NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

JOB SEEKER GUIDANCE

FROM THE NICE MODERNIZE TALENT MANAGEMENT WORKING GROUP
NOVEMBER 2022

CONTENTS

INTRODUCTION

Early career entrants may find it challenging to find their first cybersecurity-related position. If they do not have experience or demonstrable skills in cybersecurity, employers may overlook them in the hiring process. Many job seekers report they apply, over and over, and never even get an interview!

What are the techniques a job seeker should use to position themselves so that employers will invite them to interview, include them in their candidate pool, and extend them an offer? Which positions are most appropriate for someone just starting in the cybersecurity field? Or, is that simply the wrong question to ask? Does the appropriate career entry job depend on career pathway, on sector, or on job seeker's interest and talent?

The members of the Modernize Talent Management Working Group, a public working group of the NICE Community Coordinating Council, created this project to satisfy the project charter that was created to address, in part, Objectives 3.3 and 3.4 of the NICE Strategic Plan:

3.3 "*Align qualification requirements according to proficiency levels to reflect the competencies and capabilities required to perform tasks in the NICE Framework.*"

3.4 "*Promote the establishment of more entry-level positions and opportunities that provide avenues for growth and advancement.*"

This project team met on a regular basis during the first half of calendar 2022 and the following document reflects the recommended guidance of the membership.

The project was led by Brian Ford.

WHAT IS AN ENTRY LEVEL POSITION?

For the purposes of this document, the project team has chosen to consider the needs of all those seeking to enter the cybersecurity profession from a variety of starting points. For the sake of continuing discussion, the working group found the term "**entry level**" problematic. Therefore, other terminology was discussed.

EARLY CAREER LEVEL

There are different interpretations of the term 'entry-level'. Some cybersecurity practitioners actively push back: 'Is there really an entry-level position in cyber security?' Many would state that other positions help develop and demonstrate certain skills that qualify an individual for cybersecurity work. CyberSeek.org, the NICE-grant funded website that documents cybersecurity workforce supply and demand, shows few open "entry level" defined positions. This would indicate the majority of hiring is not occurring at that level.

Therefore, it may be useful to expand the notion of what entry level work in cybersecurity is. It may be a first position - a career entry point into cybersecurity. For some, that may be a transition from a college degree program, from active duty military, or from an apprenticeship program. It may include a move from a feeder role in an adjacent field such as software development, IT help desk or network management.

The guidance in this report is meant for someone seeking to enter into a cybersecurity career from a number of different starting points. We will consider those individuals to be at the **early career** level.

Reskilling

Someone r**eskilling** is currently employed in a different field, such as marketing and needs to go through a job training program to learn cybersecurity job skills. They would benefit from a program like an apprenticeship, where they can skip over general education requirements one might find in a college course and focus on the job-related knowledge requirements.

Reskilling programs might also be found in-house at an employer who is able to identify talented individuals and retain them by providing them with a program of education and training that leads to a new job.

Upskilling

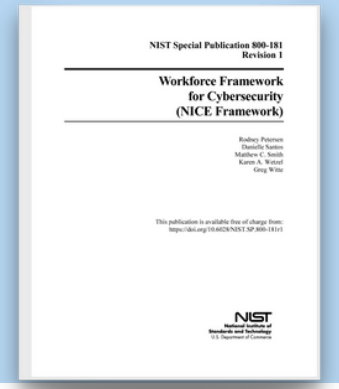
Upskilling is a program that enables the employee to continue to grow in their knowledge and skills while on the job, leading them to increased job opportunities with the same employer. This may include educational opportunities via a learning management system or the employer may simply reimburse via a tuition credit program.

Upskilling may not necessarily be tied to a new job program, but be part of ongoing opportunities for continuing knowledge and growth.

GETTING STARTED

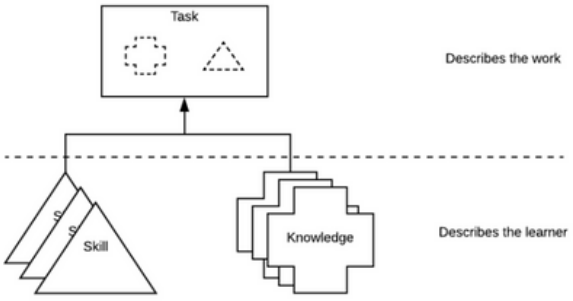
Cybersecurity as a field of work is highly varied. You might work as a software developer, contributing to a product or platform or application. Perhaps you want to become an analyst, reviewing cybersecurity systems and events to look for anomalous behavior that might indicate a security breach. You could be an attorney reviewing contracts for vendors to ensure that their cybersecurity posture is sufficient to eliminate introduction of risk to your own organization. Or perhaps you work on policy for your company, ensuring that cybersecurity best practices govern the decisions made across the organization.

UNDERSTANDING THE NICE WORKFORCE FRAMEWORK FOR CYBERSECURITY



The NICE Framework provides the language for describing the tasks, knowledge, and skills that are needed to perform the cybersecurity work performed by individuals and teams. It defines 52 work roles found in cybersecurity. Anyone performing cybersecurity work may have a job that includes one or more of those work roles. Some of those jobs are what you think of when you close your eyes and think of cybersecurity: a person in front of a monitor watching computer systems report activity and working with teams to understand that activity across their organization's network. The exciting thing about cybersecurity work is that it's not just one type - there is incredible variety in the field and new work types are being created all the time. If you are curious, love to learn and enjoy a growing industry, this is your field of work!

Cybersecurity work is found in every conceivable sector of government, academic and industry. Healthcare cybersecurity issues might include securing patient medical devices, operating room monitors and patient medical data storage and transmission. In the Finance sector, the cybersecurity team works to prevent breaches that could cause loss of funds for their customers. They also work to build security into the financial system. The automotive industry is just as concerned with driving security as with driving safely. Every sector is vulnerable to ransomware, where just one breached, networked computer can take the entire business down until the ransom is paid or a secured image is restored.



Therefore it is very useful for the job seeker to spend some time determining where they will target their job search. Some questions to consider include: Is there a particular industry or field that you are really interested in? Have you already had some professional experience that you could build on? Consider performing a personal assessment of your aptitude and attitude that will help you identify areas of cybersecurity work or sectors where you will find your best fit.

HOW TO RESEARCH CYBERSECURITY CAREERS

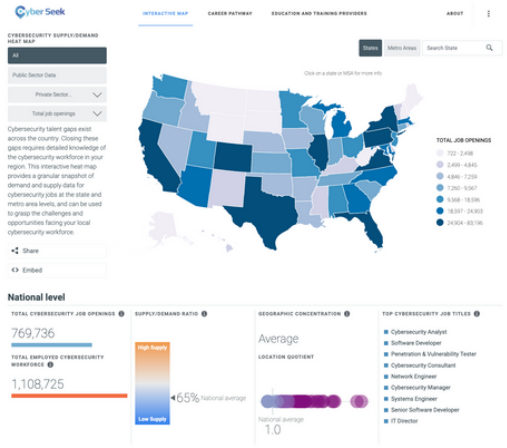
Here are some useful websites and webinars to review to help you refine your career search.

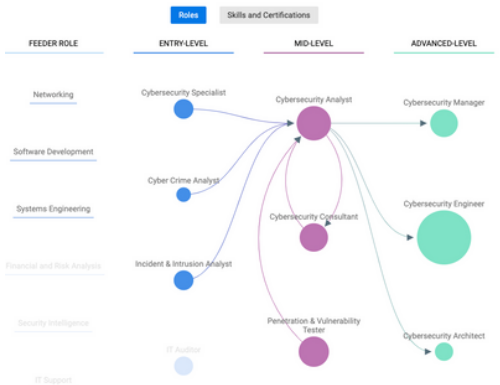
NICE Discovering Cybersecurity Careers site
https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/framework-focus

NICE Work Roles videos from Women in CyberSecurity (WiCyS)
https://www.youtube.com/c/WomeninCyberSecurityWiCySorg

NICE Webinars
https://www.nist.gov/itl/applied-cybersecurity/nice/events/webinars

CyberSeek.org
A "heat map" of cybersecurity jobs across the U.S. and a career pathways tool aligned to the NICE Workforce Framework





WHAT AREA OF CYBERSECURITY ARE YOU INTERESTED IN?

You should consider your existing skill set and knowledge. Have you already taken courses in cybersecurity or completed industry certifications? What job tasks or professional skills are you able to perform as a result of completing these programs?

Credit: U.S. Air Force

Were you in the military and did you perform cybersecurity-related tasks as part of your professional duties? If you are a transitioning member of the military, take a look at websites that will help you translate your military experience to civilian terminology.
For example, https://www.mynextmove.org/vets/.

NICE has more information and helpful links for Veterans at https://www.nist.gov/itl/applied-cybersecurity/nice/resources/veteran-resources. If you are still in the military, consider the DOD's SkillBridge program, only available to those still on active duty to aid in your transition to civilian life.

It is recommended that any job seeker review the work roles of the NICE Workforce Framework for Cybersecurity to home in on the best area(s) of cybersecurity work for your abilities and knowledge of today; or the areas you would like to move into (see earlier mention). One should also consider geographic regions where jobs are plentiful.

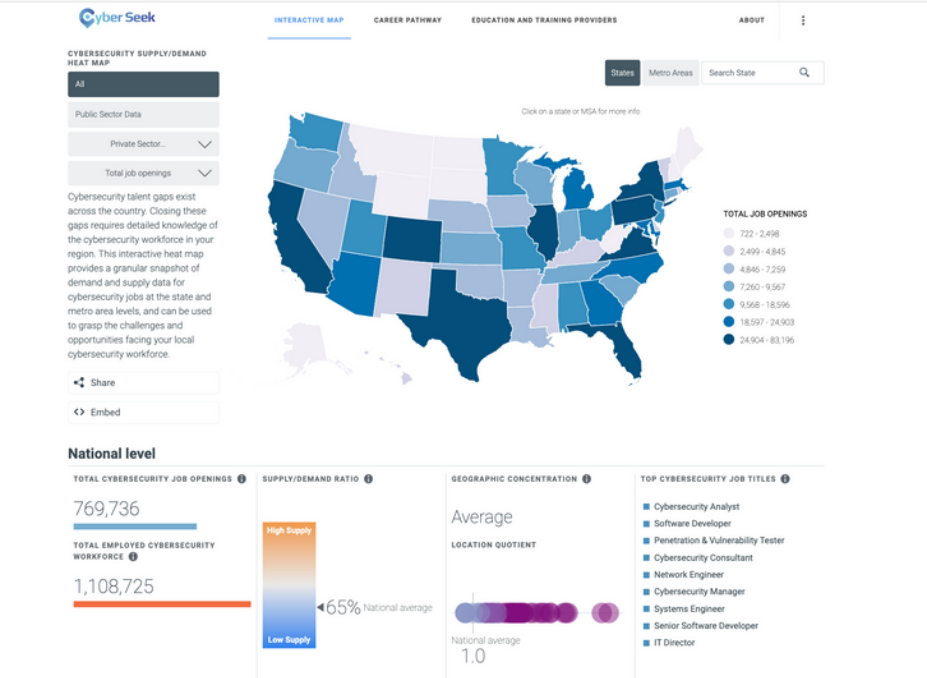
For this, CyberSeek's heat map shows where the highest number of job openings are to be found and what employers are looking for. You can also look at how jobs align with the NICE Framework. And you can find training and education partners in those regional locations too.

USING CYBERSEEK

The CyberSeek map of demand for cybersecurity talent in the United States, shows the most commonly sought titles include Cybersecurity Analyst, Software Developer, Cybersecurity Consultant and Penetration and Vulnerability Tester.

None of these are considered entry level or career entrant positions in cybersecurity. Looking at the Career Pathway tool, you will find information on how to enter pathways leading to those and other related roles.

With just the titles designated as Entry Level on CyberSeek, you'll see: Cybersecurity Specialist, Cyber Crime Analyst, Incident and Intrusion Analyst, IT Auditor. If you are interested in becoming a Cybersecurity Specialist, it's important to know when you go out to look at job boards or career sites, a Cybersecurity Specialist might be called by other names, like Information Security Specialist, Security Specialist, Information Technology Specialist or Operations Specialist. Typical requirements for these roles include a Bachelors (62%) and a few industry certifications.



CyberSeek.org as of November 4, 2022

REQUIREMENTS

You might see cybersecurity, computer science, information security, or other degrees required in the entry or early career cybersecurity job listings. You may be discouraged because perhaps you lack a college degree or your degree is in an unrelated field. Should you give up? Good news – many companies are reconsidering the importance of a degree in cybersecurity and emphasizing skills-based hiring initiatives. This does not mean that companies will stop valuing the importance of higher education but with such high demand for cybersecurity talent, there is a sense of urgency to reduce artificial barriers to talent. For more on skills-based hiring, see Business Roundtable's announcement of December 2021. It is increasingly common to see degrees listed as "nice to have" or "preferred" or absent in the listed requirements altogether. Our advice to the job seeker is to not worry about them and apply regardless!

Security Clearance Requirements

Do you have one now? If yes, state any active or current security clearances on your resumé. A new employer will need to sponsor you to maintain your clearance. If they are a US government contractor, they will be highly interested in you for your clearance, even if your cybersecurity skills aren't 100% of what they need, simply because the process to clear a new employee is so lengthy, averaging 155 days to get a Top Secret and 117 for a Secret level clearance.[1]

Could you qualify for one? Be familiar with the requirements for a security clearance and opt out of any position for which you would be rejected. More information can be found here: https://clearedjobs.net/security-clearance-faqs

Feeder Roles

If you are genuinely just getting started, you might need to get some first experience in an adjacent but related role, often referred to as a "feeder" role. You will see that term used on CyberSeek. To validate these career pathways, look at people currently in the field who have the position you are aiming for, and look at what position they held previously. Do not be disheartened by the steps you may need to take.

The feeder role will vary depending on which area of cybersecurity you are targeting to enter. Remember to build on your strengths: what is your current experience, skills, knowledge, abilities? Are you a people person with customer service experience? You might do well to aim for the IT help desk (which may require some certifications such as CompTIA's A+ and Network + or similar ones).

[1] https://news.clearancejobs.com/2022/04/26/how-long-does-it-take-to-get-a-security-clearance-q2-2022-update/

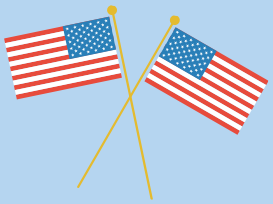
READING A JOB AD AND APPLYING FOR THE JOB

Most open positions are listed on job sites such as Indeed, Monster, GlassDoor. LinkedIn is a powerful site since you can connect directly with the hiring manager. Do not overlook the importance of company-based career websites too. They can give you an idea of the corporate culture and show you the companies in your desired geography. For example, if you were interested in working for a bank in your community, you may want to start making a list of all the banks with headquarters or major offices near you and then find out who their cybersecurity leaders are, using publicly available information. Much of this information is on their website (it will show where their offices are); on LinkedIn; and via public news announcements.

Find a job ad for a position you are interested in. Remember that it might not have been written by someone who works in cybersecurity. As a result, it might say "entry level" but then appear to require 5-10 years' of experience. Don't despair. There may be a lengthy list of desired professional certifications or programming languages. Focus on the skills the company is asking for. If you feel you fit the criteria for most of the required skills, apply. Remember, you can always offer to complete a missing certification or gain a skill within 6 months of taking the position if they truly need you to have it. Consider anything written as "desired" on the job description as something they want, not something they really require from the candidate.

Now, consider if you know anyone who works at that company. If so, contact them to let them know you have applied for the position. Ask them what they know about the position, the timeline for hiring, the team or the department. Let them know of your eagerness to be considered for the position.

APPLYING FOR A US GOVERNMENT JOB



Jobs in the US government in cybersecurity can be found on **USAJobs.gov** and at **CyberCareers.gov**. Applying for either is done at USAJobs.gov and there are some slight differences in applying for jobs with the Federal government. You will need to register for an account.

Please note that your Federal resumé will be different. For one, it can be longer, often four to six pages is quite common. You'll want to include many details that normally you would edit out for the private sector, such as quantified metrics about program successes and performance elements.

Reading a position description on USAJobs.gov can also be very different from the private sector. Note that all cybersecurity jobs get classified as 2210: Information Technology Management which is a very broad category of work. The job title may tell you very little about the actual role so be sure to pay close attention to the detailed requirements and duties to determine if the position is one you are interested in. It may also take a bit longer for someone to contact you as they will wait until the job announcement period closes before reviewing the candidate pool.

Try not to overlook government positions. The pay is becoming increasingly competitive, the benefits attractive and the work highly rewarding.

CREATING THE BEST RESUMÉ EVER

There is no such thing as the best resumé. In fact, you may need to create several versions of a resumé. If you are applying for government and private sector roles, those are two versions right there. If you are applying for roles that emphasize different skills, be sure you include those key words in the text on your resumé. Customization is key because employers use automation to screen the massive numbers of applications they receive for every open position. So from the start, create a first version of your resumé to showcase who you are and what you can do in cybersecurity.

Be brief. Use simple phrases with action verbs and where you can, include accomplishments with measured impacts. (Increased sales by 20%; drove efficiency by 35%, reduced waste by 75%, etc). Experience up top, education and courses below. Don't just list the classes you took. Your interviewer may not know what a 301 level class taught you. Be sure to focus on the skills or knowledge you gained.

Do not just list the classes you took. Include courses you took online or competitions you participated in and highlight what you learned. Review the NICE Framework where it describes knowledge, skills and task statements associated with cybersecurity work. Use those statements to identify what you know how to do.

Link to examples of your work, on GitHub, or a blog or a professional website. Are you active in professional organizations like OWASP, ISACA, ISC2, Girls Who Code, WiCyS, Women's Society of Cyberjutsu? If not, now is a great time to start and be sure to include them on your resumé. And note any leadership roles.

Career gaps – given the pandemic, these are not uncommon and should be addressed as simply as possible. It is not necessary to put these on the resumé but be prepared to discuss them in an interview if a gap of more than a few months exists.

Ask a career coach or trusted friend to review your resumé versions for typos or omissions or other issues. It is so easy to forget some accomplishment or activity that an employer might want to know about.

LINKEDIN

Be sure to spend time on LinkedIn making sure it's set up for job seeking. Use the settings to allow employers to find you by configuring the "Open to Work" feature (your current employer will not see that). Add an appropriately professional photo to your profile and choose a colorful banner image. Engage frequently and post content to keep your activity fresh; engagement keeps the LinkedIn algorithm happy. Prepare a statement for the top of your page describing the sort of position you are looking for.

Build your own network by connecting with people you know from school, previous jobs, military, training, co-workers, neighbors, friends, even relatives. Add or follow people in the industry, but do so naturally. If you attend a seminar or webinar, connect to the speaker and include a note to say you enjoyed their remarks. They will enjoy knowing they had an impact on someone.

Make sure your LinkedIn and other social media accounts do not include political or controversial opinions that might offend an employer.

COVER LETTERS AND NETWORKING

COVER LETTERS

Yes, Virginia, they still exist. Many employers still require a cover letter with your online application in addition to the resumé. This is your opportunity to shine – use it to explain any gaps in your work experience or why you are career switching or industry switching. Or why you think their company is the right one for you. Do your research and share something specific that shows you are a serious candidate. Share a specific personal anecdote about a skill of yours that is relevant to the job. If you are in a different city from the position, state your willingness to move. Don't repeat your resumé either. Keep it brief and upbeat and professional.

NETWORKING

It can't be stated enough how crucial networking is to finding a job. Yet for many of us, it's incredibly difficult. We envision awkward cocktail hours where we don't know anyone or worse, a group where month after month, it's the same few faces. In reality, networking can be done in myriad creative ways and we'd encourage you to break your internal barriers and try a few.

Join a professional organization or two. Earlier we mentioned some popular national and international organizations: OWASP, ISACA, ISC2, WiCyS, InfraGard, etc. Go to their websites, find the local chapter, and attend a meeting or online event. Each of them has a different focus and you can belong to as many or as few as make sense for you. Once you are a member, they often have job boards and hiring fairs as well as mentoring programs to help people train and prepare for new careers. And the networking is remarkable.

Lots of people are using LinkedIn to meet people at targeted companies. Let's say you've decided you want to work at this interesting company called NICE in your hometown. You can use LinkedIn to search the company name and find the people who work there. Not everyone will have a LinkedIn account but some will and some will accept your connection request. Now you can ask for an informational chat. Even a 15 minute call will help you get some information on the company. Even if the first person you chat with isn't in the department you're targeting, they might know someone who is. Or they might have some knowledge of new roles being created. That's networking.

College graduates: consider looking at your college or university's alumni directory. If you go to the alumni database of your school's website, you can search by employer. It might not be fully updated but it can be a helpful networking method as well.

Social media like Twitter can also help you spot where people work. Know who your local major employers are. Find the local Workforce Innovation and Opportunity Act (WIOA) funded job center. Look at the websites of these employers and visit the Careers section.

GETTING EXPERIENCE

How does someone gain cybersecurity experience, without having already had a first job in cybersecurity? There are several ways to do so and for any of these options, be sure to highlight them on your resumé:

- Certifications that include hands-on labs and skills assessments
- Conferences and professional organizations with training: BSide, WiCyS, Womens' Society of CyberJutsu are just a few examples.
- Build a home-based lab. There are books available with guidance on how to do this. There are community boards with guidance and comment threads on Reddit (https://www.reddit.com/r/homelab/). There are numerous online video tutorials and guides; review a few before committing to equipment and other materials. Document the labs you work on and what you learn as a result.

- Competitions: Capture the Flag (CTF), network-group hosted, collegiate, US CyberGames, and other competitions

- Volunteer work:
  - Offer to provide security awareness training for Scouts organizations
  - Local small business and organizations like churches need cybersecurity assessments

- Use the NIST Cybersecurity Framework as a guide
  - Projects at your current or previous employer
  - Ask an IT or cybersecurity colleague if you can join committees or project teams

- Network with current employer; ask to shadow the cybersecurity staff and ask questions

- Be willing to start in a related job like IT help desk (see Feeder Role on page 10) while you take courses, get certificates and build skills

INTERVIEW EXPERIENCE

You've been invited to interview for a position! **Congratulations!** Now what? First, do an internet search to see if anyone has shared interview tips for that company, because people do. Check GlassDoor for examples of interview questions, including the important technical questions common to cybersecurity. Also ask the recruiter or HR representative for information about the interview. Will it be an initial screening interview with HR or a panel interview with several participants, lasting several hours?

Do you have the name(s) of anyone who is interviewing you? Find out what you can about those people? Look them up on LinkedIn (don't connect with them yet – not appropriate), look where they went to school, what their previous roles were, do you know people in common, etc.

Research the company and their primary competition. How is the company doing? What are their strategic issues? What was last year like for them? Have they had a security breach? What is known about the causes? How is this year looking? What were their last few news releases about? Be able to talk about them at a high level. If they are publicly traded, this is very easy. Know who the CEO and President are.

Determine the interview location, find it online and determine how long it will take to get there with traffic. Plan to get there early. Bring printed copies of your resumé. Have a notepad and a pen with you.

ONLINE INTERVIEWING

Find a quiet location with a blank or simple wall behind you. Test your audio and video set up on your laptop in advance. Limit background noises. Try not to use big bulky headphones; if you can use basic headphones or even use the laptop's audio, it looks better. Make eye contact into the camera – You can put notes on a Word document that sits on screen just below the camera if that is helpful for you. Prepare some questions for the interviewers about the company, the role, day-to-day job responsibilities, the culture, etc.

In fact, don't be afraid to ask questions – about the company, about the job, about the priorities for the position. What are expected performance points within 30 days, 60 days, etc. Questions demonstrate your level of preparation and your interest in the position. Don't skip this step.

AFTER THE INTERVIEW

Write a thank you (by USPS or email) to each person you met or communicated with. If you interviewed in person, be sure to thank the administrative support person or security guard who escorted you as well. Be kind to all you engage with. Follow up after one week to ask what their expected timeframe for a next round or a decision is.

When you get an offer, review the terms with a trusted mentor (and your family), and note any deadlines for accepting the role. If you receive a rejection, remember to be gracious. Thank the interviewers for the opportunity to apply and to be considered for the position.

Hot tip! to manage the process create a tracking spreadsheet, including company name, contacts, emails, dates of interactions and all other information. Set calendar reminders for follow-ups.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

EXPLORE CYBERSECURITY CAREERS WITH NICE FRAMEWORK IN FOCUS INTERVIEWS

Some of the remarkable cybersecurity professionals you can learn about:

https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/framework-focus

NICE

NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION