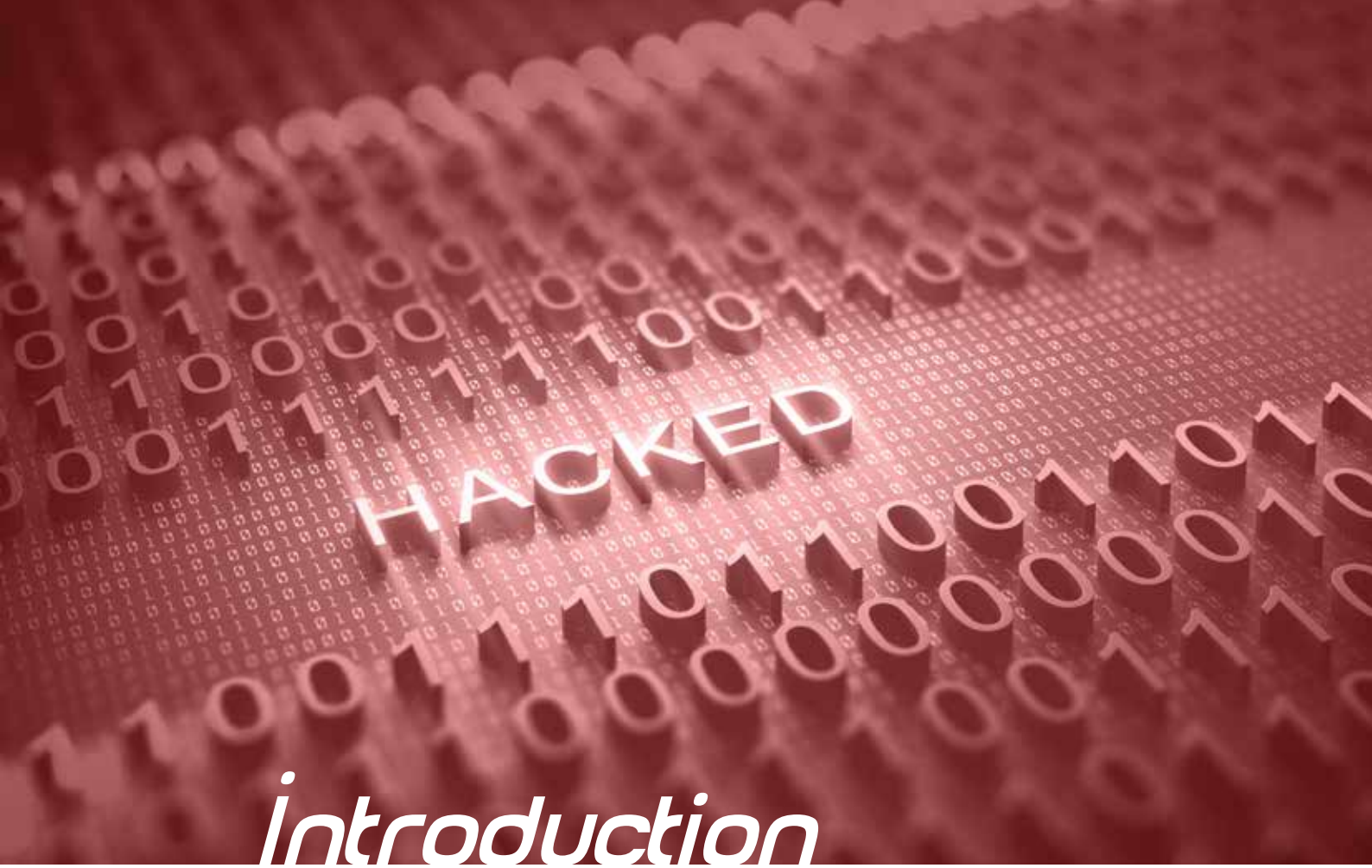
www.silensec.com

Addressing the Cyber Security Skills Gap

A READING FOR POLICY MAKERS, EMPLOYERS AND YOUNG PROFESSIONALS

Contents



Introduction

The importance of cyber security has become an undeniable fact. Every day we hear projections and reports about the growth of the cyber security industry on the one side and the skills gap that needs to be filled by that industry on the other. On the one hand we read about the importance of cyber security while on the other we read about how far we are from achieving it! According to the International Data Corporation (IDC), the premier global provider of market intelligence, worldwide revenue for security technology is to surpass $100 Billion in 2020, with the security training and certification market alone being worth over two-billion dollars.[1] Yet, employers from every corner of the world and from every industry lament the lack of skilled professionals in cyber security.

“worldwide revenue for security technology is to surpass $100 Billion in 2020, with the security training and certification market alone being worth over two-billion dollars

In order to try and solve the security skills gap it is important to clearly define the problem and to identify the challenges that must be overcome to fill that gap. In this paper we take a closer look at the Cybersecurity Skills Gap and what can be done at national level to try and fill it.

the Cyber Security Skills Gap

THE SIZE OF THE PROBLEM

A number of studies have been carried out and reports published about the on-going shortage of cybersecurity skills. Since 2015 the international professional organization ISACA has carried out surveys amongst its members in over 100 countries worldwide and produced a yearly Global Cybersecurity Status Report providing insights on cybersecurity threats and skills gaps. In their 2016 report[2] ISACA reported that over 53% of organizations experience delays as long as 6 months to find qualified security candidates while 84% of the organizations believe that half or fewer of applicants for open security jobs are qualified. The latest 2017 report by ISACA[3] shows that the situation has not improved with many organizations still not being able to fill the advertised positions. In fact, 1 in 5 organization receives fewer than 5 candidates for each advertised security position and 37% of the organizations lament that fewer than 1 in 4 of the candidates they do receive are actually qualified for the job!

> **"at least 1.5 million cyber security jobs will be left vacant by 2019**

According to cybersecurity data tool CyberSeek, in the U.S. alone 40,000 jobs for information security analysts go unfilled every year while 200,000 other cybersecurity related roles also go unfulfilled. And for every ten cybersecurity job ads that appear on the careers site Indeed, only seven people even click on one of the ads, let alone apply.

Another recent study, the 2017 Cybersecurity Trends, based on a comprehensive survey of more than 1,900 cybersecurity professionals, also reveals that organizations are struggling with a worsening cyber skill shortage while facing rising threat levels [4].

As for how many jobs will need to be fulfilled by the market, the common consensus is that at least 1.5 million cyber security jobs will be left vacant by 2019. ISACA predicts there will be a global shortage of two million cyber security professionals by 2019. By the same year, according to Symantec's CEO Michael Brown, the demand for the cybersecurity workforce is expected to rise to 6 million with a projected shortfall of 1.5 million.[5]

> 1 in 5 organization receives fewer than 5 candidates for each advertised security position

By far and large all studies and predictions agree on the current and future shortage of skills to address the cybersecurity job market.

THE IMPACT

The continued cybersecurity skills shortage creates tangible risks to organizations, the individuals and the nation. Consequently, the responsibility for a safer cyberspace and society lies with both the government, the organizations and ultimately with the individuals themselves. A country with a weak cybersecurity workforce is exposed to cyber espionage, remote interference with government elections and ultimately to the safe and reliable running of critical infrastructure services such as healthcare, transportation, power generation, distribution and much more. For a private organization, not having skilled employees certainly impacts on its ability to identify, contain and mitigate complex security incidents, which results in increased cost to the enterprise. And finally for the individuals, lack of security awareness brings about issues of personal privacy, financial fraud and abuses of personal data.

> The continued cybersecurity skills shortage creates tangible risks to organizations, the individuals and the nation

The cybersecurity skills gap permeates every aspect of the modern society and if it is not addressed its impact to society will continue to grow.

> market research shows that the ethical hacking domain is not the one in the highest demand

the Cybersecurity Skills Gap

The cybersecurity skills gap is real and growing. However attention should be also focused on defining the problem. As many may easily appreciate, cybersecurity is a wide domain encompassing a range of professions and associated skills and required experience. If the cybersecurity skills gap is to be filled it is important to understand the nature of the gap and the types of professions where the gap is wider or growing.

In that regards, a number of studies have also been carried out that can shed some light on the problem. A first report by Indeed[6], based on two years' worth of Indeed data (Q32014 to Q32016), takes a look at ten countries to identify which cybersecurity jobs are most in demand and which security field is showing the most growth. While the overall shortage of skilled staff is high across countries, the report does show that for some jobs the demand is higher than the offer.

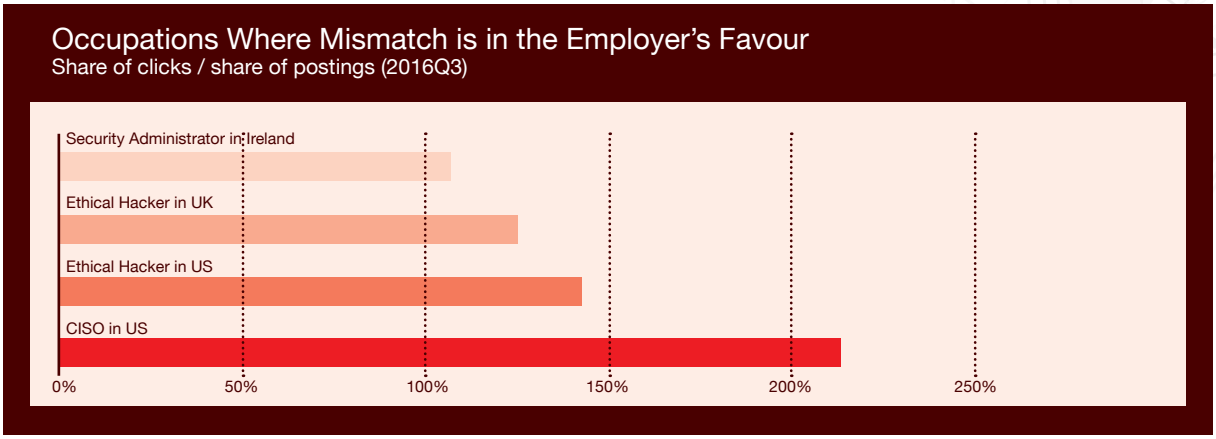
EVERYBODY IS CRAZY ABOUT ETHICAL HACKING – DON'T BE!

Many aspiring professionals approaching the cybersecurity industry are overly fascinated with and attracted by the "hacking" domain pursuing a career as Ethical Hacker, more often referred to as penetration tester. Unfortunately, market research shows that the ethical hacking domain is not the one in the highest demand. Research by Indeed shows that at least in the UK and US the demand for Ethical Hacker jobs is far less than the offer, second only to the CISO jobs.

Other high-value skills are in critically short supply, the most scarce and most frequent in demand being:

- Intrusion detection
- Secure software development
- Attack mitigation

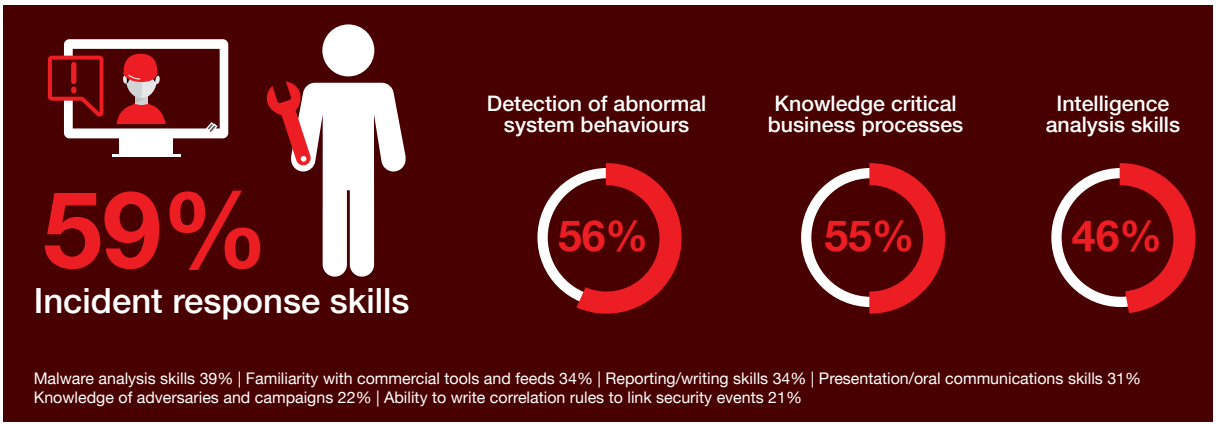
> **Incident response skills are named as the most important security skill (59%), followed by detection of abnormal system behaviors (56%), and knowledge of critical business processes (55%)**



SOURCE: Indeed Spotlight: The Global Cybersecurity Skills Gap

The results of the 2017 Cybersecurity Trends Report also confirms the importance organizations place on incident detection and response skills. According to the report, incident response skills are named as the most important security skill (59%), followed by detection of abnormal system behaviors (56%), and knowledge of critical business processes (55%). Such skills are even in greater demand than soft skills in communication and collaboration!

Other desired skills include malware analysis skills, familiarity with commercial tools and feeds, knowledge of adversaries campaigns and the ability to write correlation rules to link security events.



SOURCE: 2017 Cybersecurity Trends Report

The traditional security controls and processes still hold their value but it finally seems organizations have begun to acknowledge the fact that security incidents will occur sooner or later, thus prioritizing the improvement of their security monitoring and response capabilities, while at the same time putting greater emphasis on threat management and threat intelligence. A large 62% of respondents from the 2017 Cybersecurity Trends Report identifies "Improving Threat Detection" as the most critical threat management skills required by their organization, followed by the capability of investigating and analysing threats (43%), improving blocking threats (39%), automating incident response (37%), proactive threat hunting (36%) and aggregating security alerts (33%).

Last but surely not least, another area most organizations recognize as lacking appropriate skills is that of application security. In the US a Lead Software Security Engineer can easily earn more than a CISO. According to Jeff Williams[9], founder

Technical ability alone is not sufficient if not complimented by the ability to align security with business requirements and to communicate security issues to decision makers

and main contributor of the OWASP initiative, "application security isn't part of every software project, it's not taught regularly in university and software projects often don't account for it either." As a result each application has an average of 20.5 vulnerabilities from the list of OWASP Top 10, the top most common types of software security vulnerabilities. Not only universities are not teaching students how to develop secure applications, but secure software development is also one of the least taught skills across all commercial training vendors. As a result, the skills gap in the secure software development domain is widening and those who hold the right skills and experience can command high salaries!

IT'S NOT JUST ABOUT TECHNICAL SKILLS

According to a survey of 461 cyber security managers and practitioners at the 2016 ISACA/RSA Conference[1], the primary skills gap was identified as being the ability of candidates to understand the business (75%), while the lack of technical skills scored only 61%, equal to another non-technical issue – poor communication.

Technical ability alone, while a fundamental requirement for many security professions is not sufficient if not complimented by the ability to align security with business requirements and to communicate security issues to decision makers. Unfortunately, to a certain extent technical skills can be more easily taught and developed in isolation, whereas soft skills are based on practical experience and interaction with the business. Many young professionals fail to relate security to the business, focusing primarily on the mastering and demonstration of practical skills. Business talk almost inevitably carries the stigma of incompetence a bit like the old and equally false adage according to which "those who can do, those who can't teach!" In the cybersecurity domain, those who can talk the business lingo and translate security into real benefit for the business can see their career and their compensation progress fast and high.

JOB SEEKERS WITHOUT SECURITY CERTIFICATIONS

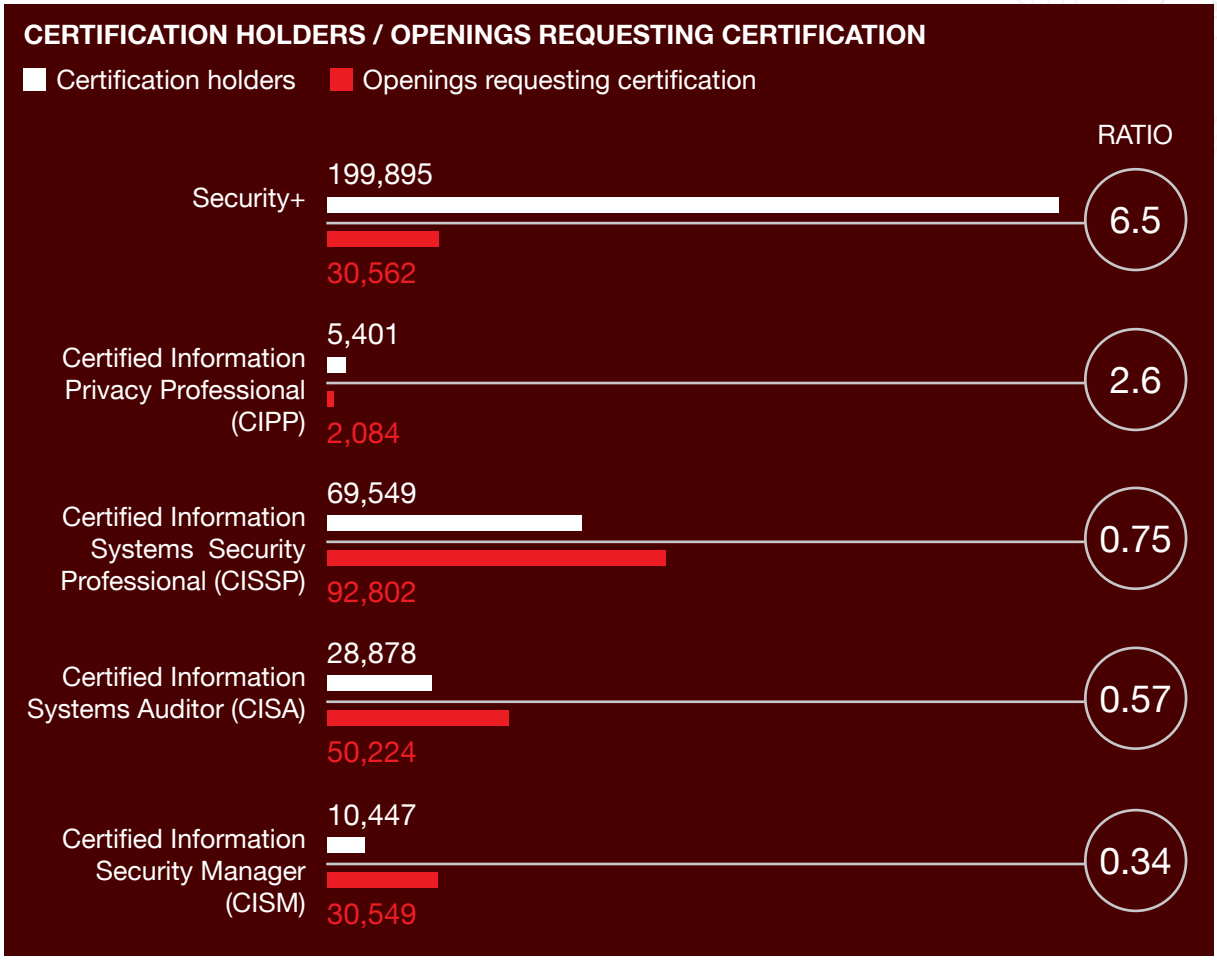
Besides lacking the required experience, the security job market has big gaps with regards to security certifications held by the job seekers. The figure in the next page (limited to the US market) shows just a sample of the required certifications and their number relative to the number of job openings that requires the certification.[2]

the security job market has big gaps with regards to security certifications

Apart from entry-level types of security certifications such as Security+, the ratio of certification holder over opening requesting certification is quite low! That is partly because, besides passing the certification exam, some certifications such as CISSP, CISA or CISM require a specific number of years of professional experience in order to be attained.

According to the 2017 Cybersecurity Trends the most sought after certification by employers is the CISSP (53%) by a margin of 3 to 1 with regards to the second certification in the list, the CISM (19%).

> **the most sought after certification by employers is CISSP (53%) by a margin of 3 to 1 with regards to the second certification in the list, the CISM (19%)**



SOURCE: State of Cybersecurity Implications for 2016. An ISACA and RSA Conference Survey

THE SECURITY ANALYST JOB

Currently, the entry-level position in the cybersecurity industry is that of the security analyst. According to ISACA, information security analyst jobs are expected to grow by 18% through 2024 a full 7 percentage points higher than the average growth rate of all occupations[14]. In 2015 the U.S. News and World Report ranked a career in information security analysis eighth on its list of the 100 best jobs.

Looking at different job ads for Security Analyst, the general job profile is that of a professional responsible for maintaining the security of information. Typical job duties include planning and implementing security measures to protect computer systems, networks and data, implementing and maintaining an Information Security Risk Management program, assisting in responding to information security incidents and investigations, carrying out, analysing and reporting on vulnerability assessments. A security analyst is also expected to carry our security research and keep up to date with the latest security trends, vulnerabilities and attacks ensuring that all information systems are protected.

> those who can talk the business lingo and translate security into real benefit for the business can see their career and their compensation progress fast and high

Education

The typical security analyst job requires a bachelor degree in computer science, programming, engineering or ideally in security, as more universities begin to make new specialized degrees more available.

Experience

From the experience perspective, analysts are expected to have previous experience in IT such as system or database administrators, network engineers, systems support etc. with emphasis on the are they will be working. For instance, if the job opening is in database security, experience as database administrator would be beneficial.

TOP 10 SECURITY JOB TITLES

When looking at the cybsersecurity skills gap, it is also important to look at the most common security job titles. According to Cyberseek.org the top 10 security job titles are:

- Cyber Security Analyst / Specialist
- Cyber Security Engineer
- Auditor
- Network Engineer / Architect
- Software Developer / Engineer
- Systems Engineer
- Systems Administrator
- Information Assurance Engineer / Analyst
- Risk Manager / Analyst

As already discussed, the analyst jobs constitute the entry-level position. Any other job title requires higher levels of certifications and experience and specialization. If employers are currently failing to fill security analysts positions, it becomes clear how other more senior positions are even more difficult to be filled. Those positions are also the most attractive ones from the point of view of compensation. According to DICE, a leading job board for tech positions, the 10 best-paying IT security jobs are as follows:

1. Lead Software Security Engineer - $233,333
2. Chief Security Officer - $225,000
3. Global Information Security Director - $200,000
4. IT Security Consultant - $198,909
5. Chief Information Security Officer - $192,500
6. Director of Security - $178,333
7. Cybersecurity Lead - $175,000
8. Lead Security Engineer - $174,375
9. Cybersecurity Engineer - $170,000
10. Application Security Manager - $165,000

The above pay scale reflects the higher and unfulfilled demand for software security skills compared to other skills. As we can see a Lead Software Security Engineer can aspire to earn much more than the Chief Security Officer.

the Challenges

Besides understanding the cybersecurity skills gap it is also very important to identify the challenges and bad practice that must be overcome for the gap to be filled. While acknowledging and understanding the nature of the problem and its impact to society, one must also identify what is actually preventing us from solving the problem and from actually widening the gap!

THE GOVERNMENT IS NOT DOING ENOUGH

Following a top-down approach, the first challenge is posed by the government. More than three out of four (76%) respondents from the 2017 Security Trends report said their government is not investing enough in building cybersecurity talent, and the same percentage said the laws and regulations for cybersecurity in their country are insufficient.

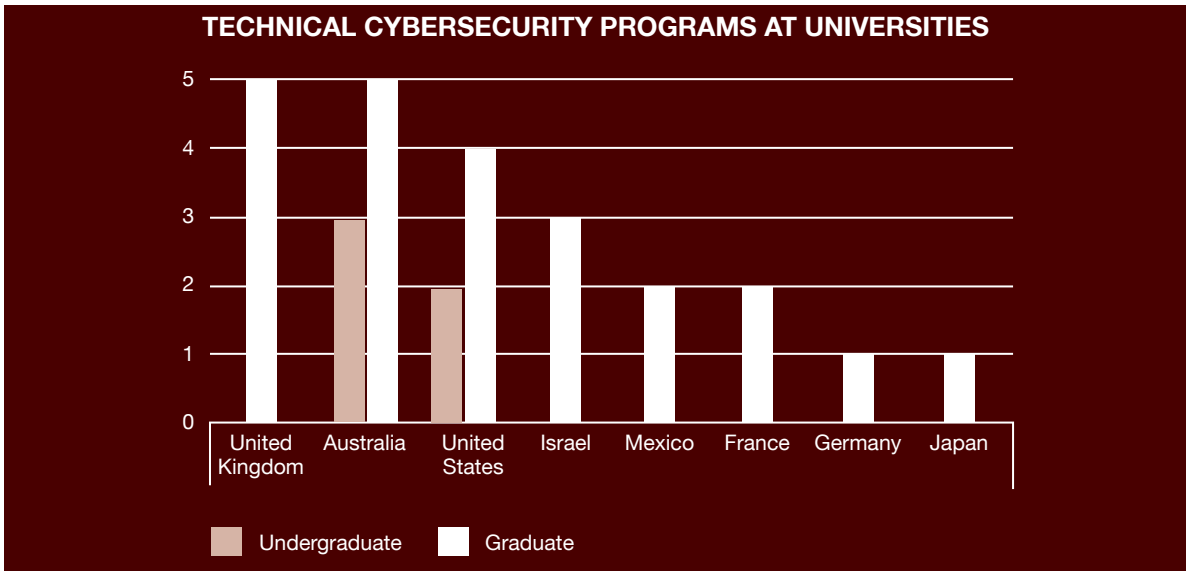
Every country in the world has understood the importance to develop and implement a national cyber security strategy. Unfortunately, while security awareness and competence building are a core element of each national cyber security strategy, the level of government commitment to building awareness and competence is mostly limited to awareness initiatives with little or no support for the competence building.

A study by Intel titled “Hacking The Skills Shortage”[8], reviews the current “educational capital” across a number of countries and presents a ranking based on the overall spending on higher education, Science, Technology, Engineering and Mathematics (STEM) programs, technical cybersecurity curricula in higher education, performance in internationally recognized capture the flag exercises, and some survey data. According to the study, the US and UK rank highest in current investment in cybersecurity education while countries such as Mexico, France, and Japan rank lowest.

> most employers rank hands on experience and professional certifications above a degree as the best two ways to acquire cyber security skills!

Lack of Cyber Security in Academia

To begin with, governments should tackle the cybersecurity skills gap through academia. For the great majority of young individuals, university offers the first opportunity to learn about cybersecurity and acquired some of the competences required by the job market. Unfortunately, cybersecurity as an academic discipline or program of study is often inaccessible to students. The "Hacking The Skills Shortage" study by Intel[8], reveals that only 7% of top universities in the countries researched offer an undergraduate major or minors in cybersecurity. As for graduate work, about a third of top universities offer a master's degree in some cybersecurity field. The majority of other countries around the world are in much worse shape and when looking at cybersecurity being taught to teenagers prior to going to university there is very little evidence of initiatives globally.



SOURCE: Hacking the Skills Shortage. A study of the international shortage in cybersecurity skills. Center for Strategic and International Studies.

Given the shortage of cybersecurity programmes offered by universities, the closest match for a potential employer is a bachelor degree in a technical field, which is also the educational requirement for most security analyst jobs. However, according to the same study by Intel, most employers rank hands-on experience and professional certifications above a degree as the best two ways to acquire cybersecurity skills!

Unfortunately, universities cannot easily integrate hands-on experience and professional certifications into their curriculum due to additional costs, quality control and lack of staff. First, the cost of including professional certifications to the curriculum would mean higher tuition fees for the students and all the issues such increase would bring along. Second, universities too have challenges in sourcing for staff capable of delivering the hands-on experience and certifications sought after by the industry. In fact, universities can hardly compete with the industry where a suitable professional can command much higher compensation. Last but not least, universities have rigorous yet slow quality and accreditation processes, and it takes time for a new programme of study to be developed, validated and be made ready for students intake.

If Academia is to address to the cybersecurity skills gap it has to somehow incorporate practical learning and professional certifications into its academic programs and government must push for more cybersecurity programs in higher education.

> **universities cannot easily integrate hands-on experience and professional certifications into their curriculum due to additional costs, quality control and lack of staff**

Lack of Competence Building Support

Retraining a country's workforce and training the new generations cannot happen without the commitment and support of the country's government both from a policy making and resources viewpoint. Research on government spending in cybersecurity education reveals only few examples such as in UK and Israel.

In the UK the Government has created two apprenticeships aligned to the Cyber Security Professional and Cyber Intrusion Analyst job roles. Specifically, the Government offers offering training funding to employers whereby for every £1,000 employers spend on security training aligned to those job roles, the government will contribute a further £2,000. Once the employee is signed-up to the apprentice programme, employers will receive cash incentives from the government throughout the programme, which can reach £10,800.

> **In most countries of the world, organisations are given little to no support towards cyber security training**

Also in the UK, a new programme led from by the Department for Culture Media and Sport (DCMS) and due to start in September 2017 has set aside up to £20m in order to deliver cyber security training to teenagers in schools and have at least 5,700 teenagers trained by 2021[11].

Israel[12] has created the National Cyber Education Center to oversee educational programs such as Magshimim, which trains talented youth from underprivileged areas in college-level cyber skills, and develop new initiatives to increase the talent pool for military intelligence units and prepare children for eventual careers in the high-tech industry and academia.

If government is to address the cybersecurity skills gap it has to develop funded initiatives to sustain and encourage the development of cybersecurity skills. However, in most countries of the world, organizations are given little to no support towards cybersecurity training.

Security Competition And Exercises

Over recent years more and more cybersecurity competitions have been developed at national level and across nations to develop and identify cyber talents. Cybersecurity competitions can be broadly divided into two categories:

1. **Live Hacking Competitions** on operational targets where participants are called to test real systems in a quest to identify real vulnerabilities and improve the operational security of target systems
2. **Cyber Competition Games** where participants are called to compete in emulated environments to solve security related challenges from domains such as web security, mobile security, crypto puzzles, reverse engineering and forensics.

Cybersecurity competitions provide an effective channel to identify talent and develop cybersecurity skills. Over three in five survey respondents from the 2017 Cybersecurity Trends report say national hacking competitions play a key role in developing cybersecurity talent. Overall, two in five respondents cite hacking competitions as

among the most effective way to acquire skills, with Australia and Israel most likely to agree. In Israel, 62% of respondents say that these competitions are among the top five most effective ways to acquire cybersecurity skills.

Unfortunately, as of today, cybersecurity competitions are far and few in between with notable exceptions from a few countries around the world and lack a structured and programmatic approach.

If government is to address the cybersecurity skills gap it has to promote more gaming and technology exercises.

Notable examples include the U.S. where the government has introduced two initiatives to strengthen the cyber security environment in the Defense Department and the Army[10]. The initiatives are called “Hack the Pentagon” and “Hack the Army” respectively and provide a legal avenue for digital security researchers to find and disclose vulnerabilities on DoD’s public websites and a range of operationally relevant web sites.

Another notable example is in Europe where the European Union Agency for Network and Information Security (ENISA) organizes an annual event called the European Cyber Security Challenge (ECSC) where young contestants from all EU member states participate.

If government is to address the cybersecurity skills gap it has to promote more gaming and technology exercises.

COMPANIES DO NOT INVEST ENOUGH IN STAFF TRAINING

According to Gartner, in 2016 organizations spent an average of 5.6 percent of the overall IT budget on IT security and risk management, although the real numbers, also according to Gartner range from approximately 1 percent to 13 percent of the IT budget. On average between 4 and 7 percent of the IT overall budget should be under the CISO alone for the security needs of the organization. When it comes to what portion of that budget companies dedicate to security training, results from the 2017 Cybersecurity trends identify “Training/Education/Certification” as the top forth area that will see an increase in security spend in 2017. However that data has to be put into the context of what is the current spending in that very same area. For instance, according to the 2016 SANS IT Security Spending Trends[13] staff training and certification comes 7th in the list of operational areas that account for security spending with areas such as “protection and prevention” and “Detection and Response” being the top priorities.

There are many reasons why, in the face of growing cybersecurity threats today, companies choose yet not to adequately invest in cybersecurity training. The following are some of the most traditional ones:

- Companies prefer to invest in systems rather than competences under the belief that the former remain as an asset to the company even after the employees leave;
- While ROI on security spending alone is usually difficult to justify, it is even more so for spending on security training and therefore difficult to get management approval.
- Companies often decide not to train their staff for fear they may leave once the training is over.
- Training costs money, period!

As a result, very few companies have mature competence building programmes, often relying on poaching staff from other companies through better pay packages and opportunities.

Unfortunately, very few organizations realize that, after salary, opportunities for training are the second highest motivating factor in recruitment and staff retention followed by the reputation of the employer's IT department and potential for advancement.

If companies are to address the cybersecurity skills gap they have to shift the balance of the security spending from security systems to people and processes, thus also reducing their risk exposure to staff leaving the company. In the end a security system operated by a person lacking the required competences is not an asset but a liability and ultimately a bad investment!

COST OF TRAINING AND CERTIFICATIONS

While it is true that companies do not invest enough in competence building for their staff, it is also important to acknowledge cost of training and certification as one of the key underlying causes and as one of the main reasons behind the gap in certified professionals faced by the cybersecurity market. Today, the cost of a security certification, inclusive of the supportive training course can range from a few $100s to several $1,000s depending on the type of certification (online vs face to face, accredited vs not accredited and simple vs advanced subject) and not inclusive of the personal time required to study the training material and prepare for the final certification exam. Student and young professionals cannot easily afford such costs or at all and those who can have to balance it with personal commitments and that increases the time required to attain the certification, which in turn translates to slower career development. Besides the high costs of training and certifications companies also have to deal with the indirect costs associated disruption of operations when members of staff attend a training course or study towards a certification.

The cost of training and certification is one of the underlying causes of the cybersecurity skills gap

If the cybersecurity skills gap is to be reduced, entry-level security training and certifications have to become more accessible to the masses.

> If companies are to address the cybersecurity skills gap they have to shift the balance of the security spending from security systems to people and processes

NOT ENOUGH STRUCTURED TRAINING AND EDUCATION

Filling the cybersecurity skills gap means helping a new generation of professionals acquire new skills and competences beginning from the fundamentals. While quality of training and education varies across vendors and educational providers, much of the issue lies in use of primarily self-learning content, available online.

Nobody can argue against the value of online training. It can be accessed anywhere and anytime, it is usually more affordable and it doesn't bear the cost of traveling to a training venue and the associated travel and accommodation expenses. Unfortunately online-learning is more suited for good self-learners or mature learners who already have enough competence to help them digest the self-paced learning material. Furthermore, online self-paced learning is traditionally more suited for the acquisition and testing of knowledge rather than practical competences.

> If training and education is to address the cybsersecurity skills gap it must be delivered through formal and structured methods where online learning is only an add-on and not the primary method.

However, formal education and training offer a unique advantage and that is structured, guided and goal oriented learning. What we pay as individuals when enrolling on a university programme or formal training course is the structured learning made of lectures, tutorials (including lab set and computing facilities), workshops and the final assessment. We also pay for the formative assessment given through the on-going guidance and feedback of the lecturer/trainer. The financial commitment we make when we enrol in a formal course of education or training also pushes us to complete the course of study and pass the related assessment, which completes the learning process.

Almost any subject, however complex it may be, can be learned online today and with only the cost of an Internet connection and a computer. That however may not be, and in most case it isn't, the best way to go about it. The majority of learners do not have the experience to sieve through the wealth of free cybersecurity training videos and tutorials that can be found online in a structured way that is conducive to effective and efficient learning and the lack of formal assessment (both formative and summative) is the most critical learning component!

If training and education is to address the cybsersecurity skills gap it must be delivered through formal and structured methods where online learning is only an add-on and not the primary method.

> If the cybersecurity skills gap is to be reduced, entry-level security training and certifications have to become more accessible to the masses

YOUNG PROFESSIONALS NOT DOING IT RIGHT!

In the end it is only fair that individuals should take part of the blame and understand the role they play in meeting the needs of the cybersecurity job market and what they can do about it. Government initiatives and changes of attitude towards cybersecurity by companies will take their time to bring about considerable results. Meanwhile, young generations are also to blame for not being part of the solution!

The cybersecurity domain is fantastic. It is so broad and so full of opportunities that, whether you want to work in compliance or secure software development, penetration testing or computer forensics or any other specialized discipline, chances are that you will easily find employment, especially if you are good enough! The same variety of cybersecurity disciplines is also the reason why it may be quite difficult at first to choose a path and an area of specialization. In certain regards it is similar to studying medicine. One has to develop a good knowledge of the human body and a good appreciation of different medical professions before choosing a specific career.

> Young generation should take part of the blame for not being part of the solution

Currently very few universities around the worlds have developed undergraduate and postgraduate programmes capable of equipping students with the right body of knowledge and competence to also guide the students towards their career path. That being said there are still lots of options for students or young professionals to do something today instead of complaining about the university or the government or the lack of opportunities in the workplace! Examples include:

- **Taking free online courses available from websites such as udemy.com or cybrary.it –** These websites make hundreds of security courses available for free from beginner to more advanced levels;
- **Building your own labs –** There exist unlimited resources available online to help build practice labs. A notable example is the “Avatar Project”, a guide designed to teach students about virtualization and how to build virtual machine lab environments to practice their trade;
- **Participating in cybersecurity challenges and competitions whenever possible –** Cybersecurity competitions can help an individual assess his/her level of competence and even give a feel for some of the professionals roles he/she may decide to pursue. Besides they are an excellent social means of expanding one’s network of peers who are interested in cybersecurity;
- **Joining cybersecurity fora or Linkedin groups –** Ethical professionals are always too happy to help someone who is passionate in cybersecurity and give them useful career advice;

- **Reading up on different cybersecurity professions –** For instance, many young students or professionals want to be ethical hackers but very few know much about the ethical hacker profession, what it involves, the responsibilities etc. Befriend security professionals and ask about their job and try to mature an understanding of what cybersecurity job you would like to pursue!

- **Maintaining a security blog –** This is a great method of improving one's writing skills while at same time learning from the comments of peers and expanding one's professional network;

- **Maintaining a deliverable-approach! –** This is probably the most important advice. It does not matter how many of the above things you do. What matters is what you learn from it and what you have to show for in the end;

If the cybersecurity skills gap is to be reduced, individuals must become part of the solution while waiting for one!.

Closing the Gap

Much has been said about the cybersecurity skills gap and the challenges to be overcome in order to fill that gap. What can be done and how can we address the Gap? In this section we expand on some of the points made earlier in the paper and provide some final remarks on the matter. The following table summarizes the key recommendations to address the cybersecurity skills gap challenges.

CHALLENGE	RECOMMENDATIONS	TARGET
Lack of Competence Building Support	• Increasing government expenditure on cybsersecurity training through matched funding and/or financial incentives • Pushing for more cybersecurity programs in schools and higher education.	Government
Lack of Cybersecurity in Academia	• Partner with professional cybersecurity training vendors to offer extra-curriculum professional certifications and hands-on experience • Organize Cybersecurity Games and Competitions and/or facilitate students to participate	Academia
Security Competition and Exercises	• Promoting gaming and technology exercises	Government
Companies Do not Invest Enough in Staff Training	• Shift spending from security systems to people and processes • Develop better competence building programmes, which can be delivered by competent in-house staff and pay for staff certification attempts	Organizations
Cost of Training and Certifications	• Develop better competence building programmes, which can be delivered by competent in-house staff and pay for staff certification attempts	Government, Academia and Organizations
Lack of Adequate Training	• Prioritize formal and structured training over online/self-learning especially to begin with	ALL
Young Professionals Not Doing It Right!	• Follow a goal-oriented approach to produce tangible deliverables at every step of the learning process	Individuals

The biggest challenge of them all is probably the cost of training and certifications. In order to make a positive impact to the current and growing cybersecurity skills gap, training and certifications costs have to become more accessible to the masses. Specifically, all structured and formal entry-level training and certifications cannot be only accessible to a privileged few. At the moment, only self-learning online courses meet that requirement although, as discussed in this paper they are not best suited for people lacking prior competence and experience in the field of cybersecurity.

Government and organizations must work to build successful competence building programmes within which competent professionals can deliver affordable yet effective training path to a wider audience in collaboration with commercial providers. Government and organizations must empower themselves to deliver more competence building programmes without having to choose between training a single individual with the associated the fear of losing that member of staff or not training at all!

Academia must empower themselves to provide their students with more professional certifications and hands-on experience without losing their academic identity.

Finally, young generations must be given access to quality and structured cybersecurity education in a way that is affordable and towards the fulfillment of the collective responsibility for a safer cyberspace.

About Silensec

Silensec is an Information Security Management Consulting and Training company specialized in the development and delivery of advanced services across all areas of information security from the protection of infrastructure up to the classification and protection of data. For over a decade Silensec has also trained thousands of professionals and delivered competence building services to clients worldwide including government, financial institutions and telecommunication companies and more. Silensec's mission it to help people develop exceptional competences and professionalism in all areas of information security. To help address the growing cybersecurity skills gap, Silensec has developed a comprehensive set of training and competence building products and services aimed at professionals, private organizations, academia and government.

SILENSEC TRAINING

SOLE
SILENSEC ONLINE LEARNING ENVIRONMENT

Silensec has developed a portfolio of over 30 training courses across the different categories of awareness, proaction, prevention, detection, reaction and compliance. Courses offered range from ethical hacking to mobile forensics, reverse engineering and malware analysis up to security management and security standards compliance. Silensec courses have been delivered to professionals and organizations worldwide.

Technical courses are delivered and assessed hands-on through Silensec Online Learning Environment (SOLE), a state of the art cloud-based platform where students can practice their cybersecurity skills and gain practical experience.

SILENSEC ACADEMY

Silensec Academy empowers academia and large organizations to train as many professional as they can while at the same time ensuring quality, structure learning and the development of practical competences. Silensec Academy provides a cost-effective way for developing wide-reaching competence building programmes that can positively impact the growing cybersecurity skills gap. Silensec Academy is aimed at universities, large corporate organizations and government.

SILENSEC CYBER RANGE

For many years Silensec has helped governments and national CERTs, universities and private organizations around the world in the development and running of cyber security competitions and challenges. Leveraging on that experience Silensec has developed a Cyber Range Platform that can be used by both individuals and organizations to practice cyber security skills in a fun and challenging way. The design of the Silensec Cyber Range combines gamification principles with interactive challenges to test cyber security competence across a wide range of domains, either individually or in a team against others.

Silensec Cyber Range Platform provides a scalable turnkey solution with pre-built scenarios, challenges and a wide range of pre-configure virtual machines which enable an organization to set up a cyber competition within a few minutes!

SILENSEC SECURITY AWARENESS

Silensec pioneers innovative methods for the delivery of security awareness content. Over the years Silensec has produced and published editorial illustrations on current cybersecurity news, and security best practice. Fortune 500 organizations rely on Silensec for the development of security awareness newsletters and content. Other services include the development of national security awareness campaigns such as online child safety and more.

References

[1] Press Release – Worldwide Revenue for Security Technology Forecast to Surpass $100 Billion in 2020, According to the New IDC Worldwide Semiannual Security Spending Guide https://www.idc.com/getdoc.jsp?containerId=prUS41851116

[2] State of Cybersecurity Implications for 2016. An ISACA and RSA Conference Survey https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

[3] State of Cybersecurity Implications for 2017 http://www.isaca.org/cyber/pages/state-of-cyber-security-2017.aspx

[4] 2017 Cybersecurity Trends Report http://www.cybersecurity-insiders.com/wp-content/uploads/2017/02/Cybersecurity-Trends-Report-2017.pdf

[5] Cybersecurity job market to suffer severe workforce shortage http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

[6] Indeed Spotlight: The Global Cybersecurity Skills Gap http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/

[7] The Fast-Growing Job With A Huge Skills Gap: Cyber Security. https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#7556d6b45163

[8] Hacking the Skills Shortage. A study of the international shortage in cybersecurity skills. Center for Strategic and International Studies. http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

[9] New OWASP Top 10 Reveals Critical Weakness in Application Defenses. http://www.darkreading.com/application-security/new-owasp-top-10-reveals-critical-weakness-in-application-defenses/a/d-id/1328751

[10] DoD, Army Ramp Up Cybersecurity Measures With New Initiatives. https://www.defense.gov/News/Article/Article/1010626/dod-army-ramp-up-cybersecurity-measures-with-new-initiatives/

[11] UK government to deliver ‘cyber curriculum’ to tackle cyber security skills gap http://www.cbronline.com/news/cybersecurity/uk-government-cyber-curriculum-tackle-cyber-security-skills-gap/

[12] Israel, teaching kids cyber skills is a national mission. https://apnews.com/e477309a4a1e407ca4ae6568d3035625/In-Israel,-teaching-kids-cyber-skills-is-a-national-mission

[13] IT Security Spending Trends https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

[14] ISACA 2016 Cybersecurity Job Index https://www.isaca.org/cyber/Documents/2016-cyber-security-jobs-infographic.pdf

SILENSEC TRAINING COURSES

proaction courses

developing cyber threat intelligence capabilities

active defense

protection courses

CERTIFIED Linux Ninja™

ethical hacking fundamentals

CERTIFIED Ethical Ninja™ SAMA

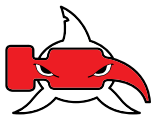
ethical hacking

CERTIFIED Ethical Ninja™ SENPAI

advanced ethical hacking

CERTIFIED Ethical Ninja™ SENSEI

extreme ethical hacking



CERTIFIED Mobile Security™ SHARK

mobile ethical hacking

CERTIFIED Octopus Ninja™

evasion techniques

detection courses

CERTIFIED Black Bundi™

intrusion detection

CERTIFIED Red Bundi™

corporate security monitoring

CERTIFIED Red CHUNGU™

log management and analysis

protecting corporate databases

protecting web applications

managing corporate security with siem technologies

reaction courses

CERTIFIED Rev Code™ PANTHER

malware analysis and reverse engineering

CERTIFIED Forensic eSpector™

computer forensics

CERTIFIED Forensic BEE™

mobile forensics

management courses

lead implementer

lead implementer

lead implementer

boot camp

Follows us on our social media channels for regular security cartoons, editorials and weekly newsletter

Silensec Silensec @Silensec Silensec @Silensec

silensec™
iso27001 Certified

UK Office
Sheffield Technology Parks
Cooper Buildings, Arundel Street
Sheffield S1 2NS
England

Cyprus Office
59 Hara Court
Thessalonikis street
3025 Limassol
Cyprus

Africa Office
Woodvale Place, 3rd floor
Woodvale Grove, Westlands
P O Box 25388-00100 GPO
Nairobi, Kenya