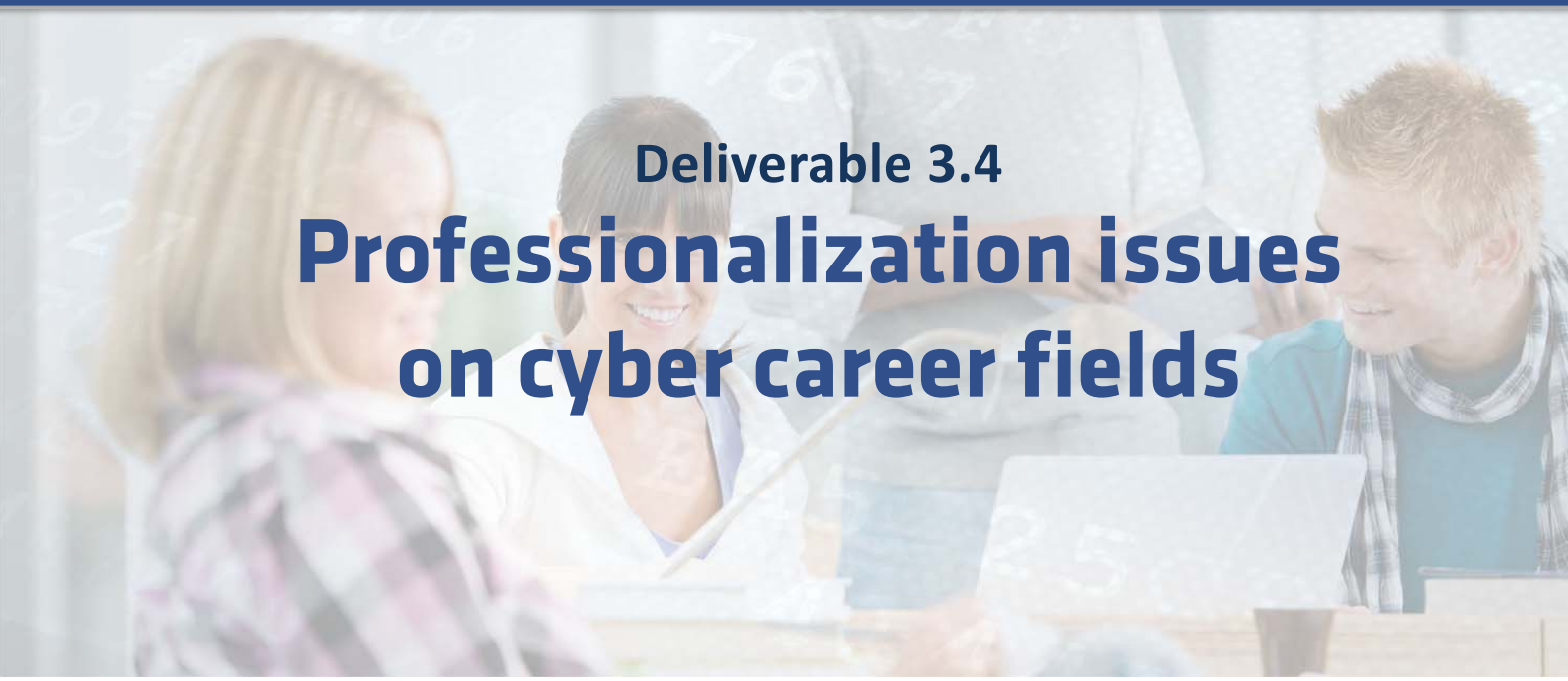

Deliverable 3.4

Professionalization issues on cyber career fields

Tempus

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

Deliverable 3.4

Professionalization issues on cyber career fields

European Commission Tempus Project:

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

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

Table of content

1. Introduction

The process of building a nation's agile, highly skilled professional cyber security workforce, required to secure, protect, and defend the Montenegrin information systems, incorporate three complementary components: workforce planning, professional development, and the identification of core professional competencies. The keyword here is "professional": to form and maintain a globally competitive cyber security workforce requires identifying core occupational competencies, setting objective standards for skills development, accreditation, and job performance of cyber security practitioners, and developing career ladders within the various cyber security disciplines, all in accordance with EU practice and principles.

The competency framework presented in Dev. 3.2 need to be extended in order to assist organizations in addressing three main objectives:

- Specifying knowledge, skill, and performance expectations.
- Determining whether current and potential employees meet job-skill requirements without additional and/or recurring development activities.
- Creating employee development plans by providing a model for assessing knowledge and skills.

It is fundamental to estimate the time and resources needed to properly train cyber security professionals, and to identify the main difficulties of maintaining high-level, up-to-date knowledge and skills. Finally, the analysis of the problems encountered in organizing and delivering professional courses will provide an important instrument to predict and tackle future problems and to correct training objectives and strategies. It will be done by cross-matching with EU practice and setting objective standards for skill development and job performances. In this report, we will discuss all efforts related to such process, and summarize all main results achieved.

2. Need for professionals

Electronic handling of information is a defining technology of our age. It is generally predicted that in 2020 the number of devices connected to the Internet will reach 35 to 50 billions, corresponding to 5 to 7 connected devices per person, on average. The society is moving fast in the digital world, and Nations have recognized the potential of digital space to develop their societies. Governments and Companies want to surf the digitalization pushing their departments to transform the business from the "old school" to the new digital one.

With enormous volumes of information stored and transmitted worldwide on a daily basis, the field of information security has grown very rapidly in order to prevent and respond to potential incidents and attacks on IT infrastructures. Yet, there is still much to do.

A Digital Single Market, wished by European Union and adopted by each Country as a Mantra, will have a huge impact also in terms of cyber security competencies. The skills required by the digital market are not only related to development, maintenance, and integration, but security plays a primary role. Not only security experts are needed, but security awareness and basic counteractions to cyber threats should be part of each employee's background. Each device connected to the Internet is a potential door inside companies and personal lives, and many malwares, such as ransomwares, exploits human vulnerabilities to break into a companies data. Also, data breaches, such as the ones LinkedIn [1] and Yahoo [2] suffered recently, present big issues also for the companies, because a lot of people use the same password for several services. If a user registers herself on a social network with the company email and uses the same password for the authentication of both digital identities (company intranet and social network), stealing her social network credentials allows gaining access to the company's data. A system is not an isle and the idea of multi-connectivity and multi-functions device is a goal for many entrepreneurs. The implications are a growth of factors that should be taken in consideration in terms of network security, secure development, privacy constraints, standard compliance.

The increasing number and varying nature of cyber threats lead to a further realization: there is a shortage of highly trained cybersecurity professionals who are capable of addressing the threat at hand. The lack of advanced cybersecurity professionals affects different sectors, ranging from governments to the private sector, with potential negative consequences for national security, economic vitality, as well as public health and safety [3]. As cyber threats continue to increase in scope and sophistication—and as more people become aware of these vulnerabilities—there is a growing demand for professionals who can secure networks and combat cyber attacks.

“The 2013 $(ISC)^2$ Global Information Security Workforce Study” [4], a study of Frost & Sullivan in partnership with $(ISC)^2$, reported a web-based survey (more than 12.000 qualified security professional respondents). The survey findings are:

- Security software development is “where the largest gap between risk and response attention by information security profession exists”.
- Information security is a stable and growing profession.
- Even with past annual growth in the double-digits, workforce shortages persist.

- Knowledge and certification of knowledge weigh heavily in job placement and advancement.
- Application vulnerabilities rank the highest in security concern.
- While attack remediation is anticipated to be rapid, security incident preparedness is exhibiting signs of strain.
- Information security professionals trump products in securing infrastructure effectiveness.
- Security concern is high for BYOD and cloud computing.
- New skills, deepening knowledge, and a wider range of technologies needed.

One-third of survey respondents predicted an increase of budget availability in terms of information security personnel, training and education and hardware & software.

In the same period, the Bureau of Labor Statistics of U.S. predicted a growth of 37% of information security analysts position from 2012 to 2022, only in U.S., a growth much faster than the average for all occupations [5]. In 2014, the "Global Cyber Security Market Research Report" [6] of MicroMarket Monitor predicted for the global cyber security market a growth from 95.60 billions dollar in 2014 to 155.74 billion dollars in 2019 at a Compound Annual Growth Rate (CAGR) of 10,30%. In Europe the market is expected to grow from 23.21 billion dollars in 2013 to 35.53 billion dollars in 2019. The demand for information security experts will increase in the next years due to the expansion of the GDP that will be produced by the digital market.

More recently, an article published by Forbes in December 2015, and titled "Cybersecurity Market Reaches $75 Billion In 2015; Expected to Reach $170 Billion By 2020" [7], presents a forecast of growth by Hemanshu "Hemu" Nigam, founder of security advisory firm SSP Blue. This means a CAGR of 9,8% from 2015 to 2020. The areas highlighted by IDC are: security analytics/SIME (10%+); mobile security (18%); and cloud security (50%). The Internet of Things (IoT), already a relevant part of the cyber security market, is expected to grow from $6,89 billions in 2015 to $28,90 billions by 2020 [8].

In "The 2015 $(ISC)^2$ Global Information Security Workforce Study" [9] of Frost & Sullivan, there is a clear representation of Information Security worldwide needs in terms of knowledge, skills and abilities. There is still a strong lack of experts in the market (security analyst, security auditor, security architect…) and also of competencies (risk assessment and management, incident investigation and response, governance…). The report concluded that corporate executives often lack a complete understanding of their company's security needs and their inability to locate enough qualified security professionals, which leads to more frequent and costly data breaches. The consequences are dramatic: a

recently released study from Cisco Systems Inc. [10] linked the shortage of nearly one million skilled cybersecurity professionals to growing cyber attacks.

Currently, the offer of the Academic world in terms of training and education in cyber security is not as wide as the circumstances would require. In general, the number of STEM (Science Technology Engineering Mathematics) graduates, although increasing, is not sufficient. Additionally, most people are not well aware of the job market opportunities on this topic. Although cybersecurity professionals are in great demand—and can command impressive salaries—there remains a critical shortage of people who wish to enter and thrive in this field. These and other issues need to be carefully analyzed.

3. Professionalization issues

The digitalization of both the public and private sector is proceeding at an ever increasing speed, and IT solutions are more and more pervasive in our daily life. The big question is: Are we ready to face it? The impression is that progress is moving faster than human capability to ride it.

Most of the attacks to information systems exploit human error: from general statistics, the entry point of an attack is the human inaccuracy for the 80-90% of the episodes [11]. The monitoring activities of a company should therefore include a careful evaluation of the readiness of its staff to prevent and counter cyber attacks, with efforts inversely proportional of the awareness of employees, clients and users in general (see Figure 1).

Figure 1: Monitoring activities should be inversely proportional to users' awareness

Additionally, a cyber threat intelligence department should monitor the Deep Web to check if some data leak could have any impact on the company. Databases released on the dark web could contain information

that could damage the business or interest of the company (see Figure 2).

Figure 2: Monitoring activities should include the deep web

Other than addressing the needs of companies, there are several other goals for professionalization in cyber carrer fields [16]:

- Establishing standards that enhance the quality of the workforce.
- Regulating workers whose jobs can affect the health, safety, or property of others.
- Enhancing public trust and confidence.
- Enabling compliance.
- Enhancing the status of an occupation.
- Regulating the supply of labor to advance the interests of its members.
- Guiding the behavior of practitioners. Establishing roles and pathways so as to better align supply and demand, increase awareness in career paths, and facilitate recruitment and retention.

These goals must be pursued with the awareness that several tradeoffs need to be carefully handed:

- Quality vs. quantity.
- Standardization vs. dynamism.
- Broad vs. niche needs.
- Better info for employers vs. false certainty.

- Certainty about worker capabilities vs. uncertainty about actual job requirements.
- Specificity vs. flexibility.
- Stimulation of supply and better matching of supply to demand vs. restriction of supply.

3.1. Educational issues

The practical implementation of both a secure information system and proper monitoring activities ultimately depends on overcoming a main obstacle: the lack of properly trained staff. This condition, illustrated in the previous section, is caused by a number of concurrent factors, but the lack of cyber security educational offering is among the most important. Currently, cyber security is often a topic faced only during Master programme, when it is too late to start forging security analysts or other operational experts, especially if these programmes include limited practical activities. Figure 3 shows a desirable educational process:

- The attention to STEM skills, foreign languages and coding principles should increase right from the kindergarten.
- The teaching of STEM matters should be strengthened in all educational layers.
- Suitable cyber security programme should be introduced from the high school, and specific cyber security degrees established in the Universities.
- Universities and Masters should reduce the theoretical courses in favor of more practical activities.
- Continuous professional training should be provided by each company to its staff.
- Finally, awareness campaign should be implemented regoularly and involve citizens of all levels and age.

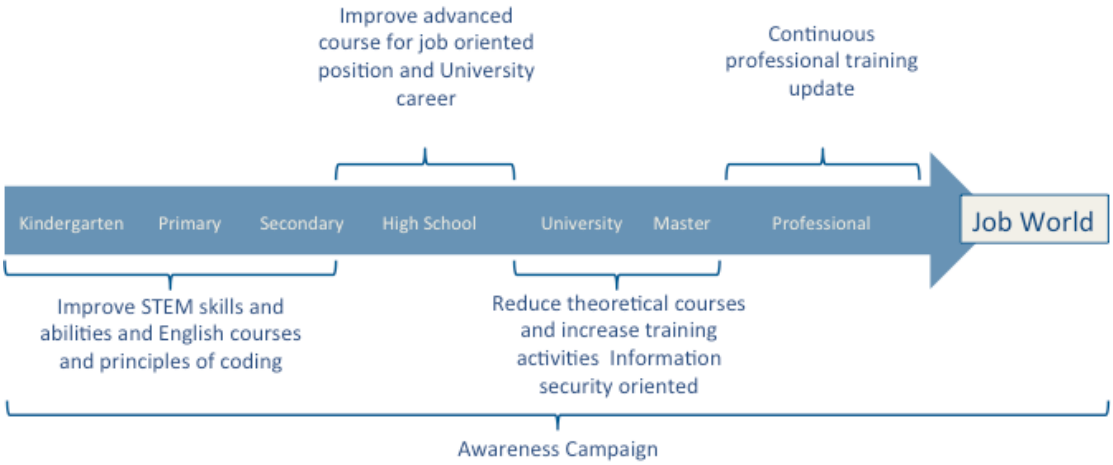

Figure 3: A graphical description of a desirable educational process

3.2. Educational v.s operational

A comparative look at the U.S. National Initiative for Cybersecurity Education (NICE) and the U.S. National Cybersecurity Framework (two communal reference points for many EU countries) immediately exhibits the existence of a disrupted bridge between the two initiatives (see Figure 4).

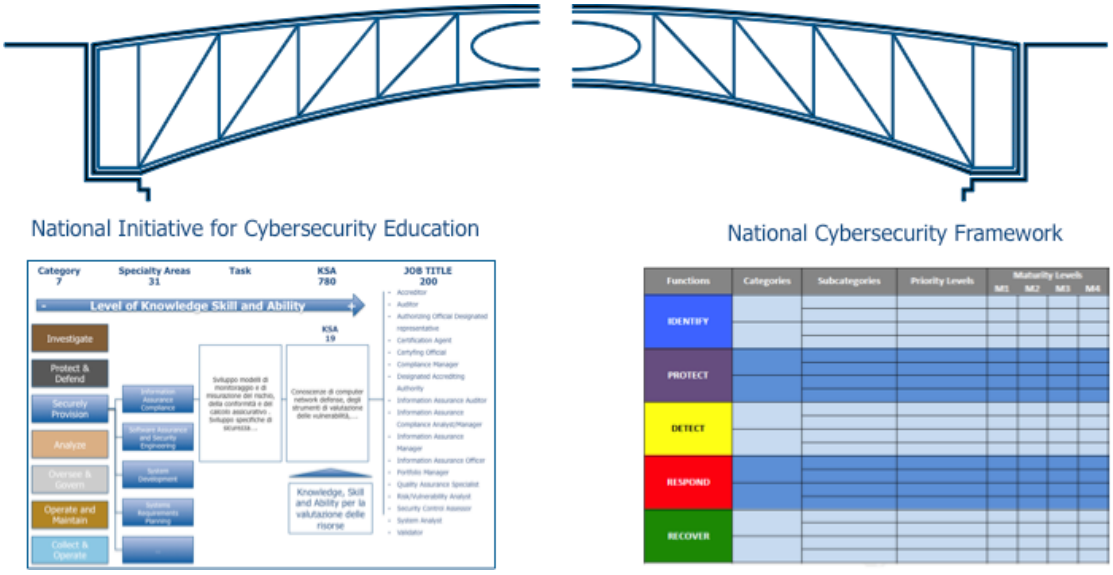

Figure 4: NICE vs. National Cybersecurity Framework

The NICE presents 7 categories (Securely Provision; Operate and Maintain; Protect and Defend; Investigate; Oversee and Govern; Collect and Operate; Analyze), and specialty areas for each category (32 in

total). Each specialty area is associated with tasks an expert should perform, and specific Knowledge, Skills and Abilities (KSA) she should demonstrate. In particular, the acquisition of these KSA allows aspiring to specific job titles, listed in the framework too.

The issue is the logical gap between the “educational” and the “operational” framework. In the National Cybersecurity Framework, there is a different categorization of the topics. The framework is in fact divided in only 5 functions (Identify; Protect; Detect; Respond; Recover) with sub-categories not directly matching the specialty areas of the NICE. The exercise of linking the NICE framework with the National Cybersecurity Framework is somehow left to the final user, making the training and hiring process much harder than expected.

The problem is exacerbated by the fact that, as with any relatively new profession, tens of thousands of individuals claim competence in cybersecurity, and it can be hard for an employer — or any organization — to judge. Early efforts to develop credentials, although well intentioned, were based on knowledge testing and unmonitored experience. It should be clear to people how to become a cybersecurity professional (what courses to take, which certifications are needed, and what skills employers require) and, for hiring managers, it should be clear how to assess the quality of job candidates (*e.g.*, whether they know how to write secure mobile apps, defend systems against cyberattacks, or protect customer credit-card data). This confusion causes the profession to grow less efficiently than it could, because of the impossibility to uderstand what credentials are needed and how much it is going to cost to get them. The lack of clarity has contributed to a widespread shortage of trained, experienced cybersecurity professionals. Similarly, it has created a challenge for employers to hire people with the right skills. HR reps find themselves confronted with a variety of certifications from about two dozen organizations [12].

3.3. Standards and frameworks

The industry has tried to respond to the needs of the marketplace by developing certifications and other educational standards for various career paths. However, since accreditations have sprung up individually, they often overlap each other or, worse, leave gaps. The report [12] identified up to 31 different cyber security specialties, dealing with such areas as information assurance compliance, systems security architecture, and digital forensics. These specialties are served by at least 23 different certification programs from such organizations as the American Society for Industrial Security [13], or the Computer Security Institute [14]. Plus, the field is rife with conflicting definitions and competing requirements.

As suggested in a 2010 report [18] by the Center for Strategic and International Studies, every country needs to develop more rigorous professional credentials as part of a robust cybersecurity program. The report emphasizes security automation to relieve cybersecurity staff of repetitive tasks, "including but not limited to configuration and patch management". The authors additionally propose to build on existing work to develop a taxonomy of high-level cybersecurity specialties and certifications that would help drive education and training.

The Pell report [3] offers recommendations for developing a more organized cybersecurity profession, including establishing clear bodies of knowledge and educational paths. There are many different roles to fill in cybersecurity, and each role needs to have its own education and experience path. If you think of security like medicine, you need first responders, nurses, doctors, brain surgeons, and everything in between. While large cybersecurity certification programs, such as the Certified Information Systems Security Professional (CISSP) [17], can be expected to serve the emergency medical responders, nurses, and maybe doctors, they cannot help the brain surgeons and other specialists. Each specialty should also develop its own code of ethics [12], something currently lacking. Indeed, to learn how to secure an information system, security professionals also learn how to break in.

Several initiatives were designed specifically to address this issue in a timely manner, including the Council on CyberSecurity's U.S. Cyber Challenge [22], and the National Centers of Academic Excellence [23], sponsored by the National Security Agency and the Department of Homeland Security. In 2013, however, the Computer Science and Telecommunications Board of the National Research Council issued a report titled "Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making" [24], in which the distinguished panel concluded, in part, "Cybersecurity is a young field, and the technologies, threats and actions taken to counter the threats that characterize the endeavor are changing too rapidly to risk imposing the rigidities that typically attend professional status". The panel recommended, "Activities by the federal government and other entities to professionalize a cybersecurity occupation should be undertaken only when that occupation has well-defined and stable characteristics". Cybersecurity is indeed a dynamic field, and threats seem to change by the minute. Waiting for the field to stabilize, however, is a dangerous notion. With almost daily reports calling into question the robustness of our cyberinfrastructure, there are things we can and must do now to shore up the nation's cyberdefenses.

4. Conclusions

To address the acute gap between market demand and supply in the cybersecurity industry—a gap that is only expected to widen in the next future—cyber professionals (and the companies that will hire them) not only need a standardized way to measure their training, education, and experience in cybersecurity; they also need a well-defined career path that rewards those with higher level technical skills.

The definition of this career path should be pursued thanks to a constant interconnection between the academic and the work environments. Universities should establish a more unified educational path for students interested in a cybersecurity career, establishing nationally (or, better, internationally) accredited programs that universities can adhere to and publicize. The professionalization path is long, and uncertain, and changes would be needed in education, certifications, and in on-the-job training. Specific mechanisms for professionalization further include a code of conduct or ethics, and clearly defined links between competency frameworks and training activities.

The growth of digitalization and cyber security starts from the education and awareness. Educational programme should contemplate more topics in STEM matters and have a progressive and deep engagement in cyber security for the students interested. Universities should start to create dedicated programme on cyber security with operational training.

From the standpoint of a company, there are several actions that can be undertaken to support the process of building a workforce capable of protecting critical cyber resources [19]. There is empirical evidence that implementing the SANS' “20 Critical Controls for Effective Cyber Defense” [20] can dramatically reduce organizational risk, and this requires that security is built into the system development process. Cyber security professionals must be asked to demonstrate successful, practical experience in the role assigned to them — for example, intrusion detection or network administration, and in order to make it possible companies must support the development of more rigorous credentials.

Corporate leaders often display the tendency to treat cybersecurity as an isolated problem that should be uniquely competence of already overwhelmed IT departments [3]. Further, research [15] shows (and our survey realized for Dev. 3.1 partially confirms) that managers are naturally optimistic about their company’s security posture, and/or do not fully understand cybersecurity risks, thus leading to dangerous security leaks. Managers should instead be responsible for building a team of trusted experts, fostering a culture of security, and developing sound strategies to protect their digital investments.

References

[1] http://fortune.com/2016/05/18/linkedin-data-breach-email-password/

[2] https://en.wikipedia.org/wiki/Yahoo!_data_breaches

[3] http://pellcenter.org/wp-content/uploads/2015/05/Professionalizing-Cybersecurity.pdf

[4] "The 2013 $(ISC)^2$ Global Information Security Workforce Study", Michael Suby, 2013, Forst & Sullivan, Booz Allen Hamilton, $(ISC)^2$

[5] http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[6] http://www.micromarketmonitor.com/market-report/cyber-security-reports-7651948375.html

[7] http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#58e521f22191

[8] http://www.csoonline.com/article/2984193/cyber-attacks-espionage/new-cybercrime-wave-drives-iot-security-spending.html

[9] https://www.cybercompex.org/fileSendAction/fcType/0/fcOid/445471828686010375/filePointer/445471828686010530/fodoid/445471828686010527/frostsullivan-ISC2-global-information-security-workforce-2015.pdf

[10] http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

[11] https://www.gcsec.org/keyportal/uploads/newsletter-2016-july_august-2016.pdf

[12] http://theinstitute.ieee.org/career-and-education/career-guidance/no-clear-path-for-prospective-cybersecurity-specialists

[13] https://www.asisonline.org/Certification/Pages/default.aspx

[14] http://www.cybersecurityforensicanalyst.com/

[15] https://www.lancope.com/sites/default/files/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf

[16] https://www.nap.edu/read/18446/chapter/4

[17] https://www.isc2.org/cissp/default.aspx

[18] https://www.csis.org/analysis/human-capital-crisis-cybersecurity

[19] http://www.fedtechmagazine.com/article/2014/04/case-professionalizing-cybersecurity

[20] http://www.spectrami.com/wp-content/files_mf/1429533426LR_SANS_Top_20_Whitepaper.pdf

[21] https://benchmarks.cisecurity.org/docs/user-guides/CIS-CAT%20Users%20Guide.pdf

[22] http://www.uscyberchallenge.org/

[23] https://www.nsa.gov/what-we-do/information-assurance/

[24] https://www.nap.edu/catalog/18446/professionalizing-the-nations-cybersecurity-workforce-criteria-for-decision-making