality, there are numerous methods that can be used, often at little to no cost, and often more impactful than taking a course. For example, having the opportunity to participate in or lead a cross-functional team will develop team-building and leadership skills, negotiating, conflict resolution, and organization skills. Depending on the assignment given to the team, it can also be an opportunity to learn more about how your company operates from others on the team. Other methods of development include job shadowing, sojourning, mentoring and observation of others who are more experienced.

PART 4 | MENTORING

PURPOSE OF A MENTOR

Merriam-Webster defines a mentor as "someone who teaches or gives help and advice to a less experienced and often younger person". A mentor can provide valuable insight regarding a specific job, a career path, or soft skills. A mentor can usually provide advice based on experience or provide an unbiased external view of your skills and developmental maturity. Open and honest criticism is often hard to solicit from co-workers or managers. A mentor can often provide insight others are unwilling to openly discuss directly with you.

There are many types of mentors you may seek. The type of mentor should be matched with your goals. Some mentor types are:

- People in leadership roles
- Peers
- Subject Matter Experts (SMEs)

When seeking a mentor, it's best to have a topic or skill as your focus. Some common areas of focus are:

- Career development
- Specific job challenges or projects
- Individual development (soft skills)
- Exploring new areas or job shadowing

CHOOSING A MENTOR

A mentor can be a powerful role model, while also giving advice on areas in need of development, choice of career paths, etc. Choose someone who is most likely to tell you what you need to hear, not what you want to hear. Define your personality and communication style. What kind of mentor would best complement you? You may choose someone who's your opposite (an extrovert to your introvert, for example), or someone in whom you see yourself (and vice versa). If you are struggling with choosing a mentor, ask others if they know who exemplifies the skills or traits you seek.

DEFINING THE MENTORING RELATIONSHIP

It important to define the term of the mentoring arrangement, how the mentoring will occur (meeting, periodic phone call to check in, lunch or dinner meeting, meeting frequency, etc.). Each mentor will have their own thoughts about this. Strike a balance. Remember the mentor is giving their time, so it's best to accommodate them. Explain what you want out of the mentorship. Use the following as a guide:

1. Identify development needs and goals. Focus on the top 1-3 items
2. Seek out a mentor that is appropriate for your goals. Be thoughtful in your approach and gaining the potential mentor's support
    a. Gain agreement on the relationship during the first meeting
    b. Meeting frequency?
    c. Meeting location (phone or in person)?
    d. Length of engagement (typically 3-6 months)?
    e. What's the focus of the engagement? Topics for discussion?

   f. Discuss any resources needed
   g. Set expectations (what does the mentor & mentee want?)
   h. Stay organized
   i. Initiate meetings and scheduling
3. Be prepared for each meeting. Also, give your mentor advance notice of any new topics
   a. Take notes
   b. Track progress
   c. Do what you said you were going to do
   d. Thank the mentor
   e. Be respectful of their time
   f. Understand scheduling conflicts may arise – stay flexible
   g. Let them know if the engagement is helping. Share feedback and accomplishments
   h. Remember, the mentor is providing free time out of their schedule. You need to do all the preparation and execution.

PART 5 | CAREER DEVELOPMENT RESOURCES

SELF-STUDY

Self-Study is one of the most important aspects of career development. This method of learning takes discipline and sometimes costs money, but if you have access to the Internet, it can be very worthwhile. Taking the initiative to develop your skillset on your own can not only make you stand out from your peers, but it can also provide for faster career advancement. Listed below are just a few of the many self-study opportunities available, which can be taken at the learner's own pace:

- Cyberdegrees.org offers various MOOCS (Massive Open Online Courses), which can be found at http://www.cyberdegrees.org/resources/free-online-courses/).
- SANS, the most trusted and the largest source of information security training in the world, offers many free courses which can be found at http://www.cyberaces.org/

CYBER COMPETITIONS

Virginia Area Cybersecurity Cybercamps

The Virginia Department of Education features the Virginia CyberCamp 2016 program. From a field of eligible school divisions, 32 CyberCamp 2016 applications were accepted. The camps, using a grant of $62,500 each, provide classroom and extended classroom instruction and include project-driven learning, field trips, guest speakers, and a culminating recognition program. Look for it in 2017, too.

Visit the Interactive Cybercamp Map at http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cybercamps/index.shtm

U.S. Cyber Challenge

The mission of U.S. Cyber Challenge (USCC) is to significantly reduce the shortage in today's cyber workforce by serving as the premier program to identify, attract, recruit and place the next generation of cybersecurity professionals. USCC's goal is to find 10,000 of America's best and brightest to fill the ranks of cybersecurity professionals where their skills can be of the greatest value to the nation.

USCC works with the cybersecurity community to bring accessible, compelling programs that motivate students and professionals to pursue education, development, and career opportunities in cybersecurity.

USCC Summer Camps feature one week of specialized cybersecurity training that includes workshops, a job fair, and a culminating "Capture the Flag" competition. The workshops are led by college faculty, top SANS Institute instructors, and cybersecurity experts from the community. The workshops and presentations focus on a variety of topics ranging from intrusion detection, penetration testing and forensics. Participants can also participate in a job fair that provides them the opportunity to meet with USCC sponsors and discuss potential employment. The weeklong program ends with a competitive "Capture the Flag" competition and an awards ceremony attended by notables in the cybersecurity industry and government.

For more information, visit the U.S. Cyber Challenge website at http://www.uscyberchallenge.org/

MITRE Cyber Academy

The MITRE Cyber Academy is a not-for-profit organization chartered to work in the public interest and foster the education and collaboration of cyber professionals. They provide a growing set of resources to help you develop your technical skills as a cyber security professional. These resources include a Cybersecurity Training Portal, and a Cyber Practice Range. The MITRE Cyber Academy also offers an annual Cyber Competitions for students at the college and high school levels.
http://mitrecyberacademy.org/

SANS NetWars

SANS NetWars is a suite of hands-on, interactive learning scenarios that enable information security professionals to develop and master the real-world, in-depth skills they need to excel in their field. In SANS award-winning courses, attendees consistently rate our hands-on exercises as the most valuable part of the course. With NetWars, participants learn in a cyber range while working through various challenge levels, all hands-on, with a focus on mastering the skills information security professionals can use in their jobs every day.

Core NetWars is a computer and network security challenge designed to test a participant's experience and skills in a safe environment while having a little fun with your fellow IT security professionals.

Topics Include:

- Vulnerability Assessment
- Packet Analysis
- Penetration Testing
- System Hardening
- Malware Analysis
- Digital Forensics and Incident Response

Digital Forensics and Incident Response (DFIR) NetWars is an incident simulator packed with a vast amount of forensic, malware analysis, threat hunting, and incident response challenges designed to help you gain proficiency without the risk associated when working real life incidents. It is unique in that it provides time-limited challenges that can be used to test the skills you've mastered, and at the same time, help you identify the skills you are missing.

NetWars CyberCity, SANS most in-depth and ambitious offering, is designed to teach warriors and infosec pros that cyber action can have significant kinetic impact in the physical world. As computer technology, networks, and industrial control systems permeate nearly every aspect of modern life, military, government, and commercial organizations are realizing an increasing need for skilled defenders of critical infrastructures. SANS engineered and built CyberCity to help organizations grow these capabilities in their teams.

CyberCity is a 1:87 scale miniaturized physical city that features SCADA-controlled electrical power distribution, as well as water, transit, hospital, bank, retail, and residential infrastructures. CyberCity engages participants to defend the city's components from terrorist

cyber-attacks, as well as to utilize offensive tactics to retake or maintain control of critical assets.

For more information on each of the SANS NetWars offerings, visit the SANS NetWars website at http://www.sans.org/netwars/

CERTIFICATIONS

Certifications offer employers a mechanism to validate the familiarity an existing or prospective employee has with role specific cyber security concepts. Certifications aren't necessarily an indication of experience and competency. Nevertheless, pursuit of a cyber security related certification can be a great way to focus learning activities and grow knowledge using a standardized, structured process.

CISSP – Certified Information Security Systems Professional

The CISSP is one of the most widely recognized cyber security certifications. It draws from a comprehensive, up-to-date, global common body of knowledge (CBK) that's designed to provide security leaders with a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices. The CISSP exam tests one's competence in the 8 domains of the CISSP CBK, which cover:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

ISACA – Information Systems Audit and Control Association

CISA – Certified Information Systems Auditor

The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals. Being CISA-certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise.

CISM – Certified Information Systems Manager

The uniquely management-focused CISM certification promotes international security practices and recognizes the individual who manages designs, and oversees and assesses an enterprise's information security.

CSX – CSX Certification

The Cybersecurity Fundamentals Certificate exam tests for foundational knowledge in cybersecurity across five key areas:

- Cybersecurity concepts
- Cybersecurity architecture principles
- Cybersecurity of networks, systems, applications and data

- Incident responses
- The security implications of the adoption of the emerging technologies

The certificate is particularly relevant for recent college/university graduates, entry level professionals and those looking for a career change to cybersecurity. The certificate program is also one of the best ways to gain foundational knowledge in cybersecurity and begin to build your skills and knowledge in this crucial area. There are more advanced CSX certifications that can be obtained for further specialization (i.e., CSX Practitioner, CSX Specialist, and CSX Expert).

GIAC – Global Information Assurance Certification

GIAC is designed to build the hands-on skills that go beyond theory and tests on the pragmatics of security administration, management, audit, and software security.

GIAC offers more than 20 specialized information security certifications that correspond to specific job duties. The family of GIAC certifications target job-based skill sets rather than taking a one-size-fits-all approach. The GIAC certification process validates the specific skills of security professionals and developers with standards established on the highest benchmarks in the industry. The higher-level certifications, Gold and Expert Level, offer a way for outstanding performers to distinguish themselves through even more hands-on focused activities.

DCITA - Defense Cyber Investigations Training Academy

DCITA provides in-residence and online training to DoD elements that protect DoD information systems from unauthorized use, criminal, fraudulent, and foreign intelligence activities.

The DCITA curriculum offers courses organized into specialty areas. Since its founding in 1998, the Academy has recorded more than 19,000 student enrollments in DCITA courses.

For more information on courses, registration, and certification programs, visit www.DCITA.edu.

Key curriculum topics Include:

- Computer search and seizure
- Network intrusions
- Digital forensics
- Basic and advanced forensic examination
- Online undercover techniques

DCITA confers DoD certifications in digital media collection, digital forensic examination, and cyber-crime investigation.

The Academy is accredited by the Council on Occupational Education (COE), a national organization that supports quality in career and technical education. DCITA has also received college credit recommendations for several courses from the American Council on Education (ACE), the major national coordinating body for postsecondary education.

DCITA is the lead organization for the National Center for Digital Forensics and Academic Excellence (CDFAE) program, collaborating with colleges, universities, and institutions of higher learning to establish and promote a consistent digital forensics core curriculum nationally.

INTERNSHIPS, SCHOLARSHIPS, POST-SECONDARY EDUCATION

Internships are a great way to learn about the field of cyber security, to create a network of contacts, learn more about a specific company, or to gain school credit. As different employers have different internship opportunities available, it best to check with the individual organization regarding upcoming opportunities. Listed below are a few of the opportunities available:

The Department of Homeland Security offers cybersecurity internship programs

https://www.dhs.gov/homeland-security-careers/cybersecurity-internship-program
https://www.dhs.gov/homeland-security-careers/dhs-cybersecurity

DHS also offers a program called Cybercorps Scholarships for Service through the National Initiative for Cybersecurity Careers & Studies (NICCS)

https://niccs.us-cert.gov/education/cybercorps-scholarship-service-sfs

The FBI offers paid, summer internships, called the Honors Internship Program

https://www.fbijobs.gov/students/honors-internship-program

The NSA offers multiple opportunities for high school and college students with scholarships, summer internships, and special programs, including work study programs

https://www.intelligencecareers.gov/icstudents.html

Several Virginia area schools offer opportunities to study cyber security, often through their computer science programs. Listed below are the various schools, with a link to their website:

- George Mason University (http://www.gmu.edu)
- James Madison University (http://www.jmu.edu) – Note that JMU offers a special program in Information Security as part of their MBA curriculum)
- Tidewater Community College (http://www.tcc.edu)
- University of Virginia (http://www.virginia.edu/)
- Virginia Tech (http://www.vt.edu)

PART 6 | REFERENCES AND RESOURCES

2015 (ISC)2 Global Information Security Workforce Study
<https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf>

Cisco Launches $10 Million Global Cybersecurity Scholarship to Increase Talent Pool; Introduces New and Updated Certifications <http://www.marketwired.com/press-release/cisco-launches-10-million-global-cybersecurity-scholarship-increase-talent-pool-introduces-nasdaq-csco-2133988.htm>

Cybersecurity Nexus http://www.isaca.org/CYBER/Pages/default.aspx

Governor McAuliffe's Executive Order Launching "Cyber Virginia" and the Virginia Cyber Security Commission <https://cyberva.virginia.gov/media/4396/cyber-commission-report-final.pdf>

Piedmont Virginia Community College Charlottesville VA PVCC expands cybersecurity program to meet growing demand for information security analysts
http://www.pvcc.edu/programs/information-systems-technology-cybersecurity-specialization

Tidewater Community College, part of the Virginia Community College Tidewater Community College is a National Center of Academic Excellence in Cyber Defense (CAE2Y), designated in 2016 by the United States National Security Agency (NSA) and the Department of Homeland Security (DHS).
<http://www.tcc.edu//academics/information-technology/certifications>

Virginia's 21st Century Career Pathway Cybersecurity
http://www.doe.virginia.gov/administrators/superintendents_memos/2016/040-16a.pdf