



DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

RECOMMENDED SKILLS FOR A CYBERSECURITY CAREER

A GUIDE FOR PEOPLE INTERESTED IN STARTING A CAREER IN CYBERSECURITY

ISBN 978-973-0-37813-9

PROGRAM TITLE:
Building a Network and a Learning Platform for Raising the Level of Cybersecurity

PURPOSE OF THE PROGRAM:
Building a network of students, cybersecurity experts, and organizations
for analyzing the cybersecurity challenges and opportunities


International Visitor Leadership Program (IVLP)


Romanian Association for Information Security Assurance

A project developed by the Romanian Association for Information Security Assurance.
This project was funded in part by a grant from the United States Department of State.
The opinions, findings, and conclusions stated herein are those of the author[s]
and do not necessarily reflect those of the United States Department of State.

eBook: Recommended Skills for a Cybersecurity Career

Authors: Costel CIUCHI, Larisa GĂBUDEANU, Maria GHICA, Grațiela MĂGDĂLINOIU, Ioan-Cosmin MIHAI

Website: https://www.cyberclub.ro/skills-for-a-cybersecurity-career/

Version: 1

ISBN: 978-973-0-37813-9

DOI: 10.19107/Skills-4-Cybersecurity

Table of Contents

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

About this Guide

Year after year, the cyber talent gap is increasing — currently estimated to have 3,5 million open positions worldwide — presenting all sorts of headaches for leaders and the organizations they aim to protect. Moreover, organizations have a short window to identify, foster and hopefully retain a pipeline of emerging cybersecurity leaders to ensure the long-term sustainability and effectiveness of their security programs.

We will continue to see this gap increasing, as well as the urgency to explore new ways to attract more people to choose cybersecurity as their career choice. The cyberattacks demand countermeasures and illustrate why cybersecurity professionals are so important: the demand for skilled cybersecurity professionals has skyrocketed, creating a tremendous hiring landscape for tech-savvy professionals. As with any technical field, cybersecurity is fast-changing. Anyone who works in the area will need to be committed to keeping current with best practices and emerging industry trends and will always need to be learning and self-educating - both on and off the clock.

Years of experience in the field allow me to say that soft-side communications and leadership skills are profoundly lacking in the cybersecurity business. This has always been an issue in the technology field, but it is becoming more critical in business today because cybersecurity experts have to develop an ability to explain technical concepts in ways that business people understand: explain to top management what the risks are to the organization's profit and reputation if it is hit with a data breach.

While some of the skills penciled in this guide are ones you should naturally have — for example, an inclination for analytical thinking and technology — others are ones you will need to develop through formal training and education. While working closely with individuals in other roles and departments, it is essential to be able to effectively communicate and explain your findings, concerns, and solutions to others. It is essential to be able to speak clearly and concisely on cybersecurity strategy and policy and to convey technical information to individuals of different levels of technical comprehension.

Depending on your background, a certificate or degree in cybersecurity is a good place to start - providing you with a solid foundation in the principles of cybersecurity, in addition to a cybersecurity overview across a variety of platforms, programming and development, digital forensic investigation, specific technical skills, and more. The awe-inspiring guide and his authors provide insight into cybersecurity education and training essential to building a well-informed and competent workforce. I would go beyond diversity, as the lack of women in cybersecurity goes well before you get to the profession. We shall get more girls interested in the field in the early days of school and maintain that interest in high school and college.

A cybersecurity professional working in this crucial field cannot succeed without the help of a professional organization capable of providing the knowledge, the networking community, and the tools he/ she will need to succeed. This guide will deliver all of these and more. So read it today and get ready to face the cyber threats of tomorrow!

Liliana MUȘEȚAN

Head of Cybersecurity Unit

General Secretariat of the Council of European Union

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

PROS and CONS of Working in Cybersecurity

Cybersecurity activities involve the following:

SWIFT TRANSITION FROM IT

IT background can be a reasonable basis for learning cybersecurity, depending on the IT domain.

CONTINUOUS CHANGING ENVIRONMENT

Both in terms of new technologies and threats, techniques, and tactics against which to defend the organization.

DIVERSITY OF SPECIALISATION OPPORTUNITY

Given the vast landscape of cybersecurity activities, there is a large variety of cybersecurity specialization domains in which to specialize.

GLOBALIZATION OF CYBERSECURITY

Cybersecurity principles are similar worldwide; thus, a cybersecurity professional can work anywhere in the world.

INCREASING AUTOMATION

There is increased development of automation tools for repetitive tasks, which cybersecurity professionals must manage alongside repetitive manual tasks.

CONTINUOUS RESOURCE AND TRAINING NEEDS

Changing technology and threat landscape leads to the need for continuous training needs and continuous need for cybersecurity tool resources.

INCREASE AWARENESS AT THE MANAGEMENT LEVEL

Over the last few years, the management of various organizations has been more aware of cybersecurity threats, given the increased threat landscape in this field.

CYBERSECURITY GAPS

As per cybersecurity workforce reports, there is a wide gap of cybersecurity professionals worldwide, which leaves room for newcomers in this domain.

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

IT Technical Skills

Valuable IT technical skills for a cybersecurity career:

COMPUTER SYSTEMS
Knowledge of computer systems design, functions, and maintenance.

OPERATING SYSTEMS
Knowledge of operating systems design, structure, and security.

COMPUTER NETWORKS
Knowledge related to computer network design, installation, and maintenance.

SCRIPTING AND PROGRAMMING
Knowledge of developing tools and scripts to automate tasks in cybersecurity.

DATA ANALYSIS AND VISUALIZATION
The ability to collect, analyze, and present data clearly and effectively.

STATISTICAL ANALYSIS
The ability to use statistical techniques to identify trends or patterns.

RISK MANAGEMENT
Knowledge of identifying and evaluating potential cyber risks to an organization.

MACHINE LEARNING
Understanding machine learning algorithms to identify patterns or trends.

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Cybersecurity Skills

Advantageous skills in cybersecurity:

CYBERSECURITY STANDARDS AND LEGAL REQUIREMENTS

Knowledge of appropriate standards, best practices, and legal requirements based on the type of IT landscape and business processes addressed.

COMPUTER SYSTEMS AND NETWORKS SECURITY

Understanding the basics of computer systems and network security concepts and technologies.

CYBERSECURITY TOOLS

Knowledge of cybersecurity tools, their working methods, implementation, and maintenance.

VULNERABILITY ANALYSIS

Understanding the process of identifying and evaluating vulnerabilities and prioritizing their mitigation.

MALWARE AND CYBER THREATS ANALYSIS

Knowledge to analyze malware and understand cyber threats' tactics, techniques, and procedures.

INCIDENT RESPONDER

Knowledge to identify and respond to cybersecurity incidents, including incident analysis, consequence mitigation, and lessons learned.

CYBERSECURITY APPLICATIONS DEVELOPMENT

Knowledge of developing applications for cybersecurity, including security architecture and security-by-design processes on the development lifecycle.

CRYPTOGRAPHY

Knowledge of cryptography and securing data and communications in different business scenarios.

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Soft Skills

Recommended skills for better handling of various situations in cybersecurity:

PROFESSIONALISM
Being able to maintain confidentiality and always acting ethically.

METICULOUSNESS
Being detail-oriented to identify and address potential security threats.

COMMUNICATION SKILLS
Being able to communicate effectively with coworkers, supervisors, and clients.

TIME MANAGEMENT SKILLS
Being able to deal with multiple tasks and priorities at once.

ORGANIZATIONAL SKILLS
Keeping track of a large amount of information and staying organized.

ADAPTABILITY
Being able to adapt to new technologies and techniques.

RESILIENCE
Being able to face high levels of stress and long work hours.

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Management Skills

Valuable skills for leading and managing teams, projects, or initiatives:

LEADERSHIP
The ability to develop and execute plans for projects and initiatives.

COACHING
The ability to teach and guide in achieving goals and improving performance.

PLANNING AND ORGANIZING
The ability to lead and motivate teams to achieve common goals.

RESOURCE MANAGEMENT
The ability to effectively manage resources, including budgets and personnel.

DECISION-MAKING
The ability to make effective decisions in complex and rapidly changing situations.

DELEGATION
The ability to assign tasks and responsibilities to others.

CONFLICT RESOLUTION
The ability to effectively resolve conflicts and disputes.

FLEXIBILITY
The ability to adapt and respond to changes in technology and business needs.

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Examples of Certifications

Beneficial certification for a cybersecurity career:

Certified Ethical Hacker (CEH)

It demonstrates an understanding of the latest hacking tools, methodologies, and techniques used to hack an organization lawfully. This certification is helpful for ethical hacking and vulnerability identification/management professionals.

Certified Network Defender (CND)

It focuses on creating network administrators trained in protecting, detecting, and responding to threats on the network. This certification is helpful for network security operations, secure application architecture, and management professionals.

Certified Information Systems Auditor (CISA)

It demonstrates the capacity to audit, control, monitor, and assess an organization's information technology and business systems. This certification is helpful for cybersecurity auditors and management professionals.

Certified Information Security Manager (CISM)

It proves the expertise in information security governance, program development, risk, and incident management. This certification is helpful for secure application architecture, software development, and risk management professionals.

Certified Incident Handler (CIH)

It demonstrates knowledge about incident identification, containment, and response. This certification is helpful for SOC analysis, incident containment, and response professionals.

Cloud Security Certification (CCSP)

It demonstrates knowledge about cloud computing and approaches for securing its use within an organization. This certification is helpful for secure application architecture, software development, and risk management professionals.

Certified Information Systems Security Professional (CISSP)

It certifies the capacity to design, implement, and manage a cybersecurity program effectively. This certification is helpful for mid-level cybersecurity management, secure application architecture, and software development professionals.

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Cybersecurity Activities

Types of activities in cybersecurity based on the NIST NICE framework:

ANALYZE

(e.g., threat intelligence analysis, vulnerability identification, ethical hacking)
Performing specialized reviews of relevant cybersecurity information such as vulnerabilities, exploitation, and other types of threat intelligence.

COLLECT AND OPERATE

(e.g., junior soc analysis, senior soc analysis)
Collecting and analyzing information within the organization to identify potential cyber threats.

INVESTIGATE

(e.g., forensic investigator)
Analyzing events and data related to IT systems and networks to identify evidence of cyber-attacks and cybercrime.

OPERATE AND MAINTAIN

(e.g., network security operations, IT system security operations)
Providing support, management, and procedures to ensure security specifics are correctly implemented and maintained.

OVERSEE AND GOVERN

(e.g., cybersecurity management, consulting)
Providing governance, oversight, direction, and management for the cybersecurity program within an organization.

PROTECT AND DEFEND

(e.g., vulnerability management, incident containment, and response)
Identifying, analyzing, and mitigating cyber threats to IT systems and networks of the organization.

SECURELY PROVISION

(e.g., secure application architecture, cyber risk management)
Designing and providing security specifications for various IT systems and computer networks.

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Cybersecurity Workforce Frameworks

Main international frameworks for competencies, skills, and profiles in cybersecurity:

U.S. NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) CYBERSECURITY WORKFORCE FRAMEWORK

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology in the U.S. Department of Commerce, is a partnership between the government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The NICE Workforce Framework for Cybersecurity establishes a common language to describe and share information about cybersecurity work. It is used by various learners (students, job seekers, employees), organizations, companies, and the government to help promote careers, define jobs, recruit staff, and develop their workforce.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

More information: https://nist.gov/nice

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

The European Cybersecurity Skills Framework (ECSF) is the result of the joint effort of ENISA and the ENISA Ad-hoc working group on Cybersecurity Skills Framework. The ECSF role profiles document lists the 12 typical cybersecurity professional role profiles along with their identified titles, missions, tasks, skills, knowledge, and competencies. The main purpose of this framework is to create a common understanding between individuals, employers, and providers of learning programs across EU Member States. It represents support for the identification of a critical skill set required from a workforce perspective. It enables learning providers to support the development of this set and policymakers to support the targeted initiatives and mitigate identified skills gaps.

More information: https://www.enisa.europa.eu/

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Tips and Tricks

Activities that can help cybersecurity newcomers to specialize in certain aspects of cybersecurity include:

CYBERSECURITY ASSOCIATIONS

Joining a cybersecurity professional organization in a specific country or globally in the cybersecurity area of your interest.

CONTRIBUTE TO THE CYBERSECURITY COMMUNITY

Sharing your experience and volunteering in projects for the community is helpful for networking and learning new things.

LEARN BY TEACHING

Learning and sharing knowledge and best practices can help understand a topic more deeply.

INTERACTIVE SKILL DEVELOPMENT

User-interactive tools such as cyber ranges, CFTs, and other labs can help with hands-on experience.

CYBERSECURITY EVENTS

Given the globalization of cybersecurity, in-person and online events can be attended worldwide.

CYBERSECURITY IS EMBEDDED IN IT ACTIVITIES

IT activities in certain roles include specific cybersecurity operations and management activities that can help transition into cybersecurity.

DAILY ROUTINE

Staying up to date with the cybersecurity news regarding the latest cyber threats, vulnerabilities, and tools.

CERTIFICATIONS

There are specific entry-level certifications for general cybersecurity topics or more specialized areas of cybersecurity that can help with knowledge gathering.

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Authors

Costel CIUCHI, Ph.D., is a cybersecurity professional with significant experience developing public administration apps/infrastructures. He is a senior expert in the IT Directorate, General Secretariat of the Government (InfoSec, cybersecurity, interoperability), an external expert for the European Union Agency for Cybersecurity (ENISA), and an Associate Professor at the University Politehnica of Bucharest; he conducts research activities in cybersecurity, decision-making, and risk management.

Larisa GĂBUDEANU is a cybersecurity and data protection expert and a Ph.D. candidate at Babeș-Bolyai University. She has extensive experience in cybersecurity and data protection in a regional banking group, alongside her academic background in such domains. She also has a vast experience as a lawyer in an international law firm, counseling international clients and coordinating projects related to IT law and data protection matters.

Maria GHICA, a University College London IT and Business Masters in Science graduate, is currently supporting and advising The Director of the Romanian National Cyber Security Directorate in defining and designing the cyber security operational and support processes, procedures, infrastructure, and organizational aspects, as well as drafting national and international cyber-related policies, guidelines and legal and regulatory initiatives, and is involved in multiple European-level cyber projects.

Grațiela MĂGDĂLINOIU is a cybersecurity and data privacy professional with a broad experience in advisory and business ethics and compliance. She has been leading the Romania Chapter of the Information Systems Audit and Control Association (ISACA) for several years, aiming to grow the local professional community, build reliable solid, long-term relationships with regulatory and academic institutions, and partner with other professional associations.

Ioan-Cosmin MIHAI, Ph.D., is a researcher and trainer with an experience of more than 18 years in cybercrime, cybersecurity, and open-source intelligence. He is a cybercrime training officer at the European Union Agency for Law Enforcement Training, an external expert for the European Union Agency for Cybersecurity, an associate professor at the Romanian Police Academy, and founder and vice-president of the Romanian Association for Information Security Assurance.

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Romanian Association for Information Security Assurance

The Romanian Association for Information Security Assurance (RAISA) is a professional, non-governmental, non-partisan political, nonprofit, and public benefit association founded in 2012. It aims to promote and support information security activities in compliance with applicable laws and to create a community for exchanging knowledge between experts.

Website: https://www.raisa.org

REPRESENTATIVE PROJECTS

CyberCon Romania

CyberCon Romania Conference focuses on cybersecurity's latest trends, challenges, and future strategic directions. It brings relevant experts from public institutions, private companies, universities, and NGOs to raise awareness, strengthen the cybersecurity culture, and share best practices in fighting cybercrime.

Website: https://www.cybercon.ro

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

The International Conference on Cybersecurity and Cybercrime (IC3) aims to encourage the exchange of ideas about the evolution of cyberspace, information security challenges, and new facets of cybercrime. The event started in 2014 as an initiative to provide the appropriate framework for students to present their research in this field.

Website: https://proceedings.cybercon.ro

International Journal of Information Security and Cybercrime

The International Journal of Information Security and Cybercrime (IJISC) is a scientific peer-reviewed journal founded in 2012 and indexed in international databases. The scientific journal aims to bring together the latest research and development in information security and the latest methods to prevent and combat cybercrime.

Website: https://www.ijisc.com

ISBN: 978-973-0-37813-9, DOI: 10.19107/SKILLS-4-CYBERSECURITY

Recommended Skills for a Cybersecurity Career