Analysis of cyber security skills issues

Astrakhantsev Roman  
Faculty of cybersecurity  
HSE

Russia, Moscow

rgastrakhantsev@edu.hse.ru

***This essay is based on an analysis of two articles, the main idea if which is to show what problems an employer, who is looking for qualified personnel in the field of cyber security, may face.***

***Keywords—cyber security, skills, professional certifications, supply and demand, lack of staff.***

Nowadays, a cyber security profession is becoming more demanded. There is nothing surprising, because in a context where digital transformation and hyper-convergence are sources of risks, vulnerabilities, attacks and system failures, a cyber resilience strategy can help your business withstand costly cybersecurity incidents. It will help protect against these risks, protect critical applications and data, as well as eliminate the consequences of hacking or system failure and take control of the situation.

***Shortage of cyber security skills***

A growing shortage of cybersecurity skills and recent studies show that prospects will not improve soon.

There is a statistic of this shortage in both articles. The first article gives examples of industry studies. They write: “30% of organizations were struggling with skills shortages”, “a ‘problematic shortage’ of cyber security skills as their top issue.”, “65% of organizations reported a skills shortage, with 51% considering that their organization was at moderate or extreme risk as a result.”1 Studies from the second article tell us that there will be a global shortfall of around 1.5 million security practitioners by 2020 and 82% of respondents considered there is a shortage of cyber-security skills.2 In this way, we can observe the outstripping of demand over supply.

***Why is it difficult to find a qualified specialist?***

What is the first association that comes to mind with the word “professionalism”? I think that most people will say “experience”. Indeed, it is exceedingly difficult to imagine a professional who has no years of experience. That is why in both articles there are two definition in the Merriam-Webster dictionary. So, the word “professionalism” defines as “the skill, good judgement, and polite behavior that is expected from a person who is trained to do a job well.”2 And “experience” is “practical knowledge, skill, or practice derived from direct observation of or participation in events or in a particular activity”.1 In these definitions we see a reference to skills. The lack of skills can be a challenge even for the security industry itself: the company itself typically needs to interview 40 people in order to hire one expert. But what should they be looking for?

Skills and abilities required to deliver cyber security is a blurry area. Cybersecurity skills include both technical and non-technical topic areas. “The technical topic areas span various issues around system, device and network security, which in turn include a range of underlying mechanisms. Non-technical elements include managerial, human, legal and physical protection perspectives.”1 That does not mean that all cyber security staff should be expected to cover all areas, but the organization as a whole must find a way to do so.

There are top five skills most used among the 250 cyber professionals that responded: cyber security strategy; cyber security management; user education; risk assessment; and security operations. Furthermore, skills exist at different levels: 1– Knowledge, 2– Knowledge and Understanding, 3– Apply, 4– Enable,5– Advise, 6– Initiate, Enable, Ensure.2 Table 1 presents correlation of these levels and skills, that match them. As we can see, the set of skills has a clear structure, ranging from possessing basic knowledge to the ability to lead.

So, cyber security specialists should have a good level of supporting knowledge and some of the skills, but there will equally be various aspects that they have not been able to put into practice. That is why employers should still be prepared to invest in relevant training and allow experience to be gained.

***Where to get these skills?***

If we talk about degree title, we can find these skills at both bachelor’s and master’s levels. But here is not so simple, too. The simple presence of cyber-security in the title does not mean the underlying coverage will be the same. Currently recognizes eight-degree types, spanning bachelor’s, Integrated master’s and master’s programs, with coverage ranging from general cyber-security to specific areas of digital forensics and network security. There is also recognition that cyber-security does not exist in isolation, with several of the certified routes requiring a tangible segment of underpinning computer science to accompany it.2

Another way to get the appropriate qualifications is professional certification. There is a wide selection of relevant certificates, suitable for various security specializations and experience levels. There are a number of certificates identified as the top five leaders in the field of cyber security, such as: Security+, Certified Ethical Hacker (CEH), GIAC Security Essentials (GSEC), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP). These five may be similar in terms of all being popular in the market, they are far from the same when it comes to their underlying characteristics. Security + and CISSP are notably dissimilar in terms of their depth and experience requirements.2

The situation with industry and professional certifications is different, insofar as many of them take a more topic-specialized stance in the first place. It is still important to understand what aspects of security they relate to, and thereby what being a holder of the certification implies that someone can understand and do.

|  |  |
| --- | --- |
| **L**  **e**  **v**  **e**  **l** | **Skill example** |
| 1–  Knowledge | Can describe the concepts and principles of threat intelligence, modelling and assessment |
| 2– Knowledge and Understanding | Can explain the principles of threat intelligence, modelling and assessment. |
| 3– Apply | Undertakes/assesses routine threat intelligence/modelling tasks or threat assessments under supervision |
| 4– Enable | Undertakes/assesses routine threat intelligence/modelling tasks or threat assessments without close supervision |
| 5– Advise | Undertakes/assesses complex threat intelligence/modelling tasks or threat assessments without supervision. |
| 6– Initiate | Leads corporate threat intelligence processes, reporting to the Board. |
| **Table 1: Сorrelation of level and skills** | |

The certifications denote something considerably different in terms of topic and experience. If we talk about supply and demand for different professional certifications, CISSP is the certification with the highest level of overall demand. The newer and more specialized CIPP certification, for which supply and demand are consequently lower at present. CISA and CISM are certificates, focusing on non-technical aspects. Furthermore, these certificates require candidates to have several years of relevant work experience.

The certifications are a representation of those in a form designed to enable others to make a preliminary assessment of the holder’s knowledge, skills and competencies. Therefore, a certification means that, at some point in time, the person had the knowledge, skills and competencies commensurate with that certification, and could pass the requisite tests.1 So, the certifications become a proxy for representing knowledge and skills.

***Conclusions***

Summing up all of the above, I would like to note that cybersecurity is a new promising area with its own specific features.

As such it is important to recognize the breadth of skills needed and ensure that they are in some way covered. So, to do this is to recruit talent with suitable certifications or qualifications, but for this to work we need to understand what they cover and whether it matches what we need.

If we take a siloed approach to cyber security skills, then we risk severely limiting the protection that can be achieved. Equally, in seeking a solution, it is not just about recognizing that a spectrum of skills is required - we also need to get them to work together in an effective manner.1

It is important not only to recognize that all qualifications and certificates are different from each other, but to understand what can be expected from them as a consequence.

The cybersecurity specialist has a lot of responsibility, so mastering the relevant skills is the most important part on the way to creating a secure information society.

**References**

1. Furnell, S; Bishop M. ’Addressing cyber security skills: the spectrum, not the silo’. Computer Fraud & Security, Feb 2020. <https://www.sciencedirect.com/science/article/abs/pii/S1361372320300178>
2. Furnell, S; Fischer, P; Finch, A. ‘Can’t get the staff? The growing need for cyber-security skills’. Computer Fraud and & Security, Feb 2017. <https://www.sciencedirect.com/science/article/abs/pii/S1361372317300131>