Skill Shortage, the new threat

The cyber threats continue to grow in modality, intensity and in terms of sophistication, in this scenario the needs of security teams constantly change and require more and more specialized personnel. Increasingly we are witnessing situations where we face the emerging risk with a lack of personnel and a difficulty in attracting and recruiting adequately qualified personnel, a situation that already represents a risk for itself. Capacity and capacity deficits are occurring while major safety incidents damage organizational performance and reputation. Building tomorrow’s security workforce is essential to address this challenge and provide solid, long-term security for organizations in the digital age.

Filling the skills gap will require organizations to change attitudes and approach to recruitment, training and participation in collaborative pipeline development initiatives. A too rigid and traditional approach to identifying candidates, together with overworked and insufficient working environments, clearly needs new tactics and new ideas. GCSEC is active on EU research programme and awareness campaign. It has developed projects on information sharing, ICS and Smart Grid security, E-crime, Cyber Educational Programme and so on. The last years it has organized events and workshops on ATM security, Advanced Persistent Threat, PSD2 Security and already published studies, such as, “DNS Health and Security” in collaboration with ICANN, “Information Sharing and Public-Private Partnerships: Perspectives and Proposals” in collaboration with UNICRI and “Best Practices in Computer Network Defense: Incident Detection and Response” in collaboration with NATO.

The study on “Mind the Gap: the cyber security skills shortage and public policy interventions” represents the last stone and result of the collaboration with Oxford Centre for Doctoral Training in Cyber Security. We believe that more should be done to prepare our countries to a better and safer digital world. The first step to facilitate the digitalization, in accordance with the Third Pillar “Trust and Security” of European Digital Single Market Strategy is to mind the gap of skills and competencies in cyber security. In this study, we have done an overview of Countries policy and experts opinions on cyber security educational programme, highlighting some recommendations for the future.

Closing the gap between supply and demand is imperative for an enterprise to develop an effective security posture. It is evident that individuals with the required skills, qualifications and experience are either unavailable or demanding compensation that cannot be met with existing budgets. Because they are in high demand, talented security staff regularly move to new employers as they seek out better salaries and projects at more prestigious companies.

Enjoy the lecture…

Nicola Sotira
General Manager GCSEC
The cyber security skills shortage (CSSS), the lack of cyber security professionals in the labor market, is one of the most pressing challenges in cyber security policy. Various research has reported staggering numbers on the global workforce shortfall and governments of major countries have already voiced their worries. However, not everyone seems on the same page. Rik Ferguson, vice president for security research at Trend Micro, said "You’re being conned. There’s no such thing. It doesn’t exist." Even if a such a shortage existed, it would be hard to deal with as, according to CEDEFOP, we do not really know much about effective policies and practices addressing skills imbalances.

Against this backdrop, last year I have conducted exploratory research, funded and supported by Global Cyber Security Center (GCSEC), to answer two main questions: is there a CSSS and what evidence do we have? If there is one, what are countries doing to increase the pipeline of professionals? I have analyzed approximately 50 reports and interviewed 30 experts in cyber security and skills policy. Findings depict an extremely complex picture.

For sure, there is an evident and a widespread perception of the shortage. But a perception not always equal factual evidence. Indeed, the current empirical knowledge on the CSSS is piecemeal and flawed by several methodological issues, including ambiguous questionnaires, ill-formulated indicators, doubtful quantifications of the global shortage and overall poor generalizability of research findings. It is not by surprise that the account of the characteristics and nature of the CSSS varies greatly depending on data sources. For instance, industry reports almost unanimously consider the education and training system as the main culprit behind the shortage, seen as unable to produce enough graduates ready to take up jobs in cyber security. While agreeing on the need to modernize the current academic offer, national policy documents and interviews provided a more balanced view, underlying that the shortage could be exacerbated by employers themselves, who seem to be

Sources identification
- Open Source
- Public Report
- PhD Publications

Methodology definition
- Framework
- Policy's analysis domains

Other Instruments
- Interviews with experts
- Cyberweek
- Survey to Italian CISOs

Recommendations and final reports
Recommendations and suggestions definition, final reports

Collection of National Policy Defined by the top 12 Countries for ICT development and Cyber Security and Italy 1)

Data analysis
Analysis of data collected and policy defined by countries in the domains defined

Survey to Italian CISOs
Online aimed to understand the needs of Italian organizations in terms of skills and competencies

1) Policy updated to 2013-2018 version

For the experts detected a coinminer script on one of their honeypots and, the malicious code shares some parts with the Xbash malware and the KORKERDS cryptocurrency miner that leverages rootkit to avoid detection.

"We found the script capable of deleting a number of known Linux malware, coin miners, and connections to other miner services and ports, and we observed some parts of the script to be reminiscent of Xbash features and KORKERDS," reads the analysis published by Trend Micro.

Better security measures for smartphones, ENISA has created a SMASHiNG new tool
https://www.enisa.europa.eu/news/enisa-news/better-security-measures-for-
rarely providing entry-level opportunities and good quality training. One of the interviewees suggested:

“I think that the CSSS is more due to industry and government than it is to the education system. They need to get much more guidance on how to get people into the system, but then they need methodologies and approaches to nurture these people throughout their careers.”

Even though current knowledge on the CSSS does not withstand scientific scrutiny, it would be irresponsible to dismiss it as a prefabricated industry lobby operation, as some shortage critics would do. Abundant national evidence and results from interviews suggest that, at least in certain countries, there are currently numerous issues that impede a correct matching between the cyber security supply and demand. For example, there were almost 314,000 active cybersecurity job openings in the United States between 2017 and 2018; in Australia between 2014 and 2016 cybersecurity salaries increased by 2.7% compared to an average annual wage growth of 1.7 per cent in the wider IT industry, signaling a scarcity of workers which in turn drives wages up. Yet, no measurement has been able to confidently capture the incidence, scale and nature of the problem, especially at the international level.

But if a shortage of some sort exists, how governments have reacted to it?

Overall, policy responses of certain countries have been more elaborate than others, most notably in Japan, the UK and US. More complex policies have attempted to target a wide range of different groups with a multi-stakeholder approach involving the three main actors in the debate, namely the government, private sector and education system. Governments have invested more in higher education, research and the workforce, whereas fewer and vaguer initiatives have been directed towards primary and secondary schools as well as vocational or apprenticeship programs.

However, policy measures implemented by some national authorities suggest that the nature and the characteristics of the shortage are still not well understood. For example, it is not straightforward to distinguish policies that are trying to increase the pipeline of security professionals (under-supply) from those that are seeking to improve the quality of job candidates (under-skilling). However, this is important, as governments might be erroneously thinking to be tackling one aspect of the problem (usually under-supply) when in fact their policies are predominantly addressing another aspect (usually under-skilling).

Moreover, some national policies might need recalibration. For example, one of the causes of the shortage could be the lack of graduates’ professional experience and the absence of entry-level opportunities. The analysis found that, with a few exceptions, governments have primarily sought to intervene at the higher education and research level. If data are confirmed, some policies could be reconfigured to ease the transition from school to the workplace, instead of being directed towards other areas.

Finally, from the data collected it is impossible to assess the effectiveness of these policies or, in other words, whether these policies have achieved their intended impact. After a long enumeration of strategies, action plans and policies, one is still left wondering how many individuals targeted by these policies have later joined the cyber security sector. Unfortunately, it seems that not many governments have in place metrics to evaluate programs for reducing the shortage.

Further research on the CSSS is a matter of priority. In an era of increasingly sophisticated cyber-attacks with the potential to have crippling effects on all of our lives, it is wise to educate and train an adequate number of cyber security professionals who are able to fend off cyber-attacks. If data and systems are the essence of the new digitized economy, governments should adopt the necessary measures to guarantee their confidentiality, integrity and availability, including by growing the right people to do it.

The report “Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions” is available here. The Italian case study will be published by March.

Good reading to everyone!
“Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions”