LESSON 4.1 - CYBERSECURITY CAREERS

INTRODUCTION

Within the previous modules, we showcased some mechanisms, related to securing ourselves, against common vulnerabilities and have discussed the variety methods for the exploitation of those vulnerabilities. All of this serves as an example of the multi-disciplinary nature of the field of cybersecurity, which deals not only with the interoperability and functionalities of internet-connected devices, but how we as people interact with those devices, how our lives are influenced by technology and information and how our vulnerabilities as people, could be transferred to the digital world.

The field of cybersecurity combines knowledge domains and disciplines such as computer science, technology, engineering, mathematics, but also social sciences, psychology, sociology and law. Notably, cybersecurity provides a vast plethora of career paths, opportunities and very well-rewarded positions.

Currently, while faced with a shortage of qualified professionals in the field, it is speculated that one of the reasons behind this could be the **lack of awareness and adequate information about the diversity of career opportunities within the sector**. A rather unfortunate tendency, which results in disinterest in pursuing further education or career in the field, misinformation about jobs opportunities, stereotypes about professionals in the field and leaves a sector, full of opportunities and excitement, in a shortage of specialists.

Likewise, due to the rapid development of the technological backdrop against which cybersecurity functions, research in the field of cyber workforce is still catching up to a common understanding of what a successful cybersecurity professional within the various career profiles in cybersecurity should possess in terms of skills, competences and social profile. Although the field is still “young”, the cybersecurity community has reached a stage in its maturity making it capable of forecasting the future demand for the cybersecurity workforce (Department of Homeland Security, 2014).

This lesson will summarize information, related to the skills, competences and career profiles, relevant to the cybersecurity profession in to attempt to fill in the gaps within the common understanding about the careers in the field. We begin by exploring the place of the cybersecurity professional within today’s societal ecosystem, with a particular emphasis on the social value of cybersecurity. Additionally, we present some of the areas of economy, impacted by cybersecurity. Equally important, we continue with a dive into the security job profiles, skills and

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.
This publication reflects the views of its authors only, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

competences. Here, we put a special focus on the ESCO (European Skills, Competences, Qualifications and Occupations) Skills and Occupations, as well as on the e-CF (European e-Competence Framework) role profiles, with relation to cybersecurity. We conclude with examples and case studies to spark your curiosity and equally important, to increase your confidence to speak to your students about the opportunities in the field of cybersecurity.

In this lesson, we limit our scope predominantly on civilian cybersecurity career profiles and will not discuss military cybersecurity professional paths.

Photo 1 qimono from Pixabay (www.pixabay.com)

CYBERSECURITY AND SOCIETY

The inevitable ubiquity of technology nowadays has resulted in cybersecurity being a paramount in our society. Just think about all the data we and our children transfer on a day-to-day basis over various mobile applications, over e-mail, through the usage of software products, over social media or just through using our favorite browser of choice. With the click of a button, we are able to transfer information to all corners of the world, however this information transfer could be intercepted, hijacked, leaked, exploited and abused.

This is valid both for personal information, as well as for information on a government level, institutional level, with different levels of sensitivity and varying levels of privacy and potential impact on society. Even the latest technologies, such as e-banking or e-commerce, along with cloud storage and cloud computing are vulnerable and our information and our state's information depends on well-trained and highly qualified cybersecurity experts to protect. Since all technologies are used to transfer personal information, or information with different levels of sensitivity, securing those technologies has become of an utmost importance for our ability to live normal lives and being able to function in society.

Digital dependency has resulted over the past few years in an ever-increasing need for protecting our lives against cyber-crimes and data leakage along the neverstopping technological advancement. Cybercrime and cyber harassment have taken a huge toll on society thus far as cybersecurity is reported to have become the primary medium for terrorism (Wenke & Rotoloni, 2016) and economical exploitation (Europol, 2018) against which only cybersecurity and personal awareness on cybersecurity issues and prevention tactics stand.

Again through the 2018 Europol report, it is evident that the Islamic State's (IS) loss of territory from 2016 to 2017 did not equate to a loss of authority among its followers or a manifest decrease in its ability to inspire attacks. Instead, the group continues to use the internet to promote its doctrine and inspire acts of terrorism. In many ways, military defeat has made the internet even more important for the IS; the difference being that it has since shifted from using it to support its state-building ambitions toward inspiring and attempting to direct terrorist attacks in the West.

In their report on cybercrime from 2018, Europol warns us against financially motivated malware attacks as a threat that is expected to continue and even increase double-fold within the following two years. Along with illegal acquisition of data, following ignorant user behavior or data breaches in different organizational layers of society, identity theft reports continue to be on the rise with ever increasing consequences and personal implications. Take as an example the biggest data breach reported in 2017, concerning the company Equifax, which affected more than 100 million credit users worldwide. With the EU GDPR coming into effect in May 2018, the reporting of data breaches is now a legal requirement across the EU, bringing with it hefty fines and new threats and challenges.

The rise of cybercrime has led the European Union to recognize cybersecurity as one of its core values, resulting in multiple EC supported cybersecurity-related initiatives (more information here).

Cybersecurity is a profession which holds a tremendous value for society. Cybersecurity professionals, with their different job profiles and areas of expertise, help people, much like doctors, police officers or lawyers, to keep our society physically and mentally healthy, safe and secure in their day-to day life. Cybersecurity professionals help fight against, sometimes very gruesome and obscene crimes, for instance they help fight against Child Sexual Exploitation (CSE).

Again from the 2018 Europol report, it is evident that the amount of detected online Child Sexual Exploitation Material (CSEM), including Self-Generated Explicit Material (SGEM), continues to increase. As raising numbers of young children have access to internet and social media platforms, the risk of online sexual coercion and extortion continues to rise. The popularity of social media applications with embedded streaming possibilities has resulted in a strong increase in the amount of SGEM live streamed on these platforms.

There are many attack vectors and cybersecurity professionals act against them by raising public awareness and helping to increase the overall quality of society's cybersecurity habits. They help track down abusers, take down content, find and provide support to the victims and help the mitigation and prevention of such crimes.

With the maturity of the technological development, against the backdrop of which we extremely increase our use of the Internet and generate huge amounts of sensitive data, the social value of cybersecurity is expected to raise even further in the foreseeable future. Cybersecurity and security professionals continue to develop in sophistication and efficiency and the opportunities for life-long learning and development within the sector are ever-increasing, as well as the cases of value-driven professionals entering the field.

AREAS COVERED BY CYBERSECURITY

Companies nowadays appoint dedicated person or a team of people to ensure their overall cybersecurity posture. Such instance might be a general data protection policy, or a disaster recovery planning, which include risk assessment, recovery strategies and priority assignment. It is no longer acceptable to think that cybersecurity is a luxury and a privilege of only larger companies and that cybersecurity requires only a technical background. As seen from the example above, cybersecurity specialists, depending on their job profile, could also be in need of a good grasp on legal matters, current legislations, organizational policies and much others. Furthermore, any business, academic institution or government structure must have a concrete plan of action to protect, store, process, analyze, delete, manage data or recover after a security breach or disaster. Cybersecurity is now both a business and a personal priority not just an IT issue.

One of the greatest threats against an organization of any kind, be it industrial, academic or governmental is the possible failure of the so called “critical infrastructures”. Critical infrastructures are systems, or assets, are those infrastructures or assets, the failure or the incapacity of which, could have a debilitating impact on an organizations’ functions, as well as economic consequences or even pose a threat to the national security. Another very appetizing domain for cyber-attacks, where cybersecurity is of utmost importance is, of course, the financial sector. Cybersecurity professionals are much needed in the financial sector, where attacks are exponentially increasing, as well as the risks of the exploitation of potential vulnerabilities. We manage our money online – we use online banking platforms and applications to avoid going to the physical bank and do them. By being negligent, a user with malware on their device, could compromise its own financial security, but also, worst case scenario, in a case of a lack of adequate cybersecurity infrastructure, could penetrate the financial service´s network.

Same thing goes for insurance companies, state agencies, educational and academic units and many more.

In all domains of today’s society, the need for global cybersecurity awareness and increase of common knowledge has emerged. There are is no question that the global scope of the technological advancement, enabled through the Internet, will require a global effort to ensure its cybersecurity posture, however the first step after increasing our own personal awareness on cybersecurity issues and basic cyber hygiene, is to encourage locally cybersecurity professionals and represent the cybersecurity profession objectively. And the objective representation of a cybersecurity professional is not a “lonely hacker in a basement”, but a much needed professional, working in a multi-faceted discipline, requiring a wide spectrum of competences, skills and qualifications. Let’s give a few examples on that.

EXAMPLES OF AREAS TO WORK IN: HEALTHCARE SYSTEMS

One such example is the healthcare system. When we think of cybersecurity we either think of our personal protection and safety and the protection of our personal data or our organization’s sensitive documents. However, healthcare is actually among the most vulnerable targets for cyberattacks. This happens for several reasons, however the most likely are:

- The amount of personal data and sensitive information which is being managed in hospital and healthcare data bases, repositories and systems.
- A small IT department with limited expertise in cybersecurity or a lack of a cybersecurity expert in the IT teams.
- Limited budget flexibility, especially when it comes to state healthcare systems, which does not allow for carrying our cybersecurity audits or reinforcing the existing infrastructures, or training the IT department or the administration.

You have to remember that we are not talking only about big healthcare systems, but also about small private hospitals, hospitals in small cities, laboratories and others. Cybersecurity plays a huge role in a system like this, as well as the lack thereof.

Recent reports, such as this one from 2018 by Symantec, shows that cyber-attacks against healthcare units and systems have increased dramatically, throughout the past few years. This means not only a risk to our personal data and privacy. A cyberattack against a hospital infrastructure, for instance, might target IoT equipment, which tracks a patient's condition, or disrupt a robotically-assisted surgery. Increasingly more, IoT devices enter our healthcare. Such are the HVAC systems or medical devices. Those devices are often easier to attack and even more frighteningly, are often connected to the hospital's main network, which means that they could even serve as a gateway for a more sophisticated attack. Even destabilizing medical devices, without attacking through them the entire hospital infrastructure, could have devastating consequences. Attacking a medical device could kill a patient or worsen their condition. This article from the healthcare business tech[1] goes into more details about device attack in healthcare.

A mass cyber-attack against a hospital infrastructure might be supply chain attacks, with potentially lethal consequences. This is a big reason behind why some healthcare units nowadays require their vendors to have a sound cybersecurity plan.

So far, one of the most common attacks against healthcare systems remains the ransomware attack, due to the attractiveness of the data, which is processed in healthcare systems.

EXAMPLES OF AREAS TO WORK IN: INDUSTRIA AND CRITICAL INFRASTRUCTURES

A SCADA (Supervisory Control and Data Acquisition) system is most commonly defined as a control system architecture, which uses sensors, microcontrollers, networked data communications and graphical user interfaces for process management, nut also uses other peripheral devices, such as programmable logic controller (PLC) and discrete PID controllers to interface with the process plant or machinery[2]. The use of SCADA systems has been also considered for management and operations of project-driven-process in construction. (Antunes & Poshdar, 2018).

[1] http://www.healthcarebusinesstech.com/medical-device-cybersecurity/

[2] https://en.wikipedia.org/wiki/SCADA#cite_note-Antunes2018-1

Source: afcyber.af.mil

A very famous attack against a SCADA system is the 2010 Stuxnet attack against Iran's nuclear plant. Stuxnet by itself is a malicious cyber worm, which targeted specifically the PLCs of the Iranian nuclear plant that controlled machinery and industrial equipment, including centrifuges, used to separate nuclear material. Long story short, this worm attacked the centrifuges of the Iranian nuclear plant, causing the fast-spinning centrifuges to tear themselves apart, ruining almost one fifth of the nuclear centrifuges. More about the Stuxnet attack is available here[3].

We all can imagine the danger of a physical disruption in a nuclear plant and what devastating consequences it could bring. And this sort of damage could be done through a cyber-attack, which only showcases the importance on a global level to decrease the shortage of qualified cybersecurity professionals and to encourage careers in cybersecurity.

Another area, which is highly dependent on cybersecurity is transportation. Consider airport and flight security or oil tankers and platforms security. In their white paper on Research and Innovation in Cybersecurity from 2019, AEGIS[4] point out that a general concern for the maritime domain is that infrastructure and transportation are not up-to-date in terms of security protection. The lifetime of a modern vessel is about 25-30 years, but there are a lot of non-modern vessels out there over 30 years old that are often not updated with the latest technologies. Additionally, they often have devices with poor security.

In the context of IoT, the importance of adequate cybersecurity protection becomes even more evident, as a lot of the transportation systems, including airport systems, rely on modern technology to identify passengers and to protect the IT infrastructures on board. The transportation sector's navigation systems

[3] https://en.wikipedia.org/wiki/Stuxnet

[4] http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-White-Paper-on-Research-and-Innovation-in-Cybersecurity.pdf

often rely on modern technologies as well, which could be compromised through cyber-attacks.

Again from the from 2019, AEGIS[5] white paper: “For example, there are serious potential consequences if cyber-attacks target the container tracking software used by ports or navigation systems. There is a risk to life and property if such attacks cause vessel collisions. Even without collisions, systematic delays would cause finance and transportation issues, which in turn could create an impact worldwide on commerce activities. Likewise, attacker threat groups specialized in business email compromise (BEC) and business email spoofing (BES) fraud target maritime shipping firms resulting in millions of dollars stolen on an annual basis.”

DIFFERENT PROFILES FOR DIFFERENT KNOWLEDGE AREAS

There are many references in the labor market when talking on occupations, jobs, profiles and skills. We have preferred using the most standard references such as ESCO, the new EU labor classification, e-CF or European Standard 16234 and the ONET portal of USA. As an introduction, we should clarify some basic concepts:

- We have adopted the definition of occupation by ESCO[6], which also clarifies the idea of job: “An occupation is a grouping of jobs involving similar tasks and which require a similar skill set. Occupations should not be confused with jobs or job titles. While a job is bound to a specific work context and executed by one person, occupations group jobs by common characteristics”.
- It is possible to define an occupational profile for each occupation (as it is possible to define a profile for a specific job). In the case of ESCO, the profiles contain an explanation of the occupation in the form of description, alternative names, they list the knowledge, skills and competences that experts considered relevant terminology for this occupation on a European scale.

The following is the list occupation from the ESCO portal[7], each one with name, description and main tasks.

- Chief ICT security officer: protect company and employee information against unauthorized access. They also define the Information System security policy, manage security deployment across all Information Systems and ensure the provision of information availability. They are also known as CISO, as alternative name.

[5] http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-White-Paper-on-Research-and-Innovation-in-Cybersecurity.pdf

[6] https://ec.europa.eu/esco/portal/escopedia/Occupation

[7] https://ec.europa.eu/esco/portal/occupation

- ICT Security Manager: ICT security managers propose and implement necessary security updates. They advise, support, inform and provide training and security awareness and take direct action on all or part of a network or system
- ICT auditor manager: ICT auditor managers monitor ICT auditors responsible for auditing information systems, platforms, and operating procedures in accordance with established corporate standards for efficiency, accuracy and security. They evaluate ICT infrastructure in terms of risk to the organization and establish controls to mitigate loss. They determine and recommend improvements in the current risk management controls and in the implementation of system changes or upgrades.
- ICT resilience manager: ICT resilience managers research, plan and develop models, policies, methods, techniques and tools that enhance an organization's cyber security, resilience and disaster recovery.
- ICT security technician: ICT security technicians propose and implement necessary security updates and measures whenever is required. They advise, support, inform and provide training and security awareness.
- ICT security consultant: ICT security consultants advise and implement solutions to control access to data and programs. They promote a safe exchange of information.
- ICT security administrator: ICT security administrators plan and carry out security measures to protect information and data from unauthorized access, deliberate attack, theft and corruption.
- Ethical hacker: Ethical hackers perform security vulnerability assessments and penetration tests in accordance with industry-accepted methods and protocols. They analyze systems for potential vulnerabilities that may result from improper system configuration, hardware or software flaws, or operational weaknesses.
- IT auditor: IT auditors perform audits of information systems, platforms, and operating procedures in accordance with established corporate standards for efficiency, accuracy and security. They evaluate ICT infrastructure in terms of risk to the organization and establish controls to mitigate loss. They determine and recommend improvements in the current risk management controls and in the implementation of system changes or upgrades.

We can add another occupation profile from ONET portal[8], the US public database of occupational information:

- Information Security Analyst: Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses.

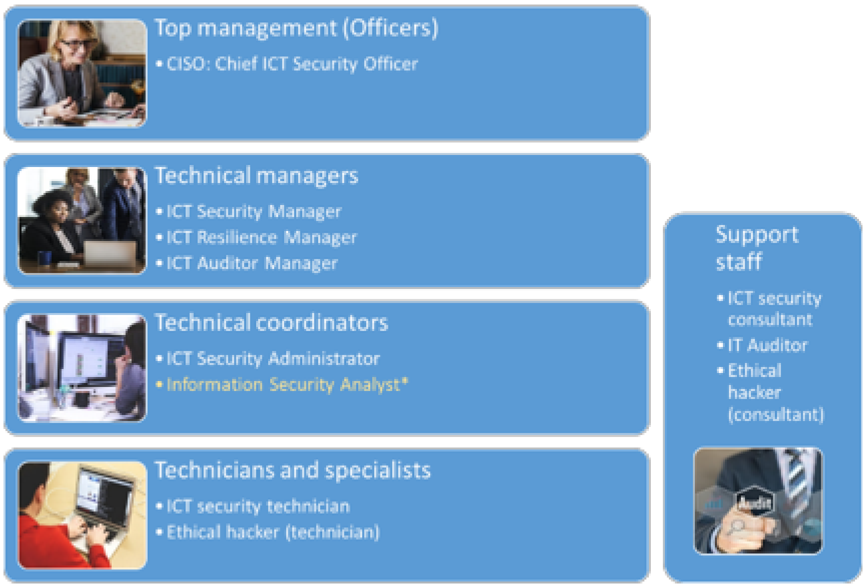
[8] https://www.onetonline.org/

SKILLS REQUIRED

Regarding the required skills for these occupations, the commonest ones are the following ones:

- I mplement ICT risk management: develop and implement procedures for identifying, assessing, treating and mitigating ICT risks, such as hacks or data leaks, according to the company's risk strategy, procedures and policies. Analyze and manage security risks and incidents. Recommend measures to improve digital security strategy.
- Manage IT security compliances: guide application and fulfilment of relevant industry standards, best practices and legal requirements for information security.

- Manage disaster recovery plans: prepare, test and execute, when necessary, a plan of action to retrieve or compensate lost information system data.Execute ICT audits: organize and execute audits in order to evaluate ICT systems, compliance of components of systems, information processing systems and information security. Identify and collect potential critical issues and recommend solutions based on required standards and solutions.
- Identify ICT system weaknesses: analyze the system and network architecture, hardware and software components and data in order to identify weaknesses and vulnerability to intrusions or attacks.


Top management (Officers)
• CISO: Chief ICT Security Officer
Technical managers
• ICT Security Manager
• ICT Resilience Manager
• ICT Auditor Manager
Technical coordinators
• ICT Security Administrator
• Information Security Analyst*
Technicians and specialists
• ICT security technician
• Ethical hacker (technician)
Support staff
• ICT security consultant
• IT Auditor
• Ethical hacker (consultant)
Audit

While the above list represents identified occupations, the possibilities of working in cybersecurity is not restricted to working in exactly those occupations. Specific jobs in specific companies are not always perfectly matching an official occupation but embraces a set of roles to be developed, frequently in flexible way, within the activities of a job. A role is the part that is played within a specific work process within an organization. For example, ICT system administrators, which administer configuration and resources of systems and ICT infrastructure, may play a role of cybersecurity specialist as part of their job as ICT as they need to evaluate risks or implement security techniques on all or part of a network or system within their area of responsibility.

Many jobs and even occupations which are not full-time devoted to cybersecurity frequently requires that the corresponding professionals play roles connected to IT security. In our research on ESCO, we have also found out some occupations that also include tasks and skills related security skills as they frequently require playing specific roles in the area. Some typical examples of such occupations are the following: ICT system administrator, Webmaster, ICT network engineer, digital forensics expert, ICT capacity planner ICT application developer, database administrator, ICT disaster recovery analyst, etc.

Referred to role profiles, we can review the European e-Competence Framework (e-CF)[9] which is a specific reference of 40 competences applicable to the Information and Communication Technology (ICT) workplace published officially as the European Norm EN 16234-1 by CEN. Its related document CWA 16458-1:2018 defines 30 ICT Professional Role Profiles performed by ICT Professionals in any organization, using the e-CF as the basis for competence identification[10]. The two directly related to cybersecurity are the following ones:

- Cyber Security Manager: defines the digital security strategy and manages implementation across the organization. Embeds proactive cyber security protection by assessing, informing, alerting and educating the entire organization.
- Cyber Security Specialist: defines, proposes and implements necessary cyber security technique and practices in compliance with security policy and regulation. Contributes to security practices, awareness and compliance by providing advice, support, information and training.

The figure is aimed at representing a summary diagram of these occupations (not the roles) showing hierarchical level and specialization/transversal scope. One can realize that the “ethical hacker” occupation has been placed in two segments, as consultant and as technician.

CYBERSECURITY CAREERS

Cybersecurity careers are varied and very different in nature. They involve teams of different types of professionals and have a rich social part because cybersecurity professionals must understand the needs of users, whether they are citizens or companies in any sector.

The most known career is Ethical hacker although media have not created a fair image of the tasks carried out by these professionals. Movies, books, the

[9] http://www.ecompetences.eu/

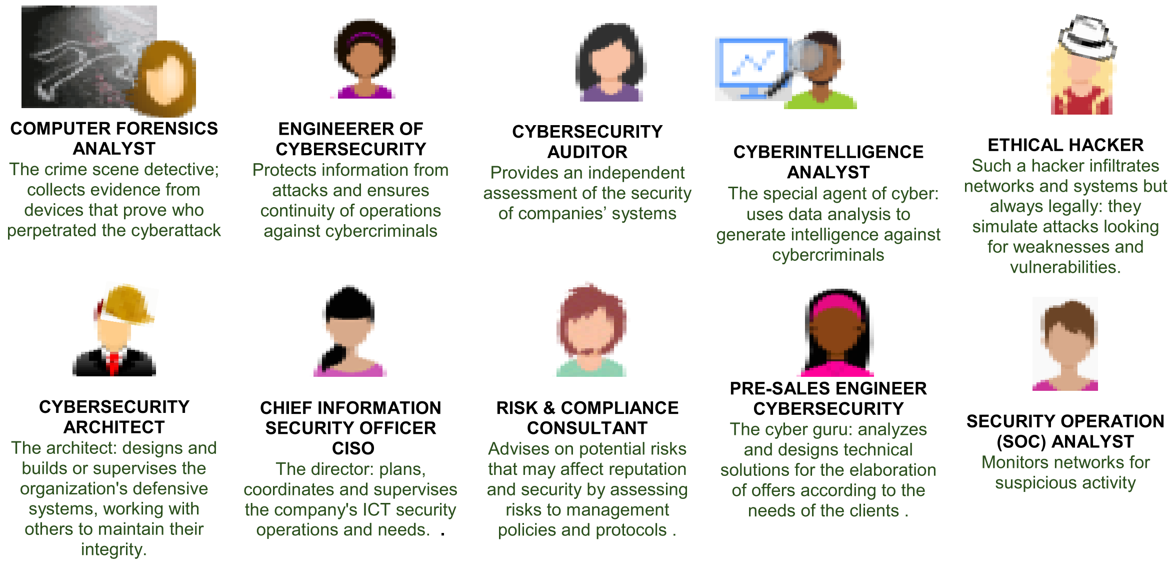
[10] ftp://ftp.cencenelec.eu/CEN/WhatWeDo/Fields/ICT/eEducation/WS/eSkills/ICTSkills/CWA%2016458-1_2018.pdf

newspapers, etc. draw hackers between the line of good and evil and, too often, closer to breaking the law than doing good. Nothing to do with reality, where standards and normative define and regulate their activities and where ethics (hence its name) plays a fundamental role.

Cybersecurity is a fairly new professional area and is therefore under development and expansion. That is why, there are many other careers and only a few know about them. In addition, as technology is now everywhere, cybersecurity professionals work in every sector:

- Industry and environment: cyber-resilient systems for critical infrastructures, ICS/SCADA security, protection of intelligent industrial networks and Smart Grids
- Transport and communications: protection of intelligent cars, security and protection of drones and satellite communication systems.
- Finance and insurance: fraud detection in banking and insurance, SIEM (Security Information Event Management)
- Health and pharmacy: protection of ehealth devices (IoT), encryption of health research information, secure storing of health data record.
- Education: cyber-education, cybersecurity labs.
- Defense and eGovernment: cyber-intelligence, cyber-defense and incidents simulation.

This makes cybersecurity a profession in which, depending on the occupation, very different tasks can be performed. From ethical hackers testing and exploiting network vulnerabilities, to consultants of technological risks who study the businesses of different customers to advise them on the different ways to mitigate them and the consequences of each of them, through cyberintelligence analysts who, with business data and existing risks, must perform analysis and obtain intelligence to defend their customers. All of them with the task of protecting, such cyberspace policemen, doing their bit towards a more secure network for all. Below, we have created a summary with some of these occupations using comparison with other more traditional jobs to provide teachers with resources to show students with examples.



COMPUTER FORENSICS ANALYST
The crime scene detective; collects evidence from devices that prove who perpetrated the cyberattack

ENGINEERER OF CYBERSECURITY
Protects information from attacks and ensures continuity of operations against cybercriminals

CYBERSECURITY AUDITOR
Provides an independent assessment of the security of companies' systems

CYBERINTELLIGENCE ANALYST
The special agent of cyber: uses data analysis to generate intelligence against cybercriminals

ETHICAL HACKER
Such a hacker infiltrates networks and systems but always legally: they simulate attacks looking for weaknesses and vulnerabilities.

CYBERSECURITY ARCHITECT
The architect: designs and builds or supervises the organization's defensive systems, working with others to maintain their integrity.

CHIEF INFORMATION SECURITY OFFICER CISO
The director: plans, coordinates and supervises the company's ICT security operations and needs. .

RISK & COMPLIANCE CONSULTANT
Advises on potential risks that may affect reputation and security by assessing risks to management policies and protocols .

PRE-SALES ENGINEER CYBERSECURITY
The cyber guru: analyzes and designs technical solutions for the elaboration of offers according to the needs of the clients .

SECURITY OPERATION (SOC) ANALYST
Monitors networks for suspicious activity

HOW TO BECAME A CYBERSECURITY PROFESSIONAL

And, how to become a cybersecurity professional? The studies required to become a cybersecurity professional have changed over the last few years and depend on the country, even the region within a country, as this is a fairly new area. According to Cybersecurityeducation.org[11], "employers often prefer potential employees who at least have a bachelor's degree in disciplines such as information systems (IS), information technology (IT), applied mathematics, computer programming, engineering, or another computer-related field. Further education may be necessary during your career with certification from organizations and businesses such as Microsoft, Cisco, or other major software companies that need security workers."However, in recent years, cybersecurity teams are recruiting different backgrounds professionals. Although technical training is still the core, criminologists, sociologists, psychologists, lawyers, marketing and advertising professionals, graphic designers, etc. are also required. All of them with the necessary specialized training in cybersecurity.

Let us see in more detail an example of career path such as incident responder[12]. The incident responders are the first to come in rescue when a cyber-emergency happens. They are the fire fighters of the cyberspace. In the daily tasks they recognize vulnerabilities in the systems, develop procedures to respond each emergency, run penetration test, risk analysis and security audits to prevent attacks, act quickly then an cyberattack comes, and provide incident reports to management teams. They have a global view of cybersecurity. Figure 1 shows a general career path as an incident responder. The lower position into the Computer Security Incident Response Team (CSIRT) is accessed too through specialized

[11] Source: https://www.cybersecurityeducation.org/careers/security-engineer/
[12] Source: https://www.cybersecurityeducation.org/careers/incident-responder/

cybersecurity studies such as a vocational degree in cybersecurity or a degree in cybersecurity engineering, depending on the position and salary. Another option is to study computer engineering, telecommunications, or applied mathematics or physics and then get a master's degree in cybersecurity or a couple of relevant certifications such as CPT and GCIH.

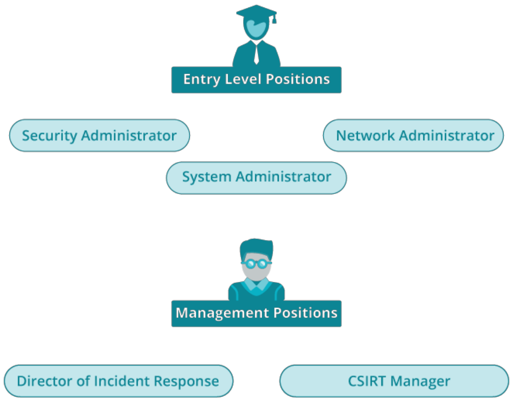


Figure 1. Career paths as an incident responder.
Source: https://www.cybersecurityeducation.org/careers/incident-responder/

Regarding salaries, according to Simplyhired.com(https://www.simplyhired.com/salaries/search?q=incident+manager&l=) an CSIRT Manager has an average salary among 47.000 and 120.000 EUR.

SUMMARY

In this lesson, we reviewed career profiles related to the field of cybersecurity and summarized skills and competences needed, based on various competence frameworks. Likewise, we explored the place of the cybersecurity profession within the framework of the contemporary socio-economical ecosystem.

Within this lesson, we discussed why cybersecurity is a multi-disciplinary domain and that being successful within the cybersecurity domain requires a job-specific mixture of domain specific knowledge, social intelligence as well as, of course technical skills. Notwithstanding, regardless the fact that the technical skills are a crucial part of cybersecurity careers and are easier to be quantitatively assessed and measured among candidates, we recognize the need of disseminating the idea that this is only one of the aspects, required for a career in cybersecurity. Thus, we encourage teachers, whose students are interested in pursuing a career or education in cybersecurity but are afraid they lack the technical background to succeed, to talk to them about cybersecurity taking a more holistic approach. Vulnerability mitigation, threat detection and resilience management require not only technical knowledge, but understanding everyday behavior (Choo K., 2011) and how user habits might inform us on and increase the risk of vulnerabilities in networks, software, web-platforms and device usage (Arachchilage, 2013).

Cybersecurity as a sector requires from its professionals not only technical aptitude, but also social and organizational fit. (Dawson, 2018). Cybersecurity as an industry domain is able to provide opportunities for career and personal development to students with various skills, competences and knowledge. One such job might be related to cybercrime investigation, where, depending on the job profile, some technical skills might be required, however social skills and criminal psychology expertise, might be more important (Ono M., 2011).

The profession of a cybersecurity specialist is not a single job, task or knowledge base. Cybersecurity welcomes multiple types of domains, sciences and competences, which makes it a platform, by itself, for life-long learning, self-development and opportunity for growth and we are responsible for the adequate representation of the sector to young girls and boys, who are still making their choice about a desired career or education path.

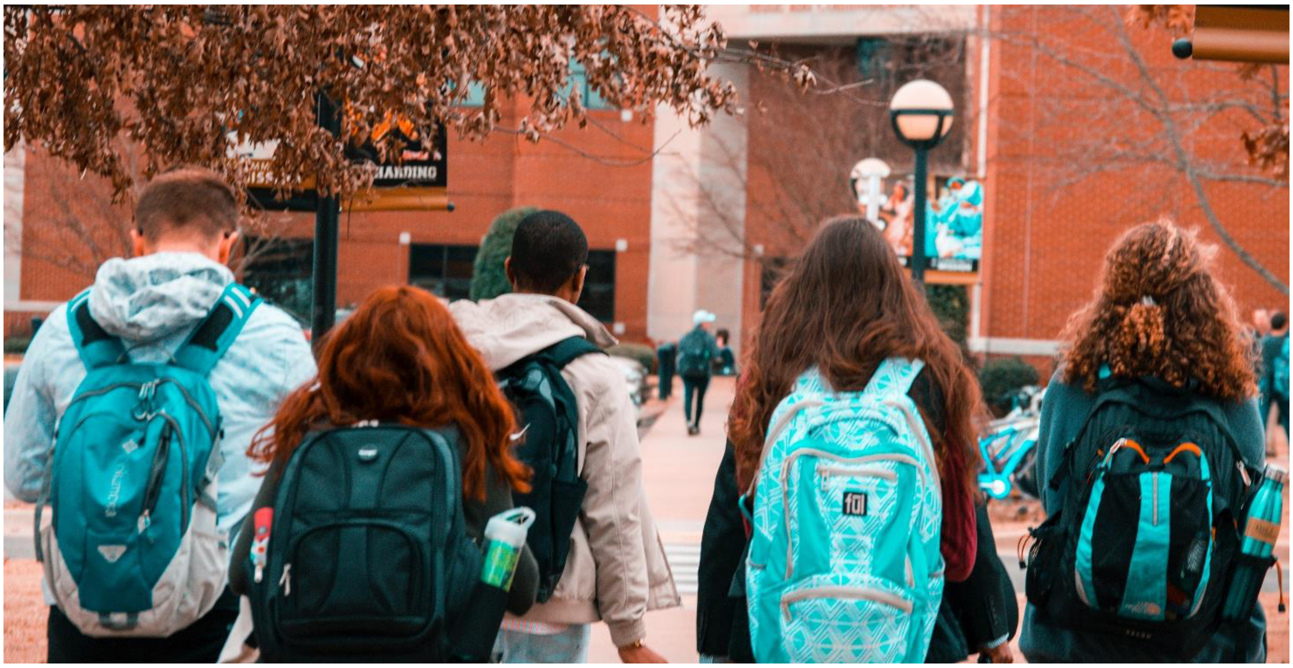


Photo 1 by Stanley from Pexels (www.pexels.com)

REFERENCES

Antunes, R., & Poshdar, M. (2018). Envision of an integrated information system for project-driven production in construction. *Proc. 26th Annual Conference of the International. Group for Lean Construction (IGLC)*, (págs. 134–143). doi:10.24928/2018/0511

Arachchilage, N. A. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior 29* , 706–714. doi:10.1016/j.chb.2012.12.018

Choo K., R. (2011). The cyber threat landscape: challenges and future research directions. *Computer Security 30*, 719–731. doi:10.1016/j.cose.2011.08.00

Dawson, J. &. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology, 9*, 744. doi:10.3389/fpsyg.2018.00744

Department of Homeland Security. (2014). *Best Practices for Planning a Cybersecurity Workforce White Paper*. U.S. Department of Homeland Security.

Newhouse W., K. S. (August de 2017). Cybersecurity Workforce Framework, NIST Special Publication. *National Initiative for Cybersecurity Education (NICE), U.S. Department of Commerce.* , 800-881. doi:10.6028/NIST.SP.800-181

Ono M., S. D. (2011). Cognitive ability, emotional intelligence, and the big five personality dimensions as predictors of criminal investigator performance . *Criminal Justice and Behavior, 38*, 471–491. doi:10.1177/009385481